TENDER REFERENCE: SAS/OP/2025/007/T

SCHOOL OF THE ARTS SINGAPORE

TENDER FOR

PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE

Name of Tenderer	**:**	_____
Closing Date/Time	**:**	**21 JANUARY 2026 at 1400 hours**
Submit To	**:**	**Tender Submission Box 1** **Level 2, Beside Security Counter**

SCHOOL OF THE ARTS SINGAPORE

TABLE OF CONTENT

Singapore Arts School Ltd
Co. Reg. No. 200500775C
1 Zubir Said Drive
Administration Office #05-01
Singapore 227968

Tel: 6338 9663
Fax: 6338 9763

Our Ref : **SAS/OP/2025/007/T**

12 December 2025

Dear Sir/Mdm,

INVITATION TO TENDER (ITT) - PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE (ITT REFERENCE NO: SAS/OP/2025/007/T)

1. **Singapore Arts School Ltd. (SAS)**, the company that manages the **School of the Arts, Singapore (SOTA)**, governed by the Ministry of Culture, Community and Youth (MCCY), invites proposals for the Tender for **Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services for a contract period of fourteen (14) months (excluding Software Warranty Period)** at 1 Zubir Said Drive, Singapore 227968 as described in the attached documents.

2. You must submit your proposal and any accompanying information to our **Tender Submission Box 1** at Level 2, beside Security Counter at 1 Zubir Said Drive, Singapore 227968 by **21 January 2026, 1400 hours Singapore Time**. All late and/or incomplete submissions will be disqualified.

3. The documents enclosed in this ITT include:

(a)	Schedule 1	:	Instruction to Tenderers
(b)	Schedule 2	:	Form of Tender
(c)	Schedule 3	:	Schedule of Price
(d)	Annex A	:	ERP Conditions of Contract
	(i) Appendix 1	:	Payment Terms
	(ii) Appendix 2	:	Intentionally left blank
	(iii) Appendix 3	:	Conflict Of Interest Declaration Form
	(iv) Appendix 4	:	Undertaking to Safeguard Official Information
	(v) Appendix 5	:	Declaration
(e)	Annex B	:	Selection Criteria
(f)	Annex C	:	General Requirement Specifications

Singapore Arts School Ltd
Co. Reg. No. 200500775C
1 Zubir Said Drive
Administration Office #05-01
Singapore 227968

Tel: 6338 9663
Fax: 6338 9763

(g)	Annex D	:	Combined Functional Requirements
(h)	Annex E	:	Project Schedule
(i)	Annex F	:	Proposed Project Team and Track Record
(j)	Annex G	:	Technical Requirement Specifications
(k)	Annex H	:	Statement of Compliance
(l)	Appendix A	:	High-level Current Corporate System Landscape

4. The Invitation to Tender must be submitted by the Tenderer's authorised representatives.

5. There will be two (2) **Online Tender Briefings** conducted via Microsoft Teams:

   a) First Online Tender Briefing on **22 December 2025, 1030 hours Singapore Time** for the tender requirements and documents submission.

   b) Second Online Tender Briefing on **8 January 2026**, **1030 hours Singapore Time** for tender clarifications.

6. **Attendance for both Online Tender Briefings is mandatory for participation in Tender**.

7. Tenderers must fill in the briefing registration form here (https://forms.gle/VXRVawmtSzxvgdq66) to confirm their attendances for both **Online Tender Briefing** no later than **19 December 2025, 1200 hours Singapore Time**.

8. Details of the Microsoft Teams Meeting will be provided after we receive your briefing registration.

9. Tenderers must attend the first Online Tender Briefing to obtain Annex D in Excel format, which will be sent to the email address provided in the registration form. All tender submission for Annex D must be in both printed and excel format.

Singapore Arts School Ltd
Co. Reg. No. 200500775C
1 Zubir Said Drive
Administration Office #05-01
Singapore 227968

Tel: 6338 9663
Fax: 6338 9763

10. All enquiries or clarifications regarding this Invitation to Tender should be submitted in writing via email no later than **12 January 2026, 1700 hours Singapore Time** to:

    (a) Tender Matters : Ms Lee Suling, Direct line: 63425856 &
    Email : procurement@sota.edu.sg

    (b) Requirement Specifications : Mr Lee Yew Wah, Direct Line: 63425808 &
    Email : yewwah.lee@sota.edu.sg

11. No oral representation must be binding on SAS or construed as varying or adding to any part of this Invitation to Tender.

12. SAS accepts original Tender Documents Submission and strictly without any alteration to the content and format.

13. Only shortlisted Tenderers will be invited for a presentation.

Yours sincerely
(No Signature Required)
Lee Suling,
SENIOR EXECUTIVE, OFFICE OF PROCUREMENT for CHIEF EXECUTIVE OFFICER
SINGAPORE ARTS SCHOOL LTD

Schedule 1 :
INSTRUCTION TO TENDERERS

TENDER FOR PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE

INSTRUCTION TO TENDERERS

1. The Tender Submission MUST comprise the following Tender documents:

   a) Schedules 1, 2 and 3
   b) Annexes A, B, C, D (both hardcopy and in excel format), E, F, G, and H
   c) Appendices 1, 3, 4 and 5
   d) Company Profile
   e) Supporting Documents (as set out in Annex C, Point 4.1)
      - Proof of GSR at least meeting Financial Grade S7
      - Proof of certified partner of the proposed ERP system
      - Detailed proposal
      - Schedule 3, Annexes D, E and F
   f) Documentary proof that the Primary Data Centre is located in Singapore
   g) Client Track Records for past three (3) years
   h) Two (2) most recent Audited Financial Statements or Latest Statement of Accounts
   i) Relevant Certification(s) including relevant certification of security standard attained (if any)

2. Tenderers must submit **two (2) full sets** of Tender documents in hardcopy. One (1) set is to be marked "Original" and the other marked "Duplicate" and endorsed with **company stamp and authorised signatory on every page.** Tenderers must submit **Annex D** in **excel format via thumb drive**.

3. Tender documents must be submitted to the "**TENDER SUBMISSION BOX 1"** located **at Level 2, beside security counter by 21 January 2026 (1400 hours)** in sealed envelope(s) with the following marked :

   TO: OFFICE OF PROCUREMENT

   TENDER FOR PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE

   TENDER REFERENCE: SAS/OP/2025/007/T

   School of the Arts, Singapore
   1 Zubir Said Drive Administration Office #05-01
   Singapore 227968"

4. All Tender documents appended with conditions other than those set out herein and/or at variance thereto shall be invalidated.

5. Any items which the Tenderer considers to have no value must be marked with dashes or other suitable marks placed against them in the cash columns. Any items not priced and without dashes or other suitable marks must be deemed to be no value.

6. Incomplete Tender submission will not be considered.

7. Any doubt as to the meaning of any part of these Tender documents may be clarified with SAS's representative. SAS is hereinafter known as the "Company".

8. Tenderers shall note that the award of the Contract may not necessarily be the lowest quotes of any proposal and any claims for expenses incurred in the preparation of this Tender will not be entertained.

9. All Tenders submitted must be deemed to be valid for a period of 90 days from the date of submission thereof.

10. Before the submission of their Tenders, Tenderers **must attend both mandatory Online Tender Briefing** to acquaint themselves thoroughly with the requirements, conditions and all aspects of the Tender which may affect the works under this contract. Any unforeseen difficulties and works for which provision has not been made in the Tender price quoted will under no circumstance relieve the Tenderers from the full performance of this Contract.

11. Tenderers are also reminded that the ERP Conditions of Contract (Annex A), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) attached herein must be strictly adhered to unless specified that that SAS accepts alternative proposed.

12. A "NIL" return of the Tender submission is not accepted.

13. The Contract Sum submitted excludes any Goods and Services Tax (hereinafter referred to as GST) under the Goods and Services Tax Act Singapore.

CONFIDENTIAL

PARTICULARS OF TENDERER

All sections are mandatory to fill up

Note : From IT/3 onwards, if the space provided is insufficient, please continue on an extension page setting out the required data in a similar manner.

1 **REGISTERED BUSINESS NAME AND ADDRESS OF FIRM/COMPANY**

Full Business Name	:	
Registered Address	:	
Correspondence Address	:	
Telephone Number	:	
Fax Number	:	
GST Registration	:	Yes / No (please circle one)
GST Registration No.	:	
Date and Number of Business Registration	:	
Date of Incorporation	:	
Form of Business	:	
Name (as in NRIC/FIN) and Designation of Authorised Representative	:	

2 CAPITAL

a) If Partnership to state the capital set aside for business

Capital Set Aside :

b) If Limited Company, to state the authorised and paid-up capital

Paid-up Capital :

c) Extracted from two (2) most recent Audited Financial Statements or Latest Statement of Accounts

i. Company with an annual revenue less than S$5 million, to submit company endorsed Statement of Account.
ii. Company with an annual revenue S$5 million or more, to submit Audited Financial Statement

Latest Audited Financial Statements/ Statements of Account

Please submit Audited Financial Statements or Statements of Account

Annual Report Year and Descriptions	Financial Year 20__	Financial Year 20__
Paid-Up Capital (S$)		
Current Assets (S$)		
Current Liabilities (S$)		
Non-Current Assets (S$)		
Non-Current Liabilities (S$)		
Total Revenue (S$)		
Net Profit / Loss (S$)		

3 **REGISTRATION WITH GOVERNMENT SUPPLIER REGISTRATION (GSR) / BUILDING & CONSTRUCTION AUTHORITY (BCA) - REGISTRATION SYSTEM INFORMATION**

GSR Head/ BCA Registration (with date of expiry if applicable)	Head Title / BCA Workhead(s)	Financial Category / BCA Grade

4 **DEBARMENT / SUSPENSION/PROHIBITION (OR ANY FORM OF EXCLUSION OR EQUIVALENT, IF ANY)**

Name of Authority/ Regulatory Body or Equivalent	Reasons for Debarment /Suspension/Prohibition or any form of exclusion or equivalent, if any	Effective Date of Debarment/ Suspension/Prohibition or any form of exclusion or equivalent, if any	
		From DD/MM/YYY	To DD/MM/YYY

5 **DETAILED PARTICULARS OF PARTNERS/COMPANY DIRECTORS**

FULL NAME/ DESIGNATION	WORKING EXPERIENCE

6 **PARTICULARS AND EMPLOYMENT HISTORY OF PROFESSIONAL/SUPERVISORY/TECHNICAL STAFF**

	S/NO	NAME	QUALIFICATION	INSTITUTION	YEAR AWARDED	RELEVANT WORKING EXPERIENCE IN THE LAST 5 YEARS (WITH POSITION HELD & RESPONSIBILITIES)
1 PROFESSIONAL Degree Holder or Equivalent						
2 SUPERVISORY Diploma Holder or Equivalent						
3 TECHNICAL Trade Certificate Holders						

If space provided above is insufficient, please continue on an extension page setting out the required data in a similar manner

7 **CONTRACTS SECURED IN THE LAST 3 YEARS (EXCLUDE PROJECTS MENTIONED IN SECTION 8, IT/9)**

S/N	PROJECT TITLE AND DESCRIPTION OF PROJECT#	CLIENT (Organisation, Department and Address)	DURATION & VALUE OF CONTRACT (S$)	DATE OF COMMENCEMENT & COMPLETION (DD/MM/YY TO DD/MM/YY)	OFFICER-IN-CHARGE (JOB TITLE, DESIGNATION, EMAIL, TEL & FAX NO.)
Project/s of similar service and scale					
Other Project/s					

If space provided above is insufficient, please continue on an extension page setting out the required data in a similar manner.
 # With reference to Firm/Company stated in Page IT/3, Section 1.

8 **DETAILS OF CURRENT PROJECTS IN PROGRESS OR DUE TO BE EXECUTED (EXCLUDE PROJECTS MENTIONED IN SECTION 7)**

S/N	PROJECT TITLE AND DESCRIPTION OF PROJECT#	CLIENT (Organisation, Department and Address)	DURATION & VALUE OF CONTRACT (S$)	DATE OF COMMENCEMENT & COMPLETION (DD/MM/YY TO DD/MM/YY)	OFFICER-IN-CHARGE (JOB TITLE, DESIGNATION, EMAIL, TEL & FAX NO.)
Project/s of similar service and scale					
Other Project/s					

If space provided above is insufficient, please continue on an extension page setting out the required data in a similar manner.
 # With reference to Firm/Company stated in Page IT/3, Section 1.

9 **CONTACT DETAILS FOR REFERENCE CHECK**

S/N	PROJECT TITLE AND DESCRIPTION OF PROJECT#	CLIENT (Organisation, Department and Address)	DURATION & VALUE OF CONTRACT (S$)	OFFICER-IN-CHARGE (NAME & DESIGNATION)	OFFICER-IN-CHARGE (EMAIL)	OFFICER-IN-CHARGE (TEL NO.)

If space provided above is insufficient, please continue on an extension page setting out the required data in a similar manner.

 # With reference to Firm/Company stated in Page IT/3, Section 1.

10 **DECLARATION**

I/We declare that the information provided in this offer (including the prescribed forms) are correct and true. Should there be any false statement, I/We understand that our Tender will be invalidated or if already awarded will be immediately terminated without prejudice to the Company's right to claim damages.

I/We hereby undertake to inform the Company of any changes of partnership/director or firm/company taking place during the term of the Contract.

I/We agree that SAS may conduct reference checks with any of our past and existing clients that I/we have provided in Section 7, 8 and 9.

NAME AS IN NRIC/FIN AND SIGNATURE

(AUTHORISED REPRESENTATIVE)

DATE

COMPANY STAMP

IMPORTANT NOTES :

(a) All items in in Schedules 1, 2 ,3, Annexes A, D, E, F and H must be filled. Any items which are not applicable should be clearly stated. Incomplete forms shall render the Tender to be rejected.

(b) All forms submitted must be signed by an Authorised Representative with company stamp and signatory on every page. The Authorised Representative must be the partner or director of the firm/company and legally empowered to act and endorse on behalf of the firm/company.

(c) For a Partnership Firm, the forms must be accompanied by the latest copy of computer information (Business Profile) from the Accounting and Corporate Regulatory Authority (ACRA).

(d) For a Limited Company, the forms must be accompanied by a Memorandum and Articles of Association and the latest copy of computer information (Business Profile) from ACRA.

(e) Tenderer who fails to attach items as specified in (c) and (d) as indicated above and any other required supporting documents may render the Tender to be rejected.

Schedule 2 :
FORM OF TENDER

FORM OF TENDER

TO: SINGAPORE ARTS SCHOOL LTD.

TENDER (ITT) FOR PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE

1 I/We, the undersigned having visited the site, hereby submit this **Tender for Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services for School Of The Arts, Singapore for a contract period of fourteen (14) months (excluding Software Warranty Period)** as specified in this Tender document in accordance with the ERP Conditions of Contract (Annex A), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) attached hereto, to the entire satisfaction of the Company.

2 My/Our Total Tender for the Contract is for Total Amount ("the Contract Sum") of Singapore Dollars:

_____

_____(S$_____)

*(*Amount brought forward from Schedule 3 - Schedule of Price, SOP/1, Total Contract Sum. The Contract Sum is deemed to exclude the Goods and Services Tax "GST".)*

3 Until a formal Contract is executed, this Tender together with your written acceptance thereof, will constitute a binding contract between us.

4 I/We understand that you are not bound to accept the lowest of any submitted Tender you may receive.

5 I/We further undertake that this offer will not be retracted or withdrawn for a period of ninety (90) days from the date fixed for receiving the same and it will remain binding upon me/us, and may be accepted or rejected at any time before the expiration of that period.

6 I/We understand that the Contract Period will commence within ninety (90) days of the Tender validity.

7 I/We understand that the actual commencement date of Service will be stated accordingly in the Company's Letter of Acceptance.

8 I/We warrant that I/We have obtained and shall at all times during the subsistence of the Contract (including any renewal thereof) maintain all necessary licenses, approvals, permits, consents and/or other authorisation required by the Contractor in order to fully perform and complete the works.

9 I/We understand that the Contract Sum shall be paid to the Contractor based on the payment terms specified in Annex A - ERP Conditions of Contract, COC/6 Clause 4 and Appendix 1.

10 I/We have not included any allowance in this Tender for payment to other Tenderers or to any Trade, Industry or Professional organisation acting independently or for or on behalf or any or all Tenderers.

11 I/We have read and understood all ERP Conditions of Contract (Annex A), Selection Criteria (Annex B), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) and their relation to the Schedule of Price (Schedule 3) and confirm that this Total Amount as quoted in the Form of Tender (FOT/1 Point 2) shall include all items related to all documents as stated above.

12 I/We offer to provide the System, Services and Works at the prices submitted in the Tender based on the terms and conditions as stated in the ERP Conditions of Contract (Annex A), Selection Criteria (Annex B), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D) and Technical Requirement Specifications (Annex G).

13 I/We agree, in the event of this Tender being accepted by the Company, until a formal contract is prepared and executed between us, to be bound by and to observe and perform all the covenants and obligations on my/our part respectively contained in this Tender submission, together with the Company's written acceptance thereof and notification of award.

14 The Company reserves the absolute right to amend the required item(s) before or during the Contract Period or to terminate this Contract by serving to the Tenderer, thirty (30) day's prior notice in writing.

15 I / We agree that the Company may conduct a reference check with our clients at anytime before the acceptance of Tender.

NAME AS in NRIC/FIN AND SIGNATURE (AUTHORISED REPRESENTATIVE)	: _____	NAME AND SIGNATURE (WITNESS)	: _____
DESIGNATION (AUTHORISED REPRESENTATIVE)	: _____	DESIGNATION (WITNESS)	: _____
DATE	: _____	DATE	: _____
COMPANY NAME AND COMPANY STAMP	: _____		

Schedule 3 :
SCHEDULE OF PRICE

SCHEDULE OF PRICE

PROVISION OF ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM DEVELOPMENT AND MAINTENANCE SERVICES FOR SCHOOL OF THE ARTS, SINGAPORE

The correct details of my/our offer for the proposed Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services including preliminaries and profit, in accordance with the ERP Conditions of Contract (Annex A), Selection Criteria (Annex B), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D) and Technical Requirement Specifications (Annex G) are as follows:

S/no.	Description of item	Qty	UOM	Year 1 (S$) (a)	Year 2 (S$) (b)	Year 3 (S$) (c)	Sub-Total (S$) (a + b + c)	Remarks (if any)
A	**One-time professional services** Phase 1 Design, development, delivery, installation, testing and commissioning of a SaaS system for Finance, Human Resource and Procurement and shall include but not limited to professional services, training, data integration and migration, security requirements etc **NOTE: HR module to complete by 30 June 2026** Estimated project duration of 6 to 7 months + 1 month Performance Gurantee Period (PGP)	1	LOT					
2	Implementation of Payroll Module	1	LOT					
3	Software Warranty Period - 12 months upon commissioning of SaaS system	1	LOT					
4	Phase 2 Implementation of Budgeting and Planning Module	1	LOT					
5	Any other items *If this is left unspecified, it shall be deemed that any other work/service has been included in the contract price*	1	LOT					
B	**Annual subscription / maintenance** SaaS subscription for estimated 280 employees for three (3) years, including: Est. no. of Finance Officers - 7 Est. no. of Human Resource Officers - 6 Est. no. of Procurement Officers - 5	1	LOT					
7	Annual subscription to Payroll Module	1	LOT					
8	Annual Application Management & Support (AMS) (Optional)	1	LOT					
	Sub-Total of Year 1, 2 and 3 (S$)			(d)	(e)	(f)		
	Total Contract Sum (S$) (Excluding GST & its prevailing rates) To be carried forward to Form of Tender FOT/1, Point 2					(d + e + f)		

Note:

1 Year 1 comprises of Phase 1 Implementation and Performance Gurantee Period
2 Year 2 comprises of Phase 2 Implementation, which will run parallel with the start of the maintenance period.

All prices submitted are in accordance to the corresponding Schedules, Annexes and Appendices. All details must be verified by the Tenderer before tender submission.

I/We fully understand and agree that notwithstanding the fact that the Contract Sum as herein quoted by us is applicable to the ERP Conditions of Contract (Annex A), Selection Criteria (Annex B), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D) and Technical Requirement Specifications (Annex G) specified.

Dated this _____ day of _____ 2026

NAME AND SIGNATURE (AUTHORISED REPRESENTATIVE)	: _____	NAME AND SIGNATURE (WITNESS)	: _____
DESIGNATION (AUTHORISED REPRESENTATIVE)	: _____	DESIGNATION (WITNESS)	: _____
DATE	: _____	DATE	: _____
COMPANY NAME AND COMPANY STAMP	: _____		

SCHOOL OF THE ARTS SINGAPORE

Annex A :
ERP CONDITIONS OF CONTRACT

DATED THIS ____ DAY OF _____

BETWEEN

SINGAPORE ARTS SCHOOL LTD
(the "Company")

_____
(the "Contractor")

CONTRACT

(Tender reference: SAS/OP/2025/007/T)

CONTENTS

1 INTERPRETATION

1.1 In this Contract (as hereinafter defined), the following words and expressions shall have the meanings hereby assigned to them except where the context otherwise requires:

"**Acceptance Date**" refers to the date on which the System is accepted by SAS pursuant to **Clause 24.6**.

"**Acceptance Tests**" refers to the tests to be conducted on the System pursuant to **Clause 22.**

"Application Software" means the Software-as-a-Service (SaaS) proposed which are further customised, developed and delivered for installation in the Hardware and in conjunction with other System software as proposed in the Tenderer's proposal, so as to be capable of meeting or exceeding the project goals, objectives, outcomes and requirements of SAS as articulated in the ERP Combined Functional Requirements.

"**Commissioning Date**" refers to the date referred to in **Clause 22.8** and "Stipulated Commissioning Date" means the date the Contractor has stipulated in the Implementation Plan as to when the Commissioning of the System is to take place.

"**Contract**" includes the Instruction to Tenderers, Form of Tender, ERP Conditions of Contract, General Requirement Specifications, Combined Functional Requirements, Technical Requirement Specifications, Statement of Compliance, Tender Proposal, Letter of Acceptance and any other documents agreed to by SAS in writing, amplifying or modifying the said tender and proposals.

"**Contract Price**" refers to the Contract Sum specified in the Contractor's Tender for Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services and for the performance of services under this Contract and where the sum tendered has been varied by written agreement of SAS, it shall refer to such varied sum.

"**Hardware**" means all computer hardware, other peripherals and ancillary equipment together with all cabling within the network.

"**Implementation Plan**" means the Implementation Plan referred to in **Clause 12.4.**

"**Installation Date**" refers to the date referred to in **Clause 21.**

"**Stipulated Installation Date**" refers to the date the Contractor has stipulated in the Implementation Plan as to when the Installation is to take place.

"**IP**" is the abbreviation for intellectual property and shall include patents, copyright, industrial design and integrated circuit topography.

"**Invitation to Tender**" refers to the invitation to participate in this Tender and comprises all tender documents forwarded to the Tenderer inclusive of the Covering Letter, Instruction to Tenderers, Form of Tender, ERP Conditions of Contract, General Requirement Specifications, Combined Functional Requirements, Technical Requirement Specifications and any other documents and forms enclosed.

"**Letter of Acceptance**" refers to the letter issued by SAS accepting the Contractor's Tender

"Office Hour" refers to Monday to Friday 8:30am to 6pm.

"**Party**" refers to either SAS or the Contractor and "**Parties**" refers to both SAS and the Contractor.

"**Performance Guarantee Period**" refers to the period referred to in **Clause 24**.

"**Person**" includes any individual, companies and association or body of person, whether corporate or unincorporated.

"**Project Manager"** refers to the person designated by the Contractor pursuant to **Clause 12.3.1.**

"**SAS's Representative**" refers to the person appointed by SAS pursuant to **Clause 12.1** and any persons appointed by SAS's Representative to assist him or perform such duties or functions as may be delegated to him by SAS's Representative.

"Requirement Specifications" and "**Functional Requirements**" refers to Annex C, Annex D and Annex G:

(a) the specifications issued by SAS to the Contractor for the purpose of inviting the Contractor to submit its Tender for Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services; and

(b) other amendments or specifications as may be mutually agreed in writing between the Parties.

"SAS" is the abbreviation for Singapore Arts School Limited.

"**Services**" shall mean all Works and services to be performed by the Contractor in accordance with this Contract; including but not limited to software development, integration and maintenance including Application Management & Support (AMS).

"**Site**" shall refer to the locations where the various parts of the Application Software are to be installed as stated in the Functional Requirements or where Maintenance Services are to be provided.

"**Sub-Contractor**" refers to any person, firm or company furnishing goods and services, IP Rights or Technical Information directly to the Contractor or indirectly to the Contractor through one or more persons, firms or companies. It includes any person, firm or company engaged by the Contractor to perform any part or parts of the Works and includes the Sub-Contractor's duly appointed personnel, successors and permitted assignees and a Sub-Contractor's Sub-Contractor.

"**Contractor**" means the person, firm or company whose Tender Offer has been accepted by SAS for this Invitation to Tender. It includes the Contractor's duly appointed personnel, successors and permitted assignees and where the context so admits shall include the Contractor's employees, agents and SubContractors.

"System" means the Application Software and other software proposed by the Contractor as being capable of meeting or exceeding the project goals, objectives, outcomes and requirements of SAS as articulated in the Combined Functional Requirements. The software and Application Software components in the System must also be capable of working in combination with one another. For the avoidance of doubt, the System shall include Application Software, and/or software (including Commercial Off-the-shelf Software that is commercially available to the general public and that can be used with little or no modification) used or owned by SAS including those that may not have been developed by the Contractor.

"**System Performance Tests**" refers to the tests to be conducted on the System pursuant to **Clause 22.6**.

"**System Warranty Period**" shall have the meaning given to it in **Clause 25.**

"**Technical Information**" includes inventions, confidential information, know-how, trade secrets and, in particular, all information concerning equipment and System Software (including firmware) pertaining to design, manufacture, maintenance, installation, operation and use, in whatever form including drawings, charts, manuals, schematic representations, System Software listings in source and object code.

"System Administrator" refers the person who has been assigned to add, remove, update user access rights and permissions.

"**Tenderer**" refers to the person or persons, firm or company that submits a Tender Proposal.

"User" refers to any SAS Staff who has been given access to the System.

"**Works**" refers to the Works to be executed in accordance with this Contract including all permanent and temporary Works and any equipment to be designed, supplied, delivered, installed, testing and commissioning under this Contract.

1.2 Words importing the singular shall also include the plural and vice versa where the content requires.

1.3 The headings in this Contract are for convenience of reference only and shall not be deemed to be part of this Contract or be taken into consideration in the interpretation or construction of this Contract.

1.4 Unless otherwise provided, any reference to any statute or legislation shall be deemed a reference to such statute or legislation as amended from time to time and be deemed to include any subsidiary legislations made thereunder.

1.5 The Annexes, Schedules and Appendices mentioned in and attached to this Contract shall form an integral part of this Contract. The Conditions of Contract and the attached Schedules shall be construed as one and shall prevail over any inconsistent provisions in the annexes.

2 CLAUSE REFERENCES

All references to clauses, unless otherwise expressly stated, are references to clauses numbered in the ERP Conditions of Contract and not to those in any other document forming part of the Contract. Where a clause number is quoted, then reference is being made to that clause bearing that clause number and to all the subclauses if any, under that same clause number (E.g. a reference to Clause 8 refers to Clause 8.1 to 8.6 inclusive of all their respective subclauses if any. A reference to Clause 8.1 refers to Clause 8.1(a) to 8.1(c) inclusive of all their respective sub-clause if any).

3 SERVICES TO BE PROVIDED BY CONTRACTORS

3.1 The Contractor shall:-

(a) propose the Application Software, which together with any IT environment specified by SAS, forms the System which is capable of meeting or exceeding the requirements of this Contract;

(b) supply the Application Software to SAS free from all encumbrances;

(c) deliver the Application Software to and install the Application Software at the Site(s) by the Stipulated Installation Date

(d) provide the System, comprising the Application Software together with any IT environment specified by SAS, ready for use by the Stipulated Commissioning Date;

(e) provide the Documentation in accordance with Clause 33;

(f) provide training in accordance with Clause 28;

(g) provide software maintenance and support for the Application Software with the same scope as in Maintenance Services commencing from the installation of the Application Software until the end of the Software Warranty Period; and

(h) provide all other services specified by this Contract, upon the terms and conditions hereinafter contained.

3.2 The Contractor warrants that the Application Software, related operating manuals and Documentation supplied shall be free from all defects and encumbrances, and shall meet the requirements set out in the Requirement Specifications and such other additional specifications as may be promised by the Contractor in its Schedule 3 - Schedule of Price.

3.3 The Contractor shall designate a common service location for SAS to contact for the provision of all the Services.

3A. INTENTIONALLY LEFT BLANK

4 TERMS OF PAYMENT

4.1 Subject to the provisions of this Contract, SAS shall pay to the Contractor the Contract Sum in the manner prescribed in Schedule 3 - Schedule of Price and Appendix 1.

4.2 Payment by SAS shall not be considered as evidence of the quality of the System to which such payments relate and shall also not be regarded as a waiver of any default by the Contractor in the performance of its obligations, and it shall also not relieve the Contractor from its other obligations under the Contract.

4.2A If requested by SAS, the Contractor shall submit to SAS invoices and such other documents through the electronic invoicing System maintained by SAS or through such means and in such format as may be specified by SAS for the purposes of making payment.

4.3 SAS shall not be required to pay for expenses or cost of whatever nature other than those expressly set forth in this Contract, unless otherwise expressly agreed to in writing by SAS.

4.4 The Contract Sum is exclusive of any GST chargeable on the supply of goods, services or Works to SAS by the Contractor under this Contract. If the Contractor is a taxable person under the GST Act, SAS shall reimburse the Contractor for any such GST payable under this Contract.

4.5 Any invoice or other request for payment of monies due to the Contractor under the Contract shall, if it is a taxable person for the purpose of the GST Act, be in the same form and contain the same information as if it were a tax invoice for the purposes of the regulations made under the GST Act.

5 TAXES, FEES AND DUTIES

5.1 The Contractor shall be responsible for all corporate and personal income taxes, customs fees, duties, fines, levies, assessments and other taxes payable by the Contractor or its employees in carrying out its obligations under the Contract.

5.2 If SAS receives a request from the tax authorities or otherwise decides to pay on behalf of the Contractor or the Contractor's employees, or to withhold payments from the Contractor in order that SAS may subsequently so pay, any such taxes, fees, duties, fines, levies and assessments ("Taxes"), the Contractor agrees that SAS may deduct such Taxes from payment due to the Contractor and forward the balance to the Contractor without any obligation to gross up such payment or pay the Contractor any amount so withheld.

5.3 For the avoidance of doubt, if withholding taxes are imposed by the tax authorities on any payment due under this Contract, the Contractor shall bear all such withholding taxes and SAS shall be entitled to deduct such taxes from payment due to the Contractor and forward the balance to the Contractor without any obligation to gross up such payment or pay the Contractor any amount so withheld.

6 TIME FOR PERFORMANCE

Time shall be of the essence in this Contract and the Contractor undertakes to supply, deliver, install and integrate the Application Software, commission the System, and provide the Services in accordance with the time lines and/or stipulated dates prescribed in Annex E under this Contract.

7 SAS'S OBLIGATIONS

7.1 SAS shall not employ any of the Contractor's staff connected with the project within one (1) year after the completion of the System Warranty Period.

7.2 If the progress of the Works is delayed for reasons not attributable to the Contractor (whether attributable to SAS or not), SAS's Representative may, upon the application by the Contractor, grant such extensions of time as he deems reasonable. The Contractor shall not be entitled to claim any additional expenses incurred for such extensions of time, unless those expenses are specifically agreed to by SAS's Representative in writing as those SAS will bear before the expenses are incurred.

8 CONTRACTOR'S OBLIGATIONS

8.1 The Contractor shall with due care and diligence:

(a) carry out its obligations to SAS under this Contract;

(b) ensure that the Application Software, the Services and the System meets the requirements as set out in the Requirement Specifications; and

(c) do all things which are necessary or reasonably to be inferred from the Contract.

8.2 The Contractor shall carry out its obligations in relation to the Services and Works in conformity with the general accepted standards of skill, care and diligence appropriate to the nature of the service rendered.

8.3 The Contractor and its Sub-Contractors shall not employ any staff of SAS connected with the project until one (1) year after the completion of the System Warranty Period.

8.4 If the Contractor delays progress on any part of this Contract, for any reason not attributable to SAS, and thereby reduces any scheduled duration of activities to be carried out by SAS under this Contract, SAS shall be entitled to a corresponding time extension for completion of such activities at no additional cost to SAS, and without prejudice to the Contractor's obligation to complete the Contract in accordance with the Implementation Plan.

8.5 In the performance of this Contract, the Contractor shall at its own expense within a reasonable period of time, clear away and remove from the Site all surplus materials, rubbish and work of every kind and leave the whole of the Site clean and in workmanlike condition.

8.6 The Contractor shall ensure the Application Software is free from defects including defects arising out of faulty design, inferior materials, faulty and inferior workmanship. The Application Software shall be of high quality and fit for the purposes for which it is intended as set out in the Requirement Specifications.

8.7 Every obligation by the Contractor is taken to include an obligation by the Contractor to ensure that each of its directors, officers, employees, and agents, and that of its Sub-Contractors and others under its control performs or complies with that obligation. Any covenant by the Contractor not to do any act or thing includes an obligation not to allow that act or thing to be done by its officers, employees, and agents, and that of its Sub-Contractors.

9 RESPONSIBILITY FOR THE SYSTEM

9.1 The Contractor shall ensure that the System meets all project goals, objectives, outcomes and requirements of SAS and will provide the facilities, functions and performance standards set out in the Requirement Specifications. If modifications or changes are necessary for the System to meet the requirements as stated in the Requirement Specifications and the provisions of the Contract, the Contractor shall bear all additional costs involved in modifying or changing the System to satisfy these requirements.

9.2 The Contractor shall forthwith inform and provide SAS at no cost whatsoever technical information on new product developments and improvements which may be applicable to the System when such technical information becomes available to the Contractor.

9.3 The Requirement Specifications which set out the functions to be provided by the System to allow the Contractor to choose the manner in which the functions will be achieved by the selection of Application Software. It is anticipated that some matters of details may have to be clarified during the early stages of this Contract. In this context, SAS reserves the right to issue written clarifications on the Requirement Specifications to set out SAS's requirements more precisely.

9.4 The Contractor shall be deemed to be fully informed of SAS's requirements by the Requirement Specifications and it shall be the Contractor's duty to clarify before submission of his Tender any inadequacies or insufficiencies in the Requirement Specifications having regard to the objective of SAS's purchase of the System.

9.5 In the event that the System supplied by the Contractor is inadequate to meet the requirement as stated in the Requirement Specifications and the provisions of this Contract, the Contractor shall at its own expense, provide all additional items of equipment and System Software which are necessary for the System to meet such requirements. Any changes hereunder to meet SAS’s Requirement Specifications must be agreed to by SAS in writing.

9.6 All System supplied pursuant to Clause 9.5 shall on acceptance by SAS become the property of SAS and shall be subjected to the same warranty and maintenance by the Contractor as the entire System at no additional cost to SAS.

10 MODIFICATION OF SYSTEM

10.1 No change or modification shall be made to the proposed System offered at the time of submission of the Contractor's Tender and thereafter unless the prior written agreement of SAS has been obtained.

10.2 The Contractor shall provide written procedures and details of System changes or modifications which may have to be implemented during the various stages of the Contract, up to the expiry of the System Warranty Period. Such changes or modifications with reference to Clause 9.5 shall not be implemented unless the prior written agreement of SAS has been obtained.

11 INTENTIONALLY LEFT BLANK

12 PROJECT MANAGEMENT

12.1 SAS's Representative

The person appointed by SAS and any persons appointed by SAS's Representative to assist him or perform such duties or functions as may be delegated to him by SAS's Representative

12.2 Project Office

The Contractor shall at its own expense establish a Project Office in Singapore to coordinate the performance of this Contract.

12.3 Project Manager and Other Personnel

12.3.1 The Contractor shall designate a Project Manager and the Project Manager shall be primarily responsible for directing and coordinating the design, supply, delivery, installation, testing and commissioning of the System and all work and services which are to be executed or provided by the Contractor under the Contract and all other matters including contract administration, monitoring of progress, installation and testing of equipment, technical personnel training, logistic support, documentation preparation and operation start-up. The Project Manager shall be deemed to be the Contractor's agent in all dealings with SAS and all actions of the Project Manager shall be binding on the Contractor.

12.3.2 SAS's Representative shall have direct access to the Project Manager at all times during the performance of this Contract and if the Project Manager is absent from Singapore for any duration, the Contractor shall designate another employee to perform his duties and functions without interruption to service level.

12.4 Implementation Plan

12.4.1 Within fourteen (14) days from the issue of the Letter of Acceptance, the Contractor shall produce and maintain an Implementation Plan showing the time schedule and sequence of events necessary for the delivery, installation, integration, testing and acceptance of the Application Software including a delivery schedule for the Documentation and the respective dates for the commissioning of the System.

12.4.2 The Implementation Plan shall, unless otherwise agreed by SAS, conform with the work programme submitted by the Contractor in its Schedule 3 - Schedule of Price and shall not extend the time prescribed in Requirement Specifications.

12.5 Regular Progress Reports & Meeting

The Contractor shall deliver to SAS's Representative regular written progress and status reports in a format approved by SAS's Representative (the "Progress Reports"). Unless otherwise stipulated by SAS in writing, the Progress Reports shall be submitted on a monthly basis. The Progress Reports shall include the current project status, the expected and actual completion dates of events necessary for the delivery, installation, commissioning and acceptance of the System, the activities to be carried out by SAS and SAS's Representative, and an indication as to whether the deadlines set out in the Implementation Plan can be met. The submission and acceptance of these reports shall not in any way prejudice the rights of SAS to make any claims against the Contractor.

13 CONTRACTOR'S PERSONNEL

13.1 The Contractor shall provide all necessary personnel who are suitably qualified and competent and who have adequate skills for the performance of the Works.

13.1.1 The Contractor shall communicate in writing for the approval of SAS's Representative the names and particulars of all personnel (including those of its Sub-Contractors) that it intends to deploy for the performance of the Contract.

13.1.2 The Contractor shall provide the name and particulars required under Clause 13.1.1 in the form required by SAS's Representative.

13.1.3 Except as approved by SAS and subject to such conditions as SAS may impose, the Contractor shall ensure that each personnel shall not commence work on the Contract unless the personnel has passed the necessary level of security clearance for the category and nature of the work handled by the personnel as and when required by SAS. The personnel shall, as part of the security clearance, submit such declaration as may be required by SAS.

13.1.4 The Contractor shall take into consideration the time reasonably required for security clearance and ensure that sufficient number of personnel with the necessary level of security clearance is deployed at every stage of the implementation.

13.2 If SAS objects by notice in writing to any personnel assigned or designated by the Contractor or by any Sub-Contractor to carry out any Works or perform Services for the purposes of the Contract who, in the opinion of SAS, has misconducted himself or is a security risk or is deemed unsuitable in any way or has failed any security clearance subsequent to the commencement of Works on the Contract, the Contractor shall remove such person immediately and furnish a suitable and adequate replacement at no additional expense to SAS. If SAS has other reasons to believe that any personnel assigned or designated by the Contractor, or its Sub-Contractors or agents are unsatisfactory in any way, the Contractor and SAS shall meet immediately in order to reach a mutually acceptable solution.

13.3 The Contractor undertakes not to change its personnel designated under Clause 13.1 without SAS's or SAS's Representative's consent, whose consent shall not be unreasonably withheld. The Contractor shall not alter or reduce the quality of its personnel if this may adversely affect the progress or quality of the Works. In the event that the Contractor wishes to replace its designated personnel, the Contractor shall provide the names and particulars of the replacement staff in writing to SAS or SAS's Representative for SAS's or SAS's Representative's (as the case may be) consent.

Replacement staff shall not commence work on the project unless approval is given in writing by SAS.

13.4 The Contractor shall not, without prior written permission from SAS's Representative, bring any visitor to the Site.

14 INTENTIONALLY LEFT BLANK

15 INTENTIONALLY LEFT BLANK

16 INFORMATION AND ACCESS

16.1 SAS undertakes to provide the Contractor promptly with any information which the Contractor may reasonably require from time to time to enable the Contractor to proceed expeditiously with the performance of its obligations under the Contract.

16.2 SAS shall, for the purposes of the Contract, afford to the Contractor's Personnel during normal working hours full and safe access to the Site and shall provide adequate free working space and such other facilities as may be necessary for the delivery, installation, integration and testing of the Application Software and the commissioning of the System.

17 INTENTIONALLY LEFT BLANK

18 INTENTIONALLY LEFT BLANK

19 INTENTIONALLY LEFT BLANK

20 INTENTIONALLY LEFT BLANK

21 INSTALLATION

The Contractor shall deliver the Application Software to SAS and install and integrate the same on the Hardware at the Site in accordance with the Implementation Plan.

22 ACCEPTANCE TESTS

22.1 Conducting Acceptance Tests

22.1.1 Acceptance tests on the Application Software shall be conducted to verify and demonstrate that the Application Software meets the Requirement Specifications ("Acceptance Tests"). The Acceptance Tests shall be conducted after installation of the Application Software under Clause 21. The Acceptance Tests shall comprise of:

(a) Software Installation Tests;
(b) System integration tests, System functional tests, and System non-functional tests (e.g. security tests); and
(c) System Performance Tests.

22.1.2 The Acceptance Tests shall also apply to any substitute, replacement and converted component parts that are acquired by SAS in relation to this Contract.

22.1.3 The Acceptance Tests shall comply with the Acceptance Test Procedures proposed by the Contractor in its Schedule 3 - Schedule of Price and accepted by SAS. SAS shall however have the right to modify the Acceptance Test Procedures or specify different procedures within a reasonable time prior to the tests to meet the requirements of the Contract. The Acceptance Test Procedures proposed by the Contractor in its Schedule 3 - Schedule of Price shall be developed based on the Requirement Specifications or otherwise specified by SAS in the Contract.

22.2 Notice of Commencement and Completion of Acceptance Tests

22.2.1 The Contractor shall give to SAS in writing seven (7) days prior notice or such shorter notice as SAS's Representative may agree in writing of the place, date and time at which the Contractor proposes to conduct any Acceptance Tests.

22.2.2 The Contractor shall provide all tools and testing equipment at his own cost and expense for the purposes of the Acceptance Tests.

22.2.3 Upon completion of any Acceptance Test, the Contractor shall give notice of such completion to SAS.

(a) If SAS is satisfied that the Acceptance Test has been successfully completed, SAS shall certify that the Acceptance Test has been successfully completed.

(b) If SAS is not satisfied that the Acceptance Tests has been successfully completed, the Contractor shall within a period of seven (7) days of receipt of the notice, provide in writing a defect report.

22.3 Delay in Acceptance Tests

22.3.1 If in the opinion of SAS, the Acceptance Tests are unreasonably delayed, SAS may by notice in writing require the Contractor to conduct the tests within seven (7) days from receipt of such notice and the Contractor shall make the tests on such date or dates within the said seven (7) days.

22.3.2 If the Contractor fails to conduct such tests within the time, SAS may itself proceed to conduct the said tests. All Acceptance Tests so conducted by SAS shall be at the risk and expense of the Contractor.

22.4 INTENTIONALLY LEFT BLANK

22.5 INTENTIONALLY LEFT BLANK

22.6 System Performance Tests

22.6.1 The Contractor shall perform the software performance test in accordance with the Contract to achieve the project goals, objectives, outcomes and requirements as set out in the Requirement Specifications and as communicated by SAS to the Contractor.

22.6.2 The overall System Response Time used herein refers to the elapsed time between a user pressing a key or clicking on a mouse button or a function key on-screen to start a query or activate an action in the System, and the first completed screen response containing the results, which may include the presentation of the requested data input screen for data entry or further actions, or the appearance of the System prompt awaiting further user commands.

22.6.3 After the System has been fully installed on the Hardware at the Site, the Contractor shall load into the System test data which in the reasonable opinion of SAS is suitable to test whether the System is in accordance with the General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D) and Technical Requirement Specifications (Annex G) and with the advice and assistance of the Contractor, SAS shall operate the System for the period of seven (7) working days to:

(a) Perform SAS's routine transactions;

(b) Perform the transactions included, referenced, or incorporated in the Requirement Specifications;

(c) Carry out System functions test to determine whether the System meets the specifications, performs the functions, and meets the criteria for Systems Availability, response time and workload requirements set forth in the Requirement Specifications;

(d) Determine whether the documentation for the System meets the requirements of this Contract;

(e) Perform such other transactions as may be necessary to test the System performance specified in the Requirement Specifications.

22.6.4 The System shall be deemed to fail the System Performance Tests if

(a) it fails to provide any facility, transaction or function specified in the Requirement Specifications; or

(b) it fails to run the System Software in accordance with the Requirement Specifications and within two percent (2%) of Expected Overall System Response Time in Annex G - Technical Requirement Specifications Point 1.3.7 - Table 1, for the period prescribed for the System Performance Tests.

22.6.5 If the System fails to pass the System Performance Tests then SAS may, by written notice to the Contractor at its sole option:

(a) to have the Contractor provide a solution and to fix (without prejudice to its other rights and remedies) a new date for carrying out further tests on the System on the same terms and conditions (save that all costs which SAS may incur as a result of carrying out such tests shall be reimbursed by the Contractor). Unless otherwise agreed in writing between the Parties, all such further tests shall not be construed as any grant of extension of time by SAS and the Contractor remains liable for any delay in complying with its obligations under the Contract; or

(b) to accept the System subject to a mutually agreed reasonable reduced Contract Sum as taking into account the circumstances, is reasonable. In the absence of written agreement as to abatement within fourteen (14) days after the date of such notice SAS shall be entitled to exercise Sub-Clause (c) below; or

(c) to treat the Contractor as being in breach of Contract and to reject the System as not being in conformity with the Contract in which event SAS shall be entitled to terminate this Contract (without prejudice to SAS’s other rights and remedies) in accordance with Clause 48.

22.7 Failure of Acceptance Tests

SAS shall not be under any obligation to accept the System if it does not successfully pass any of the Acceptance Tests under the Contract. In the case of Application Software tests, the Contractor shall diagnose software failures/deficiencies. The Contractor shall submit a report to SAS detailing the cause for the failure of any Acceptance Tests and the corrective action taken.

22.8 Commissioning Date

22.8.1 As soon as the System has successfully passed all the Acceptance Tests, SAS shall forthwith issue a certificate commissioning the System and the date of the certificate shall be the Commissioning Date of the System.

22.8.2 The Contractor shall remain liable to SAS in accordance with the terms and conditions contained herein notwithstanding the signing by SAS of any certificate or document or any payment or the release of the security deposit. Subject to Clause 22.8.3 below, such certificate, document or payment shall have no legal effect other than serving as a declaration by the Contractor that it is ready to proceed with the next phase of this Contract.

22.8.3 The Acceptance Test Certificate issued in respect of the last and final Acceptance Test to be conducted under this Contract, when signed by SAS, signifies acceptance by SAS of the System and is, subject to such reservations as may be endorsed thereon by SAS, final and binding in respect of all matters covered by that Acceptance Test.

23 LIQUIDATED DAMAGES FOR LATE COMMISSIONING

23.1 In the event the Contractor fails to meet the Stipulated Commissioning Date or such Commissioning Date as extended pursuant to Clause 7.2, SAS may, in addition to the remedies under Clause 22.7, by written notification to the Contractor:

(a) impose liquidated damages at the rate of one tenth of a percent (0.1%) of the Contract Price for each day (including Sundays and Public Holidays) or part thereof up to a maximum of ten percent (10%); or

(b) purchase a System equivalent to the System as defined in clause 1 (“System”) from any other sources and any increase in cost between that equivalent System and the Contract Price shall be recoverable from the Contractor together with all payments made under this Contract. For the avoidance of doubt, the equivalent System shall be a System which has the same or the closest fit to the Requirement Specifications relating to the System. For the further avoidance of doubt, the equivalent System shall include all documentation, training and related materials required for the equivalent System to meet the Requirement Specifications.

23.2 Liquidated damages imposed under the Clause 23.1 above shall be paid to SAS in Singapore Dollars not later than thirty (30) calendar days from the date of issue of a SAS's written notification to the Contractor informing the Contractor of the liquidated damages payable.

23.3 If the Contractor fails to pay the said damages, SAS may deduct the amount due from any monies due or which may become due from SAS to the Contractor under the Contract and other contracts between the Parties or recover the same as a debt due from the Contractor in any court of competent jurisdiction.

23.4 Where the Contractor is required in the Implementation Plan to submit any plans, scripts, manuals and other documents for verification and review and the Contractor fails to meet the time schedule for submission of any such documentation, SAS shall be entitled to an extension of time for

verification and review corresponding to the period of delay without prejudice to the Contractor's obligation to meet the Stipulated Commissioning Date.

24 PERFORMANCE GUARANTEE PERIOD

24.1 In this clause the following expressions shall have the meanings hereby assigned to them:

"Operating Hours" means the scheduled operating hours of the System which will be from 0000 hours to 2400 hours from Monday to Sunday including Public Holidays

"Standard of Performance" means the level of performance achieved by the System when it is operating in conformity with the Requirement Specifications.

"System Availability Level" shall be determined according to the following formula:

System Availability = [Operating Hours - System Downtime] / [Operating Hours] x 100%.

"System Downtime" means the accumulated time during which the System is not performing in accordance with the Standard of Performance due to product failure measured from the time the Contractor is informed by phone of the product failure to the time when the System is returned to proper operation.

"Working day" means every day except for Saturday, Sundays and Public Holidays.

24.2 The Performance Guarantee Period shall commence on the Commissioning Date and continue for a period of thirty (30) days.

24.3 The System shall have successfully completed the Performance Guarantee Period if the System meets the Standard of Performance with a System Availability Level of not less than ninety-nine point nine per cent (99.9%) for each calendar month or part thereof during the period of one (1) calendar month.

24.4 In the event that the System fails to meet the requirements under Clause 24.3 the Performance Guarantee Period shall continue from day to day until the System has met the Standard of Performance with a System Availability Level of not less than ninety-nine point nine per cent (99.9%) over a period of one (1) consecutive calendar month.

24.5 SAS shall maintain daily records to monitor and determine the successful completion of the Performance Guarantee Period.

24.6 Once the System has successfully completed the Performance Guarantee Period either in accordance with Clause 24.3 or Clause 24.4 SAS shall forthwith issue a written notice to the Contractor accepting the System. The date of the notice or the date when such notice should be issued as determined from the records kept (if different from the date of the notice) shall be the Acceptance Date.

24.7 During the Performance Guarantee Period, the Contractor shall at all times and under all conditions be entirely responsible for the functioning of the System in accordance with the Requirement Specifications, and for the compliance of such additional requirements as may be mutually agreed upon between SAS and the Contractor at no additional cost to SAS.

24.8 The Contractor shall remedy and make good at no cost to SAS all defects, deficiencies, failures or damage to the System or any part thereof arising at any time prior to the commencement of the System Warranty Period. For avoidance of doubt, defects shall include and are not limited to

defective design, materials, workmanship, incorrect operating or maintenance instructions given by the Contractor in writing, and any damage to the System or operational data. The Contractor shall furnish SAS with a report to explain the defects and to advice on the corrective action taken within three (3) calendar days after the defects have been rectified.

25 SYSTEM WARRANTY PERIOD

25.1 The System Warranty Period shall commence on the Acceptance Date and shall last for twelve (12) calendar months or such longer period as may be proposed by the Contractor.

25.2 During the System Warranty Period, the Contractor shall render replacement parts and diagnostic services and any other Works and services required to make good all defects to the System at no cost to SAS, provided that written notice of such defects is promptly given to the Contractor.

25.3 Where during the System Warranty Period, the System or any part thereof is found to be:

(a) defective in either design, materials or workmanship; or
(b) not in accordance with the Contract; or
(c) having been installed, operated, stored and maintained in accordance with the written instructions of the Contractor, fails to function properly or fails to meet any performance guarantees set forth in the Contract or any additional requirements which may be mutually agreed between SAS and the Contractor;

then, the Contractor shall, at its own expense (including but not limited to transportation costs, air freight charges, costs of testing, manufacturing and examination), upon notification from SAS, replace or completely repair the defective parts of the System or otherwise completely rectify the defects.

25.4 During the System Warranty Period, the Contractor shall comply with the System Availability Level, and respond to the foregoing notification within the response time specified in the Annex G - Technical Requirement Specifications Point 7.6.10.

25.5 If the Contractor fails to respond to the notification or to render the System fully operational within the time frame referred to in Clause 25.4 above, SAS may

(a) remedy the defects itself, whether by engaging a Contractor to repair the defects or by purchasing the defective parts of the System from other sources or by such other means as may be necessary to render the System fully operational, and all costs incurred by SAS in this regard shall be borne by the Contractor.

25.6 For the avoidance of doubt, SAS's rights and remedies under this Clause are independent of; and without prejudice to any other rights and remedies of SAS.

26 INTENTIONALLY LEFT BLANK

27 MAINTENANCE AND SUPPORT SERVICES (AMS)

27.1 SAS shall be entitled to obtain AMS as an option for the support and maintenance of the System designed and/or supplied by the Contractor pursuant to the Contract ("Option").

27.2 This AMS shall be valid for a period of twelve (12) months commencing after the expiry of System Warranty Period.

28 TRAINING

28.1 The Contractor shall be responsible for the provision of suitable and adequate training for staff nominated by SAS.

28.2 The training shall include training in use of the Application Software and self-help for first line support by the computer center information Systems officers, supervisors, operators and end-users.

28.3 Unless otherwise agreed in writing between the Parties, training shall be scheduled after the System has passed the System Performance Tests, but no later than the Commissioning Date.

29 INTENTIONALLY LEFT BLANK

30 UNAUTHORISED CODE

30.1 The Contractor warrants that at the time of delivery and/or installation:

(a) the System and every part thereof are free of Unauthorised Code (hereinafter defined); and

(b) all magnetic or other storage media and all software and other materials capable of being stored on such media

(i) supplied as a software or part thereof or with any software; or

(ii) used in the performance of any Services shall not contain any Unauthorised Code.

30.2 Prior to and at the time of delivery and installation, the Contractor shall conduct a complete and thorough scan for Unauthorised Code using anti-virus software package(s) on the System prior to delivery and installation.

30.3 In the case of breach of Clause 30.1 above, the Contractor shall:

(a) Indemnify SAS fully against all costs incurred by SAS in the course of or incidental to removing the Unauthorised Code and recovering any lost or damaged data or software;

(b) Remove and replace such Unauthorised Code and/or software at its own cost.

30.4 In this clause: “Unauthorised Code” refers to any malware including viruses, Trojans, worms, bots or other Software routines designed to permit unauthorised access, to disable, erase, or otherwise harm Software, hardware or data, or to perform any such actions.

31 DOCUMENTATION

The Contractor shall at no additional charge supply and deliver the documentation needed for the operation and maintenance of the System. All subsequent updates for each set of the aforesaid documents shall be supplied at no additional charge to SAS as soon as they are available.

32 LIABILITY OF CONTRACTOR

If the Contractor is obtaining part(s) of the Application Software from a third party, the Contractor shall inform SAS in writing of the source or origin of the said part(s) of the Application Software and, for avoidance of doubt, it is expressly declared that the Contractor shall remain fully liable for that part(s) of the Application Software and the consequences arising from the use of the said part(s).

33 PATENT, COPYRIGHT AND OTHER INDEMNIFICATION

33.1 The Contractor represents and warrants that all software and intellectual property used or introduced by the Contractor under this Contract does not infringe any copyrights, and all rights in relation to inventions, registered trademarks (including service marks), registered and unregistered designs, knowhow and any other rights resulting from intellectual activity in the industrial, scientific, literary and artistic fields.

33.2 The Contractor shall indemnify SAS against any action, claim, damage, charge and cost arising from or incurred by reason of any infringement or alleged infringement of use of patents, design, copyright or other statutory or common law rights of the System, Application Software or consumables supplied or furnished by the Contractor pursuant to this Contract.

33.3 SAS shall give the Contractor prompt notice in writing of any such claim.

33.4 Without prejudice to SAS's right to defend a claim alleging such infringement, the Contractor shall, if requested by SAS, but at the Contractor's expense, defend such claim. The Contractor shall observe SAS's directions relating to the defence or negotiation for settlement of the claim.

33.5 SAS shall if requested but at the Contractor's expense provide the Contractor with reasonable assistance in conducting the defence of such claim.

33.6 If any of the said items is in any such suit brought for infringement of intellectual property rights and its use is enjoined, the Contractor shall, if requested by SAS, at the Contractor's own expense:

(a) procure for SAS the right to continue using the same; failing which,

(b) replace or modify the same so as to avoid the infringement; failing which,

(c) pay SAS for such infringing items, a sum equivalent to the purchase price of functionally equivalent items upon the return of the infringing items to the Contractor;

PROVIDED ALWAYS that such actions as aforesaid shall not prejudice or affect any right of action or remedy of SAS against the Contractor.

33.7 In the event of any actions being contemplated or instituted for an alleged infringement of patents, design, copyright or other statutory or common law rights, SAS reserves the right to cancel immediately the Contract for delivery of the System or parts hereof yet to be supplied to SAS and/or return the System or parts thereof already delivered and the Contractor shall compensate SAS with the contract price already remitted and SAS reserves its right to purchase the System or parts thereof from other sources without prejudice to all or any of SAS’s rights as contained in this Contract.

33.8 All royalties and fees claimable by or payable to any person, firm, corporation or SAS for or in connection with any copyright, invention, patent or Application Software used or required to be used in respect of the System or any part thereof in the performance of the Contract or supplied under the Contract shall be deemed to be included in the prices of the System or part hereof.

33.9 The obligation in Clause 33.1 to Clause 33.8 above do not cover claims of infringement which arises by reason only of:

(a) any modification of the System or any use of a software other than in its specified operating environment; or

(b) the combination, operation or use of the System with any product not supplied by the Contractor.

34 RELOCATION OF SYSTEM

34.1 SAS shall have the right to relocate any or all items of the System within Singapore. Any such relocation shall not affect the Contractor's obligations under this Contract although SAS shall grant extension of the Implementation Plan accordingly if it is affected.

34.2 In the event that SAS requires the Contractor's services for the relocation of the System, SAS shall give thirty (30) days' written notice of its intent to relocate the System.

34.3 The Contractor's Personnel shall arrange and supervise the dismantling, packing, unpacking and reinstallation of the System to normal operating condition for which SAS shall be charged by the Contractor at a Fair Market Value.

34.4 The Contractor shall make good any damage suffered by the System due to the negligence of the Contractor's Personnel including the Contractor's employees or agents, during the transfer to a new location.

35 LANGUAGE

35.1 All data and references, including but not limited to, documents, descriptions, diagrams, books, catalogues, instructions and markings for ready identification of major items of the System and correspondence shall be written in readily comprehensible English Language.

35.2 The personnel of the Contractor and the Sub-Contractor shall be proficient in both written and spoken English for the purpose of providing instructions, offering of advisory services, training and any other submissions as required.

36 DAMAGE AND INJURY TO PERSONS AND PROPERTY

36.1 The Contractor shall:-

(a) be responsible for and make compensation for any injury (including injury resulting in death, personal injury or disease or physical damage) occasioned to any person whomsoever; and

(b) be responsible for and reinstate and make good to the satisfaction of SAS or make due compensation for any injury or damage to any property or right of SAS;

being injury or damage arising out of or in connection with the execution of the Contract.

PROVIDED ALWAYS that the Contractor shall not be under any such liability if he is able to prove that such injury or damage was neither caused nor contributed to by his negligence, omission or default, or breach of statutory duty or that of his employees, agents, or Sub-Contractors nor by any circumstances within his or their control; and if he proves that the negligence, omission or default

of any other person (not being his employee, agent or Sub-Contractor) was in part responsible for any personal injury or loss of property to which this Clause applies, the Contractor's liability under this Clause shall not extend to the share in the responsibility attributable to the negligence, omission or default of that person.

36.2 The Contractor shall hold SAS free of any liability and indemnified against all actions, claims and demands in respect of such injury or damage (being injury or damage for which the Contractor is responsible under Clause 36.1) brought against SAS, by any person including any of his (the Contractor's) employees or agents, their personal and dependents, whether or not engaged in connection with the Contract; and where the Contractor is responsible, all costs, fees and expenses thereof pursuant to any settlement, court order or award provided that the Contractor shall be notified promptly of such claim or claims and given adequate opportunity to defend therein or to agree to any out of court settlement or compromise thereof. SAS shall at the request of the Contractor afford all reasonable assistance for the purpose of contesting any such claims or demand or action.

37 LIMITATION OF LIABILITY

37.1 In the event of any breach or default of a term of this Contract, the Contractor's cumulative liability shall not exceed the Contract Price.

37.2 In the event of any breach or default of a term of this Contract, SAS's cumulative liability shall not exceed the Contract Price.

37.3 For the avoidance of doubt, Clause 37.1 and 37.2 shall not apply to any claim relating to any:
(a) death or personal injury,
(b) patent, copyright or other intellectual property right infringement,
(c) indemnity provided under this Contract, or
(d) liquidated damage recoverable under this Contract.

38 INTENTIONALLY LEFT BLANK

39 CONFIDENTIALITY

39.1 The Contractor must keep confidential and undertakes not to divulge or communicate to any person, firm or company any such information howsoever acquired in connection with this Contract without first having obtained the written consent of SAS's Representative. Such information must not be used for any purpose other than for the performance of the Contractor's obligations under this Contract.

39.2 The Contractor shall not transfer information acquired in connection with this Contract outside Singapore, or allow parties outside Singapore to have access to it, without first having obtained the written consent of SAS.

39.3 The Contractor shall immediately notify SAS when it becomes aware that a disclosure of any information acquired in connection with this Contract may be required by law.

39.4 The Contractor shall take all reasonable precautions in dealing with any information, documents and papers passed by SAS to the Contractor so as to prevent any unauthorised person from having access to such information, documents or papers. For the purpose of this Clause 39, all information is to be treated as confidential except such as is or has become public knowledge otherwise than through breach of agreement or other legal obligation of, or through the default or negligence of, the Contractor, his employees, Sub-Contractors or agents.

39.5 The Contractor shall procure and ensure all his employees and agents and those of his Sub-Contractors or agents who are or may be involved in the execution of obligations under this Contract observes the provisions of this Clause 39 and shall, at any time, if so required by SAS, procure and ensure that such employees and agents and those of his Sub-Contractors or agents sign an Appendix 4, Undertaking to Safeguard Official Information.

39.6 The Contractor shall immediately notify SAS's Representative where the Contractor becomes aware of any breach of Clauses 39.1 to 39.5 by his employees and agents and those of his Sub-Contractors or agents who are or may be involved in the execution of obligations under this Contract.

39.7 Termination or expiry of this Contract for whatever cause shall not put an end to the obligation of confidentiality imposed on the Contractor, its employees, agents and those of this Sub-Contractors or agents under this Clause 39.

39A DATA SECURITY AND PROTECTION

39A.1 The Contractor shall take all reasonable measures to ensure that personal data held in connection with the Contract is protected against loss, and against unauthorised access, use, modification, disclosure or other misuse.

39A.2 The Contractor shall in respect of any personal data held in connection with the Contract cooperate with any reasonable requests, directions, policies or guidelines of SAS arising in connection with the handling of personal data.

40 COMPLIANCE WITH STATUTES, REGULATIONS, ETC

40.1 The Contractor shall give all notices and pay all fees required to be given or paid under any law in force in Singapore and hereby undertakes to obtain all necessary export licence for the export of all items from their countries of origin to Singapore in relation to the execution of the Contract.

40.2 The Contractor shall conform in all respects with the provisions of all laws of Singapore and shall keep SAS indemnified against all penalties and liabilities of every kind for the breach of any such laws.

41 SUB-CONTRACT, ASSIGNMENT, TRANSFER

41.1 The Contractor shall not, without the written consent of SAS, sub-contract, assign or transfer the Contract or the benefits or obligations or any part thereof to any other person. The Contractor shall be responsible for the acts, defaults, negligence or omissions of any assignee or Sub-Contractor, his agents or workmen as fully as if they were the acts, defaults, negligence or omissions of the Contractor, his agents or workmen.

41.2 In seeking the written consent of SAS, the Contractor shall provide all information requested by SAS including but not limited to information about a Sub-Contractor's registration with the relevant Government Registration Authorities (GRA).

42 FORCE MAJEURE

42.1 Neither Party shall be liable for any failure to perform his obligations under the Contract if the failure results from events which are beyond the reasonable control of either Party Provided Always that

whenever possible the affected Party will resume that obligation as soon as the factor or event occasioning the failure ceases or abates. For purposes of the Contract, such acts shall include acts of God, civil or military authority, civil disturbance, wars, strikes, fires or other catastrophes.

42.2 If the effect of any of the said event shall continue for a period exceeding six (6) months SAS may at any time thereafter upon giving notice to the Contractor elect to terminate the Contract.

42.3 In any of the events mentioned in Clause 42.1 the Contractor or SAS shall for the duration of such event be relieved of any obligation under the Contract as is affected by the event except that the provisions of the Contract shall remain in force with regard to all other obligations under the Contract which are not affected by the event.

42.4 Where SAS elects to terminate the Contract under Clause 42.2 the Contractor shall forthwith refund to SAS all amounts paid to the Contractor less the price of items and services which have been provided to SAS.

42.5 Failure of the Contractor's Sub-Contractors or Contractor shall not be regarded as events beyond the control of the Contractor's control unless such Sub-Contractors or Contractor would qualify for exemption under this Clause 42 if the provisions of this Clause 42 were applied to them.

43 PUBLIC RELEASE OF INFORMATION

The Contractor shall obtain in writing the prior approval and the consent of SAS before the release of any news item, article, publication, advertisement, prepared speech or any other information or material, pertaining to or related to any part or whole of the Contract including but not limited to the Works to be performed under the Contract, and System Software licence and support and equipment maintenance associated with the System. Such prior approval shall be sought in reasonable time.

44 GIFTS, INDUCEMENT AND REWARDS

SAS shall be entitled to terminate the Contract at any time and to recover from the Contractor the amount of any loss resulting from such termination, if the Contractor or the Sub-Contractor shall have offered or given or agreed to give to any person any gift or consideration of any kind as an inducement or reward for doing or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of the Contract with SAS or for showing or forbearing to show favour to any person in relation to any agreement with SAS or if the like acts shall have been done by any person employed by the Contractor or Sub-Contractor, or if in relation to any Contract with SAS, the Contractor or the Sub-Contractor or any person employed by the Contractor or Sub-Contractor shall have committed any offence under Chapter IX of the Penal Code or the Prevention of Corruption Act of Singapore or shall have abetted or attempted to commit such an offence or shall have given any fee or reward to any person the receipt of which is an offence under the said part of the Penal Code or under the Prevention of Corruption Act or any legislation enacted in substitution thereof for the time being in force in Singapore.

45 APPLICABLE LAW

The Contract shall be subject to, governed by and interpreted in accordance with the laws of the Republic of Singapore for every purpose and the Parties agree to submit to the exclusive jurisdiction of the Singapore courts.

46 INTENTIONALLY LEFT BLANK

47 CONDITIONS NOT TO BE WAIVED

No waiver of any breach of the Contract shall be deemed to be waiver of any other or of any subsequent breach. In no event shall any delay, failure or omission on the part of either of the parties in enforcing or exercising any right, power, privilege, claim or remedy, which is conferred by this Contract, at law or in equity, or arises from any breach by any of the other Parties of this Contract, be deemed to be or be construed as, a waiver thereof, or of any other such right, power, privilege, claim or remedy, in respect of the particular circumstances in question, or operate so as to bar the enforcement or exercise thereof, or of any other such right, power, privilege, claim or remedy, in any other instance at any time or times thereafter.

48 TERMINATION OF CONTRACT

48.1 If at any time the Contractor is in breach of any of the terms or conditions under this Contract, the Contractor shall have thirty (30) days to effect a remedy or show to SAS's satisfaction the cause of the breach of its obligations and the Contractor's intended remedy, in which case, the Contractor shall have such period, if any, as is authorised in writing by SAS to effect the remedy.

48.2 If the breach of the terms or conditions under this Contract is not remedied pursuant to Clause 48.1 above, SAS may at any time prior to the Acceptance Date terminate the Contract by notice in writing as from the date specified in the notice.

48.3 If the Contractor, being a company, shall pass a resolution or the Court shall make an order that the company shall be wound up otherwise than for the purpose of reconstruction or amalgamation or if a receiver or manager on behalf of a creditor shall be appointed, or if circumstances shall arise which entitle the Court or a creditor to appoint a receiver or manager or which entitle the Court otherwise than for the purpose of amalgamation or reconstruction to make a winding-up order, or any part thereof, without the written consent or approval of SAS, then SAS shall be at liberty to terminate the Contract summarily by notice in writing to the Contractor.

48.4 In the event of termination of the Contract as provided for in Clause 48.2 or Clause 48.3 or in accordance with law, the following shall apply:

(a) (i) all payments that shall have been made under the Contract less the value of all items delivered and accepted by SAS shall be refunded by the Contractor to SAS forthwith provided always that such refunds as aforesaid shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to SAS as a result of the termination due to breach of the Contract by the Contractor;

(ii) the Contractor shall upon written notice from SAS be required to remove, at the Contractor’s expense, the System or any part thereof specified in the notice from the Site at a date specified by SAS, and in default SAS may (without being responsible for any loss or damage):

remove and sell the same, holding the proceeds less all expenses incurred to the credit of the Contractor, or remove and return the same to the Contractor all at the Contractor’s expense.

(iii) SAS shall be entitled to recover from the Contractor any damages, losses, costs and expenses which SAS may sustain or incur in consequence of such termination; all such damages, losses, costs and expenses which are or become so recoverable under the Contract together with any sum payable by the Contractor as liquidated damages, may

be deducted from any money that may then be due to the Contractor and if the money then due to the Contractor under the Contract or deposited by him under the Contract as aforesaid is not sufficient for that purpose, the balance remaining unpaid shall be a debt due from the Contractor to SAS, and may be set off against any other monies which may be or become due to the Contractor from SAS or may be recovered as a debt due from the Contractor in any court of competent jurisdiction;

OR, at the sole discretion of SAS:

(b) (i) SAS may carry out and complete the Works on its own or employ and pay other person or persons to carry out and complete the Works and he or they may enter upon the Site and use all materials, System Software and equipment thereon, and may purchase all materials necessary for the purposes aforesaid;

(ii) the Contractor shall if so required by SAS assign to SAS and without further payment the benefit of any contract for the supply of materials and/or Works intended for the use under the Contract or for the execution of any Works and SAS shall pay the agreed price (if unpaid) for such materials or Works supplied or executed after the said termination;

(iii) the Contractor shall during the execution or after the execution of the Works under this sub-clause as and when required remove from the Site any materials within such reasonable time as SAS may specify in a written notice to the Contractor and in default, SAS may, without being responsible for any loss or damage, remove and sell the same, holding the proceeds less all the expenses incurred to the credit of the Contractor;

(iv) until completion of the Works under this sub-clause no payment shall be made to the Contractor under the Contract; provided that upon completion as aforesaid and the verification within a reasonable time of the accounts therefore, SAS shall certify the amount of expenses properly incurred by SAS and if such amount added to the monies paid to the Contractor before such termination exceeds the total amount which would have been payable on due completion, the difference shall be a debt payable to SAS by the Contractor, and if the said amount added to the said monies be less than the said total amount, the difference shall be debt payable by SAS to the Contractor; provided always the aforesaid shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to SAS as a result of the termination of the Contract or as a result of the breach of the Contract by the Contractor;

(v) in the event of the completion of the Works being undertaken by SAS, allowance shall be made, when ascertaining the amount to be certified as expenses properly incurred by SAS, for the cost of supervision, interest and depreciation on equipment and all other usual overhead charges and profits, as would be incurred were the Works carried out by the Contractor.

48.5 In addition to the rights set out in Clause 48.2 and Clause 48.3, SAS may at any time upon giving at least thirty (30) days notice in writing to the Contractor of its intention to do so, terminate the Contract or any part or further part thereof, and upon such notice being given, the Contractor shall cease or reduce work according to the tenor of the notice and shall forthwith do everything possible to mitigate losses consequent thereto.

48.6 If a notice under Clause 48.5 is given, the Contractor may submit a claim for compensation subject to Clause 48.7. The compensation shall not exceed the total of the cost incurred by the Contractor in the performance of the contract or the part terminated, as the case may be, and reasonable direct costs incurred with respect to termination and settlement with vendors as a consequence of SAS's termination.

48.7 The aforesaid compensation shall not be greater than a sum which in addition to any sums paid or due or becoming due to the Contractor under the Contract would together exceed the Contract Price.

48.8 Direct costs under Clause 48.6 shall be determined in agreement with an independent and mutually agreeable public accountant. SAS shall pay the Contractor the aforesaid compensation within ninety (90) days following submission of such total cost to SAS and verified by an independent and mutually agreeable public accountant.

48.9 Where there are segregable items not desired by SAS which the Contractor agrees to retain for its own use, the compensation payable pursuant to Clause 48.8 above shall be reduced by an amount equivalent to the total Contractor's costs for such items.

48.10 In the event of termination of the Contract under Clause 48.5, all Works carried out except for segregable items within the scope of Clause 48.9 shall become the property of SAS except that title to any proprietary System Software would not be transferable, and for the removal of doubt, it is hereby declared that title to all information captured within the System shall solely belong to SAS.

48.11 No termination of the Contract, whether pursuant to this Clause or otherwise, shall affect any right of SAS to use any System Software whether such right is acquired pursuant to the Contract or otherwise.

49 POLICY, SECURITY AND AUDIT

49.1 Policy

49.1.1 The Contractor shall fully comply with any written instructions on SAS policies pertaining to Information Communications Technology ("ICT") Management that may be issued by SAS from time to time.

49.1.2 Where the Contractor will be performing Extra Work in order to comply with new SAS ICT requirements issued by SAS after the Commencement Date of this Contract, SAS shall not be liable for any claims in respect of such Extra Work UNLESS all the conditions in Clause 54 are fully complied with.

49.1A Security

49.1A.1 The Contractor is required to maintain strict confidentiality and ensure that all information pertaining to the Site and SAS's work environment must not be disclosed to anyone except SAS's Representative and the Contractor's employees, agents or Sub-Contractors directly involved with this Contract. The Contractor is to ensure that information is not to be published or communicated to any other person in any form whatsoever except on a strictly "need-to-know" basis. Failure to comply with this confidentiality requirement shall be a ground for termination of this Contract. This clause shall be without prejudice to the provisions of Clause 39.

49.1A.2 The Contractor, its employees or agents, or Sub-Contractors shall not, without the prior written permission of SAS, bring any visitor to any location or Site at which the Contractor is providing the goods or services under this Contract.

49.2 Audit

49.2.1 The Contractor shall allow SAS to conduct periodic audits at all locations and site at which the Contractor is providing or has provided goods or services under this Contract to ensure that there are proper controls and compliance with this Contract. The Contractor shall cooperate with and

provide support, information and assistance to SAS for the purpose of such audits.

49.2.2 All audits shall be conducted in the form of a SAS audit, or a third-party audit conducted by a reputable audit firm.

49.2.3 The Contractor shall provide all support necessary for the conduct of the audits at no additional cost to SAS.

49.2.4 SAS may conduct surprise spot checks on any locations and site at which the Contractor is providing or has provided goods or services under this Contract for the purpose of such audits.

49A SECURITY AND DATA BREACH PROCEDURES

49A.1 The Contractor shall:

(a) provide SAS with the name and contact information of an employee who shall serve as SAS's point of contact for all security and data breach matters, and shall be available to assist SAS at all times (24 hours per day, 7 days per week) in resolving matters associated with a security or data breach;

(b) notify SAS of any actual, potential, or suspected physical security breach, as soon as practicable, and in any event, immediately after the Contractor becomes aware of the actual, potential, or suspected physical security breach;

(c) notify SAS of any actual, potential, or suspected cyber-security or data breach, as soon as practicable, and in any event, immediately after the Contractor becomes aware of the actual, potential, or suspected cyber-security or data breach.

49A.2 In the event of an actual, potential, or suspected security or data breach, the Contractor shall extend full cooperation and assistance to SAS, and at no cost to SAS:

(a) assist SAS with any investigation into the actual, potential, or suspected security or data breach;

(b) provide SAS with physical access to all the Contractor's Personnel, facilities and infrastructure that are used to perform this Contract;

(c) facilitate interviews with the Contractor's employees;

(d) make available all records, logs, files, data reports, and materials that may be relevant to the investigation of the security or data breach.

49A.3 The Contractor shall, at no cost to SAS, use best endeavours to immediately remedy, according to instructions or direction given by SAS, any actual or suspected security or data breach, or to prevent any potential security or data breach.

49A.4 The Contractor shall not inform any third party of any security or data breach without first obtaining SAS's prior written consent.

49A.5 The Contractor shall track all details from the point of discovery of the security or data breach to its resolution, and provide SAS with hourly updates, in the format stipulated by SAS.

49A.6 Where the actual or potential breach is caused by the Contractor's default, omission, negligence or unlawful act, the Contractor shall reimburse SAS for all reasonable costs incurred by SAS in

responding to and mitigating damages caused by any actual, potential, or suspected security or data breach.

50 ARBITRATION

50.1 a) Any dispute or difference between the Parties arising out of or relating to or in connection with this Contract including any question regarding its existence, validity or termination, shall be resolved either by reference to arbitration or by court proceedings as elected by SAS.

b) SAS may make the election on its own accord by written notice to the Contractor or shall make the election within thirty (30) days of the receipt of the Contractor's written notice which shall:-

i) state the specific dispute or difference to be resolved and the nature of such dispute or difference; and

ii) include a request that SAS makes an election whether the dispute or difference as stated shall be resolved by reference to arbitration or by court proceedings.

c) Should SAS fail to make the election within thirty (30) days of the receipt of the written notice by the Contractor, the dispute or difference shall be resolved by reference to arbitration in Singapore in the English language in accordance with the Arbitration Rules of the Singapore International Arbitration Centre ("SIAC Rules") for the time being in force which rules are deemed to be incorporated by reference into this clause.

d) SAS may elect to refer to arbitration all or any part of the dispute or difference as stated by the Contractor in his written notice.

50.2 Neither Party may commence any action in court before SAS has made the election.

50.3 The commencement of any arbitration proceedings shall in no way affect the continual performance of the obligations of the Contractor under this Contract.

50.4 (a) The arbitral tribunal shall consist of one arbitrator to be agreed upon between the Parties;

(b) Either Party may propose to the other the name or names of one or more persons, one of whom would serve as the arbitrator;

(c) If no agreement is reached within thirty (30) days after receipt by one Party of such a proposal from the other, the arbitrator shall be appointed by SAS;

(d) The Appointing Authority shall be the Chairman of the Singapore International Arbitration Centre.

50.5 Where a dispute or difference is to be resolved by arbitration, the tribunal shall not enter on the reference until after the completion or alleged completion of the Works unless with the written consent of the Parties.

50.6 Any reference to arbitration under this clause shall be a submission to arbitration within the meaning of the Arbitration Act for the time being in force in Singapore.

50.7 The application of Part II of the International Arbitration Act, and the Model Law referred thereto, to this Contract is hereby excluded.

51 INTENTIONALLY LEFT BLANK

52 CORRESPONDENCE

Any notice, request, waiver, consent or approval shall be in writing and shall be deemed to have been duly given or made when it is delivered by hand or by prepaid registered post, to the Party to which it is required or permitted to be given and made at such Party's address specified in the Invitation to Tender.

53 CUMULATIVE REMEDIES

The rights and remedies of the parties under this Contract are cumulative and are in addition and without prejudice to any rights or remedies a Party may have at law or in equity. Further, no exercise by a Party of any one right or remedy under this Contract shall operate so as to hinder or prevent the exercise by it of any other such right or remedy under this Contract, or any other right existing at law or in equity.

54 CLAIMS FOR EXTRA WORK

54.1 SAS shall not be liable for any claims for any extra work performed or to be performed falling outside the scope of this Contract. ("Extra Work") UNLESS all the following conditions are fully complied with:

(a) all claims must be submitted in writing before the performance of any Extra Work, and

(b) in submitting any claim under Sub-Clause (a) above, the Contractor shall include the price of the Extra Work and the detailed scope of the Extra Work, and

(c) SAS agrees in writing for the Extra Work to be carried out and to the payment of the claim before the performance of any Extra Work.

54.2 The Contractor agrees that it is only entitled to claim for any Extra Work provided all the conditions in Clause 54.1 are fully complied with. The Contractor further agrees that it shall not be entitled to additional payments whether under this Contract, restitution, quasi-contract or equitable grounds if all conditions in Clause 54.1 are not fully complied with.

54.3 For the avoidance of doubt, Clause 54 applies to all Extra Work including Extra Work initiated at the request of SAS.

54.4 For Extra Work initiated at the request of SAS, SAS shall reserve the right to waive any or all or any part of the conditions in Clause 54.1 at the sole discretion of SAS.

55 MEDIATION CLAUSE

55.1 Notwithstanding anything in this Contract, in the event of any dispute, claim, question or disagreement arising out of or relating to this Contract, no Party shall proceed to litigation or any other form of dispute resolution UNLESS the Parties have made reasonable efforts to resolve the same through mediation in accordance with the mediation rules of the Singapore Mediation Centre.

55.2 A Party who receives a notice for mediation from the other Party shall consent and participate in the mediation process in accordance with Clause 55.1.

55.3 Failure to comply with Clause 55.1 or 55.2 shall be deemed to be a breach of contract.

56 CONTRACTS (RIGHTS OF THIRD PARTIES)

This Contract does not create any right under the Contracts (Rights of Third Parties) Act, which is enforceable by any person who is not a party to it.

57 INTENTIONALLY LEFT BLANK

58 COEXISTENCE STRATEGY

58.1 In the event that SAS appoints more than one Contractor, whether in this tender or subsequent tenders, the Contractors are to cooperate with each other to ensure that the service levels and requirements of the System as stated in the Requirement Specifications are met. If necessary, the operations management procedures will have to be refined by both Contractors to accommodate each other's Systems.

58.2 The Contractor is also required to work with other SAS appointed Contractors for the IT Infrastructure in the development of the application software and also in the maintenance and support of the System. If necessary, the operations management procedures will have to be refined by both Contractors to accommodate each other's System.

58.3 The Contractor shall if necessary meet on a regular basis with SAS and other Contractors to discuss operational issues and other problems that may be encountered in the provision of the System and the services. The relevant technical officers involved in the provision of the services shall attend the meetings.

59 OWNERSHIP OF DOCUMENTATION AND DISPOSAL OF DOCUMENTATION UPON TERMINATION OF CONTRACT OR COMPLETION OF CONTRACT

59.1 SAS shall own all the documentation generated for the purpose of this Contract.

59.2 The Contractor, his employees, agents and/or Sub-Contractors shall within seven (7) days upon the termination of this Contract or upon the completion of this Contract:

(a) return to SAS's Representative all property, documents, papers and copies of thereof
   i. belonging to SAS,
   ii. received from SAS for the purpose of this Contract; or
   iii. produced in the course of the Contract

which may be in their possession or under their control; and

(b) securely destroy and erase all softcopies of documentation that exist in hard disks, removable storage media and other storage media or facility whatsoever.

59.3 Upon completion of the obligation under Clause 59.2, the Contractor, his employees, agents and/or Sub-Contractor shall sign the Declaration provided by SAS.

60 SET-OFF

Whenever under this Contract any sum of money (including liquidated damages and any other damages) shall be recoverable from or payable by the Contractor, the same may be deducted from any sum then due or which at any time thereafter may become due to the Contractor under this Contract or any other agreement with SAS.

61 ENTIRE AND WHOLE AGREEMENT

61.1 This Contract contains the entire and whole agreement between the Parties and supersedes all prior written or oral commitments, representations, arrangements, understandings or agreements between them.

61.2 Each Party warrants to the other that it has not entered into this Contract on the basis of any prior written or oral commitments, representations, arrangements, understandings or agreements between them.

IN WITNESS WHEREOF the Parties hereto have hereunto set their respective hands the day and year first above written.

SIGNED BY)
DIRECTOR, CORPORATE)
PLANNING & SERVICES)
for and on behalf of)
SINGAPORE ARTS SCHOOL LTD) _____

in the presence of:)
DEPUTY DIRECTOR)
FINANCE & SERVICES) _____

SIGNED BY
(Contractor's Authorised Representative)
for and on behalf of [Contractor Name]
[Name / Designation]) _____
)

in the presence of:)
)
_____) _____
[Name / Designation])

APPENDIX 1: PAYMENT TERMS

Reference: Clause 4 of Conditions of Contract

Payment shall be made by within thirty (30) days of receipt of invoice and anyother documents required by the School from the Contractor for payment purposes.

The CONTRACT PRICE shall be paid as follows:

Phase 1 For System implementation Thirty (30) days upon date of acceptance ofthe Contractor's implementation plan. Thirty (30) days upon completion of HR module under Phase 1 implementation. Thirty (30) days upon completion of Payroll module under Phase 1 implementation. Thirty (30) days upon completion of Finance and Procurement modules under Phase 1 implementation.	% of Contract Sum of One-time Setup/ Implementation Cost: 10% 40% 10% 40%
Phase 2 For System implementation Thirty (30) days upon completion of Planning and Budgeting module under Phase 2 implementation.	 100%
Phase 1 Software Warranty Period (12 months) Upon successful delivery of Services, the invoice may be issued at the end of the month for the Services rendered in the preceding month.	Price stated in the Contractor's Tender Offer for monthly maintenance.
For implementation of Optional Items, the payment milestone as follows: Thirty (30) days upon award. Thirty (30) days upon successful implementation.	% of Tender Price for Optional Items: 50% 50%
For usage of software (ERP and payroll) on subscription basis for each contractualyear.	Price stated in the Contractor's Tender Offer for yearly subscription.

APPENDIX 2: INTENTIONALLY LEFT BLANK

APPENDIX 3: CONFLICT OF INTEREST DECLARATION FORM

CONFLICT OF INTEREST DECLARATION FORM

(for Vendor - includes Supplier, Consultant, Service Provider, and any third-party company)*

The Conflict-of-Interest Declaration Form for Vendor* is to facilitate communication between you and SOTA. Declarations submitted to Singapore Arts School Limited (SAS) to inform SAS that you understand that you are required to declare to any SAS staff member if there is any potential situation or actual conflict for the awarded job, your official job duties & responsibilities involved. Vendor who makes a false declaration will face legal action proceedings may be liable to compensate SAS for any damages caused, and SAS reserve the rights to terminate the contract with the vendor with immediate effect.

Please read and complete this form with reference to the Conflict-of-Interest Declaration for Vendor.

Declaration

1. I,_____[name]_____, _____[designation]_____ , from _____ [Vendor company name] _____ hereby confirm that I have read and understood SAS conflict of interest and that I will make full disclosure of interests, relationships and/or any financial benefits that could potentially result in a conflict of interest. And I will make full disclosure to any SAS staff member when a potential or actual conflict of interest situation arises immediately.

2. I am not affiliated/ affiliated** (circle accordingly) to a vendor, supplier, or any other party providing or bidding for the provision of goods or services or have a direct or indirect interest in any business transaction(s), agreement, or investment with SAS.

3. I do not have/ have (circle accordingly) business dealing(s) or transaction(s) or directorship/ partnership or hold shares/securities/other interests with the vendor, supplier or any other party involve during SAS's procuring process which could result in a benefit to me.

4. Other types of conflicts not listed above, please declare below (strike-off if nothing to declare):
   _____
   _____
   _____
   _____

5. I acknowledge that my official duties require me to have access to documents or data relating to the procurement, and that in carrying out my duties I may be able to influence the procurement process.

6. I understand that the details of any conflict of interest I may have (whether actual, potential, or perceived, and any steps taken to mitigate this conflict) may be recorded within a conflicts assessment and that my interests will be kept under review (as required).

7. In carrying out my duties, I am aware that I will have access to confidential documents or data and that unauthorised disclosure of information could damage the integrity of the procurement and that transmission or revelation of such information to unauthorised persons will subject me to legal action.

Confirmation

I hereby confirm that the disclosure made above is accurate, complete, and correct. I agree that if I become aware of any information that might indicate that any such disclosure is outdated, inaccurate or that I have not complied with the Conflict-Of-Interest statement above, I will notify any of SAS Staff member immediately by making a new declaration.

_____
Signature
Name and Company :
Date of Declaration:

******Affiliated*** *refers to any of the following: Spouse, domestic partner, child, mother, father, brother or sister or close associates; any corporation, business or non-profit organisation of which you are serving as temporary, part-time, contract or permanent staff, officer, board member and/or partner; any corporation, business or organisation in which you have any direct or indirect interest; or any trust or other estate, in which you have a substantial interest in or in which you serve as a trustee or in a similar capacity.*

APPENDIX 4: UNDERTAKING TO SAFEGUARD OFFICIAL INFORMATION

NON-DISCLOSURE AGREEMENT TO SAFEGUARD OFFICIAL INFORMATION

1. My attention has been drawn to the *Official Secrets Act* (Chapter 213) and in particular to Section 5 thereof which related to the safeguarding of official information.

2. I understand and agree that all official information acquired by me in the course of my work in connection with this project is of a strictly secret and confidential nature, and is not to be published or communicated by me to any other person in any form whatsoever except in the course of my official duties on a strictly "need-to-know" basis.

3. I shall ensure that any other person who is authorised by me to have access to any official information shall similarly sign an undertaking to safeguard official information.

4. I undertake to return any document received from SAS, any other copies made or reproduced from such document or part thereof whenever required by SAS.

5. I further understand and agree that any breach or neglect of this undertaking may render me liable to prosecution under the Official Secrets Act.

_____	_____	
Signature	Full Name in BLOCKS (Authorised Representative)	
_____	_____	_____
Designation	Company Name and Company Stamp	Date
_____	_____	
Signature of Witness	Full Name in BLOCKS	
_____		_____
Address		Date

APPENDIX 5: DECLARATION

DECLARATION

1. My attention has been drawn to the *Official Secrets Act* (Chapter 213) and in particular to Section 5 there of which relates to the safeguarding of official information.

2. I have understand and agree that SAS shall own all documentation generated for this Maintenance Contract. The Supplier must return all property, documents, and copies received from SAS within seven days of contract termination or completion. They must securely destroy and erase all softcopies of documentation in their possession.

3. I further understand and agree that any breach or neglect of my obligation under Clause 59 of ERP Conditions of Contract and the above item 2- may render me liable to prosecution under the Official Secrets Act and civil proceedings.

_____	_____	
Signature	Full Name in BLOCKS (Authorised Representative)	
_____	_____	_____
Designation	Company Name and Company Stamp	Date
_____	_____	
Signature of Witness	Full Name in BLOCKS	
_____		_____
Address		Date

SCHOOL OF THE ARTS SINGAPORE

Annex B :
SELECTION CRITERIA

SELECTION CRITERIA

1.1 Singapore Arts School Limited (the Company) is seeking to enter into a contractual agreement with a Contractor who best addresses the Company's objective to obtain the best value from the Contractor's services. In line with this principle, the Company will adopt the following criteria for the selection of a Contractor.

Tendering for the Provision of Enterprise Resource Planning (ERP) System Development and Maintenance Services shall be evaluated based on the following criteria:

✓ a) Submission of Tender on/before the Tender Closing Date and Time

✓ b) Mandatory attendance at both Online Tender Briefings

✓c) Tenderer compliance to registration with Government Supplier Registration (GSR) Head Registration and Financial Grade:

i) **GSR Head** **:** EPU/CMP/10 - Computer Hardware and software Products, Software Development and Maintenance of System, Equipment & Computers

ii) **Financial Grade** **:** **S7 and above**
Tendering Capacity up to S$5,000,000 and above

d) Compliance with list of required Tender Documents submission (please refer to Schedule 1 - Instruction to Tenderers, Point 1)

✓e) Completeness of Schedule 3 - Schedule Of Price

✓f) Submission of Supporting Documents (as set out in Annex C, Point 4.1)

- Proof of GSR at least meeting Financial Grade S7
- Proof of certified partner of the proposed ERP system
- Detailed proposal
- Schedule 3-Schedule Of Price, Annex D-Combined Functional Requirements (in excel), Annex E-Project Schedule and Annex F-Proposed Project Team and Track Record

✓ g) Documentary proof that the Primary Data Centre is located in Singapore

h) HR module to complete by 30 June 2026

i) Financial capabilities of the Tenderer

j) Record of current contracts/ projects

k) Other relevant certifications

1.2 The Company is not bound to award to the lowest quotation.

Note: Criteria marked with ✓are critical.

SCHOOL OF THE ARTS SINGAPORE

Annex C :
GENERAL REQUIREMENT SPECIFICATIONS

1. INTRODUCTION

1.1. Overview

1.1.1. Tenderers are invited to submit a complete proposal for the design, development, delivery, installation, testing, commissioning and maintenance ofthe integrated Software-as-a-Service (SaaS) solution for Finance, Human Resource and Procurement functions (the "System") for Singapore Arts School Ltd (the "School"). There is only one legal entity located in Singapore for the use of the SaaS.

1.1.2. The Tenderer shall propose a SaaS solution that meets the requirements of the System. The Tenderer shall configure the SaaS to meet ERP Conditions of Contract (Annex A), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G) and shall be applicable to the SaaS and its related Works such as, but not limited to configurations and installations. Functionalities provided by the SaaS or configured in the SaaS shall be developed accordance to ERP Conditions of Contract (Annex A), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G)

1.2. Background

1.2.1. Due to evolving organisational needs, the School is undergoing transformation to improve its corporate processes and replace its legacy corporate systems.

1.2.2. This requires an integrated SaaS system to streamline and enhance the efficiency of the financial, human resource, and procurement operations, with the objective of building a future-ready school.

1.3. Key Objectives

1.3.1. Improve operational and process efficiency

The integrated SaaS system will leverage existing cloud services to transform corporate services and achieve operational efficiency through an integrated SaaS solution. The System will maintain seamless data integration across Human Resource, Finance and Procurement functions, facilitating a single source of truth and data accuracy throughout all business processes. It will benchmark HR, Finance and Procurement processes to the prevailing best practices to improve process efficiency. The System will also minimise manual processes during data processing to ensure timely financial closing and accurate reportingof financial performance. To position the School for the future, the System will also be AI-ready.

1.3.2. Provide centralised visibility

The integrated SaaS system will allow automatic retrieval of, and real-time access to data by management and business units. This will provide real-time data and analytics, enabling managers to make informed decisions about resource allocation and managing shortages or surpluses.

1.3.3. **Ensure scalability and flexibility**

The integrated SaaS system will be scalable and flexible enough to handle growth, changes in resource demand, or shifts in organisational structure and strategy. It will also provide for the necessary interfaces with external systems for data integration and consolidation.

1.3.4. **Support compliance and risk management**

The integrated SaaS system will leverage system functionalities to perform control checks so as to ensure compliance to applicable policies and processes,and relevant laws and regulations.

1.3.5. **Cost efficient delivery of HR, Finance and Procurement services**

The integrated SaaS system will deliver HR, Finance and Procurement services in a cost-efficient manner to achieve expected cost savings from adopting SaaS.

2. SCOPE OF TENDER

2.1. General

2.1.1. The Tenderer shall submit the proposal in accordance with ERP Conditions of Contract (Annex A), General Requirement Specifications (Annex C), Combined Functional Requirements (Annex D), Technical Requirement Specifications (Annex G), as stipulated in this Tender.

2.1.2. The Tenderer shall propose and quote separately for the Base and Optional Services and items. The School reserves the right to award any Optional Services or Items at its sole discretion at time during the Contract period. The scope of tender shall be as follows:

Base Services

(a) Supply, delivery, design, develop, install, test, integrate and migrate existing data and commission a complete suite of the System within Implementation Period of **WITHIN EIGHT (8) months** from the contract start date for Phase 1 and **SIX (6) months** for Phase 2, unless otherwise specified or agreed by the School in writing.

(b) Provide for necessary interfaces between the System and other systems within and outside the School (the “External Systems”) for data integration and consolidation.

(c) Provision of software license for SaaS system for a period of **THREE (3) years**.

(d) Provide THIRTY (30) calendar days Performance Guarantee Period (PGP).

Optional Services and Items

The School may, at its own discretion, require the Contractor to provide the following optional services and items:

(e) Provide the Application Management & Support (AMS) for the System for a period of **ONE (1) year**, to be exercised by the School.

2.1.3. Any other items necessary for the working of the System not clearly indicated by the Tenderer shall be deemed to be an intrinsic part of the System and their cost, if any, shall be included as part of the System.

2.1.4. The System shall be designed to support the following indicative user base of the School:

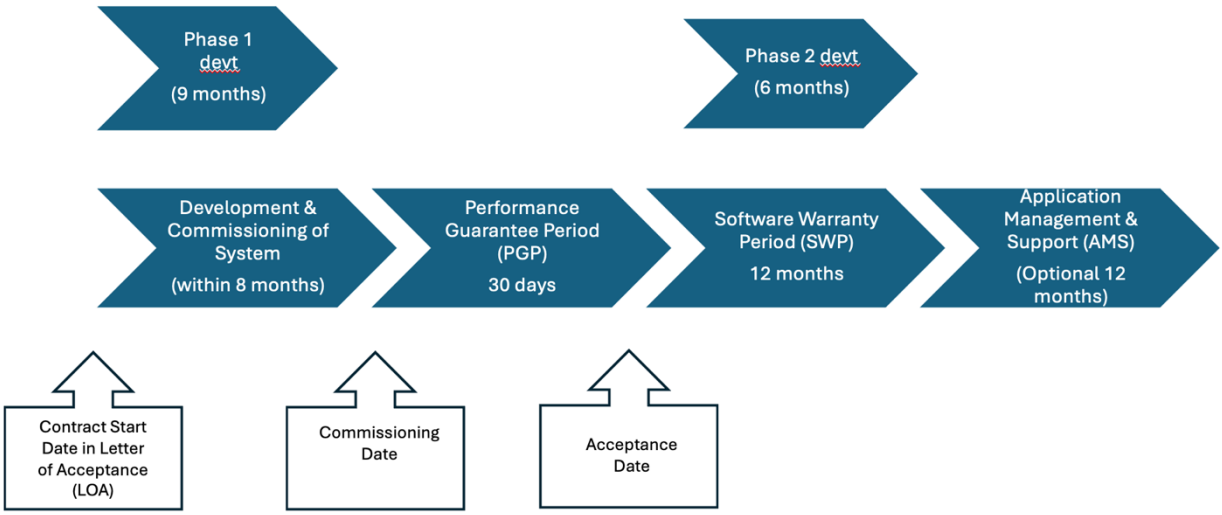
(a) Total employee population: Approximately 280 users.

(b) Core Corporate Services function users:
(i) Finance: Approximately 7 officers;
(ii) Human Resource: Approximately 6 officers; and
(iii) Procurement: Approximately 5 officers.

2.1.5. The timeline for this Contract is illustrated as follows and time shall be of essence for the Contractor in meeting the said timeline, unless otherwisespecified or agreed by the School in writing:

Figure 1: Timeline

Proposed System



3. FUNCTIONAL REQUIREMENTS

3.1. Overview

3.1.1. The following depicts the planned modules for Phase I and II of the development phase. Unless otherwise specified by the School in writing, these modules/functions shall be implemented according to their respective phases asoutlined below:

Module	Phase I (Essential Modules/Functions)	Phase II (Secondary Modules/Functions)
Finance	a) Budgetary Control b) Fixed Asset Management c) Account Receivables d) Staff Claims e) Account Payables f) Cash Management g) General Ledger h) Projects	a) Budgeting & Planning
Human Resource	a) Organisation Management b) Worker Profile c) Compensation d) Leave Administration e) Employee Benefits Administration f) Payroll g) Employee Self-service	a) Recruitment b) Performance Management c) Workforce & Succession Planning d) Attendance/Time Administration
Procurement	a) Approval of Requirements b) Small Value Purchase c) Sourcing d) Evaluation and Approval Contracting e) Contract Management f) Revenue Contracting	
General System Features (common across all functions)	a) User Account Management b) Workflow Management c) Document Management d) Basic Reporting e) Integration Capabilities f) Mobile Accessibility g) Collaboration Features h) System Administration	a) Data Analytics & Automation Tools eg. A.I. Agents

3.2. Detailed Functional Requirements

Functional Area	Detailed Specifications
Finance Functional Requirements	Please refer to Annex D - Combined Functional Requirements, tabs FIN 1.0 to FIN 8.0
Human Resource Functional Requirements	Please refer to Annex D - Combined Functional Requirements, tabs HR 1.0 to HR 7.0
IT Functional Requirements	Please refer to Annex D - Combined Functional Requirements, tabs IT 1.0 to IT 2.0
Procurement Functional Requirements	Please refer to Annex D - Combined Functional Requirements, tabs PRO 1.0 to PRO 5.0

4 Documents to submit

4.1 The following are mandatory documents to submit in the tender:

4.1.1 Proof of GSR at least meeting Financial Grade S7,
4.1.2 Proof of certified partner of the proposed ERP system,
4.1.3 Detailed proposal; and
4.1.4 Schedule 3, Annexes D, E and F

SCHOOL OF THE ARTS SINGAPORE

Annex D :
COMBINED FUNCTIONAL REQUIREMENTS

SCHOOL OF THE ARTS SINGAPORE

Annex D1: Procurement Functional Requirements

Instructions to Tenderers

1.1 Please state clearly the compliance to all requirements listed in this Annex. For each requirement, the Tenderer shall select the appropriate compliance response from the dropdown menu. Definitions of each compliance reponse are provided in the table under "Compliance Definition" below.

1.2 Any statements in this Annex pertaining to other parts of the tender will be disregarded by the School. Only the responses provided in the table under "Compliance Definition" will be accepted. Where there is a failure to indicate a proper compliance response, it shall be deemed that the Tenderer has indicated "C" and the offer shall be evaluated accordingly.

1.3 The following format provided in this Annex shall be used for submission.

1.4 Please provide explanatory notes under "Tenderer Remarks" whenever possible.

Compliance Definition

Statement of Compliance	Definition
'Compliance' or 'C'	When the System or Service meets all Specifications / requirements without any customization / modification to the standard software (i.e. via configuration). The Tenderer shall NOT add any explanatory notes against the clause that vary the meaning of full compliance to the clause and such notes provided (if any) shall be ignored.
Partial Compliance' or 'PC'	When the System or Service is able to comply with the Specifications / requirements by means of customization / modification to the standard software (i.e. not via configuration) or by adding third party software. The Tenderer must provide condensed but complete information on the customization involved or the third party software proposed, including any integration efforts required and additional charges involved.
'Non-Compliance' or 'NC'	When the System or Service does not comply with the Specifications / requirements.

Document Information

File Name: Annex D1 - Procurement Functional Requirements

			Statement of Compliance			
L1#	**L1**	**Total no. of Requirements**	**C**	**PC**	**NC**	***Tenderer Completion Status***
PRO 1.0	Requisition	55	0	0	0	*0%*
PRO 2.0	Sourcing	28	0	0	0	*0%*
PRO 3.0	Evaluation	24	0	0	0	*0%*
PRO 4.0	Approval	14	0	0	0	*0%*
PRO 5.0	Contract and Vendor Management	53	0	0	0	*0%*
		174	**0**	**0**	**0**	

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.001	The system should allow to add approver/requestor comments and allow push notificatior on approval status or request for additional information, and hold rejected PR.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.002	The system should allow to provide prompts to guide users on actions for approving PRs.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.003	The system should allow to provide a workflow and set up rule-based approval matrix and route PRs to one or more approvers in accordance with business rules, e.g., financial value, cost center, category, covering roles for QAA/AO/Requestor/BO/GRO etc. The system should then allow to approve PRs via the workflow as per appropriate delegation of financial and functional authority.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.004	The system should allow to approve PRs prior to issuing PO and link to contract to manage commitment against the contract.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.005	The system should allow department to only select PRs related to their own department from a dropdown menu.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.006	The system should allow to users to link PR against supplier contracts (framework agreements and period contracts) with no amendments/editing rights.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.007	The system should be able to identify outstanding PRs and use workflow to manage investigation (e.g ability to route to relevant approvers should PRs be outstanding for X days / route to requestor for additional information / trigger reminder to approvers after X days).	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.008	The system should allow to attach documents/quotes electronically to PRs.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.009	The system should allow PRs to be sequentially pre-numbered.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.010	The system should allow to restrict users from approving their own PRs. Users can have access to initiate & approve PRs, but they cannot approve their own PRs.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.011	The system should allow to report on the status of PRs (where are they sitting if not yet approved) and automatically discard PR upon X months.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.012	The system should allow to notify approver if PR is not yet approved and re-route it to the next approver (escalation).	Optional		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.013	The system should allow to recognize line-by-line value of a PR vs total value of PR, to ensure compliance with maximum $ approvals.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.014	The system should have the ability to perform budgetary checks and expenditure control at various stages eg. PR, PO etc to ensure PR/PO cannot be generated when budget is exceeded, and automatically prompt a notification to provide notice. This shall apply when any provisional or additional PR is submitted (e.g submit additional PR when APV exceed EPV).	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.015	The system should allow to support different requisition forms based on type of purchase.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.016	The system should allow to assign the master source of delegations of authority.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.017	The system should allow to interface with budget and planning system.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.018	The system should allow to configure PR form, and support document attachments/quote electronically to the PR.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.019	The system should allow to select vendors from an existing vendor list during the creation of requisitions.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.020	The system should allow to notify a buyer and requisitioner when a PR has been approved so that it can be put on a PO.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.021	The system should allow to support workflow process, allowing to view, create, submit and approve PR with mobile capabilities for all PRs.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.022	The system should allow to transfer or delegate and push notification (for X days) the approval authority for requsitions, permanently or temporary, in cases where approver is away for long period of time or change in approver.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.023	The system shall be configured to make certain accounting fields non-editable and be automatically populated on the basis of another field	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.024	The system shall be enabled to allow users to select pre-defined shipping location or add their own adhoc address	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.025	The system shall trigger a PR approval warning notification to corresponding approvers after **x business days**of inactivity	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.026	The system shall trigger a PR approval escalation notification after **x days of inactivity** to the supervisor of the current approver and added in the approval chain.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.027	The system should allow to raise different types of PRs (e.g SLA) and configure unique approval workflows for them	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.028	The system should be able to create Sourcing Event from PR	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.029	The system should be able to link cost centre/project code/ GL account	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.030	The system should have the ability to support different sourcing methods such as open quotation, tender, limited quotation, tender, period contract, framework agreement etc.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.031	The system should be able to maintain user log, system log and error log	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.032	The system should allow BO to input justification for limited procurement during PR endorsement and route to QAA for approval, prior to PR approval by AO	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.033	The system should allow to carry out budget check for first year only in the scenario of raising multi-year PR	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.034	The system should allow users to cancel / amend PR in the event that the PR has not been processed for approval by AO/QAA and then route to AO/QAA for approval.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.035	The system should allow authorised users with access to reject a PR stating rejection reasons.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.036	The system should allow users to support certain types of amendments / cancel / input additional information post PR approval, and then re-route for AO/QAA approval.	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.037	The system should allow for multiple PRs to be linked to a single sourcing event	Mandatory		
PRO 1.0	Requisition	PRO 1.1	Approval of Requirements	REQ.038	The system should allow to duplicate and create new PRs from past sourcing events.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.039	The system should allow to raise PR via catalogue from a list of items established.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.040	The system should allow to purchase from a punch-out catalog by navigating to the Supplier's catalog website.	Optional		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.041	The system should have the ability to connect to supplier website, to view and order from supplier catalogue and the order will be transferred to the system to complete the purchase.	Optional		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.042	The system should allow supplier to self manage their products or services i.e. upload, manage, delete, edit, publish, issue invoice, deliver orders and shipment in the system	Optional		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.043	The system should allow the ability to sort items in e-catalogue by relevance or by prices or by distance or by top sales or by latest	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.044	The system should allow the ability to choose items from e-catalogue and compare base on prices, rating, geo-location and supplier name	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.045	The system should the ability for users to select and search items from a e-catalog and add them to a shopping cart.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.046	The system should allow to link contracts / agreements to catalogue.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.047	The system should allow users to view, edit, or remove items from the cart before submitting as a PR.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.048	The system should prompt users to enter all required Purchase Requisition (PR) details, including supplier, budget code, delivery date, and other relevant information. Otherwise, the system should issue error messages and restrict completion of a PR if they are not complete, e.g., all mandatory fields are not populated	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.049	The system should retrieve and display the user's saved billing, payment terms and shipping information (e.g., address) when they reach the checkout page.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.050	The system should allow users to edit their shipping information directly on the catalogue checkout page.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.051	The system should provide a final summary of the confirmed billing and shipping details (without GST) for the user to review before placing the order.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.052	The system should automatically create a budget reservation when a Purchase Requisition (PR) is approved, reserving the corresponding funds for future expenditure.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.053	The system should trigger a warning message or prevent transactions that exceed the available budget	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.054	The system should validate the selected budget code and ensure the expenditure aligns with the predefined categories or limits.	Mandatory		
PRO 1.0	Requisition	PRO 1.2	Catalogue Buy	REQ.055	The system should provide detailed expenditure tracking, displaying actuals, reserved (approved PR) amounts, commitment (approved PO) amounts and remaining available budget by cost center.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 2.0	Sourcing	PRO 2.4	Sourcing (RFQ)	SOU.001	The system should allow to select eligible suppliers (e.g RFQ) from the approved vendor list to request for quotation.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.002	The system should allow the upload/update of sourcing documents. Information in the sourcing document includes but not limited to: a. Requirements Specifications b. Instructions to tenderers c. Conditions of Contract d. Key Performance Indicators, Service Level Agreements, Supplier Performance Metrics e. Cover Letter f. Price Schedule / PWM / Annexes & Appendixes g. Evaluation Criteria.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.003	The system should allow the Buyer to configure the sourcing document template.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.004	The system should issue automatic acknowledgement to the suppliers on receipt of completed quotations / tenders or on prompting. The system should also cater for ability for vendor to reject to quote.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.005	The system should have a file attachment function for supporting documents to be added.	Mandatory		
PRO 2.0	Sourcing	PRO 2.3	Sourcing (ITT/FA)	SOU.006	The system should allow to provide a workflow and set up rule-based approval matrix and route sourcing event to one or more approvers in accordance with business rules, e.g financial value. The system should then allow to approve tender document via the workflow as per appropriate delegation of financial and functional authority.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3	Sourcing (ITQ) Sourcing (ITT)	SOU.007	The system should be able to perform issue of corrigendum via system at least X days before ITQ/ITT closes.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.008	The system should be able to perform return of clarifications and allow vendors to raise questions in the system, consolidate the questions, and allow BO / Requestor to put up a general response to all vendors and collect tender responses via system.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.009	The system should trigger notifications to inform Requestor and Budget Owner on the approval of specifications and publish of event.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.010	The system should allow to select suppliers and trigger notifications to invite suppliers to quote / tender under limited ITQ / ITT & RFQ.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.011	The system should allow to trigger notifications to suppliers upon successful submission of quotes/tenders	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.012	The system should allow to generate invitation to quote (ITQ), invitation to tender (ITT) or request for quotation (RFQ), issue the ITQ/ITT/RFQ) and notification of a site-show/briefing to suppliers via an online supplier portal, and record the interactions (e.g including Q&A) with suppliers.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.013	The system should publish the approved sourcing documents on the supplier portal.	Mandatory		
PRO 2.0	Sourcing	PRO 2.3. PRO 2.4	Sourcing (ITT) Sourcing (RFQ)	SOU.014	The system should allow to open the quotes after the ITQ/RFQ submission deadline, i.e., support sealed bid.	Mandatory		
PRO 2.0	Sourcing	PRO 2.3. PRO 2.4	Sourcing (ITT) Sourcing (RFQ)	SOU.015	The system should allow to convert the PR into a standard sourcing event (open/limited sourcing event) and allow Buyer to edit.	Mandatory		
PRO 2.0	Sourcing	SOU 2.3 SOU 2.4	Sourcing (ITT/FA) Sourcing (RFQ)	SOU.016	The system should allow to facilitate tender approval hierarchies.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3	Sourcing (ITQ) Sourcing (ITT)	SOU.017	The system should allow authorised users to effect online or electronic communications to shortlisted or approved vendors for arrangement of site-shows/tender briefing or as needed.	Mandatory		
PRO 2.0	Sourcing	PRO 2.3. PRO 2.4	Sourcing (ITT/FA) Sourcing (RFQ)	SOU.018	The system should allow flexibility for vendors to perform amendments/additions after the submission of quotes and before closing tender and have the capability to leave audit trail record of time stamp on resubmitted information.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ) Sourcing (ITT) Sourcing (RFQ)	SOU.019	The system should restrict from adding users from other departments during the sourcing team setup	Optional		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.020	The system should be able to send reminders to vendors when due date is approaching, to confirm nonfirm non-receipt of quotation/tender and record the time stamp upon reminder sent out.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.021	The system must allow administrators to establish both predefined and configurable evaluation criteria for assessing and evaluating tenders before invitation to quote/tender.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.022	The system should allow authorised users to invite interested suppliers to the tender briefing through the system.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.023	The system should allow Buyer to set a submission deadline for each sourcing event, in which prevent suppliers from submitting or editing submissions after the deadline.	Mandatory		
PRO 2.0	Sourcing	PRO 2.3	Sourcing (ITT/FA)	SOU.024	The system should allow for establishment of evaluation criteria in the system	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.025	The system should allow to duplicate and create new sourcing events from past sourcing events.	Mandatory		
PRO 2.0	Sourcing	PRO 2.2 PRO 2.3 PRO 2.4	Sourcing (ITQ/FA) Sourcing (ITT/FA) Sourcing (RFQ)	SOU.026	The system should allow to assign and grant access to different users e.g QEP to sourcing event.	Mandatory		
PRO 2.0	Sourcing	PRO 2.4	Sourcing (RFQ)	SOU.027	The system should allow auto-selection of all suppliers pre-awarded in the framework agreement prior to the sourcing event based on the specific buy category	Mandatory		
PRO 2.0	Sourcing	PRO 2.4	Sourcing (RFQ)	SOU.028	The system should allow the selection / removal of suppliers from pre-selected list of awarded Suppliers within framework agreements before calling limited RFQ	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.001	The system should compute the approved procurement value based on the total amount of the selected quotation and any associated costs (e.g., taxes, delivery fees) for the recommended award	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.002	The system should be able to consolidate and compare quotations/tenders response side-by-side before routing for award approval.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.003	The system should be able to generate a summary of evaluation scores for all tender/quotation responses.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.004	The system should allow to provide a workflow and set up rule-based approval matrix and route evaluation to one or more approvers in accordance with business rules, e.g., financial value (e.g ITQ - <S$100K, ITT > S$100K)	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.005	The system should allow to automatically validate each submission against critical criteria (e.g., supplier qualifications, compliance with tender requirements, certification) as part of the shortlist and qualifying requirements.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.006	The system must automatically rank all tender submissions based on the scores entered for each evaluation criteria	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.007	The system must automatically identify the tender submission that provides the best value for money, based on the evaluated scores and criteria (e.g., price, quality, delivery terms).	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.008	The system should allow access to tender bids and tenderers' responses after the sourcing closes on procurement platform, where users can access directly via platform or download to their locals	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.009	The system should allow to have structured sections for critical evaluation criteria questions, and compile responses to critical evaluation criteria questions	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.010	The system should allow to store tenderers' bids in the platform and allow Procurement officer and Evaluation Committee member to retrieve all submitted quotations/tenders directly	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.011	The system should be able to auto-generate the evaluation form with the respective approving authority according to value and procuring type (eg LQ/LT etc.)	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.012	The system should allow to have a dashboard that facilitates the price reasonableness check against historical data of pricing,	Mandatory		
PRO 3.0	Evaluation	PRO 3.1	3.1 Evaluation (ITQ / FA / RFQ)	EVL.013	The system should allow to perform a price reasonableness check during the evaluation stage	Mandatory		
PRO 3.0	Evaluation	PRO 3.1	3.1 Evaluation (ITQ / FA / RFQ)	EVL.014	The system should have the ability to update or modify TEC (Tender Evaluation Committee) members and evaluation metrics/weightage before and after the event is published, the changes of evaluation metrics/weightage shall undergo approval via corrigendum if they are in place after event published	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.015	The system should allow requestors & QEP (TEC) to receive timely notifications if any items are pending actions. It includes the situation is pending QEP (TEC) evaluation and/or approval, to remind QEP (TEC) to award a selected vendor after the closing date.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.016	The system should allow QEP (TEC) to supplement and complete the scoring for qualitative criteria	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.017	The system should allow to automate the scoring of all quantitative criteria	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.018	The system should be able to bypass the price reasonableness check during evaluation if there are three or more valid bids for a particular item and route to a separate approval matrix.	Mandatory		
PRO 3.0	Evaluation	PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.019	The system should enable individual QEP (Tender Evaluation Committee (TEC)) members to submit evaluation scores or allow the Buyer to submit combined QEP (TEC) scores.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.020	The system should allow for users to declare COI prior to opening the quotes/tender and after opening the quotes/tender (upon reveal of vendor namelist).	Mandatory		
PRO 3.0	Evaluation	PRO 3.2	3.2 Evaluation (ITT / FA)	EVL.021	The system should allow for shortlist of submissions that meet the critical criteria	Mandatory		
PRO 3.0	Evaluation	PRO 3.1	3.1 Evaluation (ITQ / FA / RFQ)	EVL.022	The system should allow for routing of 'No Award' recommendation approval to QAA, in the event no reasonable quotes/tenders have been received based on price.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.023	The system should allow to store documentation and pricing details received from suppliers via the online supplier portal and assess and compare the suppliers based on a dynamic scoring criterion, including pricing.	Mandatory		
PRO 3.0	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.024	The system should allow user to select the lowest priced quotation meeting all requirements in the event that EPV exceeds APV and after QAA have approved the exception justification	Mandatory		
PRO 3.1	Evaluation	PRO 3.1 PRO 3.2	3.1 Evaluation (ITQ / FA / RFQ) 3.2 Evaluation (ITT / FA)	EVL.025	The system should allow user to select the lowest priced quotation meeting all requirements in the event that APV exceeds EPV by more than 5% AND relevant approvers have approved the exception justification	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.001	The system should automatically compare the Approved Procurement Value (APV) against the Estimated Procurement Value (EPV) upon finalizing procurement details.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.002	The system should trigger an alert when the APV exceeds the EPV by more than 10%.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.003	The system should route the procurement request back to the original requestor for justification when the APV exceeds the EPV by more than 5% (pending policy approval) and route for QEP to input comments and approve before routing to QAA for approval.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.004	The system should route the justification and the updated procurement value to relevant approvers for review after the requestor submits the justification of APV exceeding EPV	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.005	The system should prompt QAA involved in the approval to declare any potential conflicts of interest (COI) before proceeding.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.006	The system should allow to provide a workflow and set up rule-based approval matrix and route approval award to one or more approvers in accordance with business rules, e.g., financial value (ITQ - <100K, ITT >100K) & sourcing approach - open/limited. The system should then allow to approve approval of award via the workflow as per appropriate delegation of financial and functional authority.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.007	The system should have the ability introduce or remove members from the QEP/TEC or QAA/TAA anytime during the tender evaluation stage with requirement of separate Conflict of Interest (COI) declaration for any newly added member and include checking for the segregation of duties and reason for the change.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.008	The system should be able to track comments, queries and replies from QAA/TAA in a central repository	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.009	The system should be able to eliminate the necessity for QAA/TAA to approve no award for Tenders/Quotations with no response	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.010	The system should be able to withdraw the approval of an award while it is pending approval from the Quotation Approval Authority (QAA) or Tender Approving Authority (TAA) for QEP to input additional information.	Mandatory		
PRO 4.0	Approval	PRO 4.1 PRO 4.2	Approval (ITQ/FA/RFQ) Approval (ITT/FA)	APP.011	The system should be able to to alert requesting department (including requestor and budget owner) once award recommendation is approved and initiate the LOA / COC / PO document creation.	Mandatory		
PRO 4.0	Approval	PRO 4.1	Approval (ITQ/FA/RFQ)	APP.012	The system should allow for BO and OP need to endorse and support approval of award before routing to QAA for approval	Mandatory		
PRO 4.0	Approval	PRO 4.1	Approval (ITQ/FA/RFQ)	APP.013	The system should allow for routing to QAA for no award approval and trigger initiation of ITT procedures, should APV exceed 100k	Mandatory		
PRO 4.0	Approval	PRO 4.2	Approval (ITT/FA)	APP.014	The system should allow for QAA to attach proof of approval (email) from external party and approve on behalf of board external party and record the completeness of the procuring process registered in the system.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.001	The system shall default the payment terms, within the PO, from the value defined within the supplier record.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.002	The system shall split a PR document into multiple Purchase Order based on the following attributes: 1. Supplier 2. Shipping Address 3. Contracts 4. Line Item Type (Catalog vs Non-Catalog) 5. Price (lowest quote)	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.003	The system should restrict users from approving their own POs. Users can have access to initiate & approve POs, but they cannot approve their own POs.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.004	The system should allow to create a period contract, create POs to drawdown from the contract, and capture the amount to be exercised in each year.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.005	The system should allow to automatically assign accounting information to PO based on the requisition type/description.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.006	The system should be able to restrict users from purchasing from unapproved vendors. Although the system should allow unapproved vendors at the open tender stage, vendors have to approved in the system before creation of PO.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.007	The system should allow to perform data validation against POs raised against a contract to validate whether the PO is being raised against the correct contract.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.008	The system should allow to roll over open POs and committed amounts from one budget year to another.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.009	The system should allow to bypass the budget check for new item of multi-year PO or subsequent years once a multi-year PO is approved. Once approved, subsequent years PO commitment will be parked in ERP for future years budgeting exercise.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.010	The system should allow to prohibit POs from being raised against a contract that is closed and cannot be overridden by the end user.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.011	The system should allow to receive PO confirmation from vendor.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.012	The system should allow to print department/organizational terms and conditions on POs.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.013	The system should allow for segregation of duties between purchasing and payables functions. There should be segregation of duties between users, where different users have different access rights.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.014	The system should allow to automatically email original and revised PO to supplier on approval or to print hardcopy PO for mailing to supplier.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.015	The system should allow to set a threshold for the budget remaining on the period contract. When the funds remaining falls below this predetermined limit, an email notification will be generated to alert users on the amount remaining in the period contract.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.016	The system should allow to create a multi-year PO.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.017	The system should allow to track and report on open POs, generating reminders for a list of open POs on hold ,and error during creation (e.g missing cost center)	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.018	The system should allow to generate outstanding PR report to show the PRs that have yet to converted to PO.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.019	The system should allow to generate reminders for list of open POs still on hold, error during creation (i.e., missing cost center).	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.020	The system should allow to merge PRs onto a PO and centralize the creation of PO.	Optional		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.021	The system should allow to track the contract validity and expiry to notify the contract owner on the probable contract 3 months prior to expiry case to prevent any lapses to facilitate contractual commitments tracking.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.022	The system should allow to indicate if "Letter of Agreement" or "Schedule of Rates" of tender(s) is a multi-year term contract and specify the amount to be exercised each year.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.023	The system should allow to maintain and update existing contracts and create new contract	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.024	The system should allow to create and modify templates (e.g Service Level Agreement) for contract creation	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.025	The system should allow to cancel and release budget for PR/PO created by user who subsequently leaves SOTA (e.g includes user covering for permanent staff)	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.026	The system should be able to display correct tax code upon PO creation and the ability to change tax code during PO creation	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.027	The system should be able to perform a budget check for the award of Requests for Quotation (RFQs) against the overall budget of the framework agreement (FA). The system should be able to prompt upfront if any of the to be awarded value is reaching the limit.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.028	The system should perform budget check and commit the budget once PO is approved.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.029	The system should allow for the generation of PO and route for QAA approval, upon award recommendation approval	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.030	The system should allow for the approved PO to be sent to the supplier email automatically	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.1	Contracting (PO)	CON.031	The system should allow to the set up of template to send out Letter of Acceptance for different contract types	Mandatory		
PRO 5.0	Contract and Vendor Manager	PRO 5.2	Contracting (SLA)	CON.032	The system should allow to create supplier contract from requisition type "SLA"	Mandatory		
PRO 5.0	Contract and Vendor Manager	PRO 5.2	Contracting (SLA)	CON.033	The system should allow to route draft supplier contract (SLA) to QAA for approval.	Mandatory		
PRO 5.0	Contract and Vendor Manager	PRO 5.2	Contracting (SLA)	CON.034	The system should allow for amendments to contracts to be made by Buyer	Mandatory		
PRO 5.0	Contract and Vendor Manager	PRO 5.2	Contracting (SLA)	CON.035	The system should allow for the flexibility to create different supplier contracts/Service Level Agreement (SLA) template with different clauses.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.3	Establish FA	CON.036	The system should allow to issue Letter of Acceptance to suppliers under framework agreement	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.3	Establish FA	CON.037	The system should allow for the creation of multi-year framework agreements	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.3	Establish FA	CON.038	The system should allow for the ability to set up framework agreements with different rates (e.g fixed rates, flexible rates, SOR etc) and account for partial delivery.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.3	Establish FA	CON.039	The system should allow to select or remove Suppliers from the pre-selected list of awarded Suppliers within framework agreements before calling Limited RFQ	Optional		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.040	The system should allow to generate reports that reflect the amount awarded to vendor(s) within a specified timeframe and include the procuring type. E.g., User would like to view the amount awarded to Vendor A from 1 Jan 2022 to 31 Dec 2022 and its category under ITQ-LQ, ITQ, ITT, ITT-LT etc.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.041	The system should allow to trigger vendor performance evaluation and route to requestor for fill-in. Thereafter, the evaluation should be routed for approval according to the approval matrix.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.042	The system should allow to have always-on audit to leave audit trails of all processes.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.043	The system should allow to generate standard and management reports with real time data and report	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.044	The system should have the ability to view procurement dashboard with complete overview of contract including duration/period selection and export the reports.	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.045	The system should include KPI in contract performance	Mandatory		
PRO 5.0	Contract and Vendor Management	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.046	The system should allow for tracking of contract balance in real time i.e deducting original contract value by payments made to date	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.047	The system should allow Buyer to initiate contract renewal process or exercise option upon VPE review from AO.	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.048	The system should allow to perform budget commitment upon contract renewal, exercise optional scope or activate Schedule of Rates (SOR).	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.049	The system should allow to route to respective QAA for approval on contract renewal, exercising option	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.050	The system should allow user to request to activate Schedule of Rates (SOR) as per contract terms	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.051	The system should allow to check contract for SOR terms	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.052	The system should allow Buyer to issue PO upon activating the SOR.	Mandatory		
PRO 5.0	Contract Renewal and Vendor Performance Evaluation	PRO 5.4	Contract Renewal and Vendor Performance Evaluation	CON.053	The system should allow to perform qualitative evaluation of vendor data, including compliance requirements and vendor qualifications	Mandatory		

SCHOOL OF THE ARTS SINGAPORE

Annex D2: Finance Functional Requirements

Instructions to Tenderers

1.1	Please state clearly the compliance to all requirements listed in this Annex. For each requirement, the Tenderer shall select the appropriate compliance response from the dropdown menu. Definitions of each compliance reponse are provided in the table under "Compliance Definition" below.
1.2	Any statements in this Annex pertaining to other parts of the tender will be disregarded by the School. Only the responses provided in the table under "Compliance Definition" will be accepted. Where there is a failure to indicate a proper compliance response, it shall be deemed that the Tenderer has indicated "C" and the offer shall be evaluated accordingly.
1.3	The following format provided in this Annex shall be used for submission.
1.4	Please provide explanatory notes under "Tenderer Remarks" whenever possible.

Compliance Definition

Statement of Compliance	Definition
'Compliance' or 'C'	When the System or Service meets all Specifications / requirements without any customization / modification to the standard software (i.e. via configuration). The Tenderer shall NOT add any explanatory notes against the clause that vary the meaning of full compliance to the clause and such notes provided (if any) shall be ignored.
Partial Compliance' or 'PC'	When the System or Service is able to comply with the Specifications / requirements by means of customization / modification to the standard software (i.e. not via configuration) or by adding third party software. The Tenderer must provide condensed but complete information on the customization involved or the third party software proposed, including any integration efforts required and additional charges involved.
'Non-Compliance' or 'NC'	When the System or Service does not comply with the Specifications / requirements.

Document Information

File Name:	Annex D2 - Finance Functional Requirements
Disclaimer:	

			Statement of Compliance			
L1#	**L1**	**Total no. of Requirements**	**C**	**PC**	**NC**	***Tenderer Completion Status***
FIN 1.0	Expense Management	55	0	0	0	*0%*
FIN 2.0	Accounts Payable	66	0	0	0	*0%*
FIN 3.0	Assets	66	0	0	0	*0%*
FIN 4.0	Accounts Receivable	63	0	0	0	*0%*
FIN 5.0	General Ledger	75	0	0	0	*0%*
FIN 6.0	Management Reporting	22	0	0	0	*0%*
FIN 7.0	Funds & Grants Management	13	0	0	0	*0%*
FIN 8.0	Budgeting & Planning	68	0	0	0	*0%*
		325	**0**	**0**	**0**	

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.001	The system should be mobile enabled with user friendly and responsive design, such as submissions of staff claims and expense report via web browser or mobile application.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.002	The system should allow claimant to snap photo of invoice/receipt and automatically capture information of invoice/receipt via mobile applications, e.g., mobile phone, tablets.	Optional		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.003	The system should be able to interpret the information in the invoice/receipt accurately and fill in the information to the fields required in the claim template for processing. The image of invoice/receipt captured should be stored in the claim report.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.004	The system should allow claimants to amend the data captured by the system and key in the other required claim data. The system should be able to highlight details captured by system that are amended by claimants.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.005	The system should allow the attachment of supporting documents for claims /expense report submitted via web browser or mobile apps. If the supporting documents are missing system should flag the expense/ claim/claim item	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.006	The system should have a homepage (dashboard) which allows users to navigate to various functions, display of outstanding tasks, display statuses of workflows including notifications and reminders.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.007	The system should have a comprehensive search mechanism that allow users to search for any information of claims to which they have authorized access to. It should enable users to search and retrieve information using fields and ranges of fields such as reference number, claimant name, date, claim type, key words, status, etc. based on users' defined roles access to all transactions including historical records.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.008	The system should track all actions taken and comments made by all the users in the workflows and able to display these as history of the claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.009	The system should provide audit trails for all stages of the claims/expense reports and generate detailed audit reports.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.010	The system should have built-in indicators, notifications, and reminders (via emails and on the homepage) to ensure prompt action.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.011	The system should possess built-in control mechanisms such as validation rules, business rules, filtering rules, selection criteria, prompters, indicators, etc. to effectively guide users to create, submit, verify, approve, and process the claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.012	The system should allow the user to define fields to be mandatory or optional for different types of claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.013	The system should support multi-level, parallel and/or sequential verification/approval routing with built-in approval matrices. The system should allow configuration of approval rules and routing workflows based on conditions and parameters such as amount, document type, dimensions (e.g., cost center, project accounts) etc. and should be able to capture approver comments at each stage of approval.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.014	The system should allow for attachment of multiple supporting documents (e.g., receipts) at each stage of the process.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.015	The system should allow workflow actions such as routing of a claim to the next user for verification, approval/ rejection, audit, request for information, etc. Workflow email notification and notifications at the user homepage at each stage of the workflow is required to facilitate the process.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.016	The system should allow Verifier (BO) to review, verify or reject the claim before routing it to Approver for approval.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.017	The system should allow claimant, verifiers, approvers, processors to view, edit or add information in certain fields of the claim such as updating the charge codes, GST code (processors only), amending the claim amount to a lower amount.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.018	The system should allow the verifier, approver to route the requests for clarifications or supporting documents.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.019	The system should be able to handle various types of claims with configurable variables including but not limited to the following: a) Advertisement Fees b) Temp / Interns / Manpower Cost / Staff Welfare c) Training / Conference / Seminar d) Air Ticket / Hotel / Travel Insurance e) Corp Comm Related Exp f) Student Recruitment Related Expenses g) Professional / Consultation Fees h) Payment on Behalf of Students i) Refreshment & Meeting Exp / Entertainment j) Repair & Maintenance Expense k) Office Stationery l) Contract Services / Outsource Charges m) Books / Periodical / Subscription Fees n) Utilities & Communications o) Masterclasses / Workshops	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.020	The system should allow for user defined details to be provided for staff claims, such as the following: a) Invoice/receipt number b) Department name c) Cost centre code d) Account code e)Payable to f) Amount in SGD g) Description of item h) Purpose for the expense i) Reason for not issuing PO or for vendor to bill direct to SOTA	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.021	The system should allow unique claim details to be provided for each expense type (i.e., claimants are required to fill in different information for different types of expenses in the claim submission).	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.022	The system should have built-in controls and validation capabilities to ensure compliance to SOTA policies and minimize the manual verifications/checks to be performed by verifier and Finance officer.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.023	The system should be able to perform automatic validations/ checks/computations (e.g., checks on rates claimable, allowable/non allowable items, allowable claim/expense period etc.) on claims/expense according to the policies set.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.024	The system should stop the submission of claims/cash advance that have failed the validations checks and Budget Check. The system should also allow configurable warning/error messages or instructions to be displayed whenever the claim/cash advance is stopped from submission.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.025	The system should allow assignment and auto-population of charge codes (such as fund type, budget center, cost center, GL project, research project, GL account etc.) to claims on pre-determined parameters. The system should also minimize manual effort of data entry and verification of charge codes for the claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.026	The system should allow the verifier/approver/processor to change the charge codes by selecting from the drop-down list.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.027	The system should allow budget reservation checks and commitment upon the claim/cash advance submission. The system should allow commitment to be released upon rejection or withdrawal of claim/cash advance.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.028	The system should check the claim/expense amount against the budget balance available in the system based on the charge codes populated/entered in the claim/expense report.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.029	The system should allow auto generation of year end accrual for claims/expense report that have been approved.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.030	The system should stop the claim/cash advance from being submitted for further processing if there is budget shortage.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.031	The system should allow configurable error message/instructions to be triggered and/or displayed when the claim/cash advance is stopped from submission.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.032	The system should allow the claimant to save the claims/cash advance as a draft for subsequent editing/submission.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.033	The system should allow the claimant to 'amend' or 'withdraw' the claims/cash advance before submission.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.034	The system should allow the claimant to 'amend' or 'withdraw' the claim forms/cash advance request form if post-verification or post-approval edits are required and re-submit the claim/cash advances.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.035	The system should allow to generate a unique sequence number for each claim/cash advance request that will follow the claim/cash advance request throughout the whole process.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.036	The system should allow users to refer, duplicate or copy past claims/cash advances submitted by himself/herself for the ease of creation of similar new claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.037	The system should check for duplicate claims, stop the duplicate claim/cash advance from being submitted and display an error message to notify the claimant. Duplicate claims/cash advances are defined, but not limited to, as follow: a) Invoice number b) Invoice amount c) Invoice date d) Start/end date/time of mileage claim e) Start/end date/time of per diem claim	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.038	The system should allow the set-up of verifier, approver and processor matrices based on claim type, charge code at line level and amount, where relevant.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.039	The system should allow the verifiers, approvers, and processor to input comments to ask for more information/supporting documents from claimants,	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.040	The system should enable segregation control such that the verifiers and approvers cannot verify, approve, or process claims submitted by himself/herself. Where the claim is made by the approver, the claim shall be routed to the next higher level of approver.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.041	The system should only require a person to approve once, in the event that the same person holds dual roles of verifier and approver.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.042	The system should allow to deal with exception handlings with appropriate approvals such as claims submitted after the 21 days validity period (pending policy review) etc.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.043	The system should allow to generate reports/dashboard such as the following using query and with little technical expertise. a) Individual expense report (printable format) b) Expense report by expense types c) Expense report by period d) Expense report by claim status e) Expense report by charge code f) Report on claims including transactions processed/unprocessed and turnaround time on the processing of claims, trend analysis and spend expense patterns etc.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.044	The system shall allow users to extract and save the reports in relevant formats such as but not limited to: a) Adobe PDF b) Microsoft Excel/CSV c) Microsoft Word	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.045	The system shall provide an analytics dashboard where the SOTA's Office of Finance will be able to monitor all the submitted claims within SOTA and the audit trail of those claims.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.046	The system shall allow users to analyze the reports/data through drilling down the level of details and “slice-and-dice” the data.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.047	The summary charts and table should be easy to arrange into a reporting dashboard and the layout of the reporting dashboard should be easy to modify.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.048	The system should restrict users from selecting cost centres not relevant to them	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.049	The system should be able to accommodate sufficient checks to ensure that claims are submitted without errors. These rules/policies will be provided by SOTA during the project implementation.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.050	The system should have specific expenses and categories built in for the claim process. For example, team meals should be under the category of staff welfare.	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.051	The system should be able to automate the process of expense submission by staff	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.052	The system should allow to notify staff on status of expense claim e.g successful payment, pending payment	Mandatory		
FIN 1.0	Expense Management	FIN 1.1	Staff Reimbursement	REQ.053	The system should be able to provide intelligence on spend analysis	Mandatory		
FIN 1.0	Expense Management	FIN 1.2	Cash Advance	REQ.054	The system should be able to administer cash advance, incorporate cash advance request forms and creation of expense report in the system	Mandatory		
FIN 1.0	Expense Management	FIN 1.1 FIN 1.2	Staff Reimbursement Cash Advance (Theatre Productions)	REQ.055	The system should allow to provide a workflow and set up rule-based approval matrix and route expense report/cash advance approval to one or more approvers in accordance with business rules, e.g., financial value, category. The system should then allow to approve expense report/cash advance via the workflow as per appropriate delegation of financial and functional authority	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 2.0	Accounts Payable	Generic	Generic	AP.001	The system should allow for auto-calculate GST on invoice	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.002	The system should allow tosupport multi-level invoice approval workflow	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.003	The system should allow to detect and prevent processing of duplicate invoice	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.004	The system should allow to record a credit or debit memo to adjust original invoice amount	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.005	The system should allow to record advance payment	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.006	The system should allow to auto-generate invoice for recurring expenses	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.007	The system should allow to support multiperiod accounting e.g in prepaid expense	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.008	The system should allow to create payment to multiple payees e.g. student assistance	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.009	The system should allow to review and approve batch payment	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.010	The system should allow to auto generate accrual on good receipt	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.011	The system should allow to support AP closing	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.012	The system should allow to list various standard AP reports e.g ageing, trial balance, credit report and others.	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.013	The system should allow to download AP payment advice as PDF	Mandatory		
FIN 2.0	Accounts Payable	Generic	Generic	AP.014	The system should allow for handle of petty cash	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.1 FIN 2.2	Invoice Processing (PO) Invoice Processing (non-PO)	AP.015	The system should allow for the submission of invoice (with PO or no PO) via the supplier portal.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.1	Invoice Processing (PO)	AP.016	The system should allow to routing of invoice to respective verifiers for goods receipt and verification	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.1	Invoice Processing (PO)	AP.017	The system should perform an automated 3-way match between the PO, GR, and IR. If match is successful, the system should validate if amount is above threshold for auto posting, else post invoice manually.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.1	Invoice Processing (PO)	AP.018	The system should allow to retrieve PO information to create PO	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.1	Invoice Processing (PO)	AP.019	The system should allow to retrieve GR information to create GR	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.2	Invoice Processing (non-PO)	AP.020	The system should be configured to create and submit 'Supplier invoice Request' and attach the non-PO invoice. Upon submission of supplier invoice request, the system should perform budget check, account assignment combination and commitment, and automatically route for approval. SIR is used to make payment to a supplier when a PO is not required,	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.3	Adhoc Payment Request	AP.021	The system should be configured to create and submit 'Supplier Invoice Request' (SIR) and attach the supporting document. Upon submission of supplier invoice request, the system should perform budget check, account assignment combination and commitment, and automatically route for approval. Example of adhoc payment requests include awardees of Arts Development Grants, payment of competition fee etc.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.2 FIN 2.3	Invoice Processing (non-PO) Adhoc Payment Request	AP.022	The system should allow AOs to reject the supplier invoice request with reason and notify the requestor.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.2 FIN 2.3	Invoice Processing (non-PO) Adhoc Payment Request	AP.023	The system should allow to route supplier invoice request for BO / AO / Verifier approval as per approval matrix.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.3	Adhoc Payment Request	AP.024	The system should allow to the attachment of supporting document during creation of supplier invoice request.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.025	The system should allow to update invoice status for all invoices (PO, non-PO, Adhoc payment request) on invoice payment status	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.026	The system should allow to generate remittance advise and send to vendor.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.027	The system should allow to run payments in batches.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.028	The system should allow to transfer payments between bank accounts.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.029	The system should allow to automatically send notification to inform users of payment processing creation, for example but not limited to: a. The user creating the payment proposal b. The approver c. Additional users who has access to payment proposal.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.030	The system should allow for invoices approved for payment and due to be picked up for payment processing.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.031	The system should allow the user to configure system rules to trigger additional approvals for the automatically generated and approved payment voucher. For example, where the invoices processed by users and submitted to Finance for payment processing exceeds the pre-determined expected value, the voucher will be routed for an additional approval before it can be paid out.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.032	The system should allow users to put up requests with comments and/or supporting documents to hold payments.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.033	The system should reject the invoices processed by users and submitted to Finance for payment processing if payment to the vendor has already been made.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.034	The system should allow users to hold the payment indefinitely, or un-hold the payment after the invoice has been updated. The invoice should then be picked up for settlement.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.035	The system should identify the payments to be included in the settlement run based on their scheduled payment date. The scheduled payment date will be based on the user requirement.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.036	The system should facilitate various payment methods, which include, but not limited to: a. Interbank Giro b. Standing Auto-Giro c. Telegraphic Transfers d. PayNow	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.037	The system should facilitate the settlement runs by consolidating payments to be paid to the same vendor. The settlement runs can be separated by payments from different banks, by different payment types.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.038	On successful payment, the system should transmit the updated payment information to the supplier portal and generate remittance advices to inform the suppliers of successful payment.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.039	On unsuccessful payment, the system should notify users to perform the required processing e.g., reversal of the payment and holding it from further settlement until the failed payment is investigated.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.040	The system should automatically generate a list of invoices that have been held or are pending approval.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.041	The system should automatically notify users of payments pending approval and payments that have been approved.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.042	The system should allow the user to either update the scheduled payment date or further process the underlying invoice (e.g., update the payment type).	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.043	The system should allow for multiple payment batches to be run concurrently for a single vendor but disallow the same payment document to be included in any payment batch more than once.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.044	The system should allow the setting up of recurring amortization of prepayments.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.045	The system should allow the user to run a report to identify purchases that have not been paid for the period.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.046	The system should allow to support selection of bank account for payment during invoicing.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.047	The system should notify the relevant parties by email or equivalent based on their payment authorization limits to authorize the payment batches online. The system should also allow these parties to have view access to the e-invoices pertaining to the payment batches that they have to authorize.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.048	The system should automatically generate the bank interface file and allow the transmission of the file to the banking portal DBS IDEAL. The system should also allow for automatic uploading of bank return file.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.049	The system should allow to sort by payment method and automatically prepare draft payment proposal upon posting of supplier invoice.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.050	The system should allow routing of payment proposal to approvers / authorised signatory for review as per approval matrix	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.051	The system should allow the AP staff to 'amend' payment proposal if post-approval edits are required and re-submit the payment proposal for approval.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.4	Payment Processing	AP.052	The system should allow to receive payment status notification from DBS IDEAL	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.053	The system should allow to approve suppliers through workflow. For example: - During vendor onboarding when supplier enters information, the system should use workflow to approve suppliers. - When there are changes in compliance-related requirements and supplier updates information, the system should use workflow to approve these changes.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.054	The system should allow to create vendor in central vendor master data repository.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.055	The system should allow to maintain vendor data via updates/edits.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.056	The system should allow to perform supplier prequalification and assessment via an online supplier portal, including creation of vendor registration forms and due diligence forms in different formats, allow suppliers to self-input necessary details and attach supporting documents, enable users to update the supplier master data as required, etc.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.057	The system should allow to retrieve vendor information that has been saved in the system, to support users in their decision-making when approving vendors. There should also be a free text field for users to input any justification on why the vendor should be qualified.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.058	The system should support an online supplier portal, where vendors register themselves in the system. Once vendors have registered themselves, the system should support approval workflow to route vendor registration for approval. The system should then create the vendor in the vendor master and update the vendor information and approval status in the supplier portal.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.059	The system should allow to restrict user access to the vendor master, as well as configure different types of user notifications. For example: - Restrict user access to update vendor master - Notify requestor when a vendor is added - Notify vendor upon successful vendor registration approval by designated approver - Notify users when a vendor is removed.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.060	The system should allow to push notifications and send reminders to vendors via the supplier portal to request vendors to update the information/ documents submitted by the vendors. Upon the update of information, the administrator will receive a notification to validate the information/document submitted. For example, during communication between SOTA and the vendor before confirmation of the vendor, all the information/ documents that are part of this communication trail should be consolidated and stored in system.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.061	The system should allow to tag vendors to different groups and maintain vendors based on these groups.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.062	The system should allow to manage vendors centrally across all departments.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.063	The system should allow to manage vendor master file (including eliminating duplicates, updating supplier data, adding/removing suppliers).	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.064	The system should allow to identify inactive vendors for users every predetermined period e.g 6 months, 12 months for review and decide whether to block transactions from these vendors and/or deactivate vendors from vendor master.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.065	The system should be able to block blacklisted vendors from creation of any new PR / PO.	Mandatory		
FIN 2.0	Accounts Payable	FIN 2.5	Vendor Master Management	AP.066	The system should be able to check for any pending PRs / POs before removing inactive vendors for users to review.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement	Statement of	Tenderer Remarks
FIN 3.0	Assets	Generic	Generic	A.001	The system should allow to complete fixed asset life cycle, from acquisition, depreciation, transfer, disposal, gain or loss on disposal	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.002	The system should allow to handle single or multiple assets, parent and child assets relationships	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.003	The system should allow to search asset by query	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.004	The system should allow to handle work in progress of asset capitalisation	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.005	The system should allow to forecast or project depreciation in the future by	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.006	The system should allow the use of multiple asset books for single company to manage different accounting treatment	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.007	The system should allow to define the prorate convention ("beginning of the	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.008	The system should allow to define various roles and responsibilities in Fixed	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.009	The system should be able to generate a fixed asset disclosure report,	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.010	The system should allow to generate a report that shows net book value	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.011	The system should allow to generate active asset categories list.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.012	The system should allow to generate Fixed Assets reports based on various	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.013	The system should allow to generate minor assets tracking report.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.014	The system should allow to generate various fixed assets reports, e.g., asset	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.015	The system should allow to group capitalized asset lines by expenditure	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.016	The system should allow to have a monthly report for depreciation forecast	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.017	The system should allow to manage residual value for fixed assets and	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.018	The system should allow to meet various reporting requirements (e.g.,	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.019	The system should allow to perform online entry and maintenance of fixed asset records. The system should allow changes to be properly accounted for in the Asset Management module and the GL. The system should allow to accelerate asset life and account for asset impairment and retirement.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.020	The system should allow to process adjustments to assets that change the asset value or estimated useful life.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.021	The system should allow to provide automated posting of general ledger journal entries once write-down has been calculated.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.022	The system should allow to report on fixed asset list by location, asset type, asset ID, asset description, asset category, asset life, depreciation method, department, and assignment with acquisition date and historical cost.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.023	The system should allow to report original asset costs (specifically for acquired assets).	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.024	The system should allow to restrict user access in updating depreciation rates and executing unplanned depreciation based on role profiles.	Mandatory		
FIN 3.0	Assets	Generic	Generic	A.025	The system should allow user to drilldown from asset to original source documents (invoice, GR, PO, PR) and should be able to list documents in the report.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.026	The system should allow for asset to be recognised when goods are completely handed over and ownership is transferred	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.027	The system should allow for assets to be capitalised on the month of receipt with the capability to account for partial deliveries if necessary.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.028	The system should allow for depreciation to commence only when the asset is fully operational and in use, aligned with the date the asset is capitalised in the system. For assets delivered in batches, partial depreciation should be calculated based on the portion of the asset that is operational	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.029	The system should allow to assign a location code to an asset.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.030	The system should allow to assign various attributes to an asset or asset component (e.g., supplier, serial number, etc.).	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.031	The system should allow to automatically assign asset useful life upon selection of asset type/class.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.032	The system should allow to capture asset value date and asset capitalization date.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.033	The system should allow to capture sub asset number for main asset.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.034	The system should allow to link an asset to a responsibility center (cost center) while charging depreciation to a GL account specified at asset level.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.035	The system should allow to perform mass asset creation.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.036	The system should allow to record minor assets by asset classes, without performing depreciation.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.037	The system should allow to track asset barcode numbers for asset verification.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.038	The system should allow to track information on assets such as warranties, location, whether insurance is needed, etc.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.039	The system should allow user to easily update asset location by selecting from a list of pre-set locations.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.040	The system should allow users to assign the appropriate category to an asset. Note: The category determines the accounting treatment (e.g., asset clearing, depreciation method, estimated useful life, etc.).	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.041	The system should allow different asset prefixes to be assigned e.g., (FA101xxx1: Fixed Asset; MA101xxx1: Minor Asset) and for asset number to still be system-generated when there is a prefix assigned.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.042	The system should allow for partially funded assets to be amortised based on funding %.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.043	The system should allow to define the first and last month/year of depreciation.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.044	The system should allow to reverse an asset created in error, individually and mass reversal of additions.	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.045	The system should allow to identify taggable assets	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.046	The system should allow to handle non-capitalised assets ie items below asset threshold, and the tracking and tagging of such minor assets	Mandatory		
FIN 3.0	Assets	FIN 3.1	Asset Addition	A.047	The system should allow to capitalize asset with tax amount	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.048	The system should allow to retrieve asset display and prefill Net Book Value & Accumulated Depreciation	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.049	The system should allow to control gain/loss realization when retiring a single asset or a group asset.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement	Statement of	Tenderer Remarks
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.050	The system should allow to create and post asset retirement journal entries.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.051	The system should allow to route for approvers to verify and approve asset disposal as per approval matrix	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.052	The system should allow to identify the reason for the asset disposal/retirement (e.g. scrap, donations, etc.) and make it a mandatory field in the asset disposal/retirement form.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.053	The system should allow to partially retire assets and write-off missing/obsolete assets.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.054	The system should allow to perform mass retirements based on asset number and FA Book Name.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.055	The system should allow to post proceeds (cash or cash clearing) and expenses to accounts.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.056	The system should allow to record the appropriate accounting entries when an asset is disposed (e.g., the proceeds from the sale, removal costs, and the gain or loss on disposal).	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.057	The system should allow to report on retirement information by period which includes retirement type, proceeds, and salvage.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.058	The system should allow to retire minor assets that are no longer in use and remove them from the Asset Register.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.059	The system should allow to reverse an asset disposal (i.e., correct asset disposed in error), individually or mass reversal.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.060	The system should allow to track information on the sale or disposal of asset (e.g., purchaser, sale value, gain, or loss on disposal) and generate entries to the general ledger to reflect the disposal.	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.061	The system allows administrator to create validation rule to prevent accidental disposal	Mandatory		
FIN 3.0	Assets	FIN 3.2	Asset Disposal/Write Off	A.062	The system should provide a report to identify assets that are at the end of useful life and ready for retirement	Mandatory		
FIN 3.0	Assets	FIN 3.3	Asset Verificatio	A.063	The system should allow to support the transfer of fixed assets and generate the appropriate general ledger entries, based on category, location, cost center, estimated useful life, values, etc., without changing the asset number.	Mandatory		
FIN 3.0	Assets	FIN 3.3	Asset Verificatio	A.064	System should allow to generate fixed asset and minor asset listing by department	Mandatory		
FIN 3.0	Assets	FIN 3.3	Asset Verificatio	A.065	The system should allow to report on fixed asset additions, retirements, cost adjustments, accumulated depreciation, etc., by asset, asset category, project code, location, etc., for a given period. The system should also allow to generate the report in summary or detail level.	Mandatory		
FIN 3.0	Assets	FIN 3.3	Asset Verificatio	A.066	The system should allow to list the standard fixed asset reports	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement	Statement of	Tenderer Remarks
FIN 4.0	Accounts Receivable	Generic	Generic	AR.001	The system should allow to generate credit note from original invoice	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.002	The system should allow to generate recurring billing	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.003	The system should allow to match receipts to invoices	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.004	The system should allow to support advance collection	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.005	The system should allow to generate reminder for collections	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.006	The system should allow to forward the approval workflow if the manager is on leave.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.007	The system should allow to generate customer billings using different type of templates/logos.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.008	The system should allow to approve credit notes/ invoices in the system as per financial delegations	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.009	The system should allow to generate multiple types of invoices and receivables with multiple formats.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.010	The system should allow to set up and record the appropriate receivable accounting entry based on the type of transaction.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.011	The system should allow to automatically identify an invoice number at the time of entry.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.012	The system should allow to create invoices raised manually.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.013	The system should allow to have audit trails of deleted invoices.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.014	The system should allow customer PO information to be input or updated even after invoice creation.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.015	The system should allow to process refunds/returns to the correct customer.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.016	The system should allow for approvers to review, revise, and approve invoices that will be written off.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.017	The system should allow to provide multiple write-off codes (e.g., for bad debt and discharge settlements).	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.018	The system should allow to report on the outstanding balance against an invoice where a partial payment has been applied.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.019	The system should allow approvals for manual adjustment processing.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.020	The system should allow to indicate when balances are paid in full.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.021	The system should allow to process customer refunds.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.022	The system should allow to update the accounting date on payments which	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.023	The system should be able to auto generate refund requests based on a set	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.024	The system should allow to view customer metrics via dashboard for	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.025	The system should allow to capture multiple statuses for receipts based on	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.026	The system should allow to generate bills with multiple line items.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.027	The system should allow users to attach supporting documents when raising invoices and receipts.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.028	The system should allow to apply credit memos to related invoices or line items on an invoice.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.029	The system should allow for automatic offset of invoices against credit note based on specified rules.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.030	The system should allow to automatically apply debit and credit memos to corresponding invoices.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.031	The system should allow to create a debit or credit memo that is not associated with a specific invoice or invoice line.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.032	The system should allow to raise multiple credit notes against the same invoice/customer account.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.033	The system should allow to interface credit note information to create credit note from SMS to ERP AR.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.034	The system should allow to interface credit note information to create credit note from EBMS to ERP AR	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.035	The system should allow end-to-end receipt clearing and bank reconciliation processes for collections.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.036	The system should allow to remove and reapply receipts that were previously applied in error.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.037	The system should allow to have an automated receipt clearing program.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.038	The system should allow to provide the following fields for receipt entry including, but not limited to: customer name, customer number, invoice number, receipt date, amount, payment type, item quantity, and comment field.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.039	The system should allow to receive receipts and auto match to the invoice.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.040	The system should allow to process bank deposit slips.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.041	The system should allow to capture different types of payments like advance payments, partial payments, payment using credit cards, checks, credit memos, etc.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.042	The system should allow to apply multiple receipts against a single invoice, or conversely, a single receipt against multiple invoices. The system should also allow to perform auto matching function accordingly.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.043	The system should allow to automatically apply receipts against existing invoices.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.044	The system should allow to validate the remaining balances after receipt of bill payments.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.045	The system should allow to manually match open invoices against receipts that cannot be processed using an automatic cash receipts program.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.046	The system should allow to receive, merge, and match daily account information electronically from banking institutions such as DBS Ideal	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.047	The system should allow to record receipts or customer payments as: - Unapplied cash - On-account cash - Open claim.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.048	The system should allow to attach electronic documents to receipts.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.049	The system should allow to define various aging buckets for transactions based on business requirement.	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.050	The system should allow to report and display by multiple periods (30 days +, 60 days +, 90 days +).	Mandatory		
FIN 4.0	Accounts Receivable	Generic	Generic	AR.051	The system should allow to fetch aging data from SMS (student billing system) & EBMS (venue hire/booking system) application and should be able to generate combined aging report.	Optional		
FIN 4.0	Accounts Receivable	FIN 4.3	Billing (Adhoc)	AR.052	The system should be able to generate billing report and send invoice to customer	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.4 FIN 4.5	Collection (Cash, NETS) Collection (Bank Transfer, Paynow)	AR.053	The system should allow to interface receipts from DBS IDEAL to the system	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.4	Collection (Cash, NETS)	AR.054	The system ensures that funds are accounted for as customer deposit for applied correctly before the accounting is finalized and posted to the general ledger.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement	Statement of	Tenderer Remarks
FIN 4.0	Accounts Receivable	FIN 4.1 FIN 4.2	Billing (SMS) Billing (EBMS)	AR.055	The system should allow to park and post billing entries to GL account	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.1 FIN 4.5	Billing (SMS) Collection (Cash, NETS)	AR.056	The system should allow to interface billing and collection information from SMS, a Student Management System to create GL line item posting & amount from SMS, to system	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.1 FIN 4.5	Billing (SMS) Collection (Cash, NETS)	AR.057	The system should allow to interface billing and collection information from Events Booking Management System (EBMS), a venue hirer and booking system to create GL line item posting & amount from SMS	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.3	Billing (Adhoc)	AR.058	The system should allow to generate billing invoice	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.5 FIN 4.6	Collection (Cash, NETS) Collection (GIRO - SMS)	AR.059	The system should allow to reconcile bank statement against receipts	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.5 FIN 4.6	Collection (Cash, NETS) Collection (GIRO - SMS)	AR.060	The system should allow to post matched transaction from bank clearing account to main bank account	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.5 FIN 4.6	Collection (Cash, NETS) Collection (GIRO - SMS)	AR.061	The system should allow to auto clear matched item in bank clearing account	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.6	Collection (GIRO - SMS)	AR.062	The system should allow to interface successful GIRO deductions to system	Mandatory		
FIN 4.0	Accounts Receivable	FIN 4.6	Collection (GIRO - SMS)	AR.063	The system should allow to reconcile bank statement against GIRO deductions	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 5.0	General Ledger	Generic	Generic	GL.001	The system should allow to support multiple workflow approvers for a journal.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.002	The system should allow to create single and batch journals (i.e., mass upload journal).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.003	The system should allow to highlight errors when loading mass upload journals, data cannot be truncated without first issuing a warning to users and users must affirm decision before proceeding.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.004	The system allow the posting level of a journal eg. detail level posting and summarized level posting	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.005	The system should allow to review the journals in general ledger prior to posting.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.006	The system allow the posting of multiple book and multiple book code to capture transaction for specific cost centre without impacting group GL	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.007	The system should produce reports showing exceptions, e.g., any gaps in transaction numbering due to parked documents, any number skip due to technical problems, any documents pending approval, etc.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.008	The system should allow to perform mass posting, mass upload, and mass reversal auto-clearing transactions. The system should also be able to generate audit schedules and other reporting requirements like regulatory or statistical reports.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.009	The system should allow to upload journals for multiple ledgers using a single spreadsheet.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.010	The system should allow to generate journal numbering automatically. The system should also automatically refresh the journal number in each fiscal year (e.g., first document number in each FY 1000000 FY21/ 1000000 FY22/ 1000000 FY23).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.011	The system should allow to enter detailed descriptions for each journal line. The system should also allow for edits in the detailed descriptions text (only) after posting, to allow users to amend the descriptions if required but without access to amend other fields (e.g., date/amount) without workflow approval.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.012	The system should allow to post journals against projects or cost centers.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.013	The system should allow to define and capture additional information for each journal at header and line level.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.014	The system should allow to view a simulation of postings (view impact on various accounts due to the journal) before actually posting the journals.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.015	The system should allow to save journals as drafts (to be revisited later to post it).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.016	The system should allow to apply rules to journals in various stages of the process (e.g., A journal can be deleted when it is unapproved vs it cannot be deleted after it is posted).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.017	The system should allow to post journals with attachments for substantiation.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.018	The system should allow to post journals in a different accounting period.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.019	The system should allow to provide an audit trail of the changes to COA values and hierarchies. Changes in COA should be mapped and updated automatically in TB, PL, BS, CF reports.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.020	The system should allow to automate recurring journal entries for accrual processing. For example, the system should have a feature to support entry of accruals and prepayment (one-time exercise to set up frequency and rules to generate recurring accrual entries).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.021	The system should allow amortization of prepaid expense based on specific pre-defined rules.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.022	The system should allow to allocate costs based on configurable parameters such as time sheet data, number of employees, etc.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.023	The system should allow to approve, delete, and reverse journals based on previous allocation.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.024	The system should allow to perform income statement close and balance sheet close for any period.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.025	The system should roll closing balances from one period into the opening balances for the subsequent period(s) automatically without the need for additional journals to be posted. Vendors should confirm if carry forward journals can be created for Year End closing.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.026	The system should allow to perform manual journal entries.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.027	The system should allow to update account balances and perform a roll forward of closing and opening balances when a new General Ledger period is opened.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.028	The system should allow to pass year-end adjustment in specified adjustment period.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.029	The system should allow to perform period close in sub-ledgers in advance of the General Ledger close.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.030	The system should allow to generate dashboards/reports in multiple formats and for all document types (Excel, PDF, Word, PPT). This should be a generic requirement for all reports.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.031	The system should allow to view cleared and uncleared accounts.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.032	The system should allow to view discrepancies and conduct inquiry (i.e., if there are invoices/documents where posting is not done, system should allow to review and check why posting was not done).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.033	The system should allow to build checks and restrictions for journal posting and attach supporting information to the journals.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.034	The system should allow to create journal entries in batches either via an Excel template upload or feeds from other systems.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.035	The system should allow to generate a report of parked and posted journal entries.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.036	The system should allow to enforce approval workflows for journals. The system should also allow to auto-escalate approval workflow if journals are not approved after "X" days.	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.037	The system should allow to restrict user access based on roles and GL codes, and create and capture audit trails on additions/ changes/ deletions of financial transactions based on user-defined key fields. The system should allow closure of modules to block out certain periods for all users for certain modules (e.g., block PO module during YE closing).	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 5.0	General Ledger	Generic	Generic	GL.038	The system should allow to produce various standard financial reports for various accounting periods (Income Statement, Balance Sheet, Trial Balance, Cash Flow statement). The system should also allow financial reports to be prepared to the level of Entity, Cost Centre, Profit Centre, Business Unit).	Mandatory		
FIN 5.0	General Ledger	Generic	Generic	GL.039	The system should allow to automatically identify cash and non-cash transactions for cash flow statement reporting purpose.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.040	There is no separation between the sub-ledger and the General Ledger. They are part of a single, unified accounting engine. Real-Time Posting: When a sub-ledger transaction (like a supplier invoice) is approved and posted, it is simultaneously a sub-ledger event and a General Ledger journal entry. There is no batch process or delay.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.041	The system should allow to create accrual journal entries based on open items (PO).	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.042	The system should enable automatic reversal of accrual journal entries	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.043	The system should automate the accruals of services/purchase of goods/work done for monthly closing based on open PO not invoiced, goods/services received not invoiced, invoices approved not paid.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.044	The system should allow to reconcile all the sub-ledger journals.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.045	The system should allow to perform real-time posting of sub-ledger data to GL and reconcile sub-ledger to GL.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.046	The system should allow to monitor and manually match unreconciled bank statements and transactions prior to period close.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.047	The system should allow to mark the cleared and uncleared accounts as reconciled.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.048	The system to allow set up of threshold tolerance for amount not matched.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.049	The system should allow to reconcile GST.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.050	The system should allow the use of matching algorithm for bank reconciliation process.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.051	The system should allow to configure business rules to automate allocations in General Ledger, e.g. distribute cost in one account to different cost centers based on the headcount in each cost center	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.052	The system should allow to provide chart of accounts structure with multiple dimensions	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.053	The system should allow to set up Chart of Accounts hierarchies	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.054	The system should allow to close periods at end of month and allow to restrict access to select users to reopen for period adjustments	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.055	The system should allow to provide dashboard to see closing status	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.056	The system should allow to define Accounting calendar	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.057	The system should allow to post journal entries from external systems	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.058	The system should allow to support Journal entry approval workflow	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.059	The system should allow to upload excel file to post batch GL entries	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.060	The system should allow to maintain a financial calendar of events relating to closing schedule and tasks to be performed	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.061	The system should allow to maintain a dashboard to track closing process and status	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.062	The system should allow to support IFRS and other local statutory requirements	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.063	The system should allow to interface payroll entries from payroll system	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.064	The system should allow to park payroll entries to GL account	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.065	The system should allow for running of depreciation	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.066	The system should allow to perform bank recon for all cash accounts to adjust cross-month variance.	Mandatory		
FIN 5.0	General Ledger	FIN 5.1	Month/ Year E	GL.067	The system should allow to review bank recon schedule	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.068	The system should allow for generation and export of GST report in Excel or other format	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.069	The system should allow to create and maintain specific tax information for a customer e.g Tax ID & tax registration number (UEN)	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.070	The system should allow to capture the following minimum tax information in the tax (customer, vendor, product) master: - Tax code - Tax rate - Tax description - Product/Service type	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.071	The system should allow to generate tax reports which would list all the tax computations/transactions based on user-defined parameters such as tax code, service line/product type, etc.	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.072	The system should allow to link the different tax rules/codes to the customer (AR) or supplier (AP, Purchasing) master and with the flexibility to override the defaulted information at point of entry.	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.073	The system should allow to run a report that relates to GST paid on capitalized assets.	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.074	The system should allow to report (by tax code/amount) by invoice date/GL date/paid date.	Mandatory		
FIN 5.0	General Ledger	FIN 5.2	GST Submissio	GL.075	The system should allow a GST report that pulls all relevant line-item information related to a taxable transaction for review and analysis (e.g., Invoice no. Invoice Date, Tax Base, Tax, Total amount, Text, Vendor/Customer, Country of Vendor/Customer, GL code, Cost Centre, etc.).	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.001	The system should allow for users to review reports, dashboard and ad-hoc/ self-service capabilities.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.002	The system should allow for users to define, develop, and download/export their own reports via report writer with word, excel, PDF, etc.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.003	The system should be able to define and validate formula/ functions for designing reports.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.004	The system should be able to report on different periods based on current and prior versions of hierarchies.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.005	The system should allow for reports to be accessed and displayed on mobile devices and in PDF format.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.006	The system should be able to filter and sort all reports by different types/ dimensions.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.007	The system should be able to report financial statements with and without the impact of all or certain allocations.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.008	The system should be able to support real-time reporting generation, scheduling, and reports distribution.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.009	The system should be able to run ad-hoc reporting and analysis that is user-friendly and should be able to perform analysis at GL, sub-ledger and reporting level within the ERP and Reporting environment (e.g., ad-hoc reports/ pivot tables to the lowest level and to aggregate information/ roll-up based on hierarchies within GL) so that user can drill down and drill through to see more granular level data.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.010	The system should allow for users to run their own reports based on user-defined views and specific parameters selected.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.011	The system should be able to incorporate standardized naming convention.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.012	The system should be able to create full year/partial year GAAP/IFRS/Tax financial reports.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.013	The system should be able to support various financial reporting standards so numbers can be reported on those specific accounting basis (e.g., GAAP/IFRS) with comparative and drill down capability.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.014	The system should be able to prepare standardized financial statements (B/S, I/S, C/F) by defined hierarchies.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.015	The system should allow managers to access budget information via dashboard.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.016	The system should allow to update cost allocations on a monthly basis.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.017	The system should allow to analyze performance at department / faculty level.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.018	The system should be able to do management allocations and run cost allocation reports.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.019	The system should allow user access to click through transactions and view supporting documents as they scroll through transactions.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.020	The system should allow to produce configurable management reports for standard variance analysis, run rate/trend analysis, financial ratios, and actual compared to prior month, projected balance sheet, projected fund flow statement.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.021	The system should allow for various standard financial reports to perform comparative analysis. For example: - Variance analysis: actuals vs budget - Variance analysis: actuals vs forecast - Variance analysis: actuals vs actuals (year over year) - Variance analysis: budget vs forecast - Variance analysis: budget vs budget (year over year OR version vs version) - Trend analysis: period vs period - Trend analysis: year vs year.	Mandatory		
FIN 6.0	Management Reporting	FIN 6.1	Management Reporting	REP.022	The system should be able to produce the following reports as required, for e.g: a) Income and Expenditure by School Operations and Venue Management & Retail Operations b) Temasek Foundation Nurtures (TFN) utilization report c) Balance Sheet d) Restricted Fund schedule e) Fixed Deposit schedule f) Bank Reconciliation g) Capital Expenditure (CAPEX) utilization report h) Expense management dashboard i) AP/AR ageing report j) Cost center report	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 7.0	Funds & Grants Management	Generic	Generic	GM.001	Grant received in advance (GRIA) is the GL account to keep track of project grants receipts and utilization of expenses for the grantors. The system should allow allocation of projects expenses and incomes to single or multiple GRIA account based on user defined parameters such as Grantor or Intermediate Agent types and different funding sources etc. The system should allow user to define the percentage of funding by the various Grantors which will be used for allocation of the project's expenses to GRIA accounts. The system should automatically calculate and post monthly/quarterly grant utilization journal entries to the GRIA accounts based on the total expenses of all or groups of projects and the percentage of funding.	Mandatory		
FIN 7.0	Funds & Grants Management	Generic	Generic	GM.002	The system should allow to store a budget against a grant, track spend against the grant, and flag when spend is over budget.	Mandatory		
FIN 7.0	Funds & Grants Management	Generic	Generic	GM.003	The system should allow to attach supporting documentation to invoice.	Mandatory		
FIN 7.0	Funds & Grants Management	Generic	Generic	GM.004	The system should allow the usage of grant codes/elements to record the various grants and funds	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.1	Government Grants Management	GM.005	The system should allow to process fund adjustments (top up / clawback, typically received in July, from MOE for opportunity fund (funds disbursed for students with financial needs).	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.1 FIN 7.2	Government Grants Management Funds Management	GM.006	The system should allow to manually park journal entries to record grants received in advance without posting them to the financial statements until review and approval are completed.	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.2	Funds Management	GM.007	The system should allow to manually park journal entries to record Other Receivable without posting them to the financial statements until review and approval are completed.	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.1 FIN 7.2	Government Grants Management Funds Management	GM.008	The system should allow to automatically compute and post grant income, auto-matching to related eligible expenses are incurred e.g depreciation where applicable.	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.1 FIN 7.2	Government Grants Management Funds Management	GM.009	The system should allow to generate grant utilization report to determine the usage of grant funding (income and expense) and grant balance	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.2	Funds Management	GM.010	The system should allow to park and post journal entries to reclass expense from accumulated fund to restricted fund for Cultural Matching Fund, a fund that has no restriction on the usage of funds when incurred.	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.2	Funds Management	GM.011	The system should allow to transfer funds from CMF bank account to school current account.	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.3	Donation Management	GM.012	The system should allow to park and post journal entries to record donation receipt	Mandatory		
FIN 7.0	Funds & Grants Management	FIN 7.3	Donation Management	GM.013	The system should allow to review the donation schedule against existing donor agreements, receipts, and records to identify any inconsistencies or missing information.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.001	The system should allow user input of expected new capital expenditure.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.002	The system should allow user to review and update of useful lives for specific new assets.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.003	The system should allow to calculate depreciation expense for new capex.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.004	The system should allow to get depreciation data from the asset register.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.005	The system should allow to set targets at any level of a hierarchy.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.006	The system should allow to have detailed audit trail information.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.007	The system should allow to classify projects into types.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.008	The system should allow to extract official forecast and budget and load into Financial system seamlessly.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.009	The system should allow to budget for balance sheet and cash flows.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.010	The system should allow to budget for projects through to the end of the project life.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.011	The system should allow budget adjustments to be made.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.012	The system should allow to provide a dashboard supporting the control of the processes advising the stage of each "section"; for example, budgets are submitted, returned for review, or approved.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.013	The system should allow development of operating budgets using financial and non-financial information. The operating budget will be built up based on key business drivers and changes in these drivers.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.014	The system should allow to perform variance analysis.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.015	The system should allow to generate cash flow statements at operational level.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.016	The system should allow to generate balance sheet reports at an operational level.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.017	The system should allow to define drivers' variability and interdependencies.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.018	The system should allow to consolidate the planning metrics ($ amount) at a department level.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.019	The system should allow analysis of cash flows at the group level, with the ability to drill down to the department level to understand spending impacts.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.020	The system should allow users to analyze cash flows with visibility into the impact from OPEX and CAPEX activities.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.021	The system should allow to view, add, and update actuals, and maintain an audit trail of changes.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.022	The system should allow to store business rules for calculating forward projections.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.023	The system should allow to apply stored business rules to calculate and display forward projections.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.024	The system should allow to enable workflow management of planning tasks including visibility of statuses, outstanding tasks, approvals required, etc.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.025	The system should allow upload functions.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.026	The system should allow multiple users access.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.027	The system should allow to download and publish in multiple analytical and graphical formats (.pdf, .ppt, .xls, .txt).	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.028	The system should allow for driver-based analysis of variances.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.029	The system should allow to create scorecards and dashboards.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.030	The system should allow to report at all levels of the organization.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.031	The system should allow to filter by dimension or fields.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.032	The system should allow to interface with excel as an analysis & reporting tool.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.033	The system should allow to report on budget reports which have been completed by users, i.e.: which users have or haven't submitted their budget, forecast or reports.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.034	The system should allow to perform 12 month rolling forecasts.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.035	The system should allow to get a statutory view of the profit and loss forecast.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.036	The system should allow to get a management view of the profit and loss forecast.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.037	The system should be able to consolidate all projects and perform X-year cash flow projection.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.038	The system should allow to periodically compare forecast and actuals.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.039	The system should allow to generate the rolling forecast reports based on actual expenditure and remaining future years' budget to form the total project budget.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.040	The system should allow to restrict access to only when the budgeting or forecasting period is open.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.041	The system should support top down budgeting, encompassing scenarios ranging from Realistic to Pessimistic and Optimistic.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.042	The system should allow to record and manage organization planning assumptions, specific cost drivers and KPIs.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.043	The system should allow to add both operating and capital cost.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.044	The system should allow users to create and copy a new version or scenario initialized with data from prior versions.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.045	The system should allow to control multiple versions of the budget.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.046	The system should allow to support locking down of budget versions and forecast as needed.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.047	The system should allow to support multiple scenarios and versions, including the ability to submit/promote/copy from one version to another.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.048	The system should allow to provide tracking reports of each version and the changes of project budget. The system should also allow virements/variations on headcounts and staff designations, in addition to financial figures.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.049	The system should be able to provide budget utilisation via a dynamic budgeting module.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.050	The system should support forecast using advanced algorithms and/or machine learning and be able to describe further how multi year projects are rolled over and tracked from one FY to another.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.051	The system should be able to support multi-year projects (both operating and capital in nature) and uploading of budget across FYs.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.052	The system should support automated scheduling and email distribution of reports, including the ability to send report files as attachments (e.g., PDF or Excel) to designated recipients.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.053	The system should be able to plan for workforce (plan headcount and related expenses).	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.054	The system should be able to plan for projects and capital expenditure.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.055	The system should be able to support budget, forecast and reporting at the project level, with real-time aggregation to overall financial statements and management reports.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.056	The system should be able to prepare budget on various basis e.g. historical budget, actual result, zero-based, percentage-based.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.057	The system should be able to set prepare at any hierarchical level of the organisational structure.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.058	The system should be able to support rolling budget and forecast.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.059	The system should be able to support What-If modelling.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.060	The system should be able to configure workflow process.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.061	The system should be able to allocate and track expenses by project for budgeting and reporting purposes.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.062	The system should allow to create budget template, open budget period and assign access to budget owners and users as required.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.063	The system should have the ability to notify budget owners on the starting of budget process, any comments left, and approval of budget.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1 FIN 8.2	Annual Budgeting & Planning Budget Virement	BUD.064	The system should have the ability to notify SSC to review budget and allow to leave comments.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.065	The system should allow for the auto compilation of completed budget templates.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.1	Annual Budgeting & Planning	BUD.066	The system should allow for triggering of approved budget interface to PR module.	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.2	Budget Virement	BUD.067	The system should have the ability to inform requestor / budget owner of successful budget virement request .	Mandatory		
FIN 8.0	Budgeting & Planning	FIN 8.2	Budget Virement	BUD.068	The system should be able to support budget virement between departments during the financial year.	Mandatory		

SCHOOL OF THE ARTS SINGAPORE

Annex D3: HR Functional Requirements

Instructions to Tenderers

1.1 Please state clearly the compliance to all requirements listed in this Annex. For each requirement, the Tenderer shall select the appropriate compliance response from the dropdown menu. Definitions of each compliance reponse are provided in the table under "Compliance Definition" below.

1.2 Any statements in this Annex pertaining to other parts of the tender will be disregarded by the School. Only the responses provided in the table under "Compliance Definition" will be accepted. Where there is a failure to indicate a proper compliance response, it shall be deemed that the Tenderer has indicated "C" and the offer shall be evaluated accordingly.

1.3 The following format provided in this Annex shall be used for submission.

1.4 Please provide explanatory notes under "Tenderer Remarks" whenever possible.

Compliance Definition

Statement of Compliance	Definition
'Compliance' or 'C'	When the System or Service meets all Specifications / requirements without any customization / modification to the standard software (i.e. via configuration). The Tenderer shall NOT add any explanatory notes against the clause that vary the meaning of full compliance to the clause and such notes provided (if any) shall be ignored.
Partial Compliance' or 'PC'	When the System or Service is able to comply with the Specifications / requirements by means of customization / modification to the standard software (i.e. not via configuration) or by adding third party software. The Tenderer must provide condensed but complete information on the customization involved or the third party software proposed, including any integration efforts required and additional charges involved.
'Non-Compliance' or 'NC'	When the System or Service does not comply with the Specifications / requirements.

Document Information

File Name: Annex D3 - HR Functional Requirements

			Statement of Compliance			
L1#	**L1**	**Total no. of Requirements**	**C**	**PC**	**NC**	***Tenderer Completion Status***
OHR 1.0	Recruitment and Onboarding	103	0	0	0	*0%*
OHR 2.0	Personnel Administration	108	0	0	0	*0%*
OHR 3.0	Compensation and Benefits	105	0	0	0	*0%*
OHR 4.0	Appraisal	67	0	0	0	*0%*
OHR 5.0	Training	77	0	0	0	*0%*
OHR 6.0	Payroll	92	0	0	0	*0%*
OHR 7.0	Workforce Planning and Succession Planning	23	0	0	0	*0%*
		575	**0**	**0**	**0**	

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.001	The system should support Mobile features and must support Android and iOS devices. Features must be the same for both IOS and Android devices.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.002	The system should allow Reports to be exported to different formats and in printer friendly format(e.g. excel, pdf etc). Note: Excel is a must.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.003	The system should show Audit Trail to track any changes made to the system as well as the changes made to the Transactions.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.004	The system should allow to migrate data from legacy HR platform such as HRIQ.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.005	The system should allow administrator to configure the delegation authority in the Recruitment processes. E.g. HR can delegate the approval authority to a specified person for a period of time or permanently.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.006	The system should auto default the approvers based on the defined reporting hierarchy in the organization chart.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.007	The system should allow to configure automatic email for notifying relevant parties for changes, or onboarding details for new hire.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.008	The system should allow to configure automatic email for approvers at various stages in the process e.g. reminders of pending actionable items and approvals, acknowledgement of receipt of application.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.009	The system should allow Administratorr to update and track the candidate and status of the offer in the system (e.g. Extended, Cancelled, Rescinded, In Negotiation etc.)	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.010	The system should allow applicants/hiring manager to track the status of their applications.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.011	The system should allow Recruiters/Hiring Managers to click on a hyperlink in an email, portal or other environments outside application and navigate directly back to the system	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.012	The system should create an external career page that can be linked to a corporate career website that displays the list of open jobs (posted requisitions), and allows candidates to access the Recruitment page to view the job description and requirements for each of the open jobs. Interested applicants will create an account like in Careers@Gov and thereafter apply for the particular job	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.013	The system should be able to capture tracking of job advertisements, offers, acceptance, average time from job advert placed to actual start date (by staff type, Job Levels) for reporting and analysis purposes over different time frame eg. 1 yr, 3 yrs, 5 yrs, 10 yrs.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.014	The system should allow the review of the generated letters e.g. Offer, contract renewal, confirmation letters	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.015	The system should have preconfigured dashboards and reports on: - Show the approved positions - Track budgeted/approved headcount vs total staff (including short term Contractors) - Visibility on the candidate pipeline and status of recruitment and onboarding progress - Identify sourcing effectiveness based on historical data (e.g. hit rate of similar jobs across sourcing channels based on defined critiera like time period, job levels, etc.) - List of onboarding task/activities to be completed by new employees before confirmation (various eLearning programs such as PDPA, personnel declaration)	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.016	The system should have configurable message templates and email templates.	Mandatory		
OHR 1.0	Recruitment and Onboarding	Generic	Generic	RCM.017	The system should have ability for administrator to retract the onboarding steps in the case of exceptions where Manager has filled in the wrong information and would like to re-update	Optional		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.018	The system should allow Hiring manager to submit the manpower requisition for different types of hires, e.g., relief/temp, contract, perm etc.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.019	The system should be configurable to have a flexible recruitment process that allows to include/exclude certain stages during the recruitment process for different candidate types e.g., Teaching, Corporate, Relief/Temp staff. Note: For dance, music and acad staff, there is an additional audition step and the interview assessment form is typically completed only when audition is completed.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.020	The system should support requisition creation by copying or duplicating an existing requisition.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.021	The system should allow Administrator to auto close job posting once position is filled or past an expiry date.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.022	The system should capture the list of different sources of recruitment platforms available.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.023	The system should allow Hiring manager to prepare, make any necessary amendments before jobs are posted, and post the jobs on corporate website.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1	Raise MRF and Post Job	RCM.024	The system should allow requisition to be routed for approval	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.025	The system should allow Approved requisition to be routed to Administrator for actions	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.026	The system should allow to manage Requisitions to be put on hold, to be re-activated after being put on hold, to be cancelled	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.027	The system should allow Hiring Managers/Administrator to reopen a requisition previously filled or cancelled	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.028	The system should allow Hiring Manager and Administrator to set start and end date of job posting.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.029	The system should support unposting Requisitions from job site.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.030	The system should pre-populate the requisition form with the position and/or job information based on the selected position or job (e.g. position title, department, FTE, Perm/Contract/Temp status etc)	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.031	The system should provide various status to be set and updated for a candidate (i.e., schedule for 1st interview, schedule for 2nd interview, Reject, Interview scheduled, Offer, etc).	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.032	The system should show Open/Pending manpower requisition that they own.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.033	The system should show Time-to-fill (requisition posted vs candidate hired).	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.034	The system should allow Administrator to view and track the status of all recruitment activities.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.1, 1.2	Raise MRF and Post Job	RCM.035	The system should be able to check whether the requisition is for a budgeted position and within the approved manpower budget. If requisition is beyond approved manpower budget or unbudgeted, system will route for additional approvals	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.036	The system should allow administrator to setup screening tests or test questions for candidates.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.037	The system should allow users to maintain questionnaire for written test used for selection of candidate. It should also allow candidates to upload the document if it was done outside the system.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.038	The system should allow for different screening workflows with different levels of approvers to shortlist, interview, and select the candidates for different employee types e.g. Corporate, Teaching. Note: For Corporate -> RO/HOD screens candidate and interview session is arranged For Teaching -> RO/HOD screens candidate, followed by VP and Principal and interview session is arranged	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.039	The system should allow Hiring Managers to view comments/remarks by HR and also should add in their own remarks as they screen the candidate file Note: For Corporate -> RO/HOD screens candidate and interview session is arranged For Teaching -> RO/HOD screens candidate, followed by VP and Principal and interview session is arranged	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.040	The system should support recruiters/Hiring Managers to search and shortlist candidates based on specific key words (key word search in resume)	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.041	The system should support recruiters/Hiring Managers to view resume of multiple candidates (by clicking next) on screen without downloading it as pdf or word doc	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.042	The system should allow Hiring Managers/ Administrators to review and update status of candidates (shortlist, pending, not suitable etc.) with remarks field for evaluation or comments on applicants.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.043	The system should allow Hiring Managers to view all requisitions that they own as well as candidates associated and candidate progress	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.044	The system should show Pending interview assessment forms that they own.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.045	The system should allow Administrator to create interview assessment form templates in the system for interviewers to complete. System shall allow interviewers to capture their assessment of the candidate	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.046	The system should allow Interviewers to complete interview assessment form for candidates after the interview. Note: For dance, music and acad staff, the interview assessment form is typically completed after the audition is completed. The audition is scheduled after interview is completed.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.047	The system should allow option for Administrator to send emails to unsuccessful candidates (candidates who were interviewed but not selected).	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.048	The system should allow online interview assessment form for interviewers to complete, available in mobile interface for mobile devices.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.049	The system should support recommendations proposing the best profile match for talent search within applicants profiles.	Optional		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.050	The system should allow Single/Multiple/All resumes can be selected to be forwarded to Hiring Manager(s) for review.	Optional		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.051	The system should allow other users (reviewers) other than Hiring manager access to the resumes. The resumes should also be able to be sent to large group of "interviewers". E.g. faculty in school can have access to view the resumes of candidates of the same discipline area, etc.	Optional		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.052	The system should allow Hiring Managers to view scheduled interview of the candidates.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.053	The system should Integrate with Outlook/Google calendar and thus allowing Administrator to schedule interview base on hiring manager availability.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.054	The system should allow to configure automatic email such that once interview is scheduled (status change in system), email shall be issued to interviewers with a link for viewing the profile of the candidate.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.055	The system should send email to selected candidates to confirm interview date and time arrangements with hyperlink to online application form.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.056	The system should allow fo HR to schedule second interview session for certain departments and audition for dance, music, and acad staff.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.057	The system should allow Hiring Managers to view the previous comments e.g. For Teaching, VP should be able to view RO/HOD comments and decision, P should be able to view all (VP and RO/HOD comments and decision) for screening. This applies for interview assessment form.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.3	Shortlist, Interview and Selection	RCM.058	The system should be able to flag candidates who have previously applied for the same position. This should appear in the current application for RO/HOD, VP and Principal to take note.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.059	The system should provide job offer template (e.g. different offer fields, content) for different group of employees to be sent to candidates. E.g. Some offer fields are only specific to a particular group of employees e.g. Contract, Perm, Teaching, Corporate	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.060	The system should allow multiple level of approval routing for salary proposal and terms Note: HR sent proposal to HR Manager for signoff before routing to Director and Principal for approval of offer	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.061	The system should allow Information about the candidate to be copied over to the employee record when hired in the system.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.062	The system should allow administrator to create different employment letter templates in the system for different job level/appointment (permanent/casuals/adjuncts/key personnel appointment).	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.063	The system should allow HR Administrator /Hiring Manager to perform salary proposal.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.064	The system should allow Salary proposal template to be configurable, with different fields for different groups of employees, where applicable.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.065	The system should allow salary proposal conditions to be set for the following area, not limited to the list below: - monthly pay (with auto-calculation of annualised base salary) - annualised allowances - bonus Note: Remuneration packages for Teaching are different from Corporate Staff and Adjuncts.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.066	The system should allow Administrator to prepare employment letter via the system and route for approval. The approval will depends on the type of employee groups. The system should enable upload of PDF signed copies that the candidate shares over email.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.067	The system should allow employment letters to be pre-populated with relevant information whilst allowing for editing before sending to candidates. Note: only HR can send offers.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.068	The system should allow to make offer changes even after candidate accepts the offer. Note: only for non-fundamental changes such as change in start date.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.069	The system should allow flexibility in terms of re-routing of approving authority. Scenarios: 1. To handle re-routing of approval for existing requests to another approver in the event the designated approver is away (e.g. on leave). 2. To allow substitution of approval. Approver assign another user as approver prior to be away.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.070	The system should allow to restrict access to offer compensation, for e.g. based on seniority of HR team member/ role assigned to manage compensation. Note: System access may need to be restricted to based on the administrator's access. E.g. Only those given access to compensation module will be able to view. School Admin A can prepare requisition but not offer and vice versa.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.071	The system should have the functionality to set up templates to send the initial email offer to candidate and to request for additional documents Note: System-generated email offer + request for additional documents	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.072	The system should allow to maintain reference check questionnaire templates used for reference check.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.073	The system should allow HR users to capture the status after the employment check/reference check is completed. Information such as status, date completed, comments.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.074	The system should allow Managers to view details of the reference check results as part of the salary proposal review. Note: Managers include Director and Principal	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.4	Salary Proposal and Pre-boarding	RCM.075	The system should allow HR to capture the background screening status and medical checks status for the candidates. The system should also allow uploading the background screening/medical screening report to the candidate profile.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.076	The system should allow Reports to be generated that enables tracking completion of onboarding activities etc and completion status at a consolidated and individual level.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.077	The system should allow Administrator to configure notification to the relevant parties (to activate access card, print cubicle tag, medical insurance etc) x days before employee's start date, either via interface to our other system or email.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.078	The system should trigger onboarding process when candidate accepts the offer. Note: Onboarding activities comprises of requesting for network/email account, adding to distribution list, request for new laptop, room, access to systems, etc. Agents in the process involves parties from different departments (e.g. IT (OTM), Property Management (OPM), etc.)	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.079	The system should trigger a weekly new hire report to relevant departments/teams to inform them of the new hire.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.080	The system should allow the administrator to configure different email communication and checklist for onboarding, based on employee type, e.g., direct hire, relief teacher, seconded staff, including adjunct teachers (who are on contract for service). E.g. To inform new employees on their 1st day/ 1st week on the various e-Learning compliance programs and activities e.g. Code of Conduct, etc. that they need to complete.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.081	The system should allow attachment of supporting documents provided by the new hire and shall be automatically integrated to employee profile Example: payroll advice form, dependant enrolment form, birthcert, marriage cert, name preference form	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.082	The system should allow employee self-service to provide data for setting up their records e.g. bank account, dependants information, address, emergency details	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.083	The system should trigger conflict of interest, code of conduct declaration, etc upon start work.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.5	Onboarding	RCM.084	The system should provide the setup of guided process for new hire, i.e. a checklist/declaration/learning journey that the new hires will have to go through/complete.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.085	The system should allow HR/Hiring Manager to send job posting links to invite potential candidates.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.086	The system should allow Administrator to block applicant from applying for the same job more than once.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.087	The system should allow Administrator to allow applicants to submit for multiple jobs.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.088	The system should allow applicants to filter and browse for suitable jobs.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.089	The system should allow interested applicants to submit their online application/upload resumes, attach photo or other supporting documents e.g. pdf, word, excel, email etc.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.090	The system should support resume parsing to auto populate fields in the online job application form.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.091	The system should allow Candidate to reset own password in the external career site.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.092	The system should support Candidate to subscribe to email notifications for new jobs posted matching the candidate's profile.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.093	The system should support candidate to view previous job submissions.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.094	The system should track records of applicants who has applied to the company before and/or apply for more than 1 position in the company.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.6	External Candidates Apply	RCM.095	The system should allow administrator to setup separate data flow in the recruitment process. 1st flow: Candidate provide basic information when they apply for the job. 2nd flow, If the candidate has been shortlisted, they will need to provide supplementary information such as personal data (NRIC, marital status, etc).	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.096	The system should allow Administrator to select data to delete/purge data after x number of years. Note: MOM policy indicates data needs to be purged 6 months after unsuccessful application.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.097	The system should show Candidates in different stages of the Recruitment Process	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.098	The system should allow when creating the candidate application form, to provide the candidate an option to indicate if he/she wants to be considered for other position and if they want to remove access for other recruiters to see their candidate profile.	Optional		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.099	The system should allow Hiring Managers and HR to view candidates info (exp, education, profile summary) including resume. HR users should be able to view all candidates, access rights to be restricted to the different staff types.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.100	The system should support search features within applicants profiles (eg qualifications, skills)	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.101	The system should have report to show: - Number of applicants by positions - Number of shortlisted applicants by positions - Number of applicants interviewed by positions - Show candidates based on criteria such as Job profile, education, skills,etc. - Different stages/status captured in the system	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.7	Manage Candidate Pool	RCM.102	The system should allow the administrator to blacklist candidates.	Mandatory		
OHR 1.0	Recruitment and Onboarding	OHR 1.9	Rescind Offer	RCM.103	The system should allow the administrator to rescind the offer and disposition candidate for candidates whose onboarding has started but will not be joining the organization.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	Generic	Generic	PER.001	The system should allow auto-notification to parties to alert on upcoming confirmation/probation end date/contract renewal date. Notification should triggered x days before the end date.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.002	The system should have ability to create and store electronic personnel files	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.003	The system should have ability to store and maintain different types of employee documents. The document types should be maintainable by HR Admin	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.004	The system should be able to provide different access rights to different users to store/maintain/retrieve employee documents	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.005	The system should have ability to designate different employee types (e.g. Teaching, Corporate, Adjunct, Casuals, etc.)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.006	The system should have ability to track history for employees who are transferred from one employee type to another and show the various Employee ID useds by the employee	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.007	The system should allow HR to capture employee's personal particulars, which include but not limited to: a. Name: Name as per National ID/Passport, First Name, Middle Name, Last Name, business name, preferred name, legal name, full-name. Each name field to be at least 100-char in length. b. National ID: National ID Number, Date of Issue c. Date of Birth d. Place of Birth: City/Country e. Gender f. Addresses: more than one address can be captured and can to cater for different address formats by country g. Phone numbers: more than one phone number can be captured, e.g. Mobile, Home, Work h. Email Address I. Nationality j. Multiple Citizenships k. Employment Visa information: Employment Pass, Work Permit (history, current) l. Marital Status and Effective Date (history, current) m. Photo n. Highest Education Level achieved o. Passport: Passport Number, Name in Passport, Issuing Authority/Country, Date of Issue , Expiry Date (history and current information of more than one passport can be captured) p. Educational Qualifications: more than one educational qualification can be captured (e.g. description of qualification achieved, name of education institution, majors, GPA, grades, start/end year of studies) q. Professional Qualifications: (e.g. PGDE or PGCE, CPA, PMP) r. Scholarships and Awards received: Name of Scholarship, Scholarship Period (Start/End Dates), Name of Award, Date Awarded	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.008	The system should have ability to capture employee's bank details by HR: a. Bank code b. Branch Code c. Bank Account Number d. Name as per Bank Account Additional information for international staff i.e. Routing Number, Swift Code and Country	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.009	The system should provide allow employees to update their employee details via employee self-service and have separate workflows where certain updates are automatically route to HR for verification	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.010	The system should have ability to keep and maintain records of non-employees such as adjuncts and casuals Note: Adjuncts/Casuals may possess certain perquisites, access to timesheet module and payslips.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.011	The system should have ability to track various dates (e.g. actual join date and conversion date of contract/adjunct staff) for various purposes (e.g. Long Service Awards, etc.)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.012	The system should to capture the start/end of scholarship/ Sponsorship/Post Graduate Award/PGCEi programme, bond duration, University of Scholarship, Faculty etc.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.013	The system should have allow HR admin to capture employee's job information (history, current and future) of multiple jobs, which include but not limited to: a. Effective Date b. Employee Status: Active, Inactive, NPL, On Assignment, etc. c. Job status d. 3 date types - Join Group Date, Company Join Date and Service Reference Date e. Job Title f. Employee Category (Management & Support) g. Employment Type (Permanent, Contract) h. Full Time/Part Time i. Cost Centre j. Entity k. Department m. Work Location n. Supervisor o. Recruitment Source p. Reason for leaving q. Skill pool r. Cohort tagging	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.014	The system should allow HR admin to capture employee's academic appointment details such as School, Title, Track, Discipline Area, Discipline Sub Area, appointment start and end date, tenure status	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.015	The system should be able to reflect the relevant changes in relation to the event/action that has taken place Example: 1) The event recorded is "Key Personnel Appointment (Appointed)" - The system should reflect an overview of what were updated/changed due to this particular action a) Appointment information including track, rank, title, appointment start/end date, etc. b) Salary related information c) Tenured Date	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.016	The system should have ability to retain/access/maintain employee history from the hire date irrespective of how many times the employee resigned and rehired	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.017	The system should be able to cater to the data retention period for different set of information.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.018	The system should allow HR Admin to capture degree major as part of education history	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	Generic	Generic	PER.019	The system should have ability to capture details of employee contract information. The contract information should capture all valid contracts including renewal and new contract	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.020	The system should have ability to mass update employee employment events (e.g. organization change, promotion, transfer, etc.) by HR admin	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.021	The system should have ability to send automatic notifications (including reminders) of employment events such as probation confirmation, contract end (including Adjunct and Casual), completion bonus, re-employment and etc. to RO/HOD, HR	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.022	The system should support a workflow for the generated letter: (a) review by the approving authority (b) acceptance by the employee e.g. contract renewal, promotion Note: Different approval workflow for various types of data change 1. Salary Proposal: HR prepares salary proposal, Director review and approve, Principal review and approve 2. Letter: HR prepare letter, Director review and sign	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.023	The system should allow setup and maintenance of Job Grades (history, current and future) by HR	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.024	The system should allow HR admin to record the type of disciplinary action taken along with any comments (i.e., written warning, verbal warning, termination, etc.) and attach supporting documents	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.025	The system should allow HR admin to capture employee's employment events and event reasons (history, current and future), which include but not limited to: a. Hire b. Rehire c. Start of Probation d. End of Probation/Confirmation e. Start of Contract f. Contract Extension g. Contract Completion h. Entity Change (entity=company=legal entity) l. Department Change k. Work Location Change l. Job Change m. Employee Type Change n. Full Time/Part Time Change o. Direct Reporting Manager Change p. No pay leave q. Return from No pay leave r. Promotion s. Separation – Employee Initiated (Resignation) t. Separation – Employer Initiated (Retirement/Termination/Dismissal) u. Transfer v.Type of review for rehire (purpose of rehiring) w. Sabbatical leave period x. Maternity leave period	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.026	The system should allow HR admin to review and approve the information that has been updated by the employee (after checking the required supporting documents). Information includes but not limited to: a. Bank Account Information b. Language known and proficiency level c. Passport Information d. Dependent Information e. Corporate Photo f. Education Certificates	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.027	The system should allow HR admin to enable effective/future dating of pending transactions/events, and maintain transaction history	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.028	The system should have ability to capture multiple actions on the same day (e.g. promotion, increment - need for multiple actions by row, not by column)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.029	The system should have ability to add/maintain/configure business rules and email templates to auto-trigger emails to parties concerned regarding internal transfer, no pay leave, assignment, secondment, etc.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.030	The system should have ability to transfer all employee data (e.g. leave, payroll, etc.) if there is a secondment/transfer that takes place	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.031	The system should have ability to migrate all employee data into new system Note: all historical data should be migrated to the new system. This is especially important for faculty who on a normal employment trend would minimally have three employment records dating back to 8-10 years.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.032	The system should have ability to purge employee records through criteria selection	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.033	The system should be able to capture the following information: - Annual Increment (AI), Performance Bonus (PB) eligibility - AVC eligibility (9 months or 12 months scheme) - benefits related information (medical plan, flex benefit, pension) - indicator to identify re-employed case - hi-potential	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.034	The system should be able to capture the following information: - awards received (e.g. LSA, PGA, etc.) - Tax clearance information upon separation for foreigner - Cessation information (official last day, physical last day) to faciliate cessation notice to agents - company that issued the employment pass (i.e. applicable only to those holding EP that was issued by another company)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.035	The system should be able to capture the following information for adjuncts: - contractual information (contract appointment start/end date, school, title, track, type of contract, assignment information (assignment start/end date, course to be taught, number of section), payment information (contract amount, payment frequency, payment start/end date)	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	Generic	Generic	PER.036	The system should have a staff profile page capturing personal/contractual information. It should have the flexibility to identify which are the editable/non-editable fields for users to update. Note: Employee Dashboard - Staff will have their own "CV" page which will reflect personal and career information ON themselves. Personal information will allow self updates but to be approved by HR after supporting documents are also uploaded. Career Information such as Job Grade, Job Title, Join Date, Progression ad etc are reflected for Staff's information. Any changes required can only be made at HR level.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.037	The system should allow different employee type with employment events and event reasons to be maintained under the same employee record without affecting payroll	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.038	The system should allow managers to use Manager Self Service (MSS) to view their Direct/*Indirect Reporting employees' Job information such as: a. Employee Status: Active, Inactive, NPL, On Assignment, PDDL, etc. b. Join Group Date/ Join Company Date c. Job Title d. Work Location *Managers with dual/matrix reporting / Co-heads	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.039	The system should allow employees to upload supporting documents in relation to updating of their Personal Information, which include but not limited to: a. Addresses (Home) b. Phone numbers (Home, Mobile) c. Bank Account Information d. Language known and proficiency level e. Passport Information f. Emergency Contact Information g. Dependent Information h. Corporate Photo I. Education details including university courses and certificates (e.g. ACCA) m. Life events (e.g. marriage certificate, birth certificate of dependents, etc.)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.040	The system should have ability to add/remove accesses for managers on one or more MSS as appropriate. Additionally, system must allow managers or HR to assign proxy for specific MSS (e.g., leave/training approval).	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.041	The system should have ability to perform calculations within reports such as Turnover and Retention rates for a specific time interval	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.042	The system should allow HR Admin to generate Manpower report at aggregate level (including headcount, nationality) with selection criteria of Cost Center, Job Title and Employment Type (i.e. perm, contract, partner)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.043	The system should allow HR admin to run multi-dimensional reports filtered by specific dimensions available in the HR database. Some example reports include, but not limited to: a. Headcount b. Staff Movement c. Long Service Award d. Staff Profile Card e. Skill pool f. Latest Career Data g. Employee Listing	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.044	The system should also have the flexibility to extend appropriate reports to non-HR users, i.e. RO, CO, HOD, VP and Principals.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.045	The system should have ability to auto calculate the service reference date based on a pre designated criteria. It should also allow for overwriting for exception cases (such as rehire cases etc.)	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.046	The system should have the ability to auto calculate Years in Service and No Paid School Holidays based on a pre-designated criteria. E.g. Long Service Award is determined based on Years in Service of milestone of every 5 years. System needs to determine the join date, current date, NPL for current year and NPL as of November. If total NPL is more than 11 working days, NPL taken will be deducted from Years in Service.	Optional		
OHR 2.0	Personnel Administration	Generic	Generic	PER.047	The system should be able to record relationship and interface with Benefits module	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.048	The system should be able to keep a record of eligibility for the employees' immediate family members and dependents, for e.g. if they have dependents, Childcare Leave, Extended Childcare Leave and Family Care Leave based on dependents' age. Parent Care Leave based on parent and parent-in-law relationship	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.049	The system should allow HR users to generate report on employees' reporting structure. Fields include staff name, department, cost center, Reporting Officer (RO), Countersigning Officer (CO), VP, Director, Principal. If there is any exception assigned for specific module, the report will reflect accordingly.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.050	The system should allow HR users to generate report on the different roles assigned to employees. Fields include staff name, department, cost center, Role A: Head of Department, Senior Leaders, etc	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.051	The system should allow users to run a report to identify faculty who may be up for review and reappointment for Key Personnel Appointment.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.052	The system should be able to generate a report listing on transferess (change in cost center) and schedule jobs (e.g. monthly basis) to send to designated internal/external stakeholders (e.g. Osending and Receive Faculty, etc) The report should includes fields such as employee ID, name, cost center, date of transfer, etc.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.053	The system should be able to generate a report listing on leavers and schedule jobs (e.g. monthly basis) to send to designated internal/external stakeholders (e.g. Office of Registrar, Office of Finance, etc) The report should includes fields such as employee ID, name, cost center, date of leaving, etc.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	Generic	Generic	PER.054	The system should allow HR Admin to generate a detailed CV by person with data from system, where the staff profile can be configurable to what is being shown	Optional		
OHR 2.0	Personnel Administration	Generic	Generic	PER.055	The system should have ability to capture Home and Host Cost Centre for assignees/transfers/secondments	Optional		
OHR 2.0	Personnel Administration	Generic	Generic	PER.056	The system should have ability to set up groups e.g. IT, HR for the onboarding/offboarding tasks to be routed to a group where anyone can pick up for action.	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.057	The system should allow employees to generate letter of certification of employment from their personal data, based on a standard approved template	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.058	The system should allow past work experience to be differentiated into directly relevant experience and indirectly relevant experience, as well as, on full-time and part-time or freelance basis	Mandatory		
OHR 2.0	Personnel Administration	Generic	Generic	PER.059	The system should have ability for administrator to retract the onboarding steps in the case of exceptions where Manager has filled in the wrong information and would like to re-update	Optional		
OHR 2.0	Personnel Administration	2.3, 2.7, 2.8	Appointment of Key Personnel, Re-employment, Contract Management	PER.060	The system should be able to generate a report listing on contract staff/key personnel appointment/staff who are nearing retirement age and schedule jobs (e.g. monthly basis) to send to designated internal/external stakeholders (e.g. Office of Finance, etc) The report should includes fields such as employee ID, name, cost center, contract start/end date, etc.	Mandatory		
OHR 2.0	Personnel Administration	2.3, 2.7, 2.8	Appointment of Key Personnel, Re-employment, Contract Management	PER.061	The system should have the ability to generate a promotion/appointment letter	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.062	The system should have ability to send electronic notification of resignations to all relevant parties using Workflow Engine Note: This should only be triggered when the resignation has been accepted by RO/HOD	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.063	The system should have ability to generate Letter of Termination upon confirmation of voluntary exit, with ability to customise fields based on different business unit / entity requirements	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.064	The system should have the ability to trigger exit survey to the resigning employee to complete and it should send reminders to prompt the employee prior the last day of service. The system should allow the HR admin to record the feedback from the exit interview conducted with the employee.	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.065	The system should capture the exit interview outcome. It should allow the HR administrator to capture the leaving reason category and allow multiple reasons to be recorded. E.g. leaving reason category is resignation. High workload, poor leadership as reasons.	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.066	The system should have ability for administrator to report on exit interview content and status	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.067	The system should have ability to track termination by reasons along with effective date, last day worked, rehire eligibility (whether to blacklist terminated employee or not)	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.068	The system should have ability to cancel or block employee benefits upon termination	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.069	The system should have ability for HR Admin to blacklist employees from rehire	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.070	The system should have ability to notify downstreams systems upon termination of employees	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.071	The system should send out a batch cessation notice to a predefined users (e.g. IT, etc.) with the list of leavers and their last day of service.	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.072	The system should have ability to provide employee with prorated leave calculation (based on last day work)	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.073	The system should auto compute the final pay for the resigned employees, renewal and conversion inlcuding leave encashment, AWS, AVC, Completion Bonus, etc. System should pro-rate the pay components as required.	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.074	The system should auto compute the consumed amount for carpark allowance and remaining balance to be updated back as Flexible Benefits. Note: Carpark allowance is consumed for a full year as part of Flexible Benefits. Upon resignation, the actual amount consumed will be determined and reimbursed back to the staff's Flexible Benefits balance.	Optional		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.075	The system should inform predefined users when the retraction happens. E.g. IT or relevant system agents need to be informed and undo their previous termination actions	Mandatory		
OHR 2.0	Personnel Administration	2.5, 2.12	Offboarding, Cancel Offboarding	PER.076	The system should allow administrator to rescind offboarding actions for scenarios where employee retract the resignation in the midst of offboarding	Mandatory		
OHR 2.0	Personnel Administration	2.5	Offboarding	PER.077	The system should trigger notification to required stakeholders to follow up for any items and amounts to be paid to / recovered from employee x days before employee's resign (last day) date, e.g., annual leave encashment, employee voucher, sign-on bonus, training bond, counter offer bond, early termination fees for service contracts, benefits-in-kind.	Mandatory		
OHR 2.0	Personnel Administration	2.4, 2.5, 2.8	Probation, Offboarding, Contract Management	PER.078	The system should have separate approval workflows to review and approve probation, offboarding, re-employment, and contract management. 1. Probation Confirmation: RO approve > CO approve 2. Extend/Terminate Probation: RO extend/terminate > Director extend terminate 3. Offboarding: Staff submit resignation > RO review and approve 4. Re-employment: RO indicate decision to re-employ> HR processes the decision > Salary Proposal (for change in job scope) > Prepare Contract 4. Contract Management: VP indicate decision to extend > Director indicate decision to extend	Mandatory		
OHR 2.0	Personnel Administration	2.6, 2.9	Change in Workload Request, Request for External Engagements	PER.079	The system should have ability for administrator to create various forms to request and separate workflow approvals. These include: 1. Change in Workload Request 2. Request for External Engagements Note: The requestor should have ability to attach supporting documents as part of the request.	Optional		
OHR 2.0	Personnel Administration	2.6, 2.9	Change in Workload Request, Request for External Engagements	PER.080	The system should enable user to track status of the forms for Change in Workload Request and Request for External Engagements. E.g., Status of the application as Approved, Pending approval etc.	Optional		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	2.7	Re-employment	PER.081	The system should send notification to RO and HR in advance on employees reaching retirement age and have the flexibility to set the parameters on how advance the notification should be sent. E.g. notification is send 6 months prior to them reaching the retirement age. Note: HR willl follow up with employees/HOD on their next course of action. HR can use the data to identify future cases to take into consideration during contract renewal, etc.	Mandatory		
OHR 2.0	Personnel Administration	2.7	Re-employment	PER.082	The system should be able to compute the date where the employee reaches his retirement age. This information should be made available in the employee profile. The rule to generate retirement date for retirement age follows the statutory requirement. The system should allow users to generate a report retrieving the list of employees reaching their retirement age e.g. in Year 2045	Mandatory		
OHR 2.0	Personnel Administration	2.7	Re-employment	PER.083	The system should have ability to track that the employee is in the second case of re-employment and above. If so, there are additional steps to send the employee for medical check-up and update the medical check status.	Mandatory		
OHR 2.0	Personnel Administration	2.8	Contract Management	PER.084	The system should be able to generate employment letter for contract staff with or without salary adjustments and incorporate past salaries up to 1 year	Mandatory		
OHR 2.0	Personnel Administration	2.8	Contract Management	PER.085	The system should have ability to trigger a new employee contract generation before completion of current contract. The new contract should have linkage to previous contracts.	Mandatory		
OHR 2.0	Personnel Administration	2.8	Contract Management	PER.086	The system should have ability to capture contract status i.e. contract offer to employees and system track the status, and upon acceptance of contract, the system will create the necessary changes	Mandatory		
OHR 2.0	Personnel Administration	2.9	Request for External Engagement	PER.087	The system should be able to track the past total compensation of external engagements the staff has engaged in for the past academic Financial Year and flag if the total sum is equal to or more than 3 months of the staff's compensation. This information should be shown to VP during the review to approve the External Engagement.	Optional		
OHR 2.0	Personnel Administration	2.9	Request for External Engagement	PER.088	The system should be able to send notifications to inform on the updates in Request for External Engagement. E.g., changes in status like approval by VP, Director and Principal	Optional		
OHR 2.0	Personnel Administration	2.9	Request for External Engagement	PER.089	The system should be able to prompt additional fields when the submission of request for external engagements is lesser than 1 month.	Optional		
OHR 2.0	Personnel Administration	2.10, 2.11	Conflict of Interest Declaration, Overseas Travel Declaration	PER.090	The system should have ability for employees to submit Conflict of Interest Declaration form as part of the annual exercise and Overseas Travel Declaration Form. Note: Overseas travel declaration form should have the following fields: - Full Name, Department, Staff Group, Period, Travel to, Cities	Optional		
OHR 2.0	Personnel Administration	2.10, 2.11	Conflict of Interest Declaration, Overseas Travel Declaration	PER.091	The system should have relevant reports/dashboard that HR can leverage to report on completion status and analysis to report to School Leaders on Conflict of Interest and Overseas Travel Declaration.	Optional		
OHR 2.0	Personnel Administration	2.13	Positions Management	PER.092	The system should have ability to capture position information within the organization such as competencies, location, grades, job codes, etc related to the job (e.g. The position of team lead may be vacant but will have the attributes of location, competencies, skills, grades and job information. Attributes will differ from the type of employee type). When an employee is hired into the position, he/she will automatically inherit the attributes assigned to the vacant position. Faculty: info such as academic title, rank, track, discipline area, discipline sub-area Admin: Job title, business title.	Mandatory		
OHR 2.0	Personnel Administration	2.13	Positions Management	PER.093	The system should have ability to inherit the position attributes automatically when the incumbent is assigned to the position in the system.	Mandatory		
OHR 2.0	Personnel Administration	2.13	Positions Management	PER.094	The system should have ability to integrate position management with other modules such as competency, performance management and training modules.	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.095	The system should have ability to create different types of organisation relationships & dual reporting relationships including solid line, matrix, dotted line. Note: This ability caters to the scenario where employee is concurrently taking up 2 positions with separate reporting line (e.g. teacher taking up additional responsibilities as Year Mentor and directly reporting into Dean instead of Head of Literature in English, etc.)	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.096	The system should have ability to add and display staff officer on the org chart by HR User.	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.097	The system should have ability to maintain academic unit structure in addition to the main organisation structures.	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.098	The system should have ability to add / change organisation entities and easily transfers employees within and/or across entities (e.g. Faculty).	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.099	The system should allown HR User and managers to export organisation chart (option of including or excluding vacancies) at different levels (option of including direct and indirect reports) in different formats such as excel, pdf, ppt, word.	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.100	The system should allow different reporting structure to faciliate process workflow (i.e. some process that may require multiple level approval, some with 1 level of approval). Example: Leave Application with/without HR approval (RO, HR) Artistic Development Leave (Dean, VP) PPDL (RO/HOD, Dean, VP, P) Perf Appraisal (RO, CO, Schoolwide Review) Training (RO)	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.101	The system should have ability to allow HR user to mass create/update of organization unit, position for re-organisation, merger, or acquisition.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.102	The system should have ability to track budgeted headcount, actual staff and vacant by organisation entities, and by employment type (Permanent, Temporary, Contract) on organisation chart. Example: Corporate: by staff type, job level Teaching: total headacount per school, budget based on norms by track and rank Contract staff: contract staff split by long-term (1 year & above) + short term (3 mths to 12 mths; less than 3 mths). Include reporting/ dashboard to tie in with recruitment stats.	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.103	The system should have ability for real-time display on changes to org. structure based on the employee database (for each employee: full name, job titles, multi line reporting, and photo to be displayed in the org chart).	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.104	The system should allow users to have the flexibility to generate reports using the position/job attributes and employee data captured. E.g. Number of permanent position by job level (Occupied vs Vacant).	Mandatory		
OHR 2.0	Personnel Administration	2.14	Organization Structure	PER.105	The system should allow administrator to adopt a hybrid approach of Jobs and Position management to handle different workforce. E.g. Permanent/Contract employees are hired via Positions Management Adjuncts and Casuals are managed via Jobs as they are typically hired for a temporary or fixed term and forms a pool of workers to tap on.	Mandatory		
OHR 2.0	Personnel Administration	2.15	Maintain Jobs	PER.106	The system should have ability to setup job architecture for Talent Management, including the job catalogue with functional areas, job families, jobs, and positions	Mandatory		
OHR 2.0	Personnel Administration	2.15	Maintain Jobs	PER.107	The system should have ability to store job code and job evaluation information against compensation components	Mandatory		
OHR 2.0	Personnel Administration	2.15	Maintain Jobs	PER.108	The system should allow concurrent employment feature where 2 different packages with 2 job scopes are able to tag to 1 unique employee with accounting of both respective start dates.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.001	The system should be able to track and compute severance payments entitled to employee to receive when they leave employment. The system should also have ability to integrate with offboarding module to obtain information to compute severance payment	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.002	The system should have ability to feed into/from payroll data	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.003	The system should be able to track the frequency of payment of allowance plan - Monthly, semi monthly, one-time payment, quarterly payment. For example: Annual Salary but paid monthly for specific payment period. SGD120,000 per annum but paid over 6 monthly from Jul - Dec	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.004	The system should provide employee and manager self service to view their salary, related payment and view other compensation information such as Job Level /Job Title/Promotion history, etc.	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.005	The system should be able to track payslips for the employees	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.006	The system should be able to track reimbursement for the employee	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.007	The system should be able to maintain compensation structure/range (min/mid/max) for the job requisitions during hiring process	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.008	The system should be able to maintain security access for the compensation details of employees Note: cater to different sets of access (RO/HOD/VP/Principal/Compensation Administrator) It should also all segregation of access within the HR - HR users no access to Compensation data - Compensation Administrator - access to compensation data	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.009	The system should have ability to support roll up of cascading budgets where HR/HOD can set their own compensation budget for base & bonus components and cascade or distribute the remaining budget to the direct reports. HR/Business Head can allocate budgets by a fixed amount or a percentage of the budget pool.	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.010	The system should allow employees to view their benefits via mobile	Mandatory		
OHR 3.0	Compensation and Benefits	Generic	Generic	CNB.011	The system should have ability to setup and compute benefits proration, accural based on respective needs/criteria. Note: There should be reports to reflect the eligiblity and/or entitlement for the different benefits/leave plans.	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.012	The system should be able to track compensation structure/range for specific jobs/position	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.013	The system should track the compensation payment for employee in annual and monthly amount	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.014	The system should track types of allowances - amount based.	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.015	The system should track who is eligible to receive the allowances and track receipient by their eligibility and payout in payroll. The system should capture the following: 1) List of employees who are eligible for the allowances 2) List of employees who are receiving the allowances and amount received Allowances include key personnel (KP) appointment allowance	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.016	The system should be able to track salary ranges for the different groups of employees. E.g. permanent, adjuncts, casuals, teaching and corporate	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.017	The system should track pay for both Salaried and Hourly workforces Note: It should also include adjuncts who are paid on a consultancy fee basis, payment frequency is dependable on duration of the teaching assignment	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.018	The system should have ability to perform department or group level (what-if modelling) for annual compensation increases and see impact on budget by department. This feature should allow the modelling to be downloaded on Excel format. Note: different groups of employees would have different compensation packages	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.019	The system should have ability to display budget summaries including percent of budget utilized	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.020	The system should have ability for managers and authorized users with a compensation worksheet to allocate incentives including bonuses, lump sum, and short term / long term incentives Note: It can be multiple "worksheets" depending on the various exercise and should capture comments (Text Field) too.	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.021	The system should have ability to track salaries; based on department, Entity, and category and function	Mandatory		
OHR 3.0	Compensation and Benefits	3.1	Salary Benchmarking and Budgeting	CNB.022	The system should be able to provide a dashboard for HOD which contains Staff's information and progression for HOD to view. The dashboard should include live information which include salary, bonus, allowances and etc. Note: 1) HOD shld be able to add in some "remarks/notes" for each staff which serves as as reminder to help HOD. 2) HOD shld be able to also see Ratings and Salary charts to help them understand their dept better and help them plan.	Mandatory		
OHR 3.0	Compensation and Benefits	3.2	AWS and AVC	CNB.023	The system should be able to propose one time payment as amount and % payment	Mandatory		
OHR 3.0	Compensation and Benefits	3.2	AWS and AVC	CNB.024	The system should have ability to manage variable compensation Note: If there are any changes in workload or job grade, adjustments are needed. No Pay Leave will also affect the computation.	Mandatory		
OHR 3.0	Compensation and Benefits	3.2	AWS and AVC	CNB.025	The system should be able to generate pay change letter for the employee	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.026	The system should have ability to handle employees with multiple pay rates and department/cost centre assignments	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.027	The system should have ability to define several types of salary increases (merit, mandated, adjustment etc.)	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.028	The system should interface with the outcome from the promotion nomination exercise. All approved main cycle promotion should be updated in the compensation planning worksheet where the promotion increment % (PI%) can be entered either by the HOD as part of the compensation planning exercise or the Compensation Admin can upload the recommended PI%. The HOD will be able to view the finalised recommendation at the end of the exercise.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.029	The system should be able to identify Promotion cases, reflect it to the users (HODs) and allow allocation of Promotion Increment	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.030	The system should have ability to support upload from Performance Management and automatic calculation as default based on the entity rules Note: The auto calculation shld cater for "different" permutaions/rule for different employee group/type.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.031	The system should have ability to generate compensation package by job level and allow to overwrite fields for HR to input final numbers	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.032	The system should have ability to perform automated pay rate changes for groups of employees (e.g. all employees that perform the same job at the same level can receive the same rate of pay) Note: If there are changes in workload or job grade, adjustments are needed. No Pay Leave will also impact the computation.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.033	The system should have ability to support mass approvals for salary adjustments	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.034	The system should have ability to allocate salary increases by amount or percentage	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.035	The system should be able to do any lump sum payment as part of the annual salary increase process	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.036	The system should have ability to upload annual increment budget by employee	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.037	The system should have ability for leaders to see salary recommendation increases for each of their groups and to see the roll up	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.038	The system should have ability to cap compensation adjustments at maximum or indicate when over maximum	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.039	The system should have ability to warn if increase is outside the guidelines of merit guide chart	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.040	The system should have ability to track salary and promotion increase changes and the recommended salary changes before promotion. Note: This is to cater to employees who receive salary increase and subsequently after that receive a promotion with new increment. The system should track initial salary increase before the promotion increase	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.041	The system should have ability to track unlimited salary change history (e.g. salary/promotion/merit adjustments),	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.042	The system should have ability to automatically enrol employees into bonus plans based on eligibility, and ensure that the enrolment is updated with any changes to eligibilty throughout the year. For example: contract staff on short term contract is being re-appointed to long term contract, they should be eligible for e.g. AI and PB. The current eligibility for gratuity bonus should cease accordingly.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.043	The system should allow manual intervention to adjust the final bonus figure.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.044	The system should have ability to track multiple allowances (such as OT) by department	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.045	The system should have ability to create template for the total reward statement based on the information captured in the Compensation Planning worksheet. Employee should be able to view their statement once the exercise has been finalised and approved by the Management.	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.046	The system should have ability to configure, create and view compensation statements (including compensation changes)	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.047	The system should have ability to push compensation statements/letters to managers and employees to download	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.048	The system should have an approval workflow in place where there are data changes affecting pay/compensation related items	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.049	The system should provide reports Salary Position by job level, Salary movement by job level vs gender, Salary movement for promoted staff year on year Note: There are many reports required on Increments, bonuses, allowance and etc and this reports are required at various "point" in the exercise	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.050	The system should have ability to alert when its time to pay and activate some sort of work flow to payroll	Mandatory		
OHR 3.0	Compensation and Benefits	3.3	Performance Bonus and Annual Increment	CNB.051	The system should have ability to support printing Total Comp letters after increases	Mandatory		
OHR 3.0	Compensation and Benefits	3.4	Gratuity Bonus	CNB.052	The system should be able to trigger notifications to inform HR of employees' last month of service. Note: This applies to contract staff with contract start and end date.	Mandatory		
OHR 3.0	Compensation and Benefits	3.4	Gratuity Bonus	CNB.053	The system should be able to generate letter for Gratuity Bonus and create one-time payment for the staff	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 3.0	Compensation and Benefits	3.5	Birthday Greetings & Voucher	CNB.054	The system should be able to run report for employees whose birthday falls in a certain month E.g. Report is generated in early July for the people whose birthday falls in August.	Mandatory		
OHR 3.0	Compensation and Benefits	3.5	Birthday Greetings & Voucher	CNB.055	The system should prompt RO/HOD, Directors, VP and Principals of staff's upcoming birthday and allow them to write a birthday messsage for the colleague.	Optional		
OHR 3.0	Compensation and Benefits	3.6	Long Service Award	CNB.056	The system should be able to generate letter for Long Service Award awardees and create one-time payment for awardee	Mandatory		
OHR 3.0	Compensation and Benefits	3.6	Long Service Award	CNB.057	The system should be able to run report for employees who are eligible for Long Service Awards for the year (Recognition) Note: Eligibility is determined based on join date and current date. No Pay Leave for the current year is also factored in. If No Pay Leave exceeds 11 working days, NPL is deducted from the Service Years. LSA amount is determined based on milestone of every 5 years.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.058	The system should allow RO to view their subordinates' leave application/history	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.059	The system should allow Administrator to define which leaves can be applied by the employee.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.060	The system should allow Administrator to configure different workflow approval based on the leave types. Key examples include: 1. Artistic Development Leave application will be routed to Dean for approval and VP for approval. Once approved, HR will proceed to set up the leave type for employee to apply. 2. No Pay Leave application form is routed to HOD/RO for approval, followed by DD, VP, Director and Principal (Note: If the requestor is a teacher, the system need to track if the number of days is 1 or more days. This amount will have to be deducted as part of the No Pay School Holiday (NPSH) computation.) 3. PPDL application: HOD/RO will fill up PPDL nomination form with supporting documents attached, SSD will review and route to Dean for approval, followed by VP for approval, and P for approval 4. Sick Leave: No approval is required. Staff just needs to submit leave request with Medical Certificate attached as supporting document. 5. Urgent Private Affairs: Requestor submit request to RO followed by Principal for approval. Supporting documents are required during verification of Urgent Private Affairs by HR.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.061	The system should allow employees to submit the leave in half (AM) / half (PM) / full / in blocks of x days for all leave types.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.062	The system should allow employee to indicate what a half day leave is for - morning or afternoon and add comments if required	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.063	The system should allow Administrator to block employees from applying and cancelling leave/s in past leave periods, e.g. previous years	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.064	The system should allow Administrator to apply leaves, check leaves' status, leave balances and leave availability/eligibility for/on behalf of employees.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.065	The The system should allow employee to cancel their leave request. If the leave request has been approved, it should be routed to their RO for their approval. If the leave request is pending at their manager, the employee will be able to cancel the leave request successfully.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.066	The The system should support Mobile features and must support Android and iOS devices. Features must be the same for both IOS and Android devices.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.067	The system should allow administrator to configure comment fields for different leave types. The field can be open to employee and/or approvers. E.g. Employee can add remarks when they apply for leave (e.g. exam leave, Parent-Care Leave, etc). Approver can also update any remarks when they approve/reject the leave request	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.068	The system should allow employees to submit their leave application through the leave self service and via mobile apps, which will be routed for approval. Email notification is also provided to inform the approvers on the pending leave application for their approval. Besides the application of leave, the leave self service and mobile apps also allows employees to view their leave status and balances.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.069	The system should automatically trigger email notification to employee when leave application is approved.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.070	The system should automatically trigger email notification to approvers for leaves applied by employees	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.071	The system should automatically trigger email notification to employees indicated in the leave request CC list. Note: Employees are empowered to forward the notification to relevant parties that need to be informed e.g. CO, VP (in the event CO is HOD).	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.072	The system should automatically trigger email reminder for Leave Applications (alternate day) that has been pending for more than X days.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.073	The system should support configuration if employee need to apply blocks of consecutive leave (can be any leave type) of at least x days For example: Maternity Leave must be taken continuously for the first 8 weeks	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.074	The system should allow approvers to provide reason if leave application is rejected	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.075	The system should allow employees to cancel part of the approved block of leave. For example: Employee can cancel 1 day of approved leave without having to cancel the whole block of leave and reapply again.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.076	The system should allow support different leave types (e.g. sick leave, examininationleave, parental leave, etc.) with varying employee eligibilities	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.077	The system should allow support different leave types (e.g. sick leave, examininationleave, parental leave, etc.) with varying number of maximum days	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.078	The system should cater to the Singapore's statutory requirement of x days of childcare leave.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.079	The system should allow to cater to the Singapore's statutory requirement of x days of extended childcare leave.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.080	The system should allow employees to upload Medical Certificate for supervisor's verification when applying for paid sick leave	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.081	The system should allow employees to upload supporting documents for the various types of leave requests	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.082	The system shalll allow administrator to configure the leave types that requires supporting documents during leave application. E.g. for Sick leave, medical certificate will be required for up to x days, Reservist Leave will require SAF100, etc.	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.083	The system should automatically generate a report on a quarterly basis on leave summary consumed for Government Paid Leave (maternity, paternity, shared parental leave, childcare leave)	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.084	The system should automatically prompt Administrator X days/weeks prior to the end date of leaves that are long term (e.g. No Pay Leave) of employee	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.085	The system should send a notification to employees and managers to complete performance management related activities before and when they return from long leave.	Optional		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.086	The system should enable employee to fill the request form for Artistic Development Leave and route for relevant workflow approval.	Optional		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.087	The system should be able to track age, nationality, date of birth, relationship type for the dependents Note: Fields captured will be used to determine staff's eligiblilty for leave entitlement (e.g. number of Childcare and Extended Childcare leave in accordance with MOM guidelines)	Mandatory		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.088	The system should allow the no pay leave and off-in-lieu leave type to be set up without entitlement i.e. employees can apply for the leave with unlimited number of days which will get routed for approval	Optional		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.089	The system should cater to the Singapore's statutory requirement of 60 days of hospitalisation leave, of which 14 days can be taken as outpatient sick leave. The same be applied to the following combination of leave: a. 3 days of Family Care Leave, of which 2 days can be taken as Parental Care Leave (Family Care Leave to be tagged to immediate family member whose details are captured, while Parental Care Leave to be tagged to parents or parents-in-law only) b. 5 days of Child Sick Leave per child up to a cap of 20 days for 4 children, on or below the age of 13, of which x days can be taken as Child Care Leave if one child is on or below the age of 7, in the year of entitlement. (x days is dependent on the citizenship of the child, 6 days for SC or 2 days for non SC)	Optional		
OHR 3.0	Compensation and Benefits	3.7	Leave Application	CNB.090	The system should be able to enable primary and secondary approvers that can be defined by the leave administrator. This is to cater for cases where the approver is on a long leave or hospitalization and the item will get routed to the secondary approver.	Optional		
OHR 3.0	Compensation and Benefits	3.8	No Pay Leave (NPL)	CNB.091	The system should enable employee to fill the request form for No Pay Leave Application and route for relevant workflow approval. Note: Different approvers based on employee type. For Corporate, HOD/RO approves followed by DD, VP, Director, and Principal. For Teaching, HOD/RO approves followed by VP, Director, and then Principal.	Optional		
OHR 3.0	Compensation and Benefits	3.8	No Pay Leave (NPL)	CNB.092	The system should be able to track if the No Pay Leave is equivalent to 1 or more days of No Pay School Holiday (NPSH). If so, NPSH will be deducted from the next month's payroll for teachers. This will have downstream implications like Payroll module.	Mandatory		
OHR 3.0	Compensation and Benefits	3.8	No Pay Leave (NPL)	CNB.093	The system should be able to compute the impact on annual leave entitlement based on the reduced number of working days with No Pay Leave. This will have downstream implications like Payroll module. Note: If No Pay Leave is more than 11 working days, the number of working days will be lesser than the original 260 days.	Mandatory		
OHR 3.0	Compensation and Benefits	3.9	PPDL	CNB.094	The system should enable HR to view the list of eligible staff for PPDL based on Years of Service (after factoring in NPL) cut by RO.	Mandatory		
OHR 3.0	Compensation and Benefits	3.9	PPDL	CNB.095	The system should enable HOD/RO to fill PPDL Nomination Form and route for relevant workflow approval. Note: The system should enable HOD/RO to attach supporting documents and able to cater to four levels of approval. HOD/RO fills up PPDL form and routes to SSD, followed by Dean, VP and P.	Optional		
OHR 3.0	Compensation and Benefits	3.9	PPDL	CNB.096	The system allows the Administrator to file a copy of the PPDL report and track commencement of Bond.	Mandatory		
OHR 3.0	Compensation and Benefits	3.9	PPDL	CNB.097	The system allows the Administrator to set up PPDL leave type for employee to apply.	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.098	System should have the flexibility to setup the annual leave entitlement accordingly to organisation's leave policy and generate leave quota at the beginning of the year For example: 50% of the leave entitlement has to be consumed in the current year. If un-utilized, the balance will be forfeited. The other 50% has to be consumed by 30 Jun of the following year.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.099	The system should allow the administrator to create time profile to configure the leave types the employees are eligible for. E.g. Paternity/Maternity and Reservist Leave	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.100	The system should allow administrator to reassign approval tasks in case of situations where the approver is on long term leave/ pending applications to another approver.	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.101	The system should auto compute the pro-rated Annual Leave entitlement but not encashment or deduction as there can be last minute changes after an employee submits resignation. The pro-rated leave balance should be reflected to employee once the official last day is updated in the system.	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.102	The system should define the leave policy for all the leave codes in the company. It should allow the configuration of rule of each leave code e.g. Allow half day leave of application, allow carry forward, validity period, pro-ration rules, etc.	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.103	The system should allow HR Admin to define public holidays, Organization Shutdown days, Off-in-lieu days	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.104	The system should be able to re-generate new annual leave quota after pro-ration to take into account the No Pay Leave taken by employee for that calendar year. Any No Pay Leave taken in the current year will affect/pro-rate the Annual Leave amount in the current year, round up 0.5 day) Any negative quota will be reflected in the annual leave quota. Leave administrator will adjust the no-pay leave duration taken into consideration the earned leave computation.	Mandatory		
OHR 3.0	Compensation and Benefits	3.10	Conduct Leave Migration	CNB.105	System should allow unutilized annual leave to be carried forward up to a maximum defined amount of days. Unconsumed annual leave will be forfeited.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 4.0	Appraisal	Generic	Generic	APP.001	The system should be able to generate a report with a list of staff who have been promoted as part of the year-end appraisal process.	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.002	The system should have the ability to generate a promotion letter with Performance Bonus indicated as an outcome of the final calibration result.	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.003	The system should allow Administrator to define the email types/content to be sent by the system. (E.g. An email is sent when a goal is approved, goal is rejected, employee submit appraisal form to appraiser, appraisal form is approved/rejected, form acknowledged by employee/RO.)	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.004	The system should provide ad hoc reports on details about the employees, their reviewers, and the feedback the employees receive on competencies, behaviors, goals, and performance	Optional		
OHR 4.0	Appraisal	Generic	Generic	APP.005	The system should allow Administrator to change the final rating after calibration. Administrators should also have rights to grant access to RO/HOD to change final ratings	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.006	The system should have ability to link Performance appraisal to salary adjustment and incentives/bonus. Once overall rating is calculated, the system has ability to match performance rating results to compensation matrix and determine merit increase and bonus, etc.	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.007	The system should have ability to prompt RO to send the personal reminder to the team members who have not completed goal setting	Optional		
OHR 4.0	Appraisal	Generic	Generic	APP.008	The system should have ability to prompt meeting set up after the submission of goal setting and attach one-page goal discussion guide	Optional		
OHR 4.0	Appraisal	Generic	Generic	APP.009	The system should have ability to send back goals that are not approved by reporting officers to employees for amendment.	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.010	The system should have ability to allow employee to update goals anytime and route to RO for approval.	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.011	The system should allow Administrator to have the flexibility to define period notification rules as per work flow requirement (e.g. 30, 60, 90 days for email reminders to be sent)	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.012	The system should send notification to inform the approvers on those submissions for their approval/acknowledgement	Mandatory		
OHR 4.0	Appraisal	Generic	Generic	APP.013	The system should allow for different access rights to different HR Admin, such that one may view selected groups of employees only.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.014	The system should have ability for employee to fill in their achievements and progress against the goals set for mid and year-end appraisal. Note: Employees do not need to rate their performance.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.015	The system should route to RO to review employee's evaluation for mid-year and input comments in the employee's appraisal form.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.016	The system should route to RO to review employee's evaluation for year-end and indicate the employee's performance rating with comments. The system then route to CO who can view the employee's evaluation and the RO's rating and comments. The system enables CO to add in comments before proceeding to approve RO's evaluation and rating. Note: Employees are unable to view the performance rating.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.017	The system should allow tracking and maintaining of employees' appraisal based on user-definable appraisal forms and points system.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.018	The system should provide Administrator full control of the appraisal module. Administrator can allow HR or groups of viewers to view appraisal forms	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.019	The system should allow Administrators to grant access to employee, RO or HOD or designated employee right to update commentary in appraisal or change ratings.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.020	The system should allow Administrator to "Open" to start the appraisal process and "Close" completed appraisal period which will lock all data and prevent further changes.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.021	The system should allow Administrator to invalidate the appraisal forms/templates for resigned/ inactive employees	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.022	The system should enable multiple raters/matrix reporting to provide assessment of an employees in the same appraisal form/template E.g. Teacher assigned as Year Mentor will have direct reporting to Dean and dotted reporting to Head/Subject Head.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.023	The system should trigger updates final performance rating data to electronic personnel files	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.024	The system should automatically reflect changes on org hierarchy/structures into the performance management module	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.025	The system should have ability to port-out data in desired formats for inbound feeds on other modules (e.g. compensation, benefits, payroll, etc.)	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.026	The system should interface with Leave Management module and prompt the line manager to set up a performance discussion prior to an employee going for long-term leave (e.g. maternity, sabbatical, etc.) or performance planning if employee is returning to work.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.027	The system should be able to integrate with compensation module to retrieve salary related info and the data access should be restricted accordingly to their user roles	Optional		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.028	The system should have the flexibilty to setup parameters on the launch of the form. Note: High level schedule for Appraisal Cycle 1) Jun- Jul: employee to fill up mid-year appraisal form and have discussion with RO to finalize mid-year session 2) Oct-Dec: employee to fill up year-end appraisal form. RO to conduct year end review session, provide performance rating with comments. CO reviews, adds in comments and approve RO's evaluation and performance rating. 3) Jan-Feb: Conduct ranking sessions 4) Mar: Finalize calibration results and update payroll	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.029	The system should allow HR admin select a form template that they want to use, preview the template, or cancel the launch and modify the template. Note: one template for teaching staff and another for corporate staff	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.030	The system should have ability to prompt managers to schedule feedback dialogue and attach 1-page check-in conversation guide before performance appraisal is submitted	Optional		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.031	The system should have ability pre-populate data from employee talent profile onto annual review templates	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.032	The system should have ability to provide aggregated view of teams performances to spot strengths and weaknesses. This should be viewable by RO and CO.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.033	The system should allow employee to attach documents/files to support their self assessments	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.034	The system should allow user to view performance rating over different periods (current & past ratings)	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.035	The system should provide reports on engagement/participation in performance appraisal activities, e.g. mid-year review, appraisal completion, goal and learning plans completion.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.036	The system should have Dashboard and/or report to track completion status of appraisal	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.037	The system should provide for past ratings report for specified number of years/period.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.038	The system should auto trigger reminder notification to employees for completing performance review before the performance review due date	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.039	The system should allow multi-raters to be setup for performance reviews. Note: For employee, the setup i.e. the number of multi-raters may differ based on the number of roles/appointments the employee has. System must be flexible to allow the such configuration.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.040	The system should have ability to trigger reminder notification to RO/CO set up performance appraisal discussions/interviews with employees	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.041	The system should allow the Principal ease of access to supporting documents/files while reviewing the appraisal form. The user interface should be intiutive or e.g. to allow splitting of window to view multiple documents. Note: allow the Principal to pull out a CV while reading the appraisal form and size the two documents to fit into a monitor, etc.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.042	The system should link performance outcomes to C&B system and talent systems, e.g. flag up the ineligibility of staff for internal transfers/ performance bonus because of performance rating	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.043	The system should allow creation and maintenance of employees' talent profile, where employees can update their performance goals, learning and development activities and achievements as applicable	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.044	The system should auto-route appraisal documents to supervisor based on defined workflows, criteria and organisational hierarchy. System should allow Administrators to manually re-route appraisal documents where needed.	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.045	The system should auto-assign and trigger adhoc appraisals for transferred/promoted/new hires in line with HRIS and org hierarchy changes	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.046	The system should allow storing of past Annual performance ratings by calendar year	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.047	The system should allow employees to view their own past appraisal information if they have changed teams or employment groups	Mandatory		
OHR 4.0	Appraisal	4.1	Mid and Year-End Performance Process	APP.048	The system should allow HR administrators to define what constitutes a completed appraisal before it can be completed, e.g. required rating fields, commentary fields, etc. Note: Typically if fields are marked as mandatory, employee would not be able to proceed with submission	Mandatory		
OHR 4.0	Appraisal	4.2	CCA Ranking Exercise	APP.049	The system should enable administrator to configure and launch CCA evaluation form for the staff to individual SSC Advisor/ Comm ICs/ CAS Head/ EE Head/ Student Dev Head/ Year Mentor (YM) based on the Task Force/Committee/CAS/EE/YM/CM assignment for the year. Note: One employee could have multiple assignments as Co-curricular activities and could receive multiple evaluations from each rater to evaluate for the assignment.	Mandatory		
OHR 4.0	Appraisal	4.2	CCA Ranking Exercise	APP.050	The system should have ability to create an evaluation form that enables the evaluator to indicate grading and provide comments.	Mandatory		
OHR 4.0	Appraisal	4.2	CCA Ranking Exercise	APP.051	The system should enable individual SSC Advisor/Comm ICs/CAS Head/ EE Head/ Student Dev Head/ Year Mentor to receive the CCA evaluation form to be completed for all members under his/her care.	Mandatory		
OHR 4.0	Appraisal	4.2	CCA Ranking Exercise	APP.052	The system should enable the Administrator and individual SSC Advisor/Comm ICs/CAS Head/ EE Head/ Student Dev Head/ Year Mentor to track and report on the status of completion of the CCA Evaluation form.	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.053	The system should have ability to trigger notification to managers to set up check-in with employee to discuss performance and development goals	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.054	The system should have ability for employee to create and manage goals	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.055	The system should have ability to set goals on mobile device	Optional		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.056	The system should have ability to provide dashboard that shows how each team member's goals are contributing to functional priorities and key themes in goals and development actions	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.057	The system should allow the system to setup approval level E.g. RO	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.058	The system should have ability to track progress for employee goal setting. This tracking mechanism should be available at various levels - HR, RO, CO, Director, VP, Principal	Mandatory		
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.059	The system should allow setting a minimum number of goals.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 4.0	Appraisal	4.3	Create Performance Goals	APP.060	The system should have ability for employee to edit goals based on discussion with Manager	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.061	The system should allow multiple rounds of calibration (up to 3 sessions) for Teaching.	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.062	The system should allow release of calibrated ratings to be done by HR. Note: There should be no need for Administrators to upload calibrated performance ratings. Access to final performance ratings are restricted based on access rights.	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.063	The system should have ability to set up different calibration templates for different employee groups	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.064	The system should have ability to enables users to add comments on employee on calibration templates	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.065	The system must allow CO to setup/conduct departmental calibration exercise. The Performance administrator should have the capability to setup for schoolwide calibration.	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.066	The system should allow School Leaders to view 3 years of data on performance rating and CCA Ranking evaluation results as inputs when they are calibrating the ratings in the Ranking sessions. Note: Access to performance ratings are restricted based on user rights to access. E.g. Management can view school wide, HOD can only view for the department and RO can only view for the immediate team members under his/her supervision.	Mandatory		
OHR 4.0	Appraisal	4.4	Calibration Process	APP.067	The system should allow for a bell-curve distribution that specifies the quota for each performance rating category and highlight when the quota has exceeded. The system should also compute and show changes based on the indicated number for each performance grade and does not allow adminstrator to proceed when the total amount exceeds the total budget within the department and also schoolwide Note: Each faculty has its own bell-curve that is used during department calibration. There is also a quota set at school wide to ensure the overall budget is in line with the planned.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 5.0	Training	Generic	Generic	TRA.001	The system should provide RO a dashboard where they can manage the team's training schedule (e.g. who will be out on course).	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.002	The system should have ability for learning administrator to export training request details into an Excel file. The export should contain additional user information such as Job Code and Job Location which may help learning administrator determine the training budget. These details can be accessed by HR, HODs, Department administrators and assigned users/roles.	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.003	The system should have the capability to allow Administrator to perform mass append, update and cancel of employees' training record	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.004	The system should have ability to have the facility to integrate employee training history to other HR processes like career and succession planning, recruitment, promotion, talent profile, performance reviews etc.	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.005	The system should provide reports on learning and certification activities, and learner transcripts	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.006	The system should send notification to inform the approvers on those submissions for their approval/acknowledgement and employees to inform them that the course is approved.	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.007	The system should block employee from applying for training once the employee has resigned with last date of service recorded. For any existing training, the training amount should be recorded for HR to follow up as part of the offboarding checklist.	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.008	The system should allow employees to record training hours in the specified X hours/ half (AM)/ half (PM) / in blocks of x days. This enables RO to have better visibility of the staff's schedule and enables staff to have the flexibility to take leaves.	Mandatory		
OHR 5.0	Training	Generic	Generic	TRA.009	The system should have ability to allow the business leader and HR access to talent profiles. The system should have ability to provide side by side comparison of talent profiles. The talent profile should comprise of years in service, career progression, and current performance.	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.010	The system should have ability for Head of Departments to view the learning budgets, utlisation balance	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.011	The system should allow provide the function to feed into the finance budgeting system to populate the training budget for each division/department/cost center etc.	Optional		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.012	The system should have ability to capture the training cost to monitor the budget utilization for each Department / Cost Center Note: Rights to view training cost should be given to users (Dept Coordinators/ HODs) and HR Administrators	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.013	The system should have ability to create cost structure for instructors so HR can track the training costs to the organization for training costs	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.014	The system should allow Administrator/programme administrators to charge to staff department cost centre for training staff had attended.	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.015	The system should have ability to manage cost chargeback to appropriate cost centres	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.016	The system should have flexibility to allow users to generate information about a particular learning course's costs. It should also allow user to generate summary report on total training cost utilisation by Department, Schools, etc for a specific period	Mandatory		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.017	The system should be able to track the balance of the training amount that can be utilized based on a comparison of training budget vs training costs.	Optional		
OHR 5.0	Training	5.1	Training Budget and Plan	TRA.018	The system should enable the administrator to download the training budget template in various formats e.g. excel for HR to amend and send out to RO/HOD for the Department Training Plan. Note: The department training plan is used by RO/HOD to plan the trainings each employee should attend based on the training budget.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.019	The system should allow employees to submit training application form for training approval by RO. Note: RO needs to check the training is part of the individual training plan discusssed and agreed with employees offline.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.020	The system should have the flexibility to allow Learning Administrator to setup approval routing for certain group of employees to be routed to different approvers	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.021	The system should have ability to manage cancellation of learning request by learner and trigger notification to manager on learning request cancellation. Notification on cancellation of learning requests should also be triggered to department administrators and appropriate parties or course managers.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.022	The system should set an approval process for employees to withdraw from course before they're allowed to unenroll Note: For specific mandatory/identified/compliance programmes/paid programmes; include additional requirement for system to allow administrators or course/programme managers to define course cancellation/withdrawal approval processes	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.023	The system should allow employees to submit reasons for course withdrawal (e.g. medical emergency, work emergency, etc.)	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.024	The system should have ability to send reminders to employee who has not completed the course assessment after attending training	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.025	The system should have ability for employees to update training events into their own Outlook calendar	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.026	The system should have ability to send email invitation, outlook appointments and reminders to instructor and learners	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.027	The system should have the capability to allow Administrator to perform mass upload/update course schedule for a list of course that are in the system (e.g. Course ABC runs in a few schedule in 2021, same Course ABC will be running a few more schedule in 2022)	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.028	The system should allow Employee to browse or search the course catalogue for the desired course to apply, or they can put up a request for a new course.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.029	The system should enable employees/learners to submit request for a new class for the course (e.g. request a new class when they can't find it scheduled at a time they can attend or when they try to register but can only join the waitlist because the course is popular)	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.030	The system should have ability to trigger notification to learner 2 weeks before course commencement for course confirmation.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.031	The system should trigger reminder to learner to indicate completion or non-completion of learning, and to auto-update accordingly. Routing should be to PD Admin or HR based on the employee type. Note: For Teaching staff, it gets routed to PD Admin to process the training costs. For Corporate staff, it gets routed to HR to process training costs.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.032	The system should have ability to have the functionality to have a database and to keep track the hours of contribution for internal trainers	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.033	The system should have a verification process for HR/ PD Admin to check and approve external learning records submitted by employee. E.g. Employee uploading a Project certification from 'dodgy' source	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.034	The system should have the ability to send automated notifications to remind staff to submit the training invoice to the relevant stakeholders. Note: Notifications are triggered based on cadence set e.g. 5 days or 10 days post course date.	Mandatory		
OHR 5.0	Training	5.2, 5.3	Training Submission and Approval (Corporate), Training Submission and Approval (Faculty)	TRA.035	The system should allow the administrator to overwrite the training costs to reflect the actual costs after deduction of subsidies, GST etc.	Mandatory		
OHR 5.0	Training	5.3	Training Submission and Approval (Faculty)	TRA.036	The system should have the ability to send automated notifications to inform the secondary reporting for cases where the staff is holding concurrent roles. E.g. Literature teacher that takes up the role of Year Mentor reports directly to Dean Affective but still has dotted line to Head of Literature.	Mandatory		
OHR 5.0	Training	5.3	Training Submission and Approval (Faculty)	TRA.037	The system should automatically trigger email notification to employees indicated in the training request list. Note: Employees are empowered to forward the notification to relevant parties that need to be informed e.g. CO, VP (in the event CO is HOD).	Mandatory		
OHR 5.0	Training	5.4, 5.5, 5.6, 5.7	Scholarship, Post-Graduate Award, Training Sponsorship, PGCEi (for teaching)	TRA.038	The system should allow Administrators to key in information for Scholarship/Post-Graduate Award, Training Sponsorship/PGCEi; create start/end date of course, start/end date of bond period	Mandatory		
OHR 5.0	Training	5.4, 5.5, 5.6, 5.7	Scholarship, Post-Graduate Award, Training Sponsorship, PGCEi (for teaching)	TRA.039	The system should maintain a list of staff undergoing Scholarship/Post-Graduate Award, Training Sponsorship/PGCEi, staff who completed course and serving bond and staff who have completed their bond Note: During separation, the system should flag out if the staff is on serving any bond. System should trigger when staff resigns while attending programme or while serving bond. This is to facilitate HR to compute liquidated damages	Mandatory		
OHR 5.0	Training	5.4, 5.5, 5.6, 5.7	Scholarship, Post-Graduate Award, Training Sponsorship, PGCEi (for teaching)	TRA.040	The system should trigger staff who completed their studies for Scholarship/Post-Graduate Award, Training Sponsorship/PGCEi to submit their final exam transcripts and certification upon last day of course or completion of 1st/2nd year milestone for Training Sponsorship. It should also inform staff of start date of bond	Mandatory		
OHR 5.0	Training	5.4, 5.5, 5.6, 5.7	Scholarship, Post-Graduate Award, Training Sponsorship, PGCEi (for teaching)	TRA.041	The system should be able to calculate the bond defered amount when the employee resigns. Bond defered amount is calculated based on pro-ration by working days, similar to leaves encashment. Bond defered amount can be viewed by HR and Payroll. The system should allow Employee to submit education transcript and certificate after each semester for Company Sponsored Degree and Post Graduate programmes.	Mandatory		
OHR 5.0	Training	5.4	Scholarship	TRA.042	The system should enable HR to track salaries, allowances, expenses incl. Flexible Benefits that have been disbursed to staff to ensure the total amount still falls within the total budget for Scholarship.	Mandatory		
OHR 5.0	Training	5.8	Maintain Competency Model	TRA.043	The system should be able to reference the competency library from the job family framework. Competency can be a generic set across the school or it can be tied to a specific job family/function.	Mandatory		
OHR 5.0	Training	5.8	Maintain Competency Model	TRA.044	The system should have ability to pre-set required level of competency for each job and compare skills requirement	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.045	The system should allow have the flexibility to allow Administrator to configure which courses can be search / view / apply by certain group of employees.	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.046	The system should allow Learning Administrator to define the course nature for each training course (e.g. course description, course duration, schedule, etc.)	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.047	The system should have ability for administrators to enroll those employees to relevant courses on their behalf based on nomination from School Staff Developer (SSD) or RO	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.048	The system should have ability to handle approval of training request based on specific rules of approval Note: Next level of approval should be defaulted to RO based on the position reporting	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.049	The system should have functions to generate a list of employees based on identified fields, e.g. skills requirement, competency gaps, performance ratings, tenure, job levels, job families, in a particular Department / Company	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.050	The system should have ability to make courses unavailable that are no longer relevant so that an employee can no longer take the course	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.051	The system should show employees the course details and schedule when an employee clicks on the planned course in the learning platform	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.052	The system should allow process for creation of new courses by Administrator/programme managers to be added to course libraries and database	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.053	The system should allow Learning Administrator to select type of learning course (e.g. Instructor- Led, Online Only, Instructor-led with online content, etc.) and Learning Administrator can track the costs and price of the courses	Mandatory		
OHR 5.0	Training	5.9	Manage Course Catalog	TRA.054	The system should have ability for Learning Administrator to mass enroll different groups of employees to learning different learning programs based on their job functions, department, school, etc.	Mandatory		
OHR 5.0	Training	5.10	Create Training Course	TRA.055	The system should have the ability for the employee to request for a new class for existing training in the LMS. Learning Admin should be able to export the data in a report.	Mandatory		
OHR 5.0	Training	5.10	Create Training Course	TRA.056	The system should have ability to detect double registration of the same participants in different sessions with the same time slot	Mandatory		
OHR 5.0	Training	5.10	Create Training Course	TRA.057	The system should have ability to capture the registration status of each training sessions and display available training slots for other participants	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.058	The system should have ability to run report to determine learning courses with low usage/enrolment	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.059	The system should be able to generate the list of courses with low enrolment/usage/low course ratings for users to follow up. Administrators can evaluate to either archive/remove courses from the learning library or revamp the course delivery.	Optional		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.060	The system should have ability to capture assessment results and generate overall scores and by subject for each of the participants	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.061	The system should have ability to capture different course evaluation forms for different learning courses	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.062	The system should have ability to add surveys to gather employee feedback for completed courses and to assess long-term retention and application of these acquired skills	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.063	The system should have ability to conduct Pre and Post-Course review and competency assessments for employee and RO	Mandatory		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.064	The system should have ability for employees to provide rating (e.g. 5 stars, 2 stars, etc.) after they have completed a course. On the learning catalogue the average rating of the course can be shown.	Optional		
OHR 5.0	Training	5.11	Assess Training Effectiveness	TRA.065	The system should allow administrators and course/programme managers to view dashboard/reports of learners' participation/enrolment, course evaluation, and learners' satisfaction ratings of programmes to make a decision about programmes to improve or remove/archive	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.066	The system should allow sync with Employee Profile for uploading/updating learning activities (formal and informal)	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.067	The system should allow employees to view their course enrolment status	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.068	The system should have ability to show list of employees who have enrolled/registered to attend a particular training program	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.069	The system should provide the functionality to view employee's learning history, learning hours accumulated and any outstanding training requirements Note: Viewing rights should be extended to employees, managers and HR Administrators	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.070	The system should allow display of the training records that employees have attended/enrolled	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.071	The system should allow migration of historical training/learning records to be uploaded so that users can generate report or perform trending analysis Note: Historical data that were captured in manually in excel to be migrated into the new system	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.072	The system should have ability to be able to automatically update the employee training history record once completed the training and the online evaluation	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.073	The system should provide reports on training hours and key training data, including the learners, course, curriculum, organization, catalog, class, competency, etc.	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.074	The system should allow Employees and Managers to view their status of learning plan in a report format with information such as competency attained, course code, course name, learning area, training date etc	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.075	The system should have ability to be record learner's attendance upon class completion and capture attendance into the learning records on the day of the programme (physical or virtual)	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.076	The system should have ability to maintain training records of all employees including past learning history and current enrollments	Mandatory		
OHR 5.0	Training	5.13	Update Training History	TRA.077	The system should have ability for learners to update learning record after completion of external learner courses, and attach completion certification and necessary documentation, and route to HR to verify and approve/reject	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 6.0	Payroll	Generic	Generic	PAY.001	The system should be able to generate payroll reports in clear or encrypted form in accordance to regulatory standard. Note: Reports should include: 1. Payroll detailed report 2. Payroll reconciliation report 3. Payroll variance report 4. GIRO listing 5. NPL listing	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.002	The system should be able to generate statutory forms (in format approved by statutory bodies) required for submission.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.003	The system should be able to automate bank file uploads for salary crediting, etc. to external bank portals upon final bank file approvals, with ability of approval layers to be pre-defined	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.004	The system should be able to generate multiple file formats/ reports as a result of payroll run (e.g. standard payroll reconciliation file, bank cheque listing file, pay register)	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.005	The system should be able to print/reprint payslip and tax reporting form online	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.006	The system should have ability for students to view Adjuncts, Casuals, and temporary staff for their time worked for specific assignments	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.007	The system should be able to allow employees to access payslips and other pay related information both on mobile and on desktop.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.008	The system should have ability to print NRIC number & PDPA in the payslip (last 4 digits). If there is any salary change during the month, payslip should reflect the new salary and not zero.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.009	The system should have ability to view and print the results of payroll simulation in the payroll log	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.010	The system should have ability to create reporting lists to check deductions made from employee's payroll	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.011	The system should have ability to produce legal forms in printed form per employee for Year End Adjustment (e.g. Employee's Income Tax, Social Security, etc.)	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.012	The system should be able to capture retrospective updates including CPF contributions for foreign employees who obtained Singapore PR status	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.013	The system should be able to capture employees' salary information (to cap CPF contributions) for conversion cases from contract to permanent and visi-versa with different employment ID.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.014	The system should be able to generate payroll audit reports by specified fields, date, timestamp, user, etc	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.015	The system should be able to run reports for employees' payroll costs monthly.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.016	The system should be able to run monthly payroll summary and variance reports during payroll processisng.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.017	The system should have ability to store historical data of employees' benefit requests, enrollments, entitlements and claims	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.018	The system should have ability to run report on employee eligibility, actual utilisation to list all employees who have claimed for a benefit type in a certain period of time.	Mandatory		
OHR 6.0	Payroll	Generic	Generic	PAY.019	The system should display Payment Advice instead of Payslip, and Adjunct Fee instead of Salary for Adjuncts	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.020	The system should allow employees to submit their timesheet application through self service or clock their overtime via mobile apps (clock in & out), which will be routed for approval. System should support email notification to inform the approvers on the pending timesheet submission for their approval. The system should also allow employees to view their time submissions including overtime. Note: Only full-time technicians are eligible for Overtime pay.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.021	The system should allow employees to submit/clock time entries based on actual hours and minutes	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.022	The system should be configured to disallow employees to submit multiple time submissions that have overlapping time for the same date (eg, one application is 1800hr-2100, the other is 2030hr - 0100, this is not allowed)	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.023	If there are the time entry submitted has break times, system should compute the total hours of work performed, overtime, and allocate the correct OT rate according to Singapore statutory requirement Note: Only full-time technicians are eligible for Overtime pay.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.024	The system should trigger Email notification to inform the approvers on the pending claim application for their approval	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.025	The system should allow Administrator to set up email notifications and email reminders as per work flow requirement.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.026	The system should determines whether remarks are mandatory for specific field. E.g., when approvers reject an application, a reason to be indicated, purpose of claim field	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.027	The system should allow eligible employee the viewing option to see the status for their overtime application. Employees will be should view their pending overtime status and the total overtime hours taken for specific period/duration.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.028	The system should allow administrator to configure the approval workflow for time entry submission. Note: Different workflow applies for different group of employees.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.029	The system should allow employees or supervisor to generate overtime related reports (hours taken, status of overtime application) for themselves or for their employees	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.030	The system should have ability to configure rules around time entry so that employees can only enter time when a period is open for time entry	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.031	The system should have ability to allow employees to submit time entries on a daily basis and route to next level for approval Note: Approver is different for each employee type. 1. Music/Non-Music Adjuncts: OA 2. Casuals (including Technicians): OVM, Senior Manager 3. Relief Teachers: Faculty Head, followed by VP	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.032	The system should have ability to allow next level approver to make necessary adjustments to employee's timesheets. Note: Approver is different for each employee type. 1. Music/Non-Music Adjuncts: OA 2. Casuals (including Technicians): OVM, Senior Manager 3. Relief Teachers: Faculty Head, followed by VP	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.033	The system should have ability to maintain different rates for casuals, adjuncts and temp, and calculate daily rate for payment by Payroll. Note: The system should also capture the different rates for Public Holidays and Technicians for off days. E.g. Public Holidays would be twice the pay for Casuals.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.034	The system should capture the timesheet information such as: - clocking date/time - number of hours (For Relief Teachers and Temp: To deduct 1 hour as long as total number of hours is 8 hours or more within 1 day) (For Adjunct: To alert if exceed 8 hours within 1 week) - payrate to be applied (For Relief Teachers and Temp: To default the hours worked as 6.5 hours if the working date falls on a Public Holiday and is within the employment period) - approval workflow	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.035	The system should have reporting capability to allow users to generate time clocking related information based on their authorized access.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.036	The system should allow Department administrators to run their own monthly report on the timesheet status, duration, hourly rate based on base salary etc. for reporting purposes to HOD and costing to Finance. Note: This includes costing breakdown and backpayment amounts for FInance reporting.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.037	The system should allow employee to view their timesheet clocking information including the status	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.038	The system should allow Supervisors/approvers to view all the timesheet clocking they have received for their action, include all records regardless of status	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.039	The system should auto-assign employees who meets the eligibility criteria to use time sheet clocking (e.g. Adjuncts, Casuals, and Relief Teachers). Note: If the employee has resigned, the entry to timesheet clocking will be removed.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.040	The system should allow administrator to set error message if employee is unable to submit overtime under any circumstances Eg past overtime after x months, more than 72 hours, submission of overtime only for work completed 30 minutes and above etc	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.041	The system should allow Administrator to block employee from cancelling overtime that has been processed under payroll module	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.042	The system should have the flexibility to allow the delegation of the approval authority to another user.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.043	The system should capture the approver's remarks for approval/rejection.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.044	The system should provide a overview of all the applications that has been approved/rejection by the approvers.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.045	The system should support resubmission of rejected timesheet submission.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.046	The system should allow Supervisors/coordinators to view status of timesheet entries, including Overtime, and the total hours submitted for specific period/duration on behalf of employees as per set up by the Administrator.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.047	The system should have geo-fencing capabilities to ensure the employee is at the exact location when clocking-in/out.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.048	The system should be able to capture signatures as adjuncts would need student's signature to verify the student has attended the session.	Optional		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.049	**The system should have ability to administer CAYE payment to Adjuncts and credit the amount based on the specified contributions by the Adjuncts.** **Note: Adjuncts will have to opt in for CAYE contribution and this has to be process accordingly.**	Optional		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.050	The system should have the ability to track the roles the employee has and the different rates. E.g. For casuals, a staff can be either a supervisor or the staff for the particular assignment. Another example, a casual who worked on a PH will have received a higher rate.	Mandatory		
OHR 6.0	Payroll	6.1, 6.2, 6.5	Music/Non-Music Adjunct Capture Time, Casuals & OT Payroll incl. Transport, Relief Teachers and Temp Payroll	PAY.051	The system should be able to cap the number of total working hours for Relief Teachers based on number of working days per month multiplied 6.5 working hours per day irregardless of the contract end date. E.g. If the relief teacher works 108 hours but the monthly cap is 104, the total working hours will be 104 hours multiplied by the hourly rate.	Optional		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.052	The system should allow to maintain separate benefit plan for separate groups of employees	Mandatory		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.053	The system should allow employee to submit claim and attach relevant supporting documents such as receipts in various formats (e.g. photo, pdf, etc.) and route to appropriate approval authority (e..g. Manager/HR Admin) for approval (e.g. for self-administered claims like flexible benefits)	Mandatory		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.054	The system should be able to provide Manager self service to receive claims submitted by employee and approve/reject and route to HR Admin for additional verification if required	Mandatory		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.055	The system should have ability to route to HR admin to verify claims and documentations submitted by employees and approve/reject	Mandatory		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.056	System should be able to calculate pro ration, so that employee can claim only for the pro rated amount. E.g. - If employee joins mid year then employee should be able to claim only for half the amount in the system.	Mandatory		
OHR 6.0	Payroll	6.4	Flexible Benefits/Transport Claim for Casuals	PAY.057	The system should be able to run report to analyse Flexible Benefit selection and the utilisation of flex credits	Optional		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.058	The system should be able to capture employee information to support monthly CPF contributions based on statutory requirements, CDAC, SINDA etc.	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.059	The system should be able to capture employees' PR, work permit details	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.060	The system should be able to automate data interfaces with time and admin systems and calculate payroll implications for payroll register	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.061	The system should be able to synchronize with Core HR modules to obtain updates to Employee Master Data (e.g. New hires information, promotion updates, etc.)	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.062	The system should be able to allow for different CPF e-submission methods (e.g. Direct Debit, etc.) based on the organisation entity requirements	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.063	Data from external sources: The system should have the functionality to interface data from HR system into Payroll system, either by direct file transfer or API. Approved payment should be interfaced direct from 3rd party system to Payroll for processing.	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.064	The system should be able to manage payroll runs, different payment schedules, and deduction types for Singapore.	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.065	The system should be able to support validation rules or alerts that will flag variations for administrators to investigate	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.066	The system should be able to process ad-hoc / off-cycle payment to employees	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.067	The system should be able to provide the option for executing payroll reconciliation to be conducted in the system prior to running posting simulation	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.068	The system should be able to process monthly payroll cycles, with separate monthly runs for pre-defined criteria (e.g. permanent employees vs. temporary employees, etc.)	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.069	The system should be able to capture benefits-in-kind which is not payable to employees via payroll but need to be reported to IRAS for income tax declaration.	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.070	The system should capture the wage types with the respective statutory requirements, i.e whether the amount is taxable or subject to CPF contributions	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.071	The system should a feature to lock or unlock payment records based on supporting records before payroll payout. This is to cater to the maker-checker process to lock/unlock payroll related information. For example: basic pay, recurring payment, one-time payment, bank account, indicator for compensation eligibility (i.e. perf bonus, annual increment, completion bonus, sales incentives)	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.072	The system should allow the generation of CPF file after payroll run information approval, notifying pre-defined approvers for CPF file approval	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.073	The system should allow users to view current and all previous payslips.	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.074	The system should be able to publish payslip/payment advice on the 25th of every month for employee/adjuncts to view	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.075	The system should allow HR user to generate the list of employees and its approved AWS payout for uploading into system for payroll processing	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.076	The system should be able to automate CPF file information validation and highlight errors / changes based on previous CPF information for ease of review Note: The review of changes should be done using the payroll variance reports	Optional		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.077	The system should be able to include pre-defined approval layers to validate final payroll run outputs	Mandatory		
OHR 6.0	Payroll	6.6	Process Payroll	PAY.078	The system should be able to run report on monthly staff movement such as New Hires, Cessation, Salary Changes, Transfer, etc. for insurance enrolment. The file should be able to interface with payroll system for processing.	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 6.0	Payroll	6.6	Process Payroll	PAY.079	The system should be able to compute the payroll deductions due to No Pay Leave or No Pay School Holiday and deduct the amount accordingly.	Mandatory		
OHR 6.0	Payroll	6.8	Manage Manual Payroll Inputs	PAY.080	The system should be able to support off-cycle functionality including bonus payments, payroll on demand, correction payment & adjustment payments, and for all other payment applicable to the organisation's employees	Mandatory		
OHR 6.0	Payroll	6.8	Manage Manual Payroll Inputs	PAY.081	The system should be able to split the CPF contributions according to the percentage or fixed amount to be charged to the various cost centres/internal order numbers/fund codes maintained in the system.	Mandatory		
OHR 6.0	Payroll	6.8	Manage Manual Payroll Inputs	PAY.082	The system should be able to reduce manual work with natively supported automatic retroactive pay changes	Mandatory		
OHR 6.0	Payroll	6.9	Manage Final Pay	PAY.083	The system should be able to process Annual Wage Supplement (AWS) calculations annually and incorporate into end-of-the-year payroll run (e.g. December), incorporating different calculations for various employee types (e.g. permanent, contract, temporary staff, etc.)	Mandatory		
OHR 6.0	Payroll	6.9	Manage Final Pay	PAY.084	The system should have ability to administer payments for terminated employees and calculate entitlements and lump sum amount due to them based on their leaving date	Mandatory		
OHR 6.0	Payroll	6.9	Manage Final Pay	PAY.085	The system should be able to conduct necessary payout calculations in ad-hoc cases (e.g. termination, retirement).	Mandatory		
OHR 6.0	Payroll	6.9	Manage Final Pay	PAY.086	The system should be able to send an email notification to HR to calculate the bond defered amount after separation is triggered during the bond period	Mandatory		
OHR 6.0	Payroll	6.10	Payroll Disbursement	PAY.087	The system should have ability to administer payments based on employee's timesheet clocking	Mandatory		
OHR 6.0	Payroll	6.10	Payroll Disbursement	PAY.088	The system should be able to automate the generation of General Ledger (GL) files after payroll run and the validation of GL information to highlight errors/changes based on previous GL files Note: Simulation of the posting documents should highlight errors before actual posting to GL.	Mandatory		
OHR 6.0	Payroll	6.11	Post Payroll to General Ledger	PAY.089	The system should be able to automate the upload of GL information into internal Finance systems for posting, with pre-defined upload timings based on payroll types (e.g. permanent employees vs. temporary employees)	Mandatory		
OHR 6.0	Payroll	6.11	Post Payroll to General Ledger	PAY.090	The system should have ability to simulate payroll for individual employees before performing the regular payroll run for all the employees to recognize sources of errors in time to make corrections	Mandatory		
OHR 6.0	Payroll	6.12	Process Corrections and Adjustments	PAY.091	The system should be able to manage employees' salary grades payment arrears, nomus payment, etc for current payroll runs retroactively for late entries	Mandatory		
OHR 6.0	Payroll	6.12	Process Corrections and Adjustments	PAY.092	The system should be able to automate Over Time Pay file information validation and highlight errors / changes based on previous payroll run	Mandatory		

L1	L1#	L2#	L2	Req ID	Business Requirement	Requirement Priority	Statement of Compliance	Tenderer Remarks
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.001	The system should have ability to set limits on FTE for different sections (e.g. departments, etc.) and impose limits on headcount to be hired (e.g. no more than 10% of budgeted FTE, etc.)	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.002	The system should have ability to identify FTEs with joint appointments (e.g. 60% to one team and 40% to team as part of Year Mentor, etc.) and incorporate the data for budget planning	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.003	The system should have the ability to handle different workforce job levels, employment types (perm vs contract etc) and staff types (e.g. corporate, teaching staff etc.	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.004	The system should be able to provide detailed reporting and analysis through standard dashboards	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.005	The system should have ability to capture both budget and target workforce by department and School as a whole, in terms of FTE and headcount	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.006	The system should have ability to develop headcount/FTE budgets through a series of inputs, factors, multipliers, etc.	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.007	The system should allow users to compute the maximum headcount that may be hired based on FTE budget, FTE targets	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.008	The system should allow budgets to be drilled down separately for different functions within a School/Department	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.009	The system should have the ability to load standard workforce planning parameters, e.g., salary, anniversary, sick leave, shift penalties, quotas, allowances, etc	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.010	The system should be able to feed data such as FTE dollar value, total manpower costs, etc. to budgeting module under Finance	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.011	The system should allow to input contract staff FTE, headcount and expenditure by month. Note: Schools also need to plan for renewal/extension of contract staff. The system should also allow planning of short-term contract especially teachers separately.	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.012	The system should have ability to compare planned headcount and costs to actuals	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.013	The system should have ability to identify deviations and their financial impact	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.014	The system should allow each school to carry out its headcount planning per a set template which can then add up as inputs to the Schoolwide workforce plan. This is pertaining to School (full-time and adjuncts) workforce planning E.g. The template should comprises of - Demand needed for course load - Current supply from full-time, adjunct and contractors) - Identify any shortfall - Compute resources needed [shortfall/average load of school]	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.1	Workforce Planning	WFP.015	The system should have ability to distribute a report on the approved headcount information to HR	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.016	The system should have ability to recommend talent profiles with high % match to the position based on their profiles and the position's successful profiles	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.017	The system should have ability to identify and track succession risks	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.018	The system should have ability to filter and sort succession candidates by role/department/function/talent pool, etc	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.019	The system should have ability to leverage direct access by ROs for succession nomination	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.020	The system should have ability to support risk calculations on succession pools / numbers	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.021	The system should have ability to clearly assign the owners and the due dates of specific development actions in succession plan	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.022	The system should have ability to generate succession planning in excel format and dashboards	Mandatory		
OHR 7.0	Workforce Planning and Succession Planning	7.2	Succession Planning	WFP.023	The system should have ability to create real-time dashboard with accurate data to show the health of leadership pipeline, performance and potential grid, organisation view on the succession gaps, and the priority of succession needs based on impact of loss and retention risk.	Mandatory		

SCHOOL OF THE ARTS SINGAPORE

Annex D4: IT Functional Requirements

Instructions to Tenderers	
1.1	Please state clearly the compliance to all requirements listed in this Annex. For each requirement, the Tenderer shall select the appropriate compliance response from the dropdown menu. Definitions of each compliance reponse are provided in the table under "Compliance Definition" below.
1.2	Any statements in this Annex pertaining to other parts of the tender will be disregarded by the School. Only the responses provided in the table under "Compliance Definition" will be accepted. Where there is a failure to indicate a proper compliance response, it shall be deemed that the Tenderer has indicated "C" and the offer shall be evaluated accordingly.
1.3	The following format provided in this Annex shall be used for submission.
1.4	Please provide explanatory notes under "Tenderer Remarks" whenever possible.

Compliance Definition

Statement of Compliance	Definition
'Compliance' or 'C'	When the System or Service meets all Specifications / requirements without any customization / modification to the standard software (i.e. via configuration). The Tenderer shall NOT add any explanatory notes against the clause that vary the meaning of full compliance to the clause and such notes provided (if any) shall be ignored.
Partial Compliance' or 'PC'	When the System or Service is able to comply with the Specifications / requirements by means of customization / modification to the standard software (i.e. not via configuration) or by adding third party software. The Tenderer must provide condensed but complete information on the customization involved or the third party software proposed, including any integration efforts required and additional charges involved.
'Non-Compliance' or 'NC'	When the System or Service does not comply with the Specifications / requirements.

Document Information	
File Name:	Annex D4 - IT Functional Requirements
Disclaimer:	

			Statement of Compliance				
L1#	**L1**	**Total no. of Requirements**	**Comply**	**Non Compliance**	**Partial Compliance**	**N.A.**	***Tenderer Completion Status***
IT 1.0	IT 1.0	360	0	0	0	0	*0%*
		360	**0**	**0**	**0**	**0**	

L1	S/N	Process Area	Requirement	Compliance	Vendor response
	1. General Technical Requirements				
IT 1.0	1.1.1	1.1.General Requirements	The Tenderer shall propose a comprehensive solution that, to the greatest extent possible, will be delivered as a Software as a Service (SaaS) solution (excluding software tools that may be hosted on a SAS-provided infrastructure). The SaaS solution shall include all necessary components of the underlying cloud platform and infrastructure, such as compute resource, storage, network, virtualisation, operating systems, middleware and security features.		
IT 1.0	1.1.2	1.1.General Requirements	The Tenderer is responsible to work closely with the Cloud Service Provider (CSP) of the proposed SaaS solution to ensure the successful implementation and operation of the SaaS solution. The Tenderer shall clearly specify in the Tender Offer, which services shall be provided by the CSP and which shall be the responsibility of the Tenderer.		
IT 1.0	1.1.3	1.1.General Requirements	The SaaS solution shall be designed and configured to operate at optimal performance. Other salient features include maintainability, scalability, integrity, reliability, availability, tight security and control.		
IT 1.0	1.1.4	1.1.General Requirements	The SaaS solution shall be able to implement thresholds that are set to trigger alerts.		
IT 1.0	1.1.5	1.1.General Requirements	The SaaS solution shall be designed to turn on the notification features by email and/or through a mobile application.		
IT 1.0	1.1.6	1.1.General Requirements	The SaaS solution shall be designed to provide validations on input and output data. The type of validations shall include (but not limited to): a. Data length and type (e.g. alphanumeric); b. Data content (e.g. NRIC validation); c. File size and type (e.g. xls, xlsx, pdf of 5MB).		
IT 1.0	1.1.7	1.1.General Requirements	The Tenderer shall be responsible to work with the appropriate third parties in tasks such as system integration and rectifications of faults to ensure the successful implementation of the SaaS solution.		
IT 1.0	1.1.8	1.1.General Requirements	The Tenderer shall provide the technology / product roadmap for the proposed software to illustrate its planned releases, versioning and enhancements.		
IT 1.0	1.1.9	1.1.General Requirements	The Tenderer shall ensure that any impact on the interfacing systems is minimised in the context of application changes as a result of the proposed SaaS solution.		
IT 1.0	1.1.10	1.1.General Requirements	The Tenderer shall propose SaaS software delivery model.		
IT 1.0	1.1.11	1.1.General Requirements	The Tenderer shall anticipate and work with SAS for any additional hardware and / or software, which are not requested for in this Tender but are needed for the efficient operation of the SaaS solution, based on the stipulated load, performance requirements and required interfaces.		
IT 1.0	1.1.12	1.1.General Requirements	The Tenderer shall provide all necessary efforts to ensure that the SaaS solution works in SAS's current environment.		
IT 1.0	1.1.13	1.1.General Requirements	All data transfer across any network (especially through the internet) must be secure and encrypted using the latest security standard such as TLS 1.2 or above.		
IT 1.0	1.1.14	1.1.General Requirements	The Tenderer shall provide a licensed development environment capable of supporting at least five (5) staff members for development work.		
IT 1.0	1.1.15	1.1.General Requirements	The Tenderer shall provide a licensed test/staging environment with enough processing power and capacity to run SaaS solution load-testing or simulation of production data.		
IT 1.0	1.1.16	1.1.General Requirements	The Tenderer shall provide a licensed production environment that is always available using cluster technologies, RAID disks or other relevant technologies.		
IT 1.0	1.1.17	1.1.General Requirements	1.1.17 Software as a Service (SaaS) Delivery Model a. The Tenderer shall provide detailed technical specifications of the proposed hosting site(s), including: i. Server infrastructure; ii. Network/Internet Bandwidth; iii. Location/Country; iv. Site certification; v. Security infrastructure; vi. Backup and restoration infrastructure; vii. High availability infrastructure; viii. Encrypting virtual machines and storage volumes for data at rest protection; ix. Other hardware or software components needed to operate, run, and use the proposed solution.		
IT 1.0			b. The Tenderer shall provide information on data center locations of the hosting of Proposed Solution including SAS Data, exclusively within the geographical borders of Singapore.		
IT 1.0			c. The site shall be accessible with authentication from the Internet by all designated users.		
IT 1.0			d. The SaaS solution shall be accessible by SAS users securely via https without any security warnings or errors using SAS fully-qualified domain name, for example: https://<system>.sota.edu.sg/.		
IT 1.0			e. The Tenderer shall complete the external hosting risk control vendor assessment tool questionnaire as attached in Section 10 of this document.		
IT 1.0			f. Where the solution consists of a combination of different software products and components, the Tenderer shall ensure full integration across all components, maintaining a consistent user interface and user experience. For example, users should be able to access all subsystems through a single sign-on, avoiding the need to log in separately to each subsystem.		
IT 1.0	1.1.18	1.1.General Requirements	The Tenderer shall design, install, configure, test, implement and commission the SaaS, which must meet the requirements stipulated in this Invitation to Tender.		
IT 1.0	1.1.19	1.1.General Requirements	The Tenderer shall ensure that the SaaS solution is regularly tested and continues to be able to support the current and future prevailing desktop standards used by users at no additional cost to SAS. There must not be any additional cost to SAS for testing any new patches and releases on the prevailing desktop standards.		
IT 1.0	1.1.20	1.1.General Requirements	The Tenderer shall work with SAS on the deployment and testing of the SaaS and on any trouble-shooting required.		
IT 1.0	1.1.21	1.1.General Requirements	The Tenderer shall plan, coordinate, and collaborate with SAS and its appointed contractors (current vendors of the existing SAS system) for the installation, testing, integration, implementation, interfacing, deployment, and maintenance of the SaaS solution.		
IT 1.0	1.1.22	1.1.General Requirements	The Tenderer shall provide details of the application architecture of the proposed Cloud Service.		
IT 1.0	1.1.23	1.1.General Requirements	The cost for testing and implementing any releases (during the Contract Period) to the SaaS solution shall be deemed to be included in the Contract Price.		
IT 1.0	1.1.24	1.1.General Requirements	Release updates must be applied to the SaaS Solution in a timely manner (e.g within X days of update release). The Tenderer shall ensure that the CSP provide the information of the updates to SAS within the timeframe as agreed between the Tenderer and SAS. Before implementation of an update, the update must be tested to ensure that it does not have adverse effects on the SaaS Solution.		
IT 1.1	1.1.25	1.1.General Requirements	The tenderer shall work in tandem with SAS to: 1. comply with all obligations under the Personal Data Protection Act 2012 (PDPA) of Singapore 2. Data Protection Impact Assessments (DPIAs) The Vendor shall assist SAS to conduct DPIA to comply with Personal Data Protection Act 2012 (PDPA) and the Personal Data Protection Commission (PDPC) Guide. The assistance shall include: · Supplying information on personal data flows, processing activities, and technologies used. · Identifying and assessing risks to individuals' personal data. · Proposing and implementing appropriate technical and organizational measures to mitigate identified risks. The Vendor shall work in tandem with SAS to ensure DPIA performed is consistent with guidance issued by the PDPC, including the DPIA life cycle: · Plan and scope · Identify data flows and risks · Assess impact and likelihood · Implement risk mitigation measures · Review and monitor outcomes		
IT 1.0	1.2.1	1.2 User Interface	The Tenderer shall design the SaaS Solution with user-friendly and intuitive user interfaces. The workflow shall be well designed to facilitate data capturing, data processing, process tracking, process automation and presentation of results to the users.		
IT 1.0	1.2.2	1.2 User Interface	The SaaS Solution shall have a Web-based Interface and be supported by various web browsers (e.g. Safari, Google Chrome, Firefox) and Apple Operating System accessible by SAS.		
IT 1.0	1.2.3	1.2 User Interface	The Tenderer shall use the following Graphical User Interface (GUI) guidelines in the design of the SaaS Solution: a. Menus shall be structurally arranged and each option in the menu shall be easily accessible; b. Use of pictures and icons that are meaningful and highly intuitive to the users; c. Use of metaphors that closely emulate their real-world counterparts; d. Descriptive labels and control buttons names shall genuinely convey their intended behaviour; e. Grouping of related tasks to reduce overall complexity; f. Keystrokes for operation of the SaaS Solution shall be minimised; g. Use of SAS logo and content style as approved by the Office of Corporate Communications; h. Copyright is not infringed; i. Use of appropriate metadata in web content to facilitate searching by SAS's search engine.		

	1. General Technical Requirements				
IT 1.0	1.2.4	1.2 User Interface	For data entry functions, the Tenderer shall design the SaaS Solution to perform 'one-entry-many-updates' where appropriate such that when an entry is made, the SaaS solution shall automatically perform updates of all related files / tables / views, thus obviating the need for users to capture information which could be derived or which had been provided earlier.		
IT 1.0	1.2.5	1.2 User Interface	The Tenderer shall ensure that all error messages are descriptive, meaningful and easily understood for users to perform corrective actions.		
IT 1.0	1.2.6	1.2 User Interface	The Tenderer shall ensure that the SaaS Solution prompts users for confirmation before data is modified.		
IT 1.0	1.2.7	1.2 User Interface	The Tenderer shall introduce usability testing sessions involving diverse end-user groups during the development and post-implementation stages. Leverage user feedback to refine the interface and workflows, ensuring intuitive and efficient user interactions.		
IT 1.0	1.3.1	1.3 Ease of Maintenance	The SaaS solution shall be architected and designed with appropriate patterns used to allow new functions to be added and existing functions to be enhanced and/or decommissioned with minimal impact to the existing components and operations of the System.		
IT 1.0	1.3.2	1.3 Ease of Maintenance	There shall not be any hard-coded parameters in the SaaS solution (e.g. password, IP address, port number, path, file location, host name, domain name, etc.).		
IT 1.0	1.3.3	1.3 Ease of Maintenance	The Tenderer shall develop a set of comprehensive application related standards and guidelines (e.g. no duplication of codes without good reasons) to ease maintenance of the System.		
IT 1.0	1.3.4	1.3 Ease of Maintenance	The design of the SaaS solution shall be modular and flexible to allow functionality to be added and enhanced with minimal changes to the system, and without impacting the performance.		
IT 1.0	1.3.5	1.3 Ease of Maintenance	The SaaS solution shall be architected and designed with appropriate patterns used to allow new functions to be added and existing functions to be enhanced and/or decommissioned with minimal impact to the existing components and operations of the System.		
IT 1.0	1.3.6	1.3 Ease of Maintenance	The design of the SaaS solution shall allow ease of maintenance such that the software / component will adapt to a changed environment or can be modified to correct faults.		
IT 1.0	1.3.7	1.3 Ease of Maintenance	The SaaS solution shall have features to enable users to change validation rules and selection criteria without the need to alter program source codes. All changes must be made by the users using online facilities with complete audit trails.		
IT 1.0	1.3.8	1.3 Ease of Maintenance	The SaaS solution shall use parameter settings and reference / code tables, wherever possible. Parameters and reference / code tables shall be configurable / updateable with complete audit trails.		
IT 1.0	1.4.1	1.4 Up-to-date Technology	In the event of a newer version of the product or technology released before the Commissioning Date and the version is different from the Tenderer's tender proposal, the Tenderer shall assess the impact and propose the most suitable version to be adopted for production release with strong justification.During the Maintenance Period, the version of the product or technology shall not be more than 2 major versions behind the latest version available.		
IT 1.0	1.5.1	1.5 System Performance	In the event that the Service Level Agreement (SLA) outlined below is not met for amu reason, the Tenderer shall take all necessary remedial actions and provide remedial services at no additional cost to SAS. If the Tenderer diagnoses and shows concrete evidence that the problem is due to a component managed by SAS, the Tenderer shall be required to propose the necessary recommendations to SAS to resolve the issue. Definition of Severity Level •Critical: Major failure affecting all or a significant part of the Production System to the extent that normal business cannot be carried out. •Major: Complete loss of part of the business application affecting a group of users. Partial loss of critical business service causing significant operational issues. •Minor: System working for major portion of assets. Limited functionality impacted not affecting the usability of the solution. Small Group of users of a System or Services are affected.		
			<table><tr><th>Severity Level</th><th>Problem Response Time</th><th>Status Reporting</th></tr><tr><td>Critical</td><td>Within 4 hours</td><td>Every 4 hours</td></tr><tr><td>Major</td><td>Within 8 working hours</td><td>Daily</td></tr><tr><td>Minor</td><td>Within 1 working days</td><td>End of Problem Resolution</td></tr></table>		
IT 1.0	1.5.2	1.5 System Performance	The Tenderer shall review and highlight to SAS, in detail, all necessary actions required for the existing infrastructure performance requirements.		
IT 1.0	1.5.3	1.5 System Performance	The Tenderer shall provide the application performance testing benchmark results on meeting the defined set of standard benchmarked performance of the SaaS solution.		
IT 1.0	1.5.4	1.5 System Performance	For any testing performed, in the event of failure to meet the defined set of performance benchmarks, the Tenderer shall need to be able to establish whether or not the failure is caused by issues with the Cloud Hosting environment, or due to the SaaS solution's poorly written code or incorrectly set parameters for action to be taken by the parties responsible.		
IT 1.0	1.5.5	1.5 System Performance	The Tenderer shall note that the System Response Time shall be measured as the elapsed time between the moment a user initiates a computer process by pressing a key (<Enter> or <Submit>) or clicking a mouse or other input device and the moment first appearance of computer-generated output is displayed on an output device (e.g. screen of the user, printer) or elapsed time between two screens. A computer process can be a query or an update to a database, a request of an electronic document or any other logical unit of business transactions that involve interactive responses.		
IT 1.0	1.5.6	1.5 System Performance	The Tenderer shall also note that a transaction is defined as a completed unit of activity by a user of the SaaS solution utilising an online workstation interactively. The unit of activity is made up of one or more inputs by the users that result from input devices, such as a computer keyboard. Upon processing of the input by the SaaS solution, one or more characters of information response will be sent to the workstation that originated the input.		
IT 1.0	1.5.7	1.5 System Performance	The SaaS solution shall meet the online System Response Time as stated in Table 1: <table><tr><th>Type of Transaction</th><th>Expected Response Time</th></tr><tr><td>Online Transaction</td><td>Shall not exceed 5 seconds for 95% of the time and shall not exceed 10 seconds for the remaining 5% of the time.</td></tr><tr><td>Web Page Loading</td><td>Shall not exceed 3 seconds for 95% of the time and shall not exceed 5 seconds for the remaining 5% of the time.</td></tr><tr><td>User login to the System</td><td>Shall not exceed 3 seconds for 95% of the time and shall not exceed 5 seconds for the remaining 5% of the time.</td></tr></table>		
IT 1.0	1.5.8	1.5 System Performance	The SaaS solution shall provide optimal system performance for online transactions, scheduled batch jobs as well as ad hoc batch jobs submitted by the users.		
IT 1.0	1.5.9	1.5 System Performance	The SaaS solution response time is defined as the elapsed time between a user pressing a key to start a computer process and the last display of the refreshed information generated on the user's computer screen. The response time for online processing shall not exceed three (3) seconds for transactions accessing from intranet and not exceed eight (8) seconds over the internet for ninety eight percent (98%) of the transactions. Generation of reports should not impact the system response for online processing.		
IT 1.0	1.5.10	1.5 System Performance	The Tenderer shall perform stress tests that are deemed suitable by SAS on the system to certify that the system can conform to the stated performance requirements.		
IT 1.0	1.6.1	1.6 System Availability	The Tenderer shall ensure that the SaaS solution minimally achieves 99.5% availability.		
IT 1.0	1.6.2	1.6 System Availability	System maintenance activities (e.g. backup jobs) shall not impact the availability of the SaaS solution.		
IT 1.0	1.6.3	1.6 System Availability	The Tenderer shall conduct regular system maintenance, configuration, and fine tuning/optimisation to ensure the SaaS solution is always in good working condition. The Tenderer shall then inform SAS at agreed trigger points on the necessary upgrade and/or enhancement for continual achievement of optimum system performance and required Service Availability.		
IT 1.0	1.6.4	1.6 System Availability	The Tenderer shall ensure that all troubleshooting, upgrade or maintenance work on the production system shall be done strictly after office hours to avoid disruption of Service.		
IT 1.0	1.6.5	1.6 System Availability	The Tenderer shall provide SAS the planned activities at the beginning of the calendar year.		
IT 1.0	1.6.6	1.6 System Availability	The Tenderer shall inform SAS on the ad-hoc maintenance 1 month before the executions.		
IT 1.0	1.6.7	1.6 System Availability	The Tenderer shall clarify and establish the required scheduled service downtime and planned total service uptime per calendar month with SAS to avoid unnecessary disputes later.		
IT 1.0	1.6.8	1.6 System Availability	The Tenderer shall implement front end scaling based on the number of incoming requests (e.g. web pages, data transfer).		
IT 1.0	1.6.9	1.6 System Availability	The Tenderer shall implement back-end scaling such as load based scaling (jobs in queue) and time-based scaling (how long jobs have been in queue).		
IT 1.0	1.6.10	1.6 System Availability	The Tenderer shall monitor and review metrics such as concurrent limitations, increased latency, time-out errors and upgrade capacities if required.		
IT 1.0	1.6.11	1.6 System Availability	The Tenderer shall ensure that the unexpected system downtime shall not exceed six (6) hours in aggregate (that is, total downtime aggregated for all servers) for each period of thirty (30) days, which the period is to be computed on a moving average* basis.		

	1. General Technical Requirements				
IT 1.0	1.6.12	1.6 System Availability	The Tenderer shall ensure that the frequency of the unexpected system downtime shall not exceed six (6) times in aggregate (i.e. total downtime frequency for all servers) for each period of thirty (30) days, which the period is to be computed on a moving average* basis. Note: A thirty (30) days simple moving average forecast is the average of the demand from the previous thirty days; with each new day, the last day is added, and the oldest day is deleted before recalculating the new average. For instances where the system availability is computed for a fixed period instead of a rolling period, the maximum system downtime and downtime frequency would be pro-rated proportionally. For example, if the maximum downtime and frequency for thirty (30) days rolling period is 6 hours and 6 occurrences; for a 90-days Performance Guarantee Period (PGP), the figures would be 18 hours (6 hours x 3) and 18 occurrences (6 occurrences x 3) respectively.		
IT 1.0	1.6.13	1.6 System Availability	When backup, housekeeping and other system routines or tasks are being performed, the SaaS solution shall still be available to the users with no or minimum loss of system performance. The Tenderer shall highlight the expected degradation in system performance, if any.		
IT 1.0	1.6.14	1.6 System Availability	The SaaS solution shall run in an unattended mode after office hours for data backup and batch jobs.		
IT 1.0	1.6.15	1.6 System Availability	The Tenderer shall plan and schedule downtime well in advance. SAS shall be notified at least one (1) month before any scheduled downtime. The shutdown time shall not exceed twenty-four (24) hours.		
IT 1.0	1.6.16	1.6 System Availability	The Tenderer shall submit a monthly report on the relevant statistics, such as total uptime, downtime, system usage, CPU memory, CPU storage, transaction volume, etc.		
IT 1.0	1.7.1	1.7 System Reliability/Integrity	The Tenderer shall ensure that the SaaS solution is fully tested, and quality assured before implementation to achieve maximum reliability.		
IT 1.0	1.7.2	1.7 System Reliability/Integrity	The Tenderer shall propose suitable procedures for performance monitoring and analysis to enable proper capacity planning, tuning and maintenance.		
IT 1.0	1.7.3	1.7 System Reliability/Integrity	The Tenderer shall ensure that failure of any software fault in any of the functions in the SaaS solution shall not affect the integrity of the data captured/stored or lead to any loss of data in the SaaS solution.		
IT 1.0	1.7.4	1.7 System Reliability/Integrity	The SaaS solution shall be fully designed to share/reuse common modules and components.		
IT 1.0	1.7.5	1.7 System Reliability/Integrity	The SaaS solution shall be designed to maintain data accuracy and integrity within the SaaS solution and between the external system(s) it interfaces with.		
IT 1.0	1.7.6	1.7 System Reliability/Integrity	The SaaS solution shall provide for automatic recovery and restart facilities to ensure minimum downtime. The Tenderer shall provide clear descriptions / instructions on such facilities in the Tender Proposal.		
IT 1.0	1.7.7	1.7 System Reliability/Integrity	The Tenderer shall ensure that a software fault in a module shall not lead to a total SaaS solution failure.		
IT 1.0	1.7.8	1.7 System Reliability/Integrity	The Tenderer shall ensure that failure of a transaction or reporting at one PC shall not affect other users on the SaaS solution.		
IT 1.0	1.7.9	1.7 System Reliability/Integrity	The Tenderer shall ensure that failure of any transaction or a software fault in any of the functions in the system shall not affect the integrity of the data captured / stored or lead to any loss of data in the SaaS solution.		
IT 1.0	1.7.10	1.7 System Reliability/Integrity	The SaaS solution shall recover all data stored up to the last successfully completed transaction before a SaaS solution failure occurs. The effect of a failed transaction or reporting on the database or data file shall be automatically and dynamically backed up.		
IT 1.0	1.8.1	1.8 System Readiness	The Tenderer shall be responsible for the management and coordination of all activities, including working closely with the relevant parties to ensure a smooth roll-out of the SaaS solution. This shall be applicable at all SaaS solution implementations, deployments, System Integration Test, User Acceptance Test, trainings and rollouts.		
IT 1.0	1.8.2	1.8 System Readiness	The Tenderer shall submit the necessary documentations required for system readiness as part of the proposal.		
IT 1.0	1.8.3	1.8 System Readiness	The SaaS solution shall be designed without the need to have specialised staff and with low maintenance overheads (for example, automating job processes, reducing the number of tasks for a process as much as possible).		
IT 1.0	1.9.1	1.9 Service Administration	All administrative access given to SAS to access the SaaS solution hosted in the Commercial Cloud shall be performed remotely via the Internet.		
IT 1.0	1.9.2	1.9 Service Administration	Remote administrative access shall only be granted to authorised personnel who need to perform administration on the SaaS solution remotely.		
IT 1.0	1.9.3	1.9 Service Administration	The Tenderer shall implement the security requirements for remote administration in Clause 1.9.2.		
IT 1.0	1.10.1	1.0 Extensibility	The SaaS solution shall be easily integrated with other portals and applications. The Tenderer shall provide detailed information and examples on how the SaaS solution supports the current technologies and standards, including the availability of any programming interfaces.		
IT 1.0	1.11.1	1.11 Solution Platform	The Tenderer shall specify all the required software pre-requisites such as plug-ins and runtime environments required to be installed on the client machines.		
IT 1.0	1.11.2	1.11 Solution Platform	All native mobile applications provided as part of the solution shall support both iOS and Android. The page shall adopt responsive design to cater for different screen orientations if applicable.		
IT 1.0	1.11.3	1.11 Solution Platform	The SaaS solution shall offer authenticated SMTP service and encryption (use of TLS 1.2 or above) if it needs to send out email.		
IT 1.0	1.11.4	1.11 Solution Platform	The SaaS solution shall provide the feature to configure email trigger with exception details if any error occurred in the SaaS solution. Sender and recipients email addresses shall be configurable.		
IT 1.0	1.11.5	1.11 Solution Platform	The SaaS solution shall allow SAS to define the file formats in which the SaaS solution is able to export queries, reports and documents, and handle files (e.g., txt, csv, xls, xlsx, jpg, pdf etc) imported or transmitted into the SaaS solution.		
IT 1.0	1.12.1	1.12 Disaster Recovery	The Tenderer shall ensure high availability of the SaaS solution in the event of the commercial cloud service provider (CSP) experiencing data centre failures. This shall be with zero data or content loss.		
IT 1.0	1.12.2	1.12 Disaster Recovery	The Tenderer shall work with SAS in ensuring the SaaS solution's availability in an event of a disaster.		
IT 1.0	1.12.3	1.12 Disaster Recovery	The Tenderer shall propose a disaster recovery plan for the proposed SaaS solution to ensure business continuity in the event when a disaster is declared. The Tenderer shall also state the detection mechanism, the time required and the locations to carry out the recovery.		
IT 1.0	1.13.1	1. 13 Data Retention	The Tenderer should support configurable data retention policies for candidate records and employee records, ensuring compliance with company and local legal requirements (e.g., retaining records for 7 years).		
IT 1.0	1.13.2	1. 13 Data Retention	The Tenderer shall always provide the cost-optimization design/solution of the data archival based on SAS needs.		
IT 1.0	1.13.3	1. 13 Data Retention	The Tenderer shall purge the data when the retention period for the data is over.		
IT 1.0	1.13.4	1. 13 Data Retention	The SaaS solution shall have, but not limited to, the following features for housekeeping: a. Facility to archive historical data on a periodic batch basis to the Data Storage. b. The archival period shall be user-specified; Facility to physically delete historical data on a periodic batch basis, which shall be user-specified; c. Facility to archive audit logs on a periodic batch basis. The archival period shall be user-specified; d. Facility to physically delete revoked accounts which have been ineffective for a period defined by authorised users; e. Facility to retrieve archived historical data from the Data Storage. The archival period shall be user-specified; f. The tenderer shall propose an archival solution to move old data out of the main SaaS solution, to a read-only site, which administrator can export, delete records that has past it's retention requirements.		
IT 1.0	1.14.1	1.14 Data Migration	The Tenderer shall provide a data (e.g., transactional data, metadata etc) migration plan for migrating the data from database on-premises to the commercial Cloud as agreed with SAS before the execution.		
IT 1.0	1.14.2	1.14 Data Migration	The Tenderer shall implement the transform and load processes to move data from the database on-premises to the commercial Cloud.		
IT 1.0	1.14.3	1.14 Data Migration	The Tenderer shall convert the historical data from the existing relational database to the Cloud database.		
IT 1.0	1.14.4	1.14 Data Migration	The Tenderer shall conduct the post-migration audit to ensure all the historical data are retrievable smoothly in the Cloud before the old SaaS solution can be retired.		
IT 1.0	1.14.5	1.14 Data Migration	The Tenderer shall implement a backup plan to rollback in case the first attempt of data migration fails.		
IT 1.0	1.14.6	1.14 Data Migration	The Tenderer shall propose an appropriate migration tool to SAS.		
IT 1.0	1.14.7	1.14 Data Migration	The Tenderer shall provide the data reports and checklist of the whole data migration activities to SAS.		
IT 1.0	1.14.8	1.14 Data Migration	The Tenderer shall share the issue logs and audit logs of the operational migration process to SAS.		
IT 1.0	1.14.9	1.14 Data Migration	The Tenderer shall propose the solutions on the issue logs of the operational migration process for SAS approval.		
IT 1.0	1.14.10	1.14 Data Migration	The Tenderer shall run the subsequent rounds of the data migration activities until all operational required data migrate to the SaaS solution without additional cost.		
IT 1.0	1.14.11	1.14 Data Migration	The Tendered shall strengthen the data migration process by incorporating data validation tools to detect and resolve legacy data inconsistencies. Establish a fallback mechanism, such as incremental data migrations and pre-verified backups, to recover from any unexpected errors during the migration phase.		
	2. Architecture				
IT 1.0	2.1.1	2.1 General Architecture Requ	The SaaS solution shall leverage the benefits of adopting cloud, to fulfil business expectations such as availability, security, flexibility, scalability, performance, compliance and cost.		
IT 1.0	2.1.2	2.1 General Architecture Requ	The Tenderer shall propose a To-Be SaaS solution architecture design based on the functionalities of the SaaS solution.		
IT 1.0	2.1.3	2.1 General Architecture Requ	The Tenderer shall provide a loose coupling architecture design for the SaaS solution.		
IT 1.0	2.1.4	2.1 General Architecture Requ	Where there is a need for additional controls and governance to safeguard the integrity of the System, the Tenderer shall develop and document the additional controls and governance processes for the development, maintenance and operations team to comply. The controls can come in the form of manual processes or automated checks, though SAS has preference for automated checks.		

	1. General Technical Requirements				
IT 1.0	2.1.5	2.1 General Architecture Requ	The SaaS solution shall meet SaaS solution availability requirements and recover any disruptions gracefully and on a timely basis.		
IT 1.0	2.1.6	2.1 General Architecture Requ	All services and components (e.g. operating systems, logging layers, cloud configurations and databases) shall be configured to a consistent and common locale to facilitate the tracing of transactions. Presentation of data shall adopt Singapore locale (i.e. UTC+8) and in English.		
IT 1.0	2.2.1	2.2 Backup & Recovery Plan	The Tenderer shall submit a backup and recovery methodology for the Solutions in the Tender Proposal. The methodology shall include detailed description of the proposed approach to recover loss / corruption of data or SaaS solution, frequency of backup as well as the procedures for performing the backup and recovery.		
IT 1.0	2.2.2	2.2 Backup & Recovery Plan	The Tenderer shall define a cost-effective solution to securely store a copy of the data (e.g. business data, security keys, source codes, infrastructure codes, scripts, configuration data, virtual machine images, etc.) on the cloud with proper access controls.		
IT 1.0	2.2.3	2.2 Backup & Recovery Plan	The proposed solution shall include the backup strategy for each type of data and the recommended retention and archival strategy to be used (including security considerations such as encryption and password protection), subject to SAS's approval.		
IT 1.0	2.2.4	2.2 Backup & Recovery Plan	The Tenderer shall provide a backup strategy with best industry practices for each type of data and the recommended retention and archival strategy to be used.		
IT 1.0	2.2.5	2.2 Backup & Recovery Plan	The Tenderer shall perform backups of various information contained in the SaaS solution is performed with the agreed frequency consistent with the Recovery Point Objective (RPO) within 24 hours and Recovery Time Objective (RTO) within 12 hours.		
IT 1.0	2.2.6	2.2 Backup & Recovery Plan	The Tenderer shall implement the same security safeguards in the alternative site as the primary site.		
IT 1.0	2.3.1	2.3 System Integration	The SaaS solution shall integrate with the following existing SAS systems (on-premises or Cloud) using APIs or connectors: Microsoft SharePoint (Staff Directory in Staff Portal); Event Booking Management System (short as EBMS); Student Management Systems (short as SMS); DocHub for e-signature; Digital Form System (Using OutSystems); Google Authentication for user access management.		
IT 1.0	2.3.2	2.3 System Integration	The SaaS solution shall be able to integrate with third-party systems using APIs or connectors in the Cloud.		
IT 1.0	2.3.3	2.3 System Integration	The following table outlines the indicative interface requirements for the SaaS solution. The Tenderer shall assess and propose an appropriate interface design for implementation to facilitate integration and seamless end-to-end business process.		
IT 1.0	2.3.4	2.3 System Integration	To ensure seamless integration with third-party systems, the tenderer shall propose a robust error-handling framework that automatically identifies failed transactions in an error report indicating the type of error with date and time stamp. All integration shall have a control report i.e. exporting of data and importing of date to ensure data consistency and integrity across interconnected systems.		
IT 1.0					
IT 1.0	3. Infrastructure				
IT 1.0	3.1.1	3.1 Commercial Cloud Services	The Tenderer shall submit a proposal that comprises: a. The complete set of itemised PaaS commercial cloud services that are required from the commercial CSP to implement the proposed SaaS solution. This set of services are hereinafter being referred to as the "Cloud Solution". The Cloud Solution shall be: i. Configured to be distributed across the commercial CSP's multiple data centres so as to continue ensuring the availability of the Cloud Solution even in the event of the commercial CSP experiencing multiple data centre failures. This shall be with zero data loss. b. The complete set of services and infrastructure (hardware and software) from third party providers that are required to be deployed as part of the proposed solution. c. The complete itemised charges for all components of the proposed SaaS Solution including components that are not required immediately but may be needed to support service requests in the future.		
IT 1.0	3.1.2	3.1 Commercial Cloud Services	The proposed Cloud Solution shall include: a. The list and descriptions of the individual items to be subscribed from the commercial CSP as well as the units required; b. The list and descriptions of the individual items required for the proposed SaaS solution but not subscribed from the commercial CSP directly as well as the units required; c. Details explaining how the units required are derived as well as all assumptions made; and d. The following environments: i. Production (Prod); ii. System Integration Test (SIT); iii. User Acceptance Test (UAT). (ii) and (iii) in the above Clause 3.1.2(d) will be collectively known as "Testing Environments".		
IT 1.0	3.1.3	3.1 Commercial Cloud Services	The SaaS solution shall implement, deploy and support Platform as Code (PaC) for the provision and deployment of Cloud services where possible.		
IT 1.0	3.1.4	3.1 Commercial Cloud Services	The Tenderer shall submit all solution design documents and diagrams of the SaaS solution clearly detailing and identifying how the a. Components of the proposed SaaS solution are derived and how they meet the tender requirements; and b. The Proposed SaaS solution is designed such that it is able to handle scaling on demand.		
IT 1.0	3.1.5	3.1 Commercial Cloud Services	The Tenderer shall adopt best practices and open standards available in the cloud environment so as to optimise the in-built SaaS solution capabilities and to minimise customization, SaaS solution deployment time and cost.		
IT 1.0	3.1.6	3.1 Commercial Cloud Services	The Tenderer shall propose a commercial CSP that is Multi-Tier Cloud Security (MCTS) certified.		
IT 1.0	3.1.7	3.1 Commercial Cloud Services	The proposed SaaS Solution shall include the following security measures: a. Use cloud native SaaS solution and network firewalls, such as AWS Security Groups and Network Access Control List (NACL) or equivalent; b. Use cloud security detection tools, such as AWS GuardDuty or equivalent; c. Use cloud native logs whenever possible, such as AWS CloudTrail, AWS CloudWatch or equivalent; d. Receive notification when suspicious activities are detected; and e. Stream logs to Commercial Cloud logging servers.		
IT 1.0	3.1.8	3.1 Commercial Cloud Services	In the multi-tenancy, the commercial CSP shall adequately configure the infrastructure to ensure no corrupted data from other tenants could spread to SAS.		
IT 1.0	3.1.9	3.1 Commercial Cloud Services	In the multi-tenancy, the commercial CSP shall put strong authentication and access control mechanisms on the physical host to prevent a malicious user from changing the virtual machine's configuration to cause a loss of monitoring capabilities.		
IT 1.0	3.2.1	3.2.Transition Management to	The Tenderer shall duly hand over all items owned by SAS to the new commercial CSP, including assets, subscriptions, licences, SaaS solution documentation, and all SAS's account information in both hard and editable softcopy in Microsoft Office file format.		
IT 1.0	3.2.2	3.2.Transition Management to	The Tenderer shall ensure the accuracy and completeness of information documented and handed over to the new commercial CSP.		
IT 1.0	3.2.3	3.2.Transition Management to	The Tenderer shall also duly hand over all contents and all related data owned by SAS to the new commercial CSP in editable softcopy in their source code and executable format. The source code shall be the source code used to generate the deployed executables.		
IT 1.0	3.2.4	3.2.Transition Management to	The Tenderer shall brief the new commercial CSP- fully on all relevant operational information required to achieve a smooth handover process and allow the latter to shadow his team to learn the daily operational activities.		
	4.Service Management				
IT 1.0	4.1.1	4.1.Service Management and (	The goal of the Service Management and Operations is to provide ongoing day-to-day operation support, maintenance and management of the cloud services for the SaaS solution. Such provided services are operational and recurrent in nature and shall hereinafter be referred to as "Managed Services".		
IT 1.0	4.1.2	4.1.Service Management and (	The Tenderer shall itemise and state all Managed Services charges for the implementation and maintenance of the SaaS solution. The Tenderer shall provide all Managed Services for the SaaS solution.		
IT 1.0	4.1.3	4.1.Service Management and (	The Managed Services shall minimally cover the scope of the following services: a. Patch Management Services; b. Identity Administration Services; c. Backup & Recovery Services; d. Service Operation Control Centre; and e. Service Desk Services. The Tenderer shall provide any additional Managed Services with justification if required for the support of the proposed SaaS solution. The Tenderer shall itemise and state such additional Managed Services.		

	1. General Technical Requirements				
IT 1.0	4.2.1	4.2 Patch, Minor (Fix Pack) and Major (Service Packs) Management Services	The Tenderer shall note the following for the SaaS solution: a. Patch/fix pack is a generally available update provided by the product vendor or open-source communities (hereinafter collectively referred to as "Vendors") to fix a known bug or issue. b. Hotfix is a patch to fix a specific issue, not always as part of a general release. c. Minor updates/fix packs are incremental updates between Major Update/ Service Pack of software versions to fix multiple outstanding issues. d. Major Update/Service Pack is an update that fixes many outstanding issues, normally includes all patches, hot fixes, maintenance releases/ fixes packs that pre-dates the service pack as well as include new functionality. a. to d. in this Clause 4.2.1 shall collectively be referred to as "Patch(es)" in the tender documents.		
IT 1.0	4.2.2	4.2 Patch, Minor (Fix Pack) and Major (Service Packs) Management Services	The Tenderer shall propose the management process that shall be used to evaluate, propose and justify the Patches required for the SaaS solution to SAS for approval before implementing any changes.		
IT 1.0	4.2.3	4.2 Patch, Minor (Fix Pack) and Major (Service Packs) Management Services	The Tenderer shall establish and implement the following to manage all patching activities required in the SaaS solution: a. Patch management process to be approved by SAS and patch management team.		
	5.IT Security				
IT 1.0	5.1.1	5.1.General Compliance	The Tenderer shall note that all security requirements under this section are mandatory unless otherwise explicitly stated, and each security requirement, regardless of the sub-section it is located, shall be applicable to the entire scope of this Contract for the SaaS solution unless otherwise explicitly stated.		
IT 1.0	5.1.2	5.1.General Compliance	The Tenderer shall provide details of conformance (if any) / evidence of due diligences to relevant security standards (e.g. ISO 27001, Multi-Tier Cloud Security Standard) attained.		
IT 1.0	5.1.3	5.1.General Compliance	The Tenderer shall ensure that the SaaS solution is secure and shall subject all aspects of the design, implementation, operation and security controls of the proposed SaaS solution for approval by SAS. The following design principles shall be incorporated: confidentiality; compliance; availability; authentication; integrity; and access control.		
IT 1.0	5.1.4	5.1.General Compliance	The Tenderer shall provide the details of all aspects of the proposed System for review by SAS. The Tenderer shall not withhold any information pertaining to the technical details and security limitations of the proposed SaaS solution.		
IT 1.0	5.1.5	5.1.General Compliance	The Tenderer shall ensure the provision of sufficient security controls to protect the SaaS solution against unauthorised access, data loss, intrusion, malicious software infection, software vulnerability attacks, and hardware attack.		
IT 1.0	5.1.6	5.1.General Compliance	The Tenderer shall ensure that no security backdoors and loopholes exist in the SaaS solution.		
IT 1.0	5.1.7	5.1.General Compliance	The Tenderer shall wholly be responsible for any breach in security as a result of insecure implementations and/or configuration, missing patches, negligence, insider attacks, or loopholes in the solution.		
IT 1.0	5.1.8	5.1.General Compliance	The Tenderer shall be responsible for ensuring the proposed security controls can be integrated and work seamlessly with other suppliers.		
IT 1.0	5.1.9	5.1.General Compliance	The Tenderer shall implement security control measures to protect data at rest, data in motion and data in use.		
IT 1.0	5.1.10	5.1.General Compliance	Process, procedures and control measures shall be adequately and properly documented, and subject to the acceptance by SAS.		
IT 1.0	5.1.11	5.1.General Compliance	The SaaS solution shall be resilient against known cyber-attacks and easily reconfigurable to respond to new and zero-day security threats that may arise.		
IT 1.0	5.1.12	5.1.General Compliance	The security procedures and standards shall include at least the followings: Security Risk Management; Security Architecture and Design; Personnel Security; Security Incident and Response Management; Security Management and Operation Processes; Security Configuration; Security Reviews; Audits for the SaaS solution.		
IT 1.0	5.1.13	5.1.General Compliance	The Tenderer shall provide technical documentation on the network, system, database and applications when requested during security risk analysis, security standards and policy implementation specific to the SaaS solution.		
IT 1.0	5.1.14	5.1.General Compliance	Only approved commercial cloud and SaaS providers shall be used if SaaS is proposed. If the use of SaaS providers is proposed, the Tenderer shall work with SAS to perform risk assessment on the proposed SaaS.		
IT 1.0	5.2.1	5.2 Responsibilities	The Tenderer shall work with SAS to perform security risk assessments prior to using the cloud service and conduct a review at least once every 12 months thereafter. The Tenderer shall submit the security risk assessment report to SAS within 10 working days upon the completion of each security risk assessment. The Tenderer shall identify risk, respective inherent risk levels and propose treatment plans. The resultant residual risk level after treatment plans shall be approved by SAS's designated approving SAS.		
IT 1.0	5.2.2	5.2 Responsibilities	The Tenderer shall ensure that no security backdoors, loopholes or any form of mechanisms that allow unauthorised access are built into the SaaS solution.		
IT 1.0	5.2.3	5.2 Responsibilities	The Tenderer shall ensure that all software implemented is the latest most stable version. In the course of implementation, any Patches or fixes shall be implemented. The Tenderer shall discuss with SAS if any deviation is required.		
IT 1.0	5.2.4	5.2 Responsibilities	The Tenderer shall implement a procedure to track, detail and rectify any security vulnerabilities affecting all SaaS solution components (including but not limited to open-source products/libraries, commercial-off-the-shelf (COTS) products, underlying technologies and libraries).		
IT 1.0	5.2.5	5.2 Responsibilities	The Tenderer shall ensure that any login to the SaaS solution for administrative or deployment purposes are only allowed from authorised source IP addresses in Singapore. All overseas logon and unauthorised IP addresses to the SaaS solution for administrative or deployment purposes shall be denied.		
IT 1.0	5.2.6	5.2 Responsibilities	The role creation and maintenance of the SaaS solution shall be centrally managed by privileged users only. Privileged users refer to users such as the operating system administrator, application security administrator, database administrator.		
IT 1.0	5.2.7	5.2 Responsibilities	The Tenderer shall define the role and responsibilities of all the administrator(s). It is important that tasks such as user administration and audit management are established.		
IT 1.0	5.2.8	5.2 Responsibilities	The Tenderer shall document the roles and responsibilities of all users in a clear and concise manner.		
IT 1.0	5.2.9	5.2 Responsibilities	The Tenderer shall propose and document the roles and responsibilities that are only necessary to facilitate the operation and change management of the SaaS solution, such as SaaS solution, application and security administration, content management, content reviewers and approvers, and etc.		
IT 1.0	5.3.1	5.3.Data Security	Cryptographic implementations that have been certified (e.g. FIPS certification) will be preferred. The Tenderer should submit proof of such certifications (e.g.FIPS certification) as part of the Tender submission for evaluation, if available.		
IT 1.0	5.3.2	5.3.Data Security	The Tenderer shall ensure that cryptographic mechanisms implemented in the SaaS solution are capable of handling normal and peak loads without degrading the performance of the SaaS solution.		
IT 1.0	5.3.3	5.3.Data Security	All digital certificates implemented within the SaaS solution shall be digitally signed by a trusted and recognized Certificate Authority (i.e. no self-signed certificates).		
IT 1.0	5.3.4	5.3.Data Security	The Tenderer shall implement measures and processes (such as password protection or encryption) to prevent unauthorised disclosure, modification or deletion of SAS's security-classified information in the SaaS solution and end-users' computing devices such as laptops and tablets.		
IT 1.0	5.3.5	5.3.Data Security	The Tenderer shall provide a detailed description of the security measures and processes including the storage and transmission encryption software to be used in the proposal.		
IT 1.0	5.3.6	5.3.Data Security	The Tenderer shall ensure that encrypted data will continue to be usable in the event that the production SaaS solution becomes unavailable or unusable.		
IT 1.0	5.3.7	5.3.Data Security	The Tenderer shall ensure that all sensitive data in the Cloud is identified and classified in accordance with the Information Sensitivity Framework (ISF) for Entity Information to ensure the necessary safeguards are in place.		
IT 1.0	5.3.8	5.3.Data Security	The Tenderer shall ensure that processes involving data-in-motion, such as backup or migration, are protected with encryption, physical and access controls.		
IT 1.0	5.3.9	5.3.Data Security	The Tenderer shall ensure that field-level encryption is applied to add an additional layer of security to protect data throughout SaaS solution processing so that only allowed applications can read/view it.		
IT 1.0	5.3.10	5.3.Data Security	The Tenderer shall work with SAS to make sure that the sensitive data that has reached its end of its lifecycle or no longer needs to be securely erased e.g. unrecoverable in-the-clear.		
IT 1.0	5.3.11	5.3.Data Security	The Tenderer shall ensure that data is accorded access rights based on principle of least privilege throughout its life cycle.		
IT 1.0	5.3.12	5.3.Data Security	The Tenderer shall ensure to turn on the data masking feature at the UI level to protect sensitive data (e.g., personal identity number, salary, DOB, etc.) by allowing only users with field-level authorization to view a field value.		
IT 1.0	5.3.13	5.3.Data Security	The Tenderer shall propose data centres designed for the SaaS solution with fully redundant subsystems and compartmentalised security zones.		
IT 1.0	5.3.14	5.3.Data Security	The Tenderer shall ensure that data centres adhere to the strictest physical security measures: a. Multiple layers of authentication are required before access is granted to the server area; b. Critical areas require two-factor biometric authentication; c. Camera surveillance SaaS solution is located at critical internal and external entry points; d. Security personnel monitor the data centres 24/7; e. Unauthorised access attempts are logged and monitored by data centre security. f. The Tenderer shall encrypt data at rest, data in motion and data in use. g. The Tenderer shall replicate the production database and transaction logs to the secondary maintained at an off-site data centre in real-time. Backups of the database and transaction logs are encrypted for any database that contains SAS data.		
IT 1.0	5.4.1	5.4.Security Hardening	The Tenderer shall ensure all services, servers, devices and application components are securely configured (i.e., "hardened") before being installed or set up in the respective environments. SAS will provide necessary hardening guides, if available. If the hardening guide is not available, the Tenderer shall provide and maintain the hardening guide, subject to SAS's review and approval.		

	1. General Technical Requirements				
IT 1.0	5.4.2	5.4.Security Hardening	The Tenderer shall establish security hardening guidelines on all services, servers, devices and application components based on Security Best Practices Standards (e.g. NIST 800-53, CIS Benchmarks, SANS or product principal's guides).		
IT 1.0	5.4.3	5.4.Security Hardening	The Tenderer shall apply the following security measures, in conjunction with secure configuration profiles to further secure operating systems and virtualized environment: a. Disable login functionality to system-level privileged accounts, such as "root" account, where possible; b. Restrict switching to system level privileged accounts using software like "su"; c. Enable only services that are required; Remove unused or obsolete files, including backup files and virtual system images; d. Restrict transfer of data between hypervisors and their guest operating systems; e. Use separate system accounts for hypervisor and guest operating systems.		
IT 1.0	5.4.4	5.4.Security Hardening	The Tenderer shall ensure that security hardening is carried out for new or changes to components of the SaaS solution before deploying into the production environment and on an ad-hoc basis as requested by SAS at no additional cost to SAS.		
IT 1.0	5.4.5	5.4.Security Hardening	The Tenderer shall ensure the packaging hardening is completed before the Commissioning Date.		
IT 1.0	5.4.6	5.4.Security Hardening	The Tenderer shall maintain the effectiveness and adequacy of all security hardening guides to address new security threats affecting the SaaS solution. Security configuration shall be verified for compliance prior to the Commissioning Date and once every year thereafter.		
IT 1.0	5.5.1	5.5.Vulnerability and Patch Management	The Tenderer shall maintain an IT asset inventory of all infrastructure, cloud subscribed services, including software and tools deployed in the cloud. This inventory shall be used as a checklist to track vulnerabilities for the SaaS solution and for change management planning. The inventory shall be updated and reported monthly and ensure no end-of-life assets are deployed.		
IT 1.0	5.5.2	5.5.Vulnerability and Patch Management	The Tenderer shall implement tracking of expiry dates for all digital assets such as certificates, software licences, etc for renewal.		
IT 1.0	5.5.3	5.5.Vulnerability and Patch Management	The Tenderer shall ensure any changes to the Cloud does not alter compliance to the security requirements agreed as part of contract.		
IT 1.0	5.5.4	5.5.Vulnerability and Patch Management	The Tenderer shall ensure developers and third-party Tenderer follow the established software development lifecycle and release management process to control implementation of major changes.		
IT 1.0	5.5.5	5.5.Vulnerability and Patch Management	The Tenderer shall provide a vulnerability and security patch management process documents to ensure thorough tracking of security vulnerabilities for all IT assets within the SaaS solution, which include: a. Maintain and use the IT asset inventory as a source of truth for vulnerability tracking. b. Tracking of vulnerability alerts and assessing their applicability monthly or as required by SAS. c. Performing criticality review and testing. d. Conducting change management review. e. Planning for contingency or roll back. f. Implementing patches.		
IT 1.0	5.5.6	5.5.Vulnerability and Patch Management	The Tenderer shall proactively monitor information and release information about new security Patches on a timely basis. Timely bases included Real-time, Regular intervals, Scheduled releases, Ad hoc, zero-day patch and critical patch.SAS may inform the Tenderer on any advisories when available.		
IT 1.0	5.5.7	5.5.Vulnerability and Patch Management	Upon evaluation that it is an emergency one, the Tenderer shall submit a request for change to SAS to seek approval to deploy the software update.		
IT 1.0	5.5.8	5.5.Vulnerability and Patch Management	The Tenderer shall ensure that vulnerability assessment using industry recognised tools is performed on the SaaS solution on a quarterly basis.		
IT 1.0	5.5.9	5.5.Vulnerability and Patch Management	The Tenderer shall ensure that Penetration Testing (PT) using industry recognised tools is performed on the SaaS solution on a yearly basis.		
IT 1.0	5.5.10	5.5.Vulnerability and Patch Management	If any vulnerability is found due to parts and components supplied by the Tenderer, the Tenderer shall provide remedial actions to rectify the problem at no additional cost to SAS.		
IT 1.0	5.5.11	5.5.Vulnerability and Patch Management	The Tenderer shall ensure that vulnerabilities identified through the VAPT are remediated before deploying the change to the production System.		
IT 1.0	5.5.12	5.5.Vulnerability and Patch Management	The Tenderer shall perform the security scanning again after the remedial actions are taken to ensure all the vulnerabilities are resolved.		
IT 1.0	5.5.13	5.5.Vulnerability and Patch Management	The Tenderer shall implement measures to protect endpoint devices used for software deployment to mitigate risks of transferring malicious software (e.g. HIPS, EPP, EDR).		
IT 1.0	5.6.1	5.6.Authentication and Password Security	The Tenderer shall put in place strong authentication and access control mechanisms to ensure that only authorised users are granted access to controlled features (e.g. personalised views).		
IT 1.0	5.6.2	5.6.Authentication and Password Security	The SaaS solution shall support strong password policy and a process to enforce strong password administration, secure creation, distribution, termination, storage and destruction of passwords. User's credentials (i.e. User ID and Password) shall be distributed to users in such a manner that their confidentiality is maintained.		
IT 1.0	5.6.3	5.6.Authentication and Password Security	The SaaS solution shall implement the following features when using passwords (including service accounts): a. Passwords to be made up of at least TWELVE (12) characters. b. Passwords to be made up of the following categories: i. Upper case alphabet (A through Z); ii. Lower case alphabet (a through z); iii. Digits (0 through 9); iv. Special Characters (!, $, #, %, etc). c. Passwords shall be changed once every TWELVE (12) months; d. Prohibit password reuse for a minimum of THREE (3) generations; e. Passwords shall not be displayed in clear; f. Passwords shall not be the same as account ID or user ID; g. SaaS solution shall be protected against dictionary or brute-force attacks; h. The initial setup of password upon first login, and a reset of password of a User account shall be enacted upon by the associated User; i. Retries shall be limited to a maximum of SIX (6) attempted logins after which the User account shall be locked; j. Be changed upon the first login; k.Minimum password age shall be ONE (1) day; and l. Passwords shall be encrypted during transmission and storage. User self-service to reset own password (Forget Password feature).		
IT 1.0	5.6.4	5.6.Authentication and Password Security	The Tenderer shall ensure generic authentication responses for login errors and track for login errors through a system log.		
IT 1.0	5.6.5	5.6.Authentication and Password Security	The Tenderer shall implement multi-factor authentication for administration and management (including remotely) and ensure the second authentication factor is: a. Not the same as the first authentication factor; and b. Delivered out of band and independently of the device to perform the transaction or access SAS data (such as using a physical token, smart card).		
IT 1.0	5.6.6	5.6.Authentication and Password Security	The Tenderer shall ensure access to secrets is accorded the least privilege.		
IT 1.0	5.6.7	5.6.Authentication and Password Security	The Tenderer shall ensure secrets used in production environments are not reused in non-production environments (such as development or test environments).		
IT 1.0	5.6.8	5.6.Authentication and Password Security	The Tenderer shall periodically review source code and configuration to ensure that secrets are not hardcoded or embedded into source codes, configuration files, or scripts.Any changes made on source code must have date/time stamp and detail info of the changes.		
IT 1.0	5.6.9	5.6.Authentication and Password Security	The Tenderer shall seek approval from SAS to use the root/administrator account with the following details-: a. Request Title; b. Request Personal Name; c. Request Duration to use this escrow account (please indicate the date and time range); i. Request Description; ii. Request Reason/s.		
IT 1.0	5.6.10	5.6.Authentication and Password Security	The Requestor from the Tenderer who has the password of the root/administrator should not share with others.		
IT 1.0	5.7.1	5.7.Authentication and Access Control	The SaaS solution shall have the SSO feature to turn on to enable SAS to Single Sign On in multiple applications and SaaS solution using SAML protocol.		
IT 1.0	5.7.2	5.7.Authentication and Access Control	The SaaS solution shall seamlessly integrate and support the use of multi-factor authentication solution. The Tenderer shall clearly state the various MFA solutions supported.		

	1. General Technical Requirements				
IT 1.0	5.8.1	5.8.Infrastructure Security	The Tenderer shall implement the following as part of the SaaS solution: a. Host Intrusion Prevention Systems (HIPS); b. Network Intrusion Prevention Systems (NIPS); c. Next-Generation Firewall(s); d. Network Security and Monitoring; e. Database Security and Monitoring (Activity monitoring and inline blocking); f. Access Controls; g. Security Event Correlation and Monitoring; h. Distributed Denial-of-Service (DDoS) Protection; i. Web Application Firewall (WAF); j. Anti-Defacement Monitoring and Notification; k. Content Delivery Network (CDN).		
IT 1.0	5.8.2	5.8.Infrastructure Security	The Tenderer shall not allow remote access to the SaaS solution and network unless the access is properly justified and approved by SAS. The Tenderer shall implement all the following security measures if remote administrative access is required: a. All remote administration to servers shall be performed from within a management LAN meant only for administration (separate from user traffic). b. Remote administrative access shall only be performed by authorised personnel from specific SaaS solutions and access filtering based on IP address shall be implemented. MAC-based access filtering can be implemented as an additional layer of protection over IP-based access filtering. c.Personnel that are authorised to have remote administrative access shall use multi-factor authentication to authenticate to the servers and applications. d. Logging of the date time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access. e. Review the list of authorised personnel and revoke the access rights for those personnel who no longer require those access rights.		
IT 1.0	5.8.3	5.8.Infrastructure Security	The Tenderer shall implement physical security control measures and procedures to prevent any unauthorised access to the SaaS solution.		
IT 1.0	5.8.4	5.8.Infrastructure Security	The Tenderer shall provide for and ensure the use of anti-malware software to prevent, detect and remove malicious codes and other malicious contents in the SaaS solution including development, testing and production environments. The anti-malware software to be used shall be approved by SAS before implementation.		
IT 1.0	5.8.5	5.8.Infrastructure Security	The Tenderer shall ensure that the anti-malware software is able to monitor, detect and respond to advanced threats for suspicious activities on critical endpoints and servers as mitigation towards zero-day attacks.		
IT 1.0	5.8.6	5.8.Infrastructure Security	The Tenderer shall ensure the anti-malware software is memory-resident and enabled at all times for real-time detection of unauthorised codes and conduct at least monthly full system scans on the SaaS solution.		
IT 1.0	5.8.7	5.8.Infrastructure Security	The Tenderer shall ensure the latest definition files are installed into the SaaS solution on a daily basis.		
IT 1.0	5.8.8	5.8.Infrastructure Security	The Tenderer shall take actions to prevent the spread of unauthorised codes and resolve incidents related to a virus outbreak, execution of malicious codes and recovery actions without additional cost to SAS.		
IT 1.0	5.8.9	5.8.Infrastructure Security	The Tenderer shall implement load balancing of critical IT services (e.g. DNS, databases, authentication service, etc) at every layer (web server, application server, etc) across different sites.		
IT 1.0	5.8.10	5.8.Infrastructure Security	The Tenderer shall deploy clusters across multiple availability zones to ensure service can be re-launched in an alternative zone where there is an availability zone failure.		
IT 1.0	5.8.11	5.8.Infrastructure Security	The Tenderer shall implement Network Address Translation (NAT) to hide the internal IP addresses.		
IT 1.0	5.9.1	5.9.Web and Application Security	The Tenderer shall fully comply with this Clause 5.9 for any Services rendered to SAS.		
IT 1.0	5.9.2	5.9.Web and Application Security	The Tenderer shall ensure that the application is secure by design and is implemented based on a multi-tier architecture which differentiates session control, presentation logic, server-side input validation, business logic and data access, and SaaS solution management. Where appropriate, the application shall also properly segregate application security, access control, authentication, data storage and protection (e.g. encryption) between its users.		
IT 1.0	5.9.3	5.9.Web and Application Security	The Tenderer shall conduct checks on the Application Software functional capabilities and implementation to ensure that adequate security measures are taken throughout the entire lifecycle of the Application Software specified in the Purchase Order Contract.		
IT 1.0	5.9.4	5.9.Web and Application Security	The Tenderer shall ensure that all Application Software developed by the Tenderer, including mobile codes or applications (e.g. browser plug-ins, client-side scripts, applets, smartphone apps, etc.) for end-user devices, are adequately tested for security, reviewed, and approved before deployment. For any plug-in used, please provide plugin name and detail description.		
IT 1.0	5.9.5	5.9.Web and Application Security	The Tenderer shall provide an industry recognised static code analysis tool which they own, to check and identify known errors, vulnerabilities and weaknesses on all Application Software (including mobile codes or applications such as browser plug-ins, client-side scripts, applets, smartphone apps, etc.) developed by the Tenderer at no additional cost to SAS.		
IT 1.0	5.9.6	5.9.Web and Application Security	The Tenderer shall ensure that security is a key consideration at each stage of the software development lifecycle. The Tenderer shall identify security weaknesses, propose mitigation and improvement measures for review with SAS.		
IT 1.0	5.9.7	5.9.Web and Application Security	The Tenderer shall incorporate security requirements into the software development lifecycle with activities such as: threat modelling, scanning using automated testing tools for common vulnerabilities and security code reviews.		
IT 1.0	5.9.8	5.9.Web and Application Security	The Tenderer shall share details of the activities carried out, counter measures or fixes used, tools used in the testing and the findings with SAS.		
IT 1.0	5.9.9	5.9.Web and Application Security	In the event of deployment of any commercial-off-the-shelf (COTS) software, the Tenderer shall produce a security risk profile for the software. Any security vulnerability or weakness shall be documented and highlighted to SAS about its implications. The decision to deploy the software with any workaround or fixes shall be reviewed and agreed with SAS.		
IT 1.0	5.9.10	5.9.Web and Application Security	The Tenderer shall implement appropriate measures to protect sensitive information or functionality with strong access control mechanisms to ensure users accessing different levels of the SaaS solution are properly authorised. The measures shall minimally include the following: a. Check access control permissions, whenever performing direct object references; b. Disable directory browsing; c. Authentication and authorization for each private page; d. Use of role-based authentication and authorization; e. Deny all access by default.		
IT 1.0	5.9.11	5.9.Web and Application Security	The Tenderer shall ensure that where a web source offers both HTTP and HTTPS access, the SaaS solution will use HTTPS for retrieving and transporting data.		
IT 1.0	5.9.12	5.9.Web and Application Security	The Tenderer shall ensure that all remote file transfers to and from the SaaS solution are performed using SSH File Transfer Protocol (SFTP) or other secured file transfer mechanisms subject to approval by SAS.		
IT 1.0	5.9.13	5.9.Web and Application Security	The Tenderer shall ensure that all administration modules of the SaaS solution are accessible only from pre-identified network addresses.		
IT 1.0	5.9.14	5.9.Web and Application Security	The Tenderer shall implement appropriate security mechanisms to protect the confidentiality and integrity of data transmitted from taxpayers and SAS's officers to the SaaS solution, and within the SaaS solution.		
IT 1.0	5.9.15	5.9.Web and Application Security	The Tenderer shall refer to the latest Open Web Application Security Project (OWASP) Top 10 security risks as well as other emerging risks not covered by the OWASP Top 10 and implement mitigation measures against these risks.		
IT 1.0	5.9.16	5.9.Web and Application Security	The Tenderer shall ensure that the SaaS solution is secured and well protected against security attacks, including but not limited to the following: a. Misconfiguration of the cloud platform. b. Unauthorised access. c. Insecure API interfaces. d. Hijacking of accounts, services or traffic.		
IT 1.0	5.9.17	5.9.Web and Application Security	The SaaS solution shall have appropriate exception and error handling capabilities on all components and such exceptions and errors are to be logged in an exception report with detailed description of the error.		
IT 1.0	5.9.18	5.9.Web and Application Security	The Tenderer shall ensure the SaaS solution contains measures to prevent users from accessing information and services they are not authorised to, taking into consideration any trade off to usability that might restrict, or inconvenience authorised ised users. SAS allows the tender to propose the optimum approach.		
IT 1.0	5.9.19	5.9.Web and Application Security	The Tenderer shall ensure the SaaS solution is protected against brute force log-on attempts by implementing the following security measures: a. Incorporate bot mitigation tools such as CAPTCHA; b. Introduce delays between log-on attempts.		
IT 1.0	5.9.20	5.9.Web and Application Security	All network connections between external sites and SAS shall go through next-generation firewall or web application firewall (WAF). Network connections shall be made over a secure channel and access to each endpoint shall be granted through authentication. There shall be security mechanisms and protocols in place to protect the confidentiality and integrity of data transmitted. The design of the setup shall be approved by SAS before SaaS solution development commences. If any attack is detected in the data, the incident shall be logged and communicated to SAS.		
IT 1.0	5.9.21	5.9.Web and Application Security	The Tenderer shall propose real-time website monitoring service (or anti web defacement tool, AWD) to SAS. The Tenderer shall provide the tools/utilities to detect, log and alert any unauthorised changes to the SaaS solution website in real-time, and ensure that a legitimate working website is automatically restored in the event that unauthorised changes have occurred.		
IT 1.0	5.9.22	5.9.Web and Application Security	The Tenderer shall ensure that the tools/utilities proposed shall be able to integrate and inter-operate with other technology components to provide the required security services for the Contract.		

	1. General Technical Requirements				
IT 1.0	5.9.23	5.9.Web and Application Security	The proposed DDoS protection service shall include the following: a. Provision of DDoS protection service with 100% availability; b. Effective protection to keep websites 100% available: i. Faster loading of web content at user end; ii. Protection from Layer 3 to 7 DDoS attacks; API protection; c. Block all OWASP Top Ten type attacks; d. Staging environment for testing before production deployment; e. Global and dedicated capacity to mitigate attacks not less than largest DDOS network attack bandwidth detected; f. Behavioural Detection to differentiate between legitimate traffic (e.g. tax file peak period) and surge caused by DDoS attack (optional); g. Zero-Day automated DDoS protection via pattern, characteristic recognition (optional); and h. Automatic real-time signature creation (optional).		
IT 1.0	5.9.24	5.9.Web and Application Security	The Tenderer shall ensure that the design and implementation of the Application Software shall not be affected by the vulnerabilities (e.g. listed under OWASP Top Ten), which include but are not limited to: a. Injection vulnerability flaws (e.g. SQL injection, command of injection etc); b. Cross Site Scripting (XSS); c. Broken access control; d. Broken authentication and session management (i.e. use of account credentials and session cookies); e. Insecure direct object references; f. Cross Site Request Forgery (CSRF); g. Security misconfiguration; h. Insecure cryptographic Storage; i. Failure to restrict URL access; j. Insufficient transport layer protection; k. Unvalidated redirects and forwards; l. Non-validated input; m. Buffer overflows; n. Improper error handling; o. Race conditions; p. Improper error/exception handling; q. Insecure storage; r. Denial of Service (DoS); and s. Insecure configuration management.		
IT 1.0	5.9.25	5.9.Web and Application Security	The Tenderer shall ensure that the Application Software does not contain any hidden functionalities that SAS is not aware of.		
IT 1.0	5.9.26	5.9.Web and Application Security	The Tenderer shall ensure all test data, test accounts and test credentials are removed from the SaaS solution before commissioning.		
IT 1.0	5.9.27	5.9.Web and Application Security	The Tenderer shall implement the notification message or banner displayed to user before granting access to the SaaS solution.		
IT 1.0	5.9.28	5.9.Web and Application Security	The SaaS solution shall display the key points equivalent to the following: a. Usage of service/ SaaS solution may be monitored, recorded, and subject to audit; b. Unauthorised use of the service/ SaaS solution is prohibited and subject to criminal and civil penalties; c. Use of the service/SaaS solution indicates consent to monitoring and recording.		
IT 1.0	5.10.1	5.10.Development Security	The Tenderer shall propose a list of application security measures to be implemented as part of the SaaS solution. The list shall include the details to enforce code security, application vulnerabilities controls, etc. The Tenderer's proposal on application security measures shall be subject to the review and clarifications by SAS. SAS reserves the right to request for enhancements to the proposed application security architecture.		
IT 1.0	5.10.2	5.10.Development Security	The Tenderer shall implement code scanning and open-source security scanning as part of the development process. Any vulnerabilities found shall be fixed before implementation in production. Any deviation required by the Tenderer shall be discussed with SAS at the earliest possible time.		
IT 1.0	5.10.3	5.10.Development Security	The Tenderer shall ensure any automated tools used include the following: a. Detection of Open Web Application Security Project (OWASP) Top 10 web application security risks; b. Scanning for Common Vulnerabilities and Exposures (CVEs) in libraries and open-source codes; c. Highlighting areas that pose vulnerabilities and include possible resolutions; and d. Only allow deployments when security findings rated Medium and above are resolved.		
IT 1.0	5.10.4	5.10.Development Security	SAS may conduct additional source code reviews as part of a security assurance exercise. Any vulnerabilities found shall be fixed at no extra cost to SAS.		
IT 1.0	5.10.5	5.10.Development Security	The Tenderer shall perform automated testing of APIs before every release. (e.g. tools like Postman, SOAPUI).		
IT 1.0	5.10.6	5.10.Development Security	The Tenderer shall integrate automated testing of APIs into the pipeline to ensure any code change won't break APIs in production.		
IT 1.0	5.10.7	5.10.Development Security	The Tenderer shall limit access to APIs to authorised users and SaaS solution only (e.g. IP whitelisting, machine whitelisting).		
IT 1.0	5.10.8	5.10.Development Security	The Tenderer shall provide documentation of API design and ensure best practices based on industry standards (e.g. SOAPUI, REST) are followed when designing API (e.g. avoid reuse of API keys, encrypt API traffic, authenticate all API calls).		
IT 1.0	5.10.9	5.10.Development Security	The Tenderer shall place a version control Saas solution to assist developers in rolling back to a previous version in any event a show-stopping bug gets discovered.		
IT 1.0	5.10.10	5.10.Development Security	The Tenderer shall implement a deployment pipeline for code release.		
IT 1.0	5.10.11	5.10.Development Security	The Tenderer shall integrate automated security testing into the code release process (e.g. IAST, SAST, DAST).		
IT 1.0	5.11.1	5.11.Security Assurance	The Tenderer shall ensure that System Security Test (SST) is carried out on the System, ensuring that the security measures are functioning as intended. The Tenderer shall identify all technical IT security controls, as well as to recommend test cases to validate the security controls implemented in the Saas solution are functioning according to requirements and design. All issues arising from SST shall be resolved before the Commissioning Date.		
IT 1.0	5.11.2	5.11.Security Assurance	The Tenderer shall engage an independent party, subject to approval by SAS to perform the following: a. Conduct IT security risk assessment on the SaaS solution to ascertain risk areas so that adequate controls can be identified and put into the SaaS solution to mitigate risks. This shall commence during SaaS solution design. The final design of the SaaS solution shall incorporate the findings of the risk assessment. b. Verify and ensure that designs are implemented correctly and conduct SST before the Commissioning Date.		
IT 1.0	5.11.3	5.11.Security Assurance	The Tenderer shall seek SAS's approval where any deviations exist from the review. The Tenderer shall also ensure SaaS solution or manual controls are provided, along with reasons and measures to mitigate any risks that may be present. These justifications shall be documented.		
IT 1.0	5.11.4	5.11.Security Assurance	The Tenderer shall provide full support and work with the independent third party engaged by SAS to ensure all the weaknesses and vulnerabilities discovered during the IT security risk assessment, WAPT is addressed before the Commissioning Date, at no additional cost to SAS.		
IT 1.0	5.11.5	5.11.Security Assurance	The Tenderer shall perform security tests on the SaaS solution		
IT 1.0	5.11.6	5.11.Security Assurance	#VALUE!		
IT 1.0					
IT 1.0	5.12.1	5.12.User Access Management	The Tenderer shall implement Identity and Access Management (IAM) for user account management.		
IT 1.0	5.12.2	5.12.User Access Management	The Tenderer shall propose an access control matrix for authorised users to the SaaS solution for the approval by SAS.		
IT 1.0	5.12.3	5.12.User Access Management	The Tenderer shall ensure that access rights are granted on a need-to know basis, kept up-to-date and reviewed on a regular basis. The Tenderer shall ensure that any SaaS solution or user account not needed shall be deleted.		
IT 1.0	5.12.4	5.12.User Access Management	The Tenderer shall implement control measures to protect all account credentials. The Tenderer shall provide detailed documentation on the control measures and processes, which shall minimally include the security features, technologies, administration usage processes and procedures.		
IT 1.0	5.12.5	5.12.User Access Management	The Tenderer shall ensure that the account shall be locked after a specific number of unsuccessful attempts as determined by SAS.		
IT 1.0	5.12.6	5.12.User Access Management	The Tenderer shall implement a timeout or automatic logout feature to the SaaS solution for non-active sessions.		
IT 1.0	5.12.7	5.12.User Access Management	The Tenderer shall ensure that all system administrative or functional accounts are not shared.		
IT 1.0	5.12.8	5.12.User Access Management	The Tenderer shall implement security measures and processes to ensure that system administrators, database administrators or other privileged users shall not access SAS' system. The Tenderer shall ensure that logs are reviewed to identify such unauthorised access.		
IT 1.0	5.12.9	5.12.User Access Management	The Tenderer shall ensure all successful and failed authentication events for access are logged.		
IT 1.0	5.12.10	5.12.User Access Management	The Tenderer shall disable remote administrative access to the SaaS solution if such access is not required.		
IT 1.0	5.12.11	5.12.User Access Management	The Tenderer shall implement Role-Based Access Control (RBAC) and/or Attribute-Based Access Control (ABAC) mechanism that enforces access to all parts of the SaaS solution.		

	1. General Technical Requirements				
IT 1.0	5.12.12	5.12.User Access Management	The Tenderer shall implement processes and controls to ensure that: The rights to access data are granted on a need-to-know basis; Users can access only data that they have been granted access rights to.		
IT 1.0	5.12.13	5.12.User Access Management	The Tenderer shall apply the principle of least privilege to all accounts (such as users, services) to ensure excess privileges are not granted to accounts.		
IT 1.0	5.12.14	5.12.User Access Management	The Tenderer shall implement ABAC using multiple attributes such as role, location, authentication method, IP address and mutual authentication.		
IT 1.0	5.12.15	5.12.User Access Management	The Tenderer shall ensure that the access control matrix for the SaaS solution is established, roles and responsibilities are clearly documented.		
IT 1.0	5.12.16	5.12.User Access Management	The Tenderer shall implement an approval process and tracking mechanism for granting user access to the SaaS solution.		
IT 1.0	5.12.17	5.12.User Access Management	The Tenderer shall implement the permission boundary which ensures that users created by another user shall have the same or fewer permissions to prevent privilege escalation.		
IT 1.0	5.12.18	5.12.User Access Management	The Tenderer shall implement all of the following security measures if remote administration to server or applications is required: a. Remote administrative access shall only be granted to authorised personnel who need to perform administration on servers or applications remotely; b. Remote administrative access shall only be done by authorised personnel from specific SaaS solution and filtering based on IP address shall be implemented; c. Personnel that are authorised to have remote administrative access shall use multi-factor authentication to authenticate to the servers or applications; and comply to the requirements under Clause 5.6.5 and; d. Logging of the date time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.		
IT 1.0	5.12.19	5.12.User Access Management	The Tenderer shall manage the privileged accounts (such as admin account,root account) as follows: a. Only authorised administrators as required by job functions and need-to know basis can be assigned with privileged accounts and specific systems and filtering based on IP address shall be implemented; b. All privileged account requests must go through approval and authorisation process before access is granted to administrators; c. All privileged accounts must be documented; d. Individual privileged account and password must be setup and assigned to ensure accountability and traceability; Shared privilege accounts must still retain an ownership for accountability; e. Privileged accounts must be immediately disabled and removed when administrators change their job function or leave the organisation, or when it is no longer needed; f. Default privileged accounts must be removed. If the default privileged accounts cannot be removed, they must be renamed and passwords changed immediately and disabled, where possible; g. Privileged accounts shall be reviewed regularly to prevent against unauthorised accesses and activities; h. All administrative changes performed using privileged account shall have audit trails to facilitate investigation if required; and i. Segregation of roles for privileged accounts used in the SaaS solution must be enforced.		
IT 1.0	5.13.1	5.13.IT Security Incident Management	The Tenderer shall work with SAS for the IT Security Incident Handling Framework. The IT Security Incident Handling Framework will define a systematic incident response approach and incident escalation structure through which incidents are to be notified and resolved.		
IT 1.0	5.13.2	5.13.IT Security Incident Management	The Tenderer shall develop Technical Standard Operating Procedures (SOP) that specify the detailed procedures of handling different types/categories of IT security incident (including but not limited to DDoS, unauthorised access/change, malware infection, etc.) within twenty-four (24) weeks from the Letter of Acceptance. The SOP shall be reviewed minimally on an annual basis and approved by SAS.		
IT 1.0	5.13.3	5.13.IT Security Incident Management	In the event of any IT security incidents, the Tenderer shall: a. Investigate, resolve and recover from the IT security incident; b. Ensure the preservation and admissibility of evidence and information related to the IT security incident; and c. Exercise the prescribed incident response guidelines and procedures of the IT security incident management plan.		
IT 1.0	5.13.4	5.13.IT Security Incident Management	The Tenderer shall take the necessary actions to ensure that all IT security incidents are handled and managed in accordance with SAS's IT Security Incident Handling Framework and the approved SOP. The Tenderer shall also implement measures to prevent the occurrence of IT security incidents. The Tenderer shall support SAS in resolving IT security incidents when the need arises.		
IT 1.0	5.13.5	5.13.IT Security Incident Management	The Tenderer shall be responsible to inform SAS IT Security Incident Response (SITSIR) and personnel appointed by SAS required to deal with the IT security incidents.		
IT 1.0	5.13.6	5.13.IT Security Incident Management	The commercial CSP shall report any security incident including any observed or suspected security cases that may affect SAS as a customer/tenant.		
IT 1.0	5.13.7	5.13.IT Security Incident Management	For severity 1 security incident, the commercial CSP shall provide an initial incident report within 4 hours of incident detection and status update every 24 hours thereafter until incident closure.		
IT 1.0	5.14.1	5.14.Security Training and Awareness	The Tenderer shall ensure that all its personnel assigned to this project are equipped with the relevant skills and experience to operate the SaaS solution. The personnel shall be familiar with the requirements of the SaaS solution and shall adhere to the security policy, standards, procedures and incident reporting processes as approved by SAS.		
IT 1.0	5.14.2	5.14.Security Training and Awareness	The Tenderer shall ensure that all their personnel are informed of their security responsibilities and accountability/liability before putting the person in his/her assigned areas of work.		
IT 1.0	5.14.3	5.14.Security Training and Awareness	The Tenderer shall demonstrate that they have a comprehensive security program to train its personnel in security and their assigned role.		
	6. Logging & Monitoring				
IT 1.0	6.1.1	6.1.General	The Tenderer shall collect the following types of logs from all components in the SaaS solution: a. User administration activities (for e.g. add / delete / amend user accounts and profiles). b. Access (e.g. Successful and unsuccessful attempts to logins and logouts of the System, privileged access login, date and time stamp, user identification, activities performed, etc.). c. System Health (e.g. System resource usage, etc.). d. Performance (e.g. Response time, latency, throughput, etc.). e. Activities and Events (e.g. Audit trail, configuration changes, System actions – including backup and recovery activities, start-up and shutdown, profile changes, administration activities, maintenance activities etc.). f. Errors and Exceptions (e.g. Resource unavailability, application exceptions, validation failure, timeout errors, etc.). g. Security Events (e.g. malware detection, intrusion detection, access violations from local and remote requests, etc.).		
IT 1.0	6.1.2	6.1.General	The Tenderer shall ensure the logging and monitoring is a. Able to collect accurate and complete logs; b. Able to allow SAS to comply with logging and audit requirements (e.g. what needs to be logged, log retention periods); and c. Able to allow SAS to effectively perform event reconstruction, incident investigation, troubleshooting, service level monitoring, and audit.		
IT 1.0	6.1.3	6.1.General	SAS reserves the right to review the logs as and when required and the Tenderer shall provide the required logs to SAS within a timely manner to ensure the relevant SLAs are met.		
IT 1.0	6.1.4	6.1.General	The Tenderer shall ensure that the logs record all activities carried out by privileged accounts – such as system administrator and service accounts (if in use).		
IT 1.0	6.1.5	6.1.General	The Tenderer shall ensure that these audit trails be protected from being modified by unauthorised personnel including the privileged accounts.		
IT 1.0	6.1.6	6.1.General	The Tenderer shall provide tamper evidence for protecting the integrity of the audit trails.		
IT 1.0	6.1.7	6.1.General	The Tenderer shall ensure the SaaS solution keeps these logs for at least ONE (1) year.		
IT 1.0	6.1.8	6.1.General	The Tenderer shall ensure that a process is put in place for all necessary logs to be reviewed monthly or when necessary, such as after configuration changes to scan for security violations, issues or concerns and highlight them to SAS.		
IT 1.0	6.1.9	6.1.General	The Tenderer shall ensure security-related logs are available to facilitate event reconstruction and incident investigation. The Tenderer shall support the incident investigation without extra cost.		
IT 1.0	6.1.10	6.1.General	The Tenderer shall store the log files at secured locations to protect the integrity and availability.		
IT 1.0	6.1.11	6.1.General	The log files shall be readable in ASCII plain text format or UTF8.		
IT 1.0	6.1.12	6.1.General	The Tenderer shall implement that log information is accessed by authorised personnel only; operations personnel should not have access to logs to prevent risk of tampering or deletion.		
IT 1.0	6.1.13	6.1.General	The Tenderer shall ensure that log files do not contain sensitive information.		
IT 1.0	6.1.14	6.1.General	The Tenderer shall ensure there is sufficient capacity to store logs.		
IT 1.0	6.1.15	6.1.General	The Tenderer shall ensure that the auto-scaling feature turns on to provide sufficient capacity to store the log files.		
IT 1.0	6.1.16	6.1.General	The Tenderer shall provide the design solutions for the logs for audit purposes.		
IT 1.0	6.1.17	6.1.General	The SaaS solution shall alert designated recipients, via commonly supported messaging channels, when the following (but not limited to) events occur: a. Security violation; b. System backup and recovery; c. System maintenance activities.		
IT 1.0	6.1.18	6.1.General	The Tenderer shall ensure that the information to be logged include, but not limited to, the user identifier, the action taken, and date and time of the activity.		

	1. General Technical Requirements				
IT 1.0	6.1.19	6.1.General	The SaaS solution shall capture the necessary footprints, such as client IP address, date time stamps, requests/responses for forensic purposes.		
IT 1.0	6.1.20	6.1.General	The Tenderer shall provide audit reporting capabilities to extract information of a particular activity, start / end timestamp of activities or the activities of a particular user from the audit trails.		
IT 1.0	6.1.21	6.1.General	The SaaS solution shall have the facility to store the audit information for varying periods depending on the type of audit trails, before they are archived.		
IT 1.0	6.2.1	6.2.User Access Logging	The Tenderer shall implement user access logging in the proposed SaaS solution. User Access Logging shall be active at all times for all actions performed within the proposed SaaS solution by users accessing the data from any of the user interfaces.		
	7. Support				
IT 1.0	7.1.1	7.1.System Support	The Tenderer shall provide support services for the SaaS solution during the User Acceptance Testing Period, Performance Guarantee Period (PGP), System Warranty Period and Application Software Maintenance and Support Period and all service requests applied, including managing problems, proposing incident and problem resolution support structure and procedures during the Contract Period. a. Investigate and correct defects in the SaaS solution as reported by SAS within the service level. The resolving effort includes resolving errors through developing, testing and implementing changes to the SaaS solution; b. Provide corrective maintenance, troubleshoot and isolate defects, including diagnosis and correction of all latent errors in the SaaS solution; c. Manage and implement changes to the SaaS solution to minimise impact on SaaS solution availability; and d. Provide the following services even if after support hours: i. Resolution of Business Impact Level 1 problems (refer to Clause 7.6.8); ii. Restoration of SaaS solution; and iii.Testing of SaaS solution for OS, database and/or software upgrades and patches. e. The Tenderer shall state separately the maintenance pricing of all hardware / software components and equipment for the stipulated maintenance period after the initial warranty period has expired. f. The Tenderer shall take note of the stipulated system warranties in Warranties and Warranty Period of this Tender.		
IT 1.0	7.2.1	7.2.Service Request (SR) (On-demand)	Service Request (SR) refers to requests for modifications or enhancements to the SaaS solution not previously defined in the project scope. The enhancements may also include requirements to support new user requirements or future growth and expansion, which is on-demand.		
IT 1.0	7.2.2	7.2.Service Request (SR) (On-demand)	The Tenderer shall clarify the requirements, make an assessment of the SR and submit a SR proposal detailing impact analysis such as performance, integration, availability as well as the scope of work for SAS's review and approval.		
IT 1.0	7.3.1	7.3.Service Request (SR) Procedure	The Tenderer shall submit a SR procedure describing how all the proposed changes to the SaaS solution are to be processed. The procedure shall cover the progress of a proposed change from its formal definition through its implementation in a released version of the software, or to its disposal for other reasons. This shall take into consideration the mutually agreed SaaS solution change management standards with respect to prioritisation of such requests.		
IT 1.0	7.3.2	7.3.Service Request (SR) Procedure	The aim of the SR procedure is to ensure that all proposals for changes to the SaaS solution are properly evaluated in terms of their costs and benefits and their priority. Such changes include alterations to the SaaS solution documentation and operational procedures. It shall also monitor progress of processing service requests.		
IT 1.0	7.4.1	7.4.Types of Service Request (SR)	Normal Request: Requests that are not urgent. SR Proposal shall be submitted within SEVEN (7) working days; and		
IT 1.0	7.4.2	7.4.Types of Service Request (SR)	Urgent Request: Requests that are urgently required. SR Proposal shall be submitted within THREE (3) working days.		
IT 1.0	7.5.1	7.5.Turnaround time to implement Service Request (SR)	All accepted change requests shall be completed and implemented within the specified turnaround time depending on the estimated man-days required:		
IT 1.0					
IT 1.0	7.5.2	7.5.Turnaround time to implement Service Request (SR)	The Tenderer shall provide the unit cost for SR in Price Schedules.		
IT 1.0	7.6.1	7.6.Problem Management	The Tenderer shall set up the appropriate Problem Management channels and procedures with SAS.		
IT 1.0	7.6.2	7.6.Problem Management	The Tenderer shall provide support and coordinate for all SaaS solution related problems.		
IT 1.0	7.6.3	7.6.Problem Management	The Tenderer shall provide a primary and secondary contact number and email accounts for the reporting of problems. The Tenderer shall provide alternate contacts as and when the provided contacts are unavailable.		
IT 1.0	7.6.4	7.6.Problem Management	Any SaaS solution operational issues, inadequacies or problems identified that are attributable to the Tenderer's design, development or implementation of the SaaS solution shall be rectified by the Tenderer to SAS's satisfaction within TWO (2) calendar weeks upon the occurrence at no additional cost to SAS. For issues, inadequacies and problems which are not attributable to the Tenderer, the Tenderer shall work with all relevant parties to resolve the underlying issues and ensure that the SaaS solution is secured against the identified vulnerabilities.		
IT 1.0	7.6.5	7.6.Problem Management	The Tenderer shall schedule problem reviews to track unresolved problems and provide rectification efforts to prevent problems from reoccurring. Frequency of such reviews shall be specified by SAS.		
IT 1.0	7.6.6	7.6.Problem Management	The Tenderer shall perform a thorough analysis of the problem, which includes identification of the cause of the problem to its component level, the SaaS solution affected, the data or any loss suffered, the recommended solution and the preventive measures.		
IT 1.0	7.6.7	7.6.Problem Management	When alerted by SAS of potential weaknesses, threats and vulnerabilities to the SaaS solution, the Tenderer shall assess the impact and recommend any necessary measures to mitigate or remove the risks to the SaaS solution.		
IT 1.0	7.6.8	7.6.Problem Management	Unless otherwise specified by SAS, the classification of the defects or errors in the SaaS solution during the Contract Period is as specified below. In the event that SAS and the Tenderer could not agree on the assignment of a business impact level to a problem / defect, SAS shall have the final decision on the business impact level, and this shall be conclusive and binding to all parties involved in resolving the problem / defect.		
IT 1.0					
IT 1.0	7.6.9	7.6.Problem Management	The "Response Time" shall be the time between notification of the problem to the Tenderer and the response by the Tenderer to the problem.		
IT 1.0	7.6.10	7.6.Problem Management	The "Problem Resolution Time" shall begin upon notification of the problem until the problem is resolved and the defect is restored to a satisfactory working condition.		
IT 1.0	7.6.11	7.6.Problem Management	The Tenderer shall work with all parties designated by SAS and take whatever actions necessary to resolve all problems. For problems classified as business impact level ONE (1), the Tenderer shall also provide in writing a preliminary incident report to explain the incident by the following working day. Subsequently, the Tenderer shall furnish SAS with a post-incident report to explain in detail the background of the problem, the impact of the problem, the cause of the incident, the corrective actions taken and the solutions / recommendations to prevent the incident from recurring.		
IT 1.0	7.6.12	7.6.Problem Management	The Tenderer shall comply with the service levels according to the business impact level classification:		
IT 1.0	7.7.1	7.7.Problem Reporting Procedure	The Tenderer shall propose both the incident and problem resolution support team structures and the escalation procedures for incident and problem resolution including the infrastructure and mechanism for reporting, management and escalation of problems, unsatisfactory restoration or services rendered. This shall include the process, procedures, contact persons and response time. The support team shall be based in Singapore.		
	8. Batch Job				
IT 1.0	8.1.1	8.1.General	The Tenderer shall ensure that the SaaS solution has the capabilities to manage the operations of batch jobs. The batch jobs shall include, but not limited to: a. Ad hoc / routine scheduled jobs for external SaaS solution interface data transfer; b. Ad hoc / routine scheduled housekeeping jobs; c. Ad hoc / routine scheduled jobs for report generation; d. Ad hoc / routine scheduled jobs for application processing.		
IT 1.0	8.1.2	8.1.General	The Tenderer shall also ensure that the batch job module has features, but not limited to the following: a. Graphical User Interface (GUI); b. Preferably web-based; c. Access controls (for example, only authorised users can add/delete routine scheduled jobs); d. Job scheduling by date, day, time; immediate by operators/users; e. Cancellation of batch jobs by authorised operators/users; f. Job schedule and execution status enquiry for a specified time period; g. Alerts of job execution status by commonly supported messaging channels (for example, email, SMS and paging); Administrator can define the status that require alerts; h. Error logging features (for example, tracking, monitoring UI); i. Configuration to enable/disable automated restart of failed jobs; j. Prioritisation of batch job by authorised administrator; k. Proper termination of all process when a job is completed.		
IT 1.0	8.1.3	8.1.General	The Tenderer shall ensure that the batch jobs remain at a consistent state when SaaS solution anomalies, such as power outages and server failure occur: a. Jobs that were awaiting execution when the SaaS solution went down will remain in the job queue, ready for re-run when the SaaS solution is restarted; b. Jobs that were running when the server went down will be recovered and flagged with the relevant job status for alert.		

	1. General Technical Requirements				
	9. Testing				
IT 1.0	9.1.1	9.1.General	The Tenderer shall propose the testing strategy, plan and methodology for the SaaS solution.		
IT 1.0	9.1.2	9.1.General	The Tenderer shall propose automated test tools to be used for functionality, integration, interface, regression, performance and stress tests where applicable.		
IT 1.0	9.1.3	9.1.General	The test tools proposed by the Tenderer shall be integrated and shall be able to run in the proposed SaaS solution environment.		
IT 1.0	9.1.4	9.1.General	The Tenderer shall ensure that the test tools are successfully installed and configured.		
IT 1.0	9.2.1	9.2.Infrastructure	The Tenderer shall provide the necessary software and tools, at its own expense, to perform the SaaS solution network assessment tests, SaaS solution performance tests, stress tests and PGP tests.		
IT 1.0	9.2.2	9.2.Infrastructure	The Tenderer shall propose the software and tools to be used for these tests, but the use of such software and tools shall be subject to SAS's approval.		
IT 1.0	9.2.3	9.2.Infrastructure	The Tenderer shall propose a schedule for the SaaS solution health check and tunings to be performed during the Project. The proposed schedule shall be submitted for SAS's review and approval.		
IT 1.0	9.2.4	9.2.Infrastructure	The Tenderer shall submit system health check reports to show that the SaaS solution has been tuned for optimum performance.		
	10.Risk Assessment				
IT 1.0	10.1.1		With reference to Clause 1.1.17d, the Tenderer is expected to complete the Cloud Vendor Risk Assessment Tool		

External Hosting Risk Control
Vendor Assessment Tool
Questionnaire

Confidentiality Category: For restricted external use

Instructions

1. This risk assessment checklist should be completed by personnel who have direct knowledge of the service provider's information systems and operations. The information provided in this checklist should be reviewed by their superiors.

2. Each item in the checklist should be evaluated in the context of the associated control requirement to provide description of the service provider's current controls.

3. Under "Vendor Response" there are drop-down boxes with 3 answers - Yes, Partial, No,
   - Select option Yes if you comply with ALL parts of the requirements, including the options (a, b, c…); and describe in the 'Vendor Remarks' column your current control implementations in meeting the requirements
   - Select option Partial if you do not comply with some parts of the requirement or options (a, b, c…); and describe in the "Vendor Remarks' column the options you are not complying and the compensating controls, if any
   - Select option No if you do not comply with ALL parts of the requirement, including the options (a, b, c…)

4. For question with "Note", explain in the "Vendor Remarks" column the controls or specific information requested. For any descriptions, please describe to an appropriate level of granularity which could enable conclusion of the compliance status of the service provider's control implementations in meeting the requirements.

Vendor and Project Information
Vendor Name
Project Name
Contact Person

	Domain / Question	Vendor Response		Vendor Remarks		Accompanying Documents	[Reserved to Assessor]
	Application & Interface Security						
	Applications and programming interfaces (APIs) should be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications)						
AIS-1.1	Do you have a documented policy and framework following industry standards to build in security for your Systems/Software Development Lifecycle (SDLC)?		**		**		
AIS-1.2	Do you verify that all of your software suppliers adhere to industry standards described on question above for secure Systems/Software Development Lifecycle (SDLC) security?		**				
AIS-1.3	Do you review your applications for security vulnerabilities and address any issues reported prior to deployment to production?		**				
	Real-time monitoring and alerting on API availability, as well as offline trend analysis on API usage to detect and prevent API infrastructure from potential attacks and provide administrators the capability to quickly react to adverse events the soonest should be performed by the service provider						
AIS-2.1	Do you implement real-time monitoring and alerting for API availability and perform offline trend analysis on API usage to prevent, detect and react to API adverse events?		**				
	Based on the organisation's risk analysis, specific applications modules and security safeguards are rigorously tested with a combination of source code review, exception testing and compliance review to identify errant coding practices and systems vulnerabilities that could lead to security problems, violations and incidents						
AIS-3.1	Do you have the followings? a) a methodology for system testing established which consists of code review, exception testing and compliance review b) tests scoping that covers business logic, security controls and system performance under various stress-load scenarios and recovery conditions.		**				
	Audit trails, system logs are restricted from unauthorized access, including privileged ID to maintain their integrities for investigation and forensic purposes						
AIS-4.1	Do you have policies, procedures established and implemented to restrict access to audit trails, system logs? To fully achieve this requirement privileged IDs must also be restricted access as stipulated in policies and procedures.		**				
	Prior to granting clients access to data, assets, and information systems, identified security, contractual, and regulatory requirements for client access should be addressed						
AIS-5.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems, with all requirements and trust levels for customers' access defined and documented?		**				
AIS-5.2	Are all requirements and trust levels for customers' access defined and documented?		**				
	Data input and output integrity routines (i.e., reconciliation and edit checks) should be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse						
AIS-6.1	Do you implement data input and output integrity routines (i.e., reconciliation and edit checks) for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?		**				
	Policies and procedures should be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction						
AIS-7.1	Do you have policies and procedures to implement a Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?		**				
	Audit Assurance & Regulatory Compliance						
	The service provider should perform annual independent assessments of conformance to, and effectiveness of, its policies, procedures and controls						
AAC-5.1	Do you engage recognized independent audit organization to conduct annual independent assessments of conformance to, and effectiveness of, your policies, procedures and controls? If no, do you establish and implement control framework that captures standards, regulatory, legal, and statutory requirements (including PCI DSS, PDPA, MAS TRM, EU Data Directive, etc) relevant for your business and clients' needs? Note : Minimally independent audit pertaining to IT General Controls, Application Controls and penetration testing should be conducted at planned intervals.		**				
	Organizations should create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework should be reviewed at least annually to ensure changes that could affect the business processes are reflected						

AAC-6.1	Do you establish and implement control framework that captures standards, regulatory, legal, and statutory requirements (including PCI DSS, PDPA, MAS TRM, EU Data Directive, etc) relevant for your business and clients' needs? Note : To fully meet this requirement the control framework must be reviewed annually, please provide the date of the latest review.		**		**		

Organizations should comply with the Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) notice and guidelines for critical IT systems subjected to the regulation.

AAC-7.1	Do you conduct assessment against the MAS Technology Risk Management (TRM) notice and guidelines for critical IT systems subjected to the MAS regulation?		**				

Organizations should comply with the Personal Data Protection Act (PDPA) and guidelines for the collection, use, disclosure and care of personal data.

AAC-27.1	Have you assessed the personal data protection risks within your organisation and put in place personal data security policies?		**				
AAC-28.1	Is the personal data that you hold adequately classified?		**				
AAC-29.1	Is the personal data stored / processed in a secure manner for the data you hold as the data intermediary?		**				
AAC-30.1	Do you have controls to prevent external parties having easy access to the personal data that you hold as the data intermediary?		**				
AAC-31.1	Are there any remedial measures in place in the event of a IT security breach?		**				
AAC-32.1	Do you conduct or schedule regular audits on the data protection processes within your organisation?		**				
AAC-33.1	Are there contractual provisions in place to ensure proper safeguards in respect of personal data disclosed to outsourced parties who will be processing personal data on your behalf?		**				
AAC-34.1	Is there regular data housekeeping for the data you hold as the data intermediary?		**				
AAC-35.1	Do you remove personal data no longer needed for business or legal purposes for the data you hold as the data intermediary?		**				
AAC-36.1	Do you put in place the appropriate contractual arrangements or binding corporate rules to govern the transfer of personal data overseas for the data you hold as the data intermediary?		**				
AAC-37.1	Have you designated one or more individuals (who may be referred to asdataprotectionofficers)toberesponsibleforensuringthatthedata protection policies and practices of your organisation are in compliance with the PDPA?		**				
AAC-38.1	Does your data protection officer(s) know his/her roles and responsibilities in ensuring personal data in your organisation's possession or control is well-protected?		**				
AAC-39.1	Is the business contact information of your designated data protection officer(s) made available to the public?		**				
AAC-40.1	Have you developed and implemented data protection policies for your organisation to meet its obligations under the PDPA? Are your organisation's data protection policies made available to the public?		**				
AAC-41.1	Have you developed a process to receive, investigate and respond to complaints that may arise with respect to the application of the PDPA?		**				
AAC-42.1	Is information on your organisation's complaint process made available on request?		**				
AAC-43.1	Have you communicated information about your organisation's data protection policies and practices to your employees, in particular, but not limited to, employees who are handling personal data?		**				
AAC-44.1	Do your employees know who to pass the requests to if it is not their responsibility to respond to such requests?		**				
AAC-45.1	Is there a written contract in place for your engagement as a data intermediary to process personal data on behalf of and for the purposes of another organisation?		**				
AAC-46.1	Have the individuals on your marketing list given their clear and unambiguous consent, evidenced in written or other accessible form, to being contacted by you by phone call, text messages (eg. SMS/ MMS) or fax for your intended telemarketing purposes?		**				
AAC-47.1	In relation to individuals who have not given their clear and unambiguous consent for telemarketing, have you established an internal process for checking with the Do Not Call ("DNC") Registry prior to your telemarketing campaigns?		**				
AAC-48.1	If you purchase databases of contact information from third parties for your telemarketing activities, do you ensure that the third party has obtained the necessary consents for the collection, use and disclosure of the personal data by you?		**				
AAC-49.1	When you make a voice call containing a marketing message, is your calling line identity concealed or withheld from the recipient?		**				
AAC-50.1	Do your telemarketing messages include clear and accurate information identifying your organisation as well as contact details		**				
AAC-51.1	If you outsource the telemarketing function, do you ensure that your vendor complies with the Do Not Call ("DNC") provisions in the PDPA?		**				

Business Continuity Management & Operational Resilience

A consistent unified framework for business continuity planning and plan development should be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.

BCR-1.1	Do you establish and implement business continuity planning ("BCP") which detail the following requirements? a. purpose and scope, aligned with relevant dependencies b. target audience and applicability c. ownership and review cycle d. communication strategies e. roles and responsibilities f. detail recovery procedures, manual work-around, and reference information g. method for plan invocation Note: Please also indicate in remark if BS25999 or equivalent standards is used to ensure recovery and business continuity		**		**		
BCR-1.2	Do you conduct annually business continuity and disaster recovery testing?		**				

SLA and/or contracts should be established with contractors for equipment maintenance ensuring continuity and availability of operations and support personnel

BCR-2.1	Do you establish SLA and/or contracts with contractors for data centre equipment maintenance (e.g. servers, network components, facilities management hardware) to ensure continuity and availability of operations and support personnel?		**			

Policies and procedures should be established for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities in supporting business functions, workforce, and/or clients. Based on industry acceptable standards (i.e., ITIL v4 and COBIT 5), these policies and procedures should:

a. defined roles and responsibilities supported by regular workforce training

BCR-3.1	Do your define clear roles and responsibilities in your IT policies and procedures and do you conduct regular (at least annually) related workforce training? Note: Please indicate in the remark column standard used to establish policies and procedures (e.g., ITIL v4 and COBIT 5)		**		**	

b. be available for information system documentation (e.g., administrator and user guides, and architecture diagrams) to authorized personnel to ensure the following:
- Configuring, installing, and operating the information system
- Effectively using the system's security features

BCR-3.2	Do you maintain information system documentation (e.g., administrator and user guides, and architecture diagrams) for system operations (configuring, installing, using system's security features) and ensure these documentations are made available to authorized personnel?		**			

Policies and procedures should be established for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures should be incorporated as part of business continuity planning and tested accordingly for effectiveness.

BCR-4.1	Do you define retention period of critical asset in policies and procedures based on applicable legal, statutory, regulatory compliance obligations or customer specific requirement?		**			
BCR-4.2	Do you conduct monthly for testing for sampled backup data with different frequency (monthly, weekly, daily, half yearly, yearly backups etc.) to ensure of its readability and recoverability?		**			
BCR-4.3	Do you conduct recoverability test for all systems (staged over months) for different backup media type (e.g. type 3480/3490, 3590, 3590E, DLT, SDLT, LTO, 4MM, 8MM) and/or storage (e.g. DAS, NAS, SANS)?		**			

There should be a defined and documented method for determining the impact of any disruption to the organization, both the (service provider and client)

BCR-5.1	Do you conduct impact analysis covering the following points during business continuity planning? a. Identification of critical products and services b. Identification of all dependencies, including processes, applications, business partners, and third party service providers c. The understanding of threats to critical products and services d. The determination of impacts resulting from planned or unplanned disruptions and how these vary over time e. The establishment of the maximum tolerable period for disruption f. The establishment of priorities for recovery g. The establishment of recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption h. The estimate the resources required for resumption		**			

Service provider should define backup strategy and procedures to ensure client data is always available for restoration as and when needed.

BCR-6.1	Do you have a backup strategy that defines each of the followings? a. Frequency (monthly, weekly, daily, yearly etc.) b. Backup rotation scheme (14 tapes, 20 tapes etc.) c. Backup type (e.g. full, incremental, differential) d. Mode of backup (e.g. disk mirroring for real-time, archival) e. Type of backup media/ storage (e.g. DLT, SDLT, LTO, DAS, NAS, SAN) f. Backup content (e.g. system data, application data, systems & application logs etc.) g. Physical and logical location of data sources h. Security and access rights i. Encryption j. Offsite storage arrangement		**			
BCR-6.2	Do you implement independent hardware restore and recovery capabilities for virtual infrastructure ?		**			
BCR-6.3	Do you implement with your virtual infrastructure a capability for your client to restore a Virtual Machine to a previous state in time?		**			
BCR-6.4	Do you implement with your virtual infrastructure to allow virtual machine images to be downloaded and ported to a new service provider?		**			
BCR-6.5	Do you implement with your virtual infrastructure to allow machine images to be made available to clients in a way that would allow them to replicate those images in their own off-site storage location?		**			
BCR-6.6	Do you implement, as part of your cloud solution, support to software providers for independent restore and recovery capabilities?		**			

Change Control & Configuration Management

Policies and procedures should be established and implemented to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacentre facilities are thoroughly considered and authorized by the organization's business leadership or other accountable business role or function

CCC-1.1	Do you have policies, procedures established and implemented for management (e.g. technology governance committee or equivalent, consisting of business owners) to thoroughly consider and authorise the development and acquisition of new assets, new data and including new applications, systems, databases, infrastructures, networks, services, operations and facilities?		**			

External business partners should adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes)

CCC-2.1	Do you have outsourcing policies, procedures established and implemented for the following: 1. monitor and review on a regular basis your external business partners, contractors' practices to ensure they adhere to the same policies and procedures for change management, release, and testing as your internal developers (e.g. ITIL service management processes)? 2. ensure that quality are being met for all software development? 3. to detect security issues (e.g. source code defects) arising from any outsourced software development activities?		**			

Organization should follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services

CCC-4.1	Do you defined quality change control and test procedures with established baselines, testing requirements (stress test, functional testing, unit testing, regression test, etc...) , and release standards that focus on system availability, confidentiality, and integrity of systems and services?		**			

Data Security & Information Lifecycle Management

Data and objects containing data should be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization

DSI-1.1	Do you classify your information data considering at least the data type, value, sensitivity, and criticality? If you use data-labelling standard (e.g., ISO 15489, Oasis XML Catalogs Specification, CSA data type guidance) please also indicate in the remark column.		**		**	
	All data should be designated with stewardship, with assigned responsibilities defined, documented, and communicated					
DSI-2.1	Do you have policies and procedures implemented to assign data stewardship, including roles and responsibilities?		**			
	Policies and procedures should be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, service providers should ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds and that those residency requirements are complied with					
DSI-3.1	Do you have policies, procedures established and implemented to inventor, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems? The policies, procedures or data flows must cover geographic residency requirements of the data allowing or disallowing migration beyond its geographic location boundaries (country, must be implemented and shared with the client on demand or for review at least annually.		**			
	Security measures should be implemented to protect sensitive or confidential information such as passwords, client personal, account and transaction data etc. which are stored and processed in systems, endpoint devices.					
DSI-4.1	Do you have data classification, handling policies established and implemented to provide guidelines for consistent practices on handling of the client's sensitive or confidential information?		**			
DSI-4.2	Do you implement hard drive encryption on systems and mobile devices only publicly-vetted algorithms (e.g. AES 256 bits or equivalent) and review the algorithms and keys in use annually Note: Please specify in the remark column the algorithm you implement		**		**	
DSI-4.3	Do you implement automated tools on network perimeters to monitor sensitive information (e.g. personally identifiable information, keywords) based on document characteristics, hash to discover unauthorized attempts to exfiltrate data across network boundaries and block such transferes while alerting the appropriate authorities		**			
DSI-4.4	Do you implement controls to refrains the writing of data to USB tokens or USB hard drives, memory cards, etc. grom endpoint devices (notebooks, personal computer, portable storage devices and mobile devices)?		**			
DSI-4.5	Do you implement controls to block access to known file transfer and ex-filtrate sites and the rules are review as least quarterly?		**			
DSI-4.6	Do you implement hardware security modules (HSM) for the protection of private/encryption keys?		**			
DSI-4.7	Do you monitor all traffic leaving the organization and detect any unauthorized encrypted traffic?		**			
DSI-4.8	Do you implement access control to restrict logical and physical access to files and folders stored on servers, databases, storage platforms and backup media which contain sensitive information, such as passwords, transaction data?		**			
	The service provider's should have established and implemented policies, procedures and controls for clients' data segregation					
DSI-5.1	Do you segregate clients data physically (different hardware devices) and/or logically (virtualization, multiple OS, database instances etc.from one another?		**			
DSI-5.2	Do you implement application/system controls to segregate clients' data such that If all clients are using the same application on the same server concurrently, where these client's data are stored in the same data files/ database, each data field should have an appropriate meta tag/ unique identifier affixed to keep clients' commingled data separated		**			
	Segregation of clients data physically (different hardware devices) and/or logically (virtualization, multiple OS, database instances etc.) should be implemented to isolate data of one clients from another					
DSI-6.1	Do you implement encryption methodologies to protect classified e-commerce data moving through public networks and infrastructures (e.g., the Internet)? Note: Please indicate the encryption menchanism implemented, the encryption should be at minimum 3DES, AES or equivalent		**			
	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.					
DSI-7.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?		**			
	Service Provider should have policies, procedures and controls implemented to safeguard data media during transportation					
DSI-8.1	Do you have policies, procedures established and implemented to safeguard data media during transportation?		**			
DSI-8.2	Do you encrypt data media before transportation and practice split knowledge and dual control of the encryption keys so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key?		**			
DSI-8.3	Do you implement tamper-proof container/ cases with lock capability to physically protect the data media from unauthorized access during transportation?		**			
	Production data should not be replicated or used in non-production environments					
DSI-9.1	Do you have policies, procedures established and implemented to prohibit replication of production data to non-production environments? If no, do you have policies, procedures established and implemented to obtain documented approval from all clients if you use their data in non-production environments (e.g. terms of business, service agreements, etc.)?		**			
	Any use of client data in non-production environments requires explicit, documented approval from all clients whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements					
DSI-10.1	Do you have policies, procedures established and implemented to obtain documented approval from all clients if you use their data in non-production environments (e.g. terms of business, service agreements, etc.)?		**			
DSI-10.2	Do you implement secure deletion (e.g., degaussing/cryptographic wiping. of archived and backed-up data)?		**			
	Datacentre and Physical Security					
	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) should be implemented to safeguard sensitive data and information systems					
DCS-1.1	Do you have physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented? Note : The physical security perimeters implemented should be assessed by an independent auditor and provide relevant assessment reports		**			

Threat and Vulnerability Risk Assessment (TVRA) should be conducted to identify security threats to an operational weaknesses in a data centre in order to implement appropriate controls to safeguard the data centre and in turn, protecting information assets resided within the data centre

DCS-2.1	Have you or your data centre provider conducted a threat and vulnerability risk assessment on the data centre by an independent 3rd party?		**			

The scope of the Threat and Vulnerability Risk Assessment ("TVRA") conducted for both primary and secondary data centre.

DCS-3.1	Does the scope of the threat and vulnerability risk assessment on the data centres includes the followings? a. possible scenarios of threats which include theft, explosives, arson, unauthorised entry, external attacks and insider sabotage b. data centre's perimeter and surrounding environment, as well as the building and DC facility c. daily security procedures, critical mechanical and engineering systems, building and structural elements, and physical, operational and logical access controls		**			

All hardware devices, including portable devices connecting to the network should be actively managed (inventory, track and correct) so that only authorized devices are given access, and unauthorized and unmanaged devices are identified and prevented access

DCS-4.1	Do you have policies, procedures established and implemented for asset management at data centre to inventor, track and correct all hardware devices, including portable electronic devices connecting to your organisation's network?		**			

Automated equipment identification should be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location

DCS-5.1	Do you implement automated equipment identification as a method to validate connection authentication integrity based on known equipment location? Note: Please describe the technology implementation on how equipment identification and authentication are achieved e.g. network level authentication, network access control (NAC), client certificates etc.		**		**	

Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises

DCS-6.1	Do you have policies, procedures established and implemented on relocation or transfer of hardware, software, or data to an offsite premises? Note : Policy must include the requirement of written consent from the client prior to relocation		**			

Policies and procedures should be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This should include a wiping solution or destruction process that renders recovery of information impossible. The erasure should consist of a full overwrite of the drive before it is released to inventory for reuse and deployment, or securely stored until it can be destroyed

DCS-7.1	Do you have policies, procedures established and implemented governing asset management, repurposing of equipment using industry standards (e.g. NIST.SP.800-88) and to sanitize all computing resources of client data once a client has exited your environment or has vacated a resource??		**			
DCS-7.2	Do you provide evidence that secure disposal of equipment have been conducted according to a recognized industry standards (e.g. disposal certificate) upon request? Note: Indicate in the remarks the sanitisation method that is in practice (e.g. overwrite data in seven passes, and/or magnetic devices degaussing for physical destruction).		**		**	

Policies and procedures should be established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information

DCS-9.2	Do you have controls to ensure that your personnel and involved third parties have been trained to maintain a safe and secure working environment in offices, rooms, facilities and secure areas following your documented policies and procedures?		**			

Ingress and egress to secure areas should be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access

DCS-10.1	Do you have policies, procedures established and implemented to constrain and monitor ingress and egress to secure areas to ensure that only authorized personnel are allowed access?		**			

Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises should be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss

DCS-11.1	Do you have measures implemented to monitor, control and if possible isolate from data storage and processing facilities the ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises?		**			

Protection measures should be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment

DCS-16.1	Do you have policies, procedures established and implemented based on geographically-specific Business Impact Assessment to react to natural and man-made threats?		**			

Encryption & Key Management

Policies, procedures and controls should be established, implemented for the management of cryptographic keys

EKM-2.1	Do you have policy and procedures established and implemented for cryptographic keys management that including at least the following? a. procedures for lifecycle management from key generation, change, distribution, revocation, certification, storage, use, archival to destruction of cryptographic keys and public key infrastructure) b. list of approved cryptographic protocol and algorithms standards c. access controls requirements for secure key generation and exchange and storage including segregation of keys used for encrypted data or sessions d. procedure to inform client of changes within the cryptosystem upon request, especially if the client data is used as part of the service, and/or the client has some shared responsibility over implementation of the control.		**			

Cryptographic key management policy and procedures should be established to control the generation, change, revocation, destruction, distribution, certification, storage, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

EKM-6.1	Do you have policy, procedures established and implemented which defined the encryption requirements for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging. as per applicable client specific legal, statutory, and entity specific regulatory compliance obligations)?		**			
EKM-6.7	Do you implement encryption to protect data and virtual machine images for the followings? a. during transport across and between networks and hypervisor instances b. in storage such as file servers, databases and workstations c. during processing where data is used in memory Note: Please describe the encryption method/strength used for encryption of data		**		**	

Governance and Risk Management

Baseline security requirements should be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations

GRM-1.1	Do you have baseline security standard defined for application, technologies, systems and network equipments deployed within your environment? (e.g., hypervisors, operating systems, routers, etc.) Note : Please indicate in the remark column which standards your are using.		**		**		

Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use

GRM-2.1	Do you have controls implemented to continuously monitor and report the compliance of your infrastructure and application against your security baselines?		**				

Risk assessments associated with data governance requirements should be conducted at planned intervals.

GRM-4.1	Do you conduct risk assessments to evaluate data governance requirements at least once a year considering the followings? a. Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure b. Compliance with defined retention periods and end-of-life disposal requirements c. Data classification and protection from unauthorized use, access, loss, destruction, and falsification		**				

Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility

GRM-5.1	Do you have policy, procedures implemented to ensure employees are constantly educated on their responsibilities in complying with security policies, procedures and standards for the protection of the organization and clients' information assets?		**				
GRM-5.2	Do you have controls implemented to ensure your technical, business, anf executive managers are responsible for the compliance of subordinates in training requirements on information security awareness?		**				

An Information Security Management Program (ISMP) should be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

GRM-6.1	Do you maintaint a Information Security Management Program (ISMP) to continuously improve information security posture in your organization to ensure information security risks are managed within the acceptable level for the protection of your organization and clients' information assets?		**				
GRM-6.3	Do you review your Information Security Management Program (ISMP) at least once a year?		**				

Employees should be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures

GRM-10.1	Do you educate and reinforce knowledge on your employee during awareness training the disciplinary actions to be taken on non compliance with policies and procedures?		**				

Risk assessment results should include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective

GRM-11.1	Do you update or enhance your security policies, procedures, standards and controls as a result of control gaps noted from annual and/or ad-hoc risk assessment?		**				

Aligned with the enterprise-wide framework, formal risk assessments should be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods

GRM-13.1	Do you conduct formal risk assessments in alignment with your enterprise-wide framework at least annually, or at planned intervals, to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods according to industry best practices? Note : Please if frequency is not annual indicate the frequency in the remark column		**		**		

Human Resources, Awareness and Education

Pursuant to local laws, regulations, ethics, and contractual constraints, all employed candidates, contractors, and third parties should be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk

HRS-1.1	Do you have policy, procedures established and implemented pursuant to local laws, regulations, ethics and contractual constraints, subjecting background verification for all employed candidates, contractors and involved third parties ? The background verification should include, but not restrict to the following items: a. criminal, employment background check b. satisfactory character references, friend or family interviews c. medical history (where applicable) d. confirmation of claimed academic and professional qualifications e. independent identity validation, such as a passport f. credit check for those requiring access to financial systems g. federal, state, and local law enforcement records check		**				

Employment agreements should incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets

HRS-2.1	Do you have policy, procedures established and implemented requiring employees to sign-off and adhere to information governance and security policies?		**				

Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details should be identified, documented, and reviewed at planned intervals

HRS-3.1	Do you have policies, procedures established and implemented to enforce that all personnel sign non-disclosure agreement (NDA) or confidentiality agreements to commit protection of organization's confidential data?		**				

Roles and responsibilities of contractors, employees, and third-party users should be documented as they relate to information assets and security

HRS-7.1	Do you have policy, procedures established and implemented to document the roles and responsibilities of contractors, employees and third-party users in relation to the protection of organization's information assets?		**				
HRS-7.2	Do you clarify your administrative responsibilities versus those of the contractors and clients through role definition?		**				

Policies and procedures should be established and technical measures implemented for defining allowances and conditions for permitting usage of organizationally-owned or managed user endpoint devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components

HRS-8.1	Do you have policy, procedures established and implemented to define allowances and conditions for permitting usage of organizationally-owned or managed user endpoint devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components?		**				

A security awareness training program should be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data should receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization

HRS-10.2	Do you ensure that administrators and data stewards are properly trained on their legal responsibilities with regard to security? (e.g. employee annual self-assessment)		**				

Identity & Access Management

Access to, and use of, audit tools used for compliance and security assessment (e.g. SolarWinds, Qualys Guard) should be appropriately segmented and restricted to prevent compromise and misuse of log data

IAM-1.1	Do you have policy, procedures established and implemented for segmentation and restriction access to audit tools to prevent compromise and misuse of log data?		**				
IAM-1.2	Do you have controls to monitor and log access to audit tools including timestamps, account and terminate IDs, activity descriptions, object being change, before and after values etc?		**				
IAM-1.3	Do you have controls implemented to monitor privileged access (administrator level) to audit tools?		**				
IAM-1.4	Do you have controls implemented to restrict access to audit tools system / database audit logs ? (e.g. all users have only read access to folders, audit trail tables)		**				

Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software should be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures

IAM-6.2	Do you have controls implemented to prevent unauthorized access to your or your client application, program or object source code, and assure it is restricted to authorized personnel only solely for legitimate purposes? (e.g. limited access to source code repository, development releases folders, etc.)		**				

Policies, procedures, security standards should be established to implement strong authentication and authorisation mechanisms for systems, applications to prevent unauthorised access.

IAM-10.1	Do you have policy, procedures established and covering points a,b,c,d and e below on built-in security requirements for internal and clients' system/application authentication and authorisation to prevent unauthorised access? a. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) b. Account credential lifecycle management from instantiation through revocation c. Account credential and/or identity store minimization or re-use when feasible d. Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expirable, non-shared authentication secrets) e. Industry supported technologies (e.g. digital credentials, PKI, single sign-on (SSO), OpenID/OAuth, etc.) and authentication methods (user name & password, PINs, X.509 digital cert, one-time password, biometrics, smart cards, hardware tokens etc.) are used whenever appropriate, together with administrative controls for identity access management Note: Please indicate the technology and authentication method used.		**		**		

Cloud Architecture & Virtualization Security

Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs.

IVS-1.1	Do you have policy and procedures established and implemented for the management of audit logs that includes at minimum the followings? a. protection and retention based on applicable legal, statutory or regulatory compliance obligations; b. implementing unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies; and c. supporting forensic investigative capabilities in the event of a security breach		**				

A reliable and mutually agreed upon external time source should be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines

IVS-4.1	Do you synchronize all your systems to a common time reference through a synchronized time-service protocol (e.g., NTP)?		**				

The availability, quality, and adequate capacity and resources should be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements should be made to mitigate the risk of system overload

IVS-6.1	Do you provide cloud bursting capabilities? Note: If so provide additional information on how do you provide it in the remarks.		**		**		
IVS-6.2	Do you provide an auto scaling solution to support web/application layer load balancing across users?		**				

Network environments and virtual instances should be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations should be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls

IVS-8.1	Do you have network policies, procedures established and implemented for your network environment and virtual instances to restrict and monitor traffic between trusted and untrusted connections?		**				

Production and non-production environments should be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties

IVS-9.1	Do you implement clear segregation of job duties between personnel accessing production environments and personnel accessing non-production environment? Note : Please indicate if segregation feasible or not feasible in the remark column and indicate if you monitor changes and access to production as a compensating control where not feasible.		**		**		

Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, should be designed, developed, deployed and configured such that the service provider and client user access is appropriately segmented from other client users.

IVS-10.1	In your multi-tenant environment, do you design, develop, deploy and configure the environment to segment user access of one client from another client?		**				
IVS-10.2	Do you perform isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance (e.g. single client deployment and implementation of stronger access control (multi factor-authentication) for sensitive data)?		**				

Secured and encrypted communication channels should be used when migrating physical servers, applications, or data to virtualized servers and, where possible, should use a network segregated from production-level networks for such migrations

IVS-11.2	Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?		**				

Network architecture diagrams (inclusive of wireless) should clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures should be implemented and should apply defence-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks, replay attacks, WEP/WPA attacks, rogue access point (ap), man-in-the-middle) and/or distributed denial-of-service (DDoS) attacks

IVS-13.2	Do you implement technical measures and apply defence-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks, replay attacks, WEP/WPA attacks, rogue access point (ap), man-in-the-middle) and/or distributed denial-of-service (DDoS) attacks?		**				

Interoperability & Portability

Open and published APIs should be used to ensure support for interoperability between components and to facilitate applications migration

IPY-1.1	Do you have the followings to support interoperability of components? a. a documented procedure to establish and publish a list of all Application Program Interfaces (APIs) utilized in the system and/or made available in the service b. a procedure to demarcate which are standard and which are customized along with the relevant internal documentation procedures		**			

All structured and unstructured data should be available to the client and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)

IPY-2.1	For client data management, do you have the ability to provide data upon request in one of the industry-standard formats (.doc, .xls, .pdf, logs, and flat files)?		**			

Policies, procedures, and mutually-agreed upon provisions and/or terms should be established to satisfy client requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence

IPY-3.1	Do you have a set of documented policies and procedures (i.e. service level agreements) governing the use of service-to-service Application Program Interfaces (APIs) for interoperability between your system/service and third-party applications?		**			
IPY-3.2	Do you have a set of formalized and documented policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?		**			

The service provider should use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and should make available a document to clients detailing the relevant interoperability and portability standards that are involved

IPY-4.1	Do you have policies, procedures established and implemented to enforce the use of secure (e.g. non-clear text and authenticated) standardized network protocols for the followings? a. import and export of data b. administrative functions for the management of the system and/or service		**			
IPY-4.2	Do you make available, to clients, a document detailing the relevant interoperability and portability standards involved?		**			

An industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) should be used to help ensure interoperability, and should have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for client review

IPY-5.1	Do you use industry-recognized virtualization platform and standard virtualization formats (e.g. Open Virtualization Format (OVF) to help ensure interoperability for systems/services?		**			

Security Incident Management, e-Discovery and Cloud Forensics

Points of contact for contractual compliance, applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities should be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement

SEF-1.1	Do you maintain and regularly update (at least once a year) the points of contact for contractual compliance, applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities in the event that compliance liaison are required or a forensic investigation requires rapid engagement with law enforcement?		**			

Policies and procedures should be established to triage security-related events and ensure timely and thorough incident management.

SEF-2.1	Do you have a policies and procedures implemented for security incident management which includes the followings? a. a roster of the incident response team, the key point-of-contact and the roles and responsibilities of the incident response team including management personnel who will support the incident handling process by acting in key decision-making roles b. evaluation method for incidents to categorise them as security related based on risk, severity levels and with resolution time? c. definition of the scope, objectives and requirements to determine how and who should respond to the incident, as well as the monitoring and reporting activities d. specific implemented procedures for forensic investigation - a reasonable notification period, such as to notify the client within 1 hour of major incident on critical systems upon the discovery - an executive summary of the relevant incident; - an analysis of the root cause which triggered the relevant incident; - a description of the impact of the relevant incident on the client i. compliance with laws and regulations applicable to the client; ii. the client's operations; - a description of the remedial measures taken to address the root cause and consequences of the relevant incident. The report should be provided to the client within 14 days upon the discovery of a relevant incident e. defined and communicated incident reporting requirements such as (time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification). This reporting should also include notifying the appropriate authorities in accordance with all legal or regulatory requirements		**			

In the event a follow-up action concerning a person or organization after an information security incident requires legal action, proper forensic procedures, including chain of custody, should be required for the preservation and presentation of evidence to support potential legal action subject to the relevant jurisdiction. Upon notification, clients and/or other external business relationships impacted by a security breach should be given the opportunity to participate as is legally permissible in the forensic investigation

SEF-4.2	Do you have adequate policies, procedures established and implemented to support litigation holds (freeze of data from a specific point in time) for a specific client without freezing other client's data?		**			
SEF-4.3	Do you have policies, procedures established and implemented to give upon notification the opportunity to clients and/or other external business relationships impacted by a security breach to participate as is legally permissible in the forensic investigation?		**			

Mechanisms should be put in place to monitor and quantify the types, volumes, and costs of information security incidents

SEF-5.1	Do you have policies, procedures established and implemented to monitor and quantify the types, volumes and impacts on all information security incidents?		**			

Security incident information should be made available by the service provider to all affected clients and third providers periodically through electronic methods (e.g. portals)

SEF-8.1	Do you have procedures established and implemented to make security incident information available to affected clients and third party providers through electronic methods based on the followings? a. immediate notification or as per agreed notification timeline on the occurrence of incident b. periodically updates on aggregated incidents		**			

Supply Chain Management, Transparency and Accountability

Review of the risk management and governance processes of third party service providers should be executed to ensure that practices are consistent and aligned to account for risks inherited from other members of that third party service providers's cloud supply chain.

STA-4.1	Do you have outsourcing/vendor management policy and procedures implemented to monitor, control, measure and inspect the operational and information security aspects of your third party service provider and review their risk management and governance procedures? Note : All partners/third party-providers upon which your information supply chain depends on should be included.		**		

Threat and Vulnerability Management

Policies, procedures should be established and technical measures implemented to prevent the execution of malware on organizationally-owned or managed user endpoint devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components

TVM-1.2	Do you have policies, standards, procedures established and implemented to ensure that security threat detection systems using signatures, lists or behavioural patterns are updated across all infrastructure components as and when available?		**		

Policies, procedures should be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls

TVM-2.1	Do you have policies, procedures established and implemented for conducting independent reviews and assessments at the following frequency for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components to ensure the efficiency of implemented security controls? a. vulnerability assessment - Quarterly b. penetration testing - At least annually		**		

Information of weaknesses identified from network vulnerability assessment, penetration testing should be provided to clients upon request especially if client data is used as part the service and/or the client has some shared responsibility over implementation of control

TVM-6.1	Do you provide upon request the information on weaknesses identified from vulnerabilities and penetration testing? Note: If you are unable to provide, please explain how would you communicate to the customers on the identified weaknesses and remediation		**		

Mobile Security

Documented mobile device policies and procedures should be established that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider should post and communicate the policy and requirements through the service provider's security awareness and training program

MOS-4.1	Do you have mobile device policies, procedures established and implemented which stipulate: a. definition for mobile devices and the acceptable usage b. data classification permitted on each type of mobile device and the control mechanisms required c. list of pre-approved application, application stores d. requirement of centrally managed asset management system for mobile devices management e. authentication, encryption storage/transmission (data in transit or at rest) and backup requirements by device type f. risk assessment and approval requirements for new mobile device deployment/use g. security standards for hardening of mobile devices		**		

A centralized, mobile device management solution should be deployed to all mobile devices permitted to store, transmit, or process service provider's company data and/or clients' data

MOS-13.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process service provider's company data and/or clients' data?		**		

Mobile devices connecting to corporate networks, or storing and accessing company information, should allow for remote software version/patch validation. All mobile devices should have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel should be able to perform these updates remotely

End of Questionnaire

Before saving and submitting this file, please double-check that no items are marked with **

Please save this file as excel document and forward it to OTM@sota.edu.sg

Thank you very much for your participation.

Annex E :
PROJECT SCHEDULE

Project Schedule

Per Annex C, 2.1.2, SAS envisages the project to complete within eight (8) months for Phase 1, and six (6) months for Phase 2.
NOTE: HR module to complete by **30 June 2026**

Tenderer may provide additional information in another format if it clarifies its proposal, but minimally the project schedule must include the following information:

Phase 1

Task	Duration (month)	2026									
		Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Phase 2

Task	Duration (month)	2027					
		Jan	Feb	Mar	Apr	May	Jun

SCHOOL OF THE ARTS SINGAPORE

Annex F :
PROPOSED PROJECT TEAM AND TRACK RECORD

Proposed Project Team and Track Record

Details of proposed project team (please furnish details in the proposal)

S/no.	Name of team member	Role (e.g. team leader, member etc.)	Years of relevant experience

List of relevant projects completed in the last 5 years i.e. 2020 to 2024 (please furnish details in the proposal)

S/no.	Name of client	Project description	Year completed	Name of client contact person	Email of client contact person

SCHOOL OF THE ARTS SINGAPORE

Annex G :
TECHNICAL REQUIREMENT SPECIFICATIONS

CONTENTS

1 General Technical Requirements

1.1 Ease of Maintenance

1.1.1. The System shall be architected and designed with appropriate patterns used to allow new functions to be added and existing functions to be enhanced and/or decommissioned with minimal impact to the existing components and operations of the System.

1.1.2. There shall not be any hard-coded parameters in the System (e.g. IP address, port number, path, file location, host name, domain name, etc.).

1.1.3. The Contractor shall develop a set of comprehensive application related standards and guidelines (e.g. no duplication of codes without good reasons) to ease maintenance of the System.

1.2 Up-to-date Technology

1.2.1. The technical design of the System and the platform on which it operates shall harness up-to-date technologies. In addition, various web browsers (e.g., Safari, Google Chrome, Firefox) and Apple Operating System must support it.

1.2.2. In the event of a newer version of the product or technology released before the Commissioning Date and the version is different from the Contractor's tender proposal, the Contractor shall assess the impact and propose the most suitable version to be adopted for production release with strong justification. During the Software Warranty Period, the version of the product or technology shall not be more than 2 major versions behind the latest version available.

1.3 System Performance

1.3.1. In the event that the Service Level Agreement (SLA) as below cannot be met for whatever reasons. In that case, the Contractor shall carry out all necessary remedial actions and remedial services at no extra cost to SAS. If the Contractor diagnoses and shows concrete evidence that the problem is due to a component managed by SAS, the Contractor shall be required to propose the necessary recommendations to SAS to resolve the issue.

Service Level Agreement (SLA)

Severity Level	Problem Response Time	Status Reporting	Problem Resolution Time
Critical	Within 4 hours	Every 4 hours	Within 1 day
Major	Within 8 working hours	Daily	Within 4 working days
Minor	Within 1 working days	End of Problem Resolution	Within 7 working days

1.3.2. The Contractor shall review and highlight to SAS, in detail, all necessary actions required for the existing infrastructure performance requirements.

1.3.3. The Contractor shall provide the application performance testing benchmark results on meeting the defined set of standard benchmarked performance of the System.

1.3.4. For any testing performed, in the event of failure to meet the defined set of performance benchmarks, the Contractor shall need to be able to establish whether or not the failure is caused by issues with the Cloud Hosting environment, or due to the System's poorly written code or incorrectly set parameters for action to be taken by the parties responsible.

1.3.5. The Contractor shall note that the System Response Time shall be measured as the elapsed time between the moment a user initiates a computer process by pressing a key (<Enter> or <Submit>) or clicking a mouse or other input device and the moment first appearance of computer-generated output is displayed on an output device (e.g. screen of the user, printer) or elapsed time between two screens. A computer process can be a query or an update to

a database, a request of an electronic document or any other logical unit of business transactions that involve interactive responses.

1.3.6. The Contractor shall also note that a transaction is defined as a completed unit of activity by a user of the System utilising an online workstation interactively. The unit of activity is made up of one or more inputs by the users that result from input devices, such as a computer keyboard. Upon processing of the input by the System, one or more characters of information response will be sent to the workstation that originated the input.

1.3.7. The System shall meet the online System Response Time as stated in Table 1:

Table 1

Type of Transaction	**Expected Response Time**
Online Transaction	Shall not exceed 5 seconds for 95% of the time and shall not exceed 10 seconds for the remaining 5% of the time.
Web Page Loading	Shall not exceed 3 seconds for 95% of the time and shall not exceed 5 seconds for the remaining 5% of the time.
User login to the System	Shall not exceed 3 seconds for 95% of the time and shall not exceed 5 seconds for the remaining 5% of the time.

1.4 System Availability

1.4.1. The Contractor shall ensure that the System minimally achieves 99.5% availability.

1.4.2. System maintenance activities (e.g. backup jobs) shall not impact the availability of the System.

1.4.3. The Contractor shall conduct regular System maintenance, configuration, and fine tuning/optimisation to ensure the System is always in good working condition. The Contractor shall then inform SAS at agreed trigger points on the necessary upgrade and/or enhancement for continual achievement of optimum System performance and required Service Availability.

1.4.4. The Contractor shall ensure that all troubleshooting, upgrade or maintenance work on the production System shall be done strictly after Office Hours to avoid disruption of Service.

1.4.5. The Contractor shall provide SAS the planned activities at the beginning of the calendar year. The Contractor shall inform SAS on the ad-hoc maintenance 1 month before the executions.

1.4.6. The Contractor shall clarify and establish the required scheduled service downtime and planned total service uptime per calendar month with SAS to avoid unnecessary disputes later.

1.4.7. The Contractor shall implement auto-scaling based on conditions that are predefined with SAS. (e.g. scale up x% and scale down at y%).

1.4.8. The Contractor shall implement thresholds that are set to trigger alerts.

1.4.9. The Contractor shall implement front-end scaling based on the number of incoming requests (e.g. web pages, data transfer).

1.4.10. The Contractor shall implement back-end scaling such as load based scaling (jobs in queue) and time based scaling (how long jobs have been in queue).

1.4.11. The Contractor shall monitor and review metrics such as concurrent limitations, increased latency, time-out errors and upgrade capacities if required.

1.5 System Reliability/Integrity

1.5.1. The Contractor shall ensure that the System is fully tested and quality assured before implementation so as to achieve maximum reliability.

1.5.2. The Contractor shall propose suitable procedures for performance monitoring and analysis to enable proper capacity planning, tuning and maintenance.

1.5.3. The Contractor shall ensure that failure of any software fault in any of the functions in the System shall not affect the integrity of the data captured/stored or lead to any loss of data in the System.

1.6 System Readiness

1.6.1. The Contractor shall be responsible for the management and coordination of all activities, including working closely with the relevant parties to ensure a smooth roll-out of the System. This shall be applicable at all System implementations, deployments, System Integration Test, User Acceptance Test, trainings and rollouts.

1.6.2. The Contractor shall submit the necessary documentations required for System readiness as part of the proposal.

1.7 Service Administration

1.7.1. All administrative access given to SAS to access the System hosted in the Commercial Cloud Hall be performed remotely via the Internet.

1.7.2. Remote administrative access shall only be granted to authorised personnel who need to perform administration on the System remotely.

1.7.3. The Contractor shall implement the security requirements for remote administration.

1.8 Supported File Formats

The System shall allow SAS to define the file formats in which the System is able to export queries, reports and documents, and handle files (e.g., txt, csv, excel, jpg, pdf etc) imported or transmitted into the System.

1.9 Disaster Recovery (DR)

1.9.1. The Contractor shall provide SAS on the documentation required for the Business Continuity Plan (BCP) as part of the DR.

1.9.2. The Contractor shall ensure high availability of the System in the event of the commercial Cloud Service Provider (CSP) experiencing data centre failures. This shall be with zero data or content loss.

1.9.3. The Contractor shall work with SAS in ensuring the System's availability in an event of a disaster.

1.10 Data Archival

1.10.1. The Contractor shall keep the archived data (e.g., transactional data, metadata and etc) of the System for seven (7) years.

1.10.2. The Contractor shall archive the past 180 days data of the System.

1.10.3. The Contractor shall comply with the IT security requirements in Section 5 for the archived data to prevent malicious or accidental deletion or modification of records even where access credentials are granted.

1.10.4. The Contractor shall always provide the cost-optimisation design/solution of the data archival based on SAS needs. e.g. the Contractor shall recommend Amazon Web Services (AWS) S3 Glacier Archive or equivalent as the archival storage instead of using S3 standard.

1.10.5. The Contractor shall implement a data archival storage solution with highly available,99.99% durable and highly protected against degradation or corruption throughout the multi-decade retention period.

1.10.6. The Contractor shall purge the data when the retention period for the data is over.

1.11 Data Migration

1.11.1. The Contractor shall provide a data (e.g., transactional data, metadata and etc) migration plan for migrating the data from database on-premise to the commercial Cloud as agreed with SAS before the execution.

1.11.2. The Contractor shall implement the transform and load processes to move data from the database on-premise to the commercial Cloud.

1.11.3. The Contractor shall convert the historical data from the existing relational database to the Cloud database.

1.11.4. The Contractor shall conduct the post-migration audit to ensure all the historical data are retrievable smoothly in the Cloud before the old System can be retired.

1.11.5. The Contractor shall implement a backup plan to rollback in case the first attempt of data migration fails.

1.11.6. The Contractor shall propose an appropriate migration tool to SAS.

1.11.7. The Contractor shall provide the data reports and checklist of the whole data migration activities to SAS.

1.11.8. The Contractor shall share the issue logs and audit logs of the operational migration process to SAS.

1.11.9. The Contractor shall propose the solutions on the issue logs of the operational migration process for SAS approval.

1.11.10. The Contractor shall run the subsequent rounds of the data migration activities until all operational required data migrate to the System without additional cost.

1.12 Single Sign On (SSO)

The System shall have the SSO feature to turn on to enable SAS to SSO in multiple applications and Systems using Security Assertion Markup Language (SAML) protocol.

2 Architecture

2.1 General Architecture Requirements

2.1.1. The System shall leverage the benefits of adopting cloud, to fulfil business expectations such as availability, security, flexibility, scalability, performance, compliance and cost.

2.1.2. The Contractor shall provide a loose coupling architecture design for the System.

2.1.3. Where there is a need for additional controls and governance to safeguard the integrity of the System, the Contractor shall develop and document the additional controls and governance processes for the development, maintenance and operations team to comply. The controls can come in the form of manual processes or automated checks, though SAS has preference for automated checks.

2.1.4. The System shall meet System availability requirements and recover any disruptions gracefully and on a timely basis.

2.1.5. All services and components (e.g. operating Systems, logging layers, cloud configurations and databases) shall be configured to a consistent and common locale to facilitate the tracing of transactions. Presentation of data shall adopt Singapore locale (i.e. UTC+8) and in English.

2.2 Backup & Recovery Plan

2.2.1. The Contractor shall define a cost-effective solution to securely store a copy of the data (e.g. business data, security keys, source codes, infrastructure codes, scripts, configuration data, virtual machine images, etc.) on the cloud with proper access controls.

2.2.2. The proposed solution shall include the backup strategy for each type of data and the recommended retention and archival strategy to be used (including security considerations such as encryption and password protection), subject to SAS's approval.

2.2.3. The Contractor shall conduct data recoverability testing to verify the effectiveness of backup and recovery plans.

2.2.4. The Contractor shall perform backups of various information contained in the System is performed with the agreed frequency consistent with the Recovery Point Objective (RPO) within 24 hours and Recovery Time Objective (RTO) within 8 hours.

2.2.5. The Contractor shall implement the same security safeguards in the alternative site as the primary site.

2.2.6. The Contractor shall ensure that backup data is protected through encryption and access controls.

2.3 System Integration

2.3.1. The System shall integrate with the following existing SAS Systems (on-premise or Cloud) using APIs or connectors: -

(a) Microsoft SharePoint (Staff Directory in Staff Portal);
(b) Event Booking Management System (short as EBMS and In the AWS Cloud);
(c) Student Management Systems (short as SMS);
(d) Google Authentication for user access management.

2.3.2. The System shall be able to integrate with third-party Systems using APIs or connectors in the Cloud.

2.3.3 The following Table 2 outlines the indicative interface requirements for the System. The Contractor shall assess and propose an appropriate interface design for implementation to facilitate integration and seamless end-to-end business process.

Table 2

From System (Originating)	Source System Platform	To System (Receiving)	Data	Uni/ Bi-Directional
Staff Portal (Microsoft SharePoint)	On-Premise	ERP (HRIS)	Staff Directory	Uni-Directional
Event Booking Management System (EMBS)	In Cloud	ERP (Finance)	Event Booking Transactions	Uni-Directional
Student Management System (SMS)	On-Premise	ERP (Finance)	Student Fee Data	Uni-Directional
Any new third-party System	In Cloud	ERP(Finance)	Payroll Journals	Uni-Directional
ERP(HRIS)	In Cloud	Any new third-party System	Employee Master Data, Approved Claims, Leave Encashment, No-Pay and etc	Uni-Directional
ERP(HRIS)	In Cloud	Digital Form System	Employee Master Data with cost centre	Uni-Directional

3 Infrastructure

3.1 Commercial Cloud Services

3.1.1. The Contractor shall submit a proposal that comprises:

(a) The complete set of itemised Platform as a Service (PaaS) commercial cloud services that are required from the commercial CSP to implement the proposed System. This set of services are hereinafter being referred to as the “Cloud Solution”. The Cloud Solution shall be:

(i) Configured to be distributed across the commercial CSP’s multiple data centres so as to continue ensuring the availability of the Cloud Solution even in the event of the commercial CSP experiencing multiple data centre failures. This shall be with zero data loss.

(b) The complete set of services and infrastructure (hardware and software) from third party providers that are required to be deployed as part of the proposed solution.

3.1.2. The proposed Cloud Solution shall include:

(a) required are derived as well as all assumptions made; and The list and descriptions of the individual items to be subscribed from the commercial CSP as well as the units required;

(b) The list and descriptions of the individual items required for the proposed System but not subscribed from the commercial CSP directly as well as the units required;

(c) Details explaining how the units

(d) The following environments
(i) Production (Prod).
(ii) System Integration Test (SIT)
(iii) User Acceptance Test (UAT)

(ii) and (iii) in the above **Clause 3.1.2(d)** will be collectively known as “Testing Environments”.

3.1.3. The System shall implement, deploy and support Platform as Code (PaC) for the provision and deployment of Cloud services where possible.

3.1.4. The Contractor shall submit all solution design documents and diagrams of the System clearly detailing and identifying how the
(a) Components of the proposed System are derived and how they meet the tender requirements; and
(b) Proposed System is designed such that it is able to handle scaling on demand.

3.1.5. The Contractor shall adopt best practices and open standards available in the cloud environment so as to optimise the in-built System capabilities and to minimise customisation, System deployment time and cost.

3.1.6. The Contractor shall propose a commercial CSP that is Multi-Tier Cloud Security (MCTS) certified.

3.1.7. The proposed Cloud Solution shall include the following security measures:

(a) Use cloud native System and network firewalls, such as AWS Security Groups and Network Access Control List (NACL) or equivalent;

(b) Use cloud security detection tools, such as AWS GuardDuty or equivalent;

(c) Use cloud native logs whenever possible, such as AWS CloudTrail, AWS CloudWatch or equivalent;

(d) Receive notification when suspicious activities are detected; and

(e) Stream logs to Commercial Cloud logging servers.

3.1.8. The commercial CSP shall ensure that SAS’s data is isolated from other tenants in the multi-tenant cloud.

3.1.9. In the multi-tenancy, the commercial CSP shall ensure that performance of the System deployed for SAS does not interfere with other tenants' overloads in the multi-tenant cloud.

3.1.10. In the multi-tenancy, the commercial CSP shall adequately configure the infrastructure to ensure no corrupted data from other tenants could spread to SAS.

3.1.11. In the multi-tenancy, the commercial CSP shall put strong authentication and access control mechanisms on the physical host to prevent a malicious user from changing the virtual machine's configuration to cause a loss of monitoring capabilities.

3.2 Transition Management to a new commercial CSP

3.2.1. The Contractor shall duly hand over all items owned by SAS to the new commercial CSP, including assets, subscriptions, licences, System documentation, and all SAS's account information in both hard and editable softcopy in Microsoft Office file format.

3.2.2. The Contractor shall ensure the accuracy and completeness of information documented and handed over to the new commercial CSP.

3.2.3. The Contractor shall also duly hand over all contents and all related data owned by SAS to the new commercial CSP in editable softcopy in their source code and executable format. The source code shall be the source code used to generate the deployed executables.

3.2.4. The Contractor shall brief the new commercial CSP- fully on all relevant operational information required to achieve a smooth handover process and allow the latter to shadow his team to learn the daily operational activities.

4 Service Management

4.1 Service Management and Operations

4.1.1. The goal of the Service Management and Operations is to provide ongoing day-to-day operation support, maintenance and management of the cloud services for the System. Such provided services are operational and recurrent in nature and shall hereinafter be referred to as "Managed Services".

4.1.2. The Contractor shall itemise and state all charges for the implementation and maintenance of the System. The Contractor shall provide all Managed Services for the System.

4.1.3. The Managed Services shall minimally cover the scope of the following services:

(a) Patch Management Services;
(b) Identity Administration Services;
(c) Backup & Recovery Services;
(d) Service Operation Control Centre; and
(e) Service Desk Services.

4.1.4. The Contractor shall provide any additional Managed Services with justification if required for the support of the proposed System. The Contractor shall itemise and state such additional Managed Services.

4.2 Patch, Minor (Fixpack) and Major (Service Packs) Management Services

4.2.1. The Contractor shall note the following for the System:

(a) Patch/fixpack is a generally available update provided by the product vendor or open-source communities (hereinafter collectively referred to as "Vendors") to fix a known bug or issue.

(b) Hotfix is a patch to fix a specific issue, not always as part of a general release.

(c) Minor updates/fixpacks are incremental updates between Major Update/ Service Pack of software versions to fix multiple outstanding issues.

(d) Major Update/Service Pack is an update that fixes many outstanding issues, normally includes all patches, hot fixes, maintenance releases/ fixes packs that pre-dates the service pack as well as include new functionality.

(a) to (d) in this **Clause 4.2.1** shall collectively be referred to as "Patch(es)" in the tender documents.

4.2.2. The Contractor shall propose the management process that shall be used to evaluate, propose and justify the Patches required for the System to SAS for approval before implementing any changes.

4.2.3. The Contractor shall establish and implement the following to manage all patching activities required in the System:
- Patch management process to be approved by SAS and patch management team.

5 IT Security

5.1 General Compliance

5.1.1. The Contractor shall note that all security requirements under this section are mandatory unless otherwise explicitly stated, and each security requirement, regardless of the sub-section it is located, shall be applicable to the entire scope of this Contract for the System unless otherwise explicitly stated.

5.1.2. The Contractor shall provide details of conformance (if any) to relevant security standards (e.g. ISO 27001,Multi-Tier Cloud Security Standard) attained.

5.1.3 The Contractor shall ensure that the System is secure and shall subject all aspects of the design, implementation, operation and security controls of the proposed System for approval by SAS. The following design principles shall be incorporated:
(a) confidentiality;
(b) compliance;
(c) availability;
(d) authentication;
(e) integrity; and
(f) access control.

5.1.4. The Contractor shall provide the details of all aspects of the proposed System for review by SAS. The Contractor shall not withhold any information pertaining to the technical details and security limitations of the proposed System.

5.1.5 The Contractor shall ensure the provision of sufficient security controls to protect the System against unauthorised access, data loss, intrusion, malicious software infection, software vulnerability attacks, and hardware attack.

5.1.6. The Contractor shall ensure that no security backdoors and loopholes exist in the System.

5.1.7. The Contractor shall ensure that no unauthorised software or Systems exist within the environment.

5.1.8. The Contractor shall wholly be responsible for any breach in security as a result of insecure implementations and/or configuration, missing patches, negligence, insider attacks, or loopholes in the solution.

5.1.9. The Contractor shall be responsible for ensuring the proposed security controls can be integrated and work seamlessly with other suppliers.

5.1.10. The Contractor shall implement security control measures to protect data at rest, data in motion and data in use.

5.1.11. Process, procedures and control measures shall be adequately and properly documented, and subject to the acceptance by SAS.

5.1.12. The System shall be resilient against known cyber-attacks and easily reconfigurable to respond to new and zero-day security threats that may arise.

5.1.13. The security procedures and standards shall include at least the followings:
(a) Security Risk Management;
(b) Security Architecture and Design;
(c) Personnel Security;
(d) Security Incident and Response Management;
(e) Security Management and Operation Processes;
(f) Security Configuration;
(g) Security Reviews;
(h) Audits for the System.

5.1.14. The Contractor shall provide technical documentation on the network, System, database and applications when requested during security risk analysis, security standards and policy implementation specific to the System.

5.1.15. Only approved commercial cloud and SaaS providers shall be used if SaaS is proposed. If the use of SaaS providers is proposed, the Contractor shall work with SAS to perform risk assessment on the proposed SaaS.

5.1.16. The Contractor shall implement versioning control for all related documentation.

5.2 Responsibilities

5.2.1. The Contractor shall work with SAS to perform security risk assessments[1] prior to using the cloud service and conduct a review at least once every 12 months thereafter. The Contractor shall submit the security risk assessment report to SAS within 10 working days upon the completion of each security risk assessment. The Contractor shall identify risk, respective inherent risk levels and propose treatment plans. The resultant residual risk level after treatment plans shall be approved by SAS's designated approving SAS.

5.2.2. The Contractor shall ensure that no unauthorised software or libraries are installed within the System.

5.2.3. The Contractor shall ensure that no security backdoors, loopholes or any form of mechanisms that allow unauthorised access are built into the System.

5.2.4. The Contractor shall ensure that all software implemented is the latest most stable version. In the course of implementation, any Patches or fixes shall be implemented. The Contractor shall discuss with SAS if any deviation is required.

5.2.5. The Contractor shall implement a procedure to track, detail and rectify any security vulnerabilities affecting all System components (including but not limited to open-source products/libraries, Commercial-Of-The-Shelf (COTS) products, underlying technologies and libraries).

5.2.6. The Contractor shall ensure that any login to the System for administrative or deployment purposes are only allowed from authorised source IP addresses in Singapore. All overseas logon and unauthorised IP addresses to the System for administrative or deployment purposes shall be denied.

5.2.7. The Contractor shall propose and document the roles and responsibilities that are only necessary to facilitate the operation and change management of the System, such as System, application and security administration, content management, content reviewers and approvers, and etc.

5.3 Data Security

5.3.1. The Contractor shall ensure that all sensitive information (e.g. login credentials, personal information, salary, financial transactions, cryptographic keys etc.) stored in the System and during transmission is encrypted. The Contractor shall propose and provide details on the encryption to be implemented for approval by SAS.

[1] Security risk assessments shall be guided by industry established security standards and best practices. SAS may conduct security risk assessments based on existing processes and templates if industry standards have been adopted to identify and mitigate security risks.

5.3.2. Cryptography Standards

5.3.2.1. The Contractor shall ensure that cryptographic algorithms implemented in the System meet or exceed the following:

(a) Symmetric Encryption: AES with key length of 256 bits;

(b) Asymmetric Encryption: RSA Public Key Encryption with key length of 2048 bits;

(c) Digital Signature: Digital Signature Algorithm (compliance to FIPS 186-3);

(d) Hash Algorithm: SHA-2 (FIPS 180-2) with digest size of 256 bits, and

(e) Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) (supporting P-256 and B-283 curves).

5.3.2.2. Cryptographic implementations that have been certified (e.g. FIPS certification) will be preferred. The Contractor should submit proof of such certifications (e.g. FIPS certification) as part of the Tender submission for evaluation, if available.

5.3.2.3. The Contractor shall propose supported encryption standards.

5.3.3 The Contractor shall ensure that cryptographic mechanisms implemented in the System are capable of handling normal and peak loads without degrading the performance of the System.

5.3.4. All digital certificates implemented within the System shall be digitally signed by a trusted and recognised Certificate Authority (i.e. no self-signed certificates).

5.3.5. The Contractor shall provide a detailed description and documentation of how the cryptographic keys are managed appropriately throughout its lifecycle, starting from key creation/generation, usage, backup, recovery, revocation to key destruction.

5.3.6. The Contractor shall implement measures and processes (such as password protection or encryption) to prevent unauthorised disclosure, modification or deletion of SAS's security-classified information in the System and end-users' computing devices such as laptops and tablets.

5.3.7. The Contractor shall provide a detailed description of the security measures and processes including the storage and transmission encryption software to be used in the proposal.

5.3.8. The Contractor shall ensure that encrypted data will continue to be usable in the event that the production System becomes unavailable or unusable.

5.3.9. The Contractor shall segregate the production environment from non-production environments.

5.3.10. The Contractor shall ensure that all sensitive data in the Cloud is identified and classified in accordance with the Information Sensitivity Framework (ISF) for Entity Information to ensure the necessary safeguards are in place.

5.3.11. The Contractor shall ensure that processes involving data-in-motion, such as backup or migration, are protected with encryption, physical and access controls.

5.3.12. The Contractor shall ensure that field-level encryption is applied to add an additional layer of security to protect data throughout System processing so that only allowed applications can read/view it.

5.3.13. The Contractor shall work with SAS to make sure that the sensitive data that has reached its end of its lifecycle or no longer needs to be securely erased.e.g. unrecoverable in-the-clear.

5.3.14. The Contractor shall ensure that production data or production URLs are not used in non-production environment, or production data has been desensitised prior to copying out from production environment for use in the non-production environment.

5.3.15. The Contractor shall ensure that data is accorded access rights based on principle of least privilege throughout its life cycle.

5.3.16. The Contractor shall ensure to turn on the data masking feature at the UI level to protect sensitive data (e.g., personal identity number, salary, DOB, etc.) by allowing only users with field-level authorisation to view a field value.

5.3.17. The Contractor shall propose data centres designed for the System with fully redundant subSystems and compartmentalised security zones.

5.3.18. The Contractor shall ensure that data centres adhere to the strictest physical security measures:-

(a) Multiple layers of authentication are required before access is granted to the server area;

(b) Critical areas require two-factor biometric authentication;

(c) Camera surveillance Systems are located at critical internal and external entry points;

(d) Security personnel monitor the data centres 24/7;

(e) Unauthorised access attempts are logged and monitored by data centre security.

5.3.19. The Contractor shall encrypt data at rest, data in motion and data in use.

5.3.20. The Contractor shall replicate the production database and transaction logs to the secondary maintained at an off-site data centre in real-time. Backups of the database and transaction logs are encrypted for any database that contains SAS data.

5.4 Security Hardening

5.4.1. The Contractor shall ensure all services, servers, devices and application components are securely configured (i.e., “hardened”) before being installed or set up in the respective environments. SAS will provide necessary hardening guides, if available. If the hardening guide is not available, the Contractor shall provide and maintain the hardening guide, subject to SAS’s review and approval.

5.4.2. The Contractor shall establish security hardening guidelines on all services, servers, devices and application components based on Security Best Practices Standards (e.g. NIST 800-53, CIS Benchmarks, SANS or product principal’s guides).

5.4.3. The Contractor shall apply the following security measures, in conjunction with secure configuration profiles to further secure operating Systems and virtualised environment:

(a) Disable login functionality to System-level privileged accounts, such as “root” account, where possible;

(b) Restrict switching to System level privileged accounts using software like “su”;

(c) Enable only services that are required;

(d) Remove unused or obsolete files, including backup files and virtual System images;

(e) Restrict transfer of data between hypervisors and their guest operating Systems; and

(f) Use separate System accounts for hypervisor and guest operating Systems.

5.4.4. The Contractor shall ensure that security hardening is carried out for new or changes to components of the System before deploying into the production environment and on an ad-hoc basis as requested by SAS at no additional cost to SAS.

5.4.5. The Contractor shall ensure the packaging hardening is completed before the Commissioning Date.

5.4.6. The Contractor shall maintain the effectiveness and adequacy of all security hardening guides to address new security threats affecting the System. Security configuration shall be verified for compliance prior to the Commissioning Date and once every year thereafter.

5.5 Vulnerability and Patch Management

5.5.1. The Contractor shall maintain an IT asset inventory of all infrastructure, cloud subscribed services, including software and tools deployed in the cloud. This inventory shall be used as a checklist to track vulnerabilities for the System and for change management planning. The inventory shall be updated and reported monthly and ensure no end-of-life assets are deployed.

5.5.2. The Contractor shall implement tracking of expiry dates for all digital assets such as certificates, software licences, etc for renewal.

5.5.3. The Contractor shall ensure any changes to the Cloud does not alter compliance to the security requirements agreed as part of contract.

5.5.4. The Contractor shall ensure developers and third-party Contractor follow the established software development lifecycle and release management process to control implementation of major changes.

5.5.5. The Contractor shall provide a vulnerability and security patch management process documents to ensure thorough tracking of security vulnerabilities for all IT assets within the System, which include:

(a) Maintain and use the IT asset inventory as a source of truth for vulnerability tracking.
(b) Tracking of vulnerability alerts and assessing their applicability monthly or as required by SAS.
(c) Performing criticality review and testing.
(d) Conducting change management review.
(e) Planning for contingency or roll back
(f) Implementing patches.

5.5.6. The Contractor shall proactively monitor information and release information about new security Patches on a timely basis. Timely bases included Real-time, Regular intervals, Scheduled releases, Ad hoc, zero-day patch and critical patch. SAS may inform the Contractor on any advisories when available.

5.5.7. Upon evaluation that it is an emergency one, the Contractor shall submit a request for change to SAS to seek approval to deploy the software update.

5.5.8. The Contractor shall remediate any vulnerabilities made known through patch releases or security testing on the System, in all environments as well as the developers' endpoints according to the timeframe described in Table 3 below:

Table 3

Severity level of vulnerability	Timeframe by severity level of vulnerability
Emergency	Within TWENTY-FOUR (24) hours
Critical / High	Within THIRTY (30) calendar days
Medium / Low	Within SIXTY (60) calendar days

5.5.9. The Contractor shall ensure that vulnerability assessment using industry recognised tools is performed on the System on a quarterly basis.

5.5.10. The Contractor shall ensure that Penetration Testing (PT) using industry recognised tools is performed on the System on a yearly basis.

5.5.11. The Contractor shall provide the Vulnerability Assessment and Penetration Testing (VAPT) post-assessment reports in detail for the System to SAS after every scanning.

5.5.12. If any vulnerability is found due to parts and components supplied by the Contractor, the Contractor shall provide remedial actions to rectify the problem at no additional cost to SAS.

5.5.13. The Contractor shall ensure that vulnerabilities identified through the VAPT are remediated before deploying the change to production of the System.

5.5.14. The Contractor shall perform the security scanning again after the remedial actions are taken to ensure all the vulnerabilities are resolved.

5.5.15. The Contractor shall implement measures to protect endpoint devices used for software deployment to mitigate risks of transferring malicious software (e.g. HIPS,EPP,EDR).

5.6 Authentication and Password Security

5.6.1. The Contractor shall put in place strong authentication and access control mechanisms to ensure that only authorised users are granted access to controlled features (e.g. personalised views).

5.6.2. The System shall support strong password administration, secure creation, distribution, termination, storage and destruction of passwords. User's credentials (i.e. User ID and Password) shall be distributed to users in such a manner that their confidentiality is maintained.

5.6.3. The System shall implement the following features when using passwords (including service accounts):

(a) Passwords to be made up of at least TWELVE (12) characters.
(b) Passwords to be made up of the following categories:
    (i) Upper case alphabet (A through Z);
    (ii) Lower case alphabet (a through z);
    (iii) Digits (0 through 9);
    (iv) Special Characters (!, $, #, %, etc).
(c) Passwords shall be changed once every TWELVE (12) months;
(d) Prohibit password reuse for a minimum of THREE (3) generations;
(e) Passwords shall not be displayed in clear;
(f) Passwords shall not be the same as account ID or user ID;
(g) System shall be protected against dictionary or brute-force attacks;
(h) The initial setup of password upon first login, and a reset of password of a User account shall be enacted upon by the associated User;
(i) Retries shall be limited to a maximum of SIX (6) attempted logins after which the User account shall be locked;
(j) Be changed upon the first login;
(k) Minimum password age shall be ONE (1) day; and
(l) Passwords shall be encrypted during transmission and storage.

5.6.4. The Contractor shall ensure generic authentication responses for login errors.

5.6.5. The Contractor shall implement multi-factor authentication for administration and management (including remotely) and ensure the second authentication factor is:

a) Not the same as the first authentication factor; and
b) Delivered out of band and independently of the device to perform the transaction or access SAS data (such as using a physical token, smart card).

5.6.6. The Contractor shall ensure that secrets (e.g. passwords, API keys, cryptographic keys) are stored securely with access control protection implemented to eliminate the need to hardcode sensitive information in plain text. Such as AWS Secrets Manager or equivalent.

5.6.7. The Contractor shall ensure access to secrets is accorded the least privilege.

5.6.8. The Contractor shall ensure secrets used in production environments are not reused in non-production environments (such as development or test environments).

5.6.9. The Contractor shall periodically review source code and configuration to ensure that secrets are not hardcoded or embedded into source codes, configuration files, or scripts.

5.6.10. The Contractor shall seek approval from SAS to use the root/administrator account with the following details-:

(a) Request Title;
(b) Request Personal Name;
(c) Request Duration to use this escrow account (please indicate the date and time range);
(d) Request Description;
(e) Request Reason/s.

5.6.11. The Requestor from the Contractor who has the password of the root/administrator should not share with others.

5.6.12. The Contractor shall implement centralised security monitoring on privileged IDs to detect misuse of privilege and centralised logging to facilitate periodic review of privilege ID usage.

5.7 Infrastructure Security

5.7.1. The Contractor shall implement the following as part of the System:

(a) Host Intrusion Prevention Systems (HIPS);
(b) Network Intrusion Prevention Systems (NIPS);
(c) Next-Generation Firewall(s);
(d) Network Security and Monitoring;
(e) Database Security and Monitoring (Activity monitoring and inline blocking);
(f) Access Controls;
(g) Security Event Correlation and Monitoring;
(h) Distributed Denial-of-Service (DDoS) Protection;
(i) Web Application Firewall (WAF);
(j) Anti-Defacement Monitoring and Notification;
(k) Content Delivery Network (CDN); And
(l) Cyberwatch Centre (CWC) Integration.

5.7.2. The Contractor shall implement security control measures and procedures to prevent unauthorised access to System management consoles.

5.7.3. The Contractor shall not allow remote access to the System and network unless the access is properly justified and approved by SAS. The Contractor shall implement all the following security measures if remote administrative access is required:

(a) All remote administration to servers shall be performed from within a management LAN meant only for administration (separate from user traffic).

(b) Remote administrative access shall only be performed by authorised personnel from specific Systems and access filtering based on IP address shall be implemented. Media Access Control (MAC) based access filtering can be implemented as an additional layer of protection over IP-based access filtering.

(c) Personnel that are authorised to have remote administrative access shall use multi-factor authentication to authenticate to the servers and applications.

(d) Logging of the date time, IP addresses of the source and destination Systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.

(e) Review the list of authorised personnel and revoke the access rights for those personnel who no longer require those access rights.

5.7.4. The Contractor shall implement physical security control measures and procedures to prevent any unauthorised access to the System.

5.7.5. The Contractor shall provide for and ensure the use of anti-malware software to prevent, detect and remove malicious codes and other malicious contents in the System including development, testing and production environments. The anti-malware software to be used shall be approved by SAS before implementation.

5.7.6. The Contractor shall ensure that the anti-malware software is able to monitor, detect and respond to advanced threats for suspicious activities on critical endpoints and servers as mitigation towards zero-day attacks.

5.7.7. The Contractor shall ensure the anti-malware software is memory-resident and enabled at all times for real-time detection of unauthorised codes and conduct at least monthly full System scans on the System.

5.7.8. The Contractor shall ensure the latest definition files are installed into the System on a daily basis.

5.7.9. The Contractor shall take actions to prevent the spread of unauthorised codes and resolve incidents related to a virus outbreak, execution of malicious codes and recovery actions without additional cost to SAS.

5.7.10. The Contractor shall implement load balancing of critical IT services (e.g. DNS, databases, authentication service, etc) at every layer (web server, application server, etc) across different sites.

5.7.11. The Contractor shall deploy clusters across multiple availability zones to ensure service can be re-launched in an alternative zone where there is an availability zone failure.

5.7.12. The Contractor shall implement Network Address Translation (NAT) to hide the internal IP addresses.

5.8 Web and Application Security

5.8.1. The Contractor shall fully comply with this Clause 5.8 for any Services rendered to SAS.

5.8.2. The Contractor shall ensure that the application is secure by design and is implemented based on a multi-tier architecture which differentiates session control, presentation logic, server-side input validation, business logic and data access, and System management. Where appropriate, the application shall also properly segregate application security, access control, authentication, data storage and protection (e.g. encryption) between its users.

5.8.3. The Contractor shall conduct checks on the Application Software functional capabilities and implementation to ensure that adequate security measures are taken throughout the entire lifecycle of the Application Software specified in the Purchase Order Contract.

5.8.4. The Contractor shall ensure that all Application Software developed by the Contractor, including mobile codes or applications (e.g. browser plug-ins, client-side scripts, applets, smartphone apps, etc.) for end-user devices, are adequately tested for security, reviewed, and approved before deployment.

5.8.5. The Contractor shall provide an industry recognised static code analysis tool which they own, to check and identify known errors, vulnerabilities and weaknesses on all Application Software (including mobile codes or applications such as browser plug-ins, client-side scripts, applets, smartphone apps, etc.) developed by the Contractor at no additional cost to SAS.

5.8.6. The Contractor shall ensure that security is a key consideration at each stage of the software development lifecycle. The Contractor shall identify security weaknesses, propose mitigation and improvement measures for review with SAS.

5.8.7. The Contractor shall incorporate security requirements into the software development lifecycle with activities such as: threat modelling, scanning using automated testing tools for common vulnerabilities and security code reviews.

5.8.8. The Contractor shall share details of the activities carried out, counter measures or fixes used, tools used in the testing and the findings with SAS.

5.8.9. In the event of deployment of any commercial-off-the-shelf (COTS) software, the Contractor shall produce a security risk profile for the software. Any security vulnerability or weakness shall be documented and highlighted to SAS about its implications. The decision to deploy the software with any workaround or fixes shall be reviewed and agreed with SAS.

5.8.10. The Contractor shall implement appropriate measures to protect sensitive information or functionality with strong access control mechanisms to ensure users accessing different levels of the System are properly authorised. The measures shall minimally include the following:

(a) Check access control permissions, whenever performing direct object references;
(b) Disable directory browsing;
(c) Authentication and authorisation for each private page;
(d) Use of role-based authentication and authorisation;
(e) Deny all access by default.

5.8.11. The Contractor shall ensure that where a web source offers both HTTP and HTTPS access, the System will use HTTPS for retrieving and transporting data.

5.8.12 The Contractor shall ensure that all remote file transfers to and from the System are performed using SSH File Transfer Protocol (SFTP) or other secured file transfer mechanisms subject to approval by SAS.

5.8.13. The Contractor shall ensure that all administration modules of the System are accessible only from pre-identified network addresses.

5.8.14. The Contractor shall implement appropriate security mechanisms to protect the confidentiality and integrity of data transmitted from taxpayers and SAS's officers to the System, and within the System.

5.8.15 The Contractor shall refer to the latest Open Web Application Security Project (OWASP) Top 10 security risks as well as other emerging risks not covered by the OWASP Top 10 and implement mitigation measures against these risks.

5.8.16. The Contractor shall ensure that the System is secured and well protected against security attacks, including but not limited to the following:

(a) Misconfiguration of the cloud platform.
(b) Unauthorised access.
(c) Insecure API interfaces.
(d) Hijacking of accounts, services or traffic.

5.8.17. The System shall have appropriate exception and error handling capabilities on all components and such exceptions and errors are to be logged.

5.8.18. The Contractor shall ensure the System contains measures to prevent users from accessing information and services that they are not authorised to, taking into consideration any trade off to usability that might restrict, or inconvenience authorised users.SAS allows the tender to propose the optimum approach.

5.8.19. The Contractor shall ensure the System is protected against brute force log-on attempts by implementing the following security measures:
(a) Incorporate bot mitigation tools such as CAPTCHA;
(b) Introduce delays between log-on attempts.

5.8.20. All network connections between external sites and SAS shall go through next-generation firewall or web application firewall (WAF). Network connections shall be made over a secure channel and access to each endpoint shall be granted through authentication. There shall be security mechanisms and protocols in place to protect the confidentiality and integrity of data transmitted. The design of the setup shall be approved by SAS before System development commences. If any attack is detected in the data, the incident shall be logged and communicated to SAS.

5.8.21. The Contractor shall propose real-time website monitoring service (or anti web defacement tool, AWD) to SAS. The Contractor shall provide the tools/utilities to detect, log and alert any unauthorised changes to the System website in real-time, and ensure that a legitimate working website is automatically restored in the event that unauthorised changes have occurred.

5.8.22. The Contractor shall ensure that the tools/utilities proposed shall be able to integrate and inter-operate with other technology components to provide the required security services for the Contract.

5.8.23. The proposed DDoS protection service shall include the following:
(a) Provision of DDoS protection service with 100% availability;
(b) Effective protection to keep websites 100% available:
(i) Faster loading of web content at user end;
(ii) Protection from Layer 3 to 7 DDoS attacks;
(iii) API protection;
(iv) Block all OWASP Top Ten type attacks.
(c) Staging environment for testing before production deployment;
(d) Global and dedicated capacity to mitigate attacks not less than largest DDOS network attack bandwidth detected;
(e) Behavioural Detection to differentiate between legitimate traffic (e.g. tax file peak period) and surge caused by DDoS attack (optional);
(f) Zero-Day automated DDoS protection via pattern, characteristic recognition (optional); and
(g) Automatic real-time signature creation (optional).

5.8.24. The Contractor shall ensure that the design of the System does not impose risks to the operations of SAS's existing computer networks.

5.8.25. When requested by SAS, the Contractor shall provide a detailed description of the security controls implemented to be approved by SAS. These controls shall include but are not limited to the following:
(a) Input Validations (i.e. input fields shall conform to the desired formats and values);
(b) Workflow Controls;
(c) Message Integrity; and
(d) Output Validations.

5.8.26. The Contractor shall ensure that the design and implementation of the Application Software shall not be affected by the vulnerabilities (e.g. listed under OWASP Top Ten), which include but are not limited to:

(a) Injection vulnerability flaws (e.g. SQL injection, command of injection etc);
(b) Cross Site Scripting (XSS);
(c) Broken access control;
(d) Broken authentication and session management (i.e. use of account credentials and session cookies);
(e) Insecure direct object references;
(f) Cross Site Request Forgery (CSRF);
(g) Security mis-configuration;
(h) Insecure cryptographic Storage;
(i) Failure to restrict URL access;

(j) Insufficient transport layer protection;
(k) Unvalidated redirects and forwards;
(l) Non-validated input;
(m) Buffer overflows;
(n) Improper error handling;
(o) Race conditions;
(p) Improper error/exception handling;
(q) Insecure storage;
(r) Denial of Service (DoS); and
(s) Insecure configuration management.

5.8.27. The Contractor shall ensure that the Application Software does not contain any hidden functionalities that SAS is not aware of.

5.8.28. The Contractor shall ensure all test data, test accounts and test credentials are removed from the System before commissioning.

5.8.29. The Contractor shall implement the notification message or banner displayed to user and CSP operation personnel before granting access to the System.

5.8.30. The System shall display the key points equivalent to the following:
(a) Usage of service/System may be monitored, recorded, and subject to audit;
(b) Unauthorised use of the service/System is prohibited and subject to criminal and civil penalties;
(c) Use of the service/System indicates consent to monitoring and recording.

5.9 Development Security

5.9.1. The Contractor shall propose a list of application security measures to be implemented as part of the System. The list shall include the details to enforce code security, application vulnerabilities controls, etc. The Contractor's proposal on application security measures shall be subject to the review and clarifications by SAS. SAS reserves the right to request for enhancements to the proposed application security architecture.

5.9.2. The Contractor shall implement code scanning and open-source security scanning as part of the development process. Any vulnerabilities found shall be fixed before implementation in production. Any deviation required by the Contractor shall be discussed with SAS at the earliest possible time.

5.9.3. The Contractor shall conduct source code reviews using automated tools or peer reviews to uncover vulnerabilities.

5.9.4. The Contractor shall ensure any automated tools used include the following:
(a) Detection of Open Web Application Security Project (OWASP) Top 10 web application security risks;
(b) Scanning for Common Vulnerabilities and Exposures (CVEs) in libraries and open source codes;
(c) Highlighting areas that pose vulnerabilities and include possible resolutions; and
(d) Only allow deployments when security findings rated Medium and above are resolved.

5.9.5. SAS may conduct additional source code reviews as part of a security assurance exercise. Any vulnerabilities found shall be fixed at no extra cost to SAS.

5.9.6. The Contractor shall perform automated testing of APIs before every release. (e.g. tools like Postman, SOAPUI).

5.9.7. The Contractor shall integrate automated testing of APIs into the pipeline to ensure any code change won't break APIs in production.

5.9.8. The Contractor shall limit access to APIs to authorised users and Systems only (e.g. IP whitelisting, machine whitelisting).

5.9.9. The Contractor shall provide documentation of API design and ensure best practices based on industry standards (e.g. SOAPUI, REST) are followed when designing API (e.g. avoid reuse of API keys, encrypt API traffic, authenticate all API calls).

5.9.10. The Contractor shall place a version control System to assist developers in rolling back to a previous version in any event a show-stopping bug gets discovered.

5.9.11. The Contractor shall implement a deployment pipeline for code release.

5.9.12. The Contractor shall integrate automated security testing into the code release process (e.g. IAST, SAST, DAST).

5.10 Security Assurance

5.10.1 The Contractor shall ensure that System Security Test (SST) is carried out on the System, ensuring that the security measures are functioning as intended. Contractor shall identify all technical IT security controls, as well as to recommend test cases to validate the security controls implemented in the System are functioning according to requirements and design. All issues arising from SST shall be resolved before the Commissioning Date.

5.10.2. The Contractor shall engage an independent party, subject to approval by SAS to perform the following:

(a) Conduct IT security risk assessment on the System to ascertain risk areas so that adequate controls can be identified and put into the System to mitigate risks. This shall commence during System design. The final design of the System shall incorporate the findings of the risk assessment.

(b) Verify and ensure that designs are implemented correctly and conduct SST before the Commissioning Date.

5.10.3. The Contractor shall seek SAS's approval where any deviations exist from the review. The Contractor shall also ensure System or manual controls are provided, along with reasons and measures to mitigate any risks that may be present. These justifications shall be documented.

5.10.4. The Contractor shall provide full support and work with the independent third party engaged by SAS to ensure all the weaknesses and vulnerabilities discovered during the IT security risk assessment, WAPT is addressed before the Commissioning Date, at no additional cost to SAS.

5.10.5. The Contractor shall perform security tests on the System with the scope described in the Table 4 below:

Table 4

Type	**Vulnerability Assessment (VA) Scan**	**Penetration Testing (PT)**
Application software	Application software shall be tested using authenticated vulnerability assessment scans, where possible	Application software shall be tested using a variety of manual and automated techniques. Login credentials must be provided for authenticated penetration testing.

Infrastructure	Infrastructure shall be tested using authenticated vulnerability assessment scans, where possible	Infrastructure shall be tested using a variety of manual and automated techniques. Login credentials must be provided for authenticated penetration testing.

5.11 User Access Management

5.11.1. The Contractor shall implement Identity and Access Management (IAM) for user account management.

5.11.2. The Contractor shall propose an access control matrix for authorised users to the System for the approval by SAS.

5.11.3. The Contractor shall ensure that access rights are granted on a need-to know basis, kept up-to-date and reviewed on a regular basis. The Contractor shall ensure that any System or user account not needed shall be deleted.

5.11.4. The Contractor shall implement control measures to protect all account credentials. The Contractor shall provide detailed documentation on the control measures and processes, which shall minimally include the security features, technologies, administration usage processes and procedures.

5.11.5. The Contractor shall disable the login to multiple sessions using the same credential.

5.11.6. The Contractor shall ensure that the account shall be locked after a specific number of unsuccessful attempts as determined by SAS.

5.11.7. The Contractor shall implement a timeout or automatic logout feature to the System for non-active sessions.

5.11.8. The Contractor shall ensure that all System administrative or functional accounts are not shared.

5.11.9. The Contractor shall implement security measures and processes to ensure that System administrators, database administrators or other privileged users shall not access SAS' System. The Contractor shall ensure that logs are reviewed to identify such unauthorised access.

5.11.10. The Contractor shall ensure all successful and failed authentication events for access are logged.

5.11.11. The Contractor shall disable remote administrative access to the System if such access is not required.

5.11.12. The Contractor shall implement Role-Based Access Control (RBAC) and/or Attribute-Based Access Control (ABAC) mechanism that enforces access to all parts of the System.

5.11.13. The Contractor shall implement processes and controls to ensure that:
(a) The rights to access data are granted on a need-to-know basis;
(b) Users can access only data that they have been granted access rights to.

5.11.14. The Contractor shall apply the principle of least privilege to all accounts(such as users, services) to ensure excess privileges are not granted to accounts.

5.11.15. The Contractor shall implement ABAC using multiple attributes such as role, location, authentication method, IP address and mutual authentication.

5.11.16. The Contractor shall ensure clear segregation of duties for privileged roles in the service/System such as network, operating System, database, log management and security administrators to address risks associated with user-role conflict of interest.

5.11.17. The Contractor shall ensure that the access control matrix for the System is established, roles and responsibilities are clearly documented.

5.11.18. The Contractor shall implement an approval process and tracking mechanism for granting user access to the System.

5.11.19. The Contractor shall implement the permission boundary which ensures that users created by another user shall have the same or fewer permissions to prevent privilege escalation.

5.11.20. The Contractor shall implement all of the following security measures if remote administration to server or applications is required:

(a) Remote administrative access shall only be granted to authorised personnel who need to perform administration on servers or applications remotely;

(b) Remote administrative access shall only be done by authorised personnel from specific Systems and filtering based on IP address shall be implemented;

(c) Personnel that are authorised to have remote administrative access shall use multi-factor authentication to authenticate to the servers or applications; and comply to the requirements under Clause 5.6.5 and;

(d) Logging of the date time, IP addresses of the source and destination Systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.

5.11.21. The Contractor shall manage the privileged accounts (such as admin account, root account) as follows:

(a) Only authorised administrators as required by job functions and need-to know basis can be assigned with privileged accounts and specific Systems and filtering based on IP address shall be implemented;

(b) All privileged account requests must go through approval and authorisation process before access is granted to administrators;

(c) All privileged accounts must be documented;

(d) Individual privileged account and password must be setup and assigned to ensure accountability and traceability; Shared privilege accounts must still retain an ownership for accountability;

(e) Privileged accounts must be immediately disabled and removed when administrators change their job function or leave the organisation, or when it is no longer needed;

(f) Default privileged accounts must be removed. If the default privileged accounts cannot be removed, they must be renamed and passwords changed immediately and disabled, where possible;

(g) Privileged accounts shall be reviewed regularly to prevent against unauthorised accesses and activities;

(h) All administrative changes performed using privileged account shall have audit trails to facilitate investigation if required; and

(i) Segregation of roles for privileged accounts used in the System must be enforced.

5.12 IT Security Incident Management

5.12.1. The Contractor shall work with SAS for the IT Security Incident Handling Framework. The IT Security Incident Handling Framework will define a Systematic incident response approach and incident escalation structure through which incidents are to be notified and resolved.

5.12.2. The Contractor shall develop Standard Operating Procedures (SOP) that specify the detailed procedures of handling different types/categories of IT security incident (including but not limited to DDoS,unauthorised access/change, malware infection, etc.) within twenty-four (24) weeks from the Letter of Acceptance. The SOP shall be reviewed minimally on an annual basis and approved by SAS.

5.12.3. In the event of any IT security incidents, the Contractor shall:

(a) Investigate, resolve and recover from the IT security incident;
(b) Ensure the preservation and admissibility of evidence and information related to the IT security incident; and
(c) Exercise the prescribed incident response guidelines and procedures of the IT security incident management plan.

5.12.4. The Contractor shall take the necessary actions to ensure that all IT security incidents are handled and managed in accordance with SAS's IT Security Incident Handling Framework and the approved SOP. The Contractor shall also implement measures to prevent the occurrence of IT security incidents. The Contractor shall support SAS in resolving IT security incidents when the need arises.

5.12.5. The Contractor shall be responsible to inform SAS IT Security Incident Response (SITSIR) and personnel appointed by SAS required to deal with the IT security incidents.

5.12.6. The Contractor shall respond and report all security-related incidents and their status to SAS. In addition, the Contractor shall submit a detailed incident report and post-incident review report within one business week after a security incident's conclusion. The post-incident review report shall contain details of measures (corrective, detective and preventive) which need to be implemented.

5.12.7. The commercial CSP shall report any security incident including any observed or suspected security cases that may affect SAS as a customer/tenant.

5.12.8. For ALL security incidents such as virus infections, security breaches, unauthorised access, and security vulnerabilities, the commercial CSP shall provide an initial incident report within 4 hours of incident detection and status update every 24 hours thereafter until incident closure..

5.13 Security Training and Awareness

5.13.1. The Contractor shall ensure that all its personnel assigned to this project are equipped with the relevant skills and experience to operate the System.

5.13.2. The personnel shall be familiar with the requirements of the System and shall adhere to the security policy, standards, procedures and incident reporting processes as approved by SAS.

5.13.3. The Contractor shall ensure that all their personnel are informed of their security responsibilities and accountability/liability before putting the person in his/her assigned areas of work.

5.13.4. The Contractor shall demonstrate that they have a comprehensive security program to train its personnel in security and their assigned role.

6 Logging & Monitoring

6.1 General

6.1.1. The Contractor shall collect the following types of logs from all components in the System:

(a) User administration activities (for e.g. add / delete / amend user accounts and profiles).
(b) Access (e.g. Successful and unsuccessful attempts to logins and logouts of the System, privileged access login, date and time stamp, user identification, activities performed, etc.).
(c) System Health (e.g. System resource usage, etc.).
(d) Performance (e.g. Response time, latency, throughput, etc.).
(e) Activities and Events (e.g. Audit trail, configuration changes, System actions – including backup and recovery activities, etc.).
(f) Errors and Exceptions (e.g. Resource unavailability, application exceptions, validation failure, timeout errors, etc.).
(g) Security Events (e.g. malware detection, intrusion detection, access violations from local and remote requests, etc.).

6.1.2. The Contractor shall ensure the logging and monitoring is

(a) Able to collect accurate and complete logs;
(b) Able to allow SAS to comply with logging and audit requirements (e.g. what needs to be logged, log retention periods); and
(c) Able to allow SAS to effectively perform event reconstruction, incident investigation, troubleshooting, service level monitoring, and audit.

6.1.3. SAS reserves the right to review the logs as and when required and the Contractor shall provide the required logs to SAS within a timely manner to ensure the relevant SLAs are met.

6.1.4. The Contractor shall ensure that the logs record all activities carried out by privileged accounts - such as System administrator and service accounts (if in use).

6.1.5. The Contractor shall ensure the System keeps these logs for at least **ONE (1)** year.

6.1.6. The Contractor shall ensure that a process is put in place for all necessary logs to be reviewed monthly or when necessary, such as after configuration changes to scan for security violations, issues or concerns and highlight them to SAS.

6.1.7 The Contractor shall ensure security-related logs are available to facilitate event reconstruction and incident investigation.

6.1.8. The Contractor shall store the log files at secured locations to protect the integrity and availability.

6.1.9. The log files shall be readable in ASCII plain text format or UTF8.

6.1.10. The Contractor shall implement that log information is accessed by authorised personnel only; operations personnel should not have access to logs to prevent risk of tampering or deletion.

6.1.11. The Contractor shall ensure that log files do not contain sensitive information.

6.1.12. The Contractor shall ensure there is sufficient capacity to store logs.

6.1.13. The Contractor shall ensure that the auto-scaling feature turns on to provide sufficient capacity to store the log files.

6.2 User Access Logging

The Contractor shall implement user access logging in the proposed System. User Access Logging shall be active at all times for all actions performed within the proposed System by users accessing the data from any of the user interfaces.

7 Support

7 .1 System Support

7.1.1 The Contractor shall provide support services for the System during the User Acceptance Testing Period, Performance Guarantee Period (PGP), System Warranty Period and Application Software Maintenance and Support Period and all service requests applied during the Contract Period.

(a) Investigate and correct defects in the System as reported by SAS within the service level. The resolving effort includes resolving errors through developing, testing and implementing changes to the System;
(b) Provide corrective maintenance, troubleshoot and isolate defects, including diagnosis and correction of all latent errors in the System;

(c) Manage and implement changes to the System to minimise impact on System availability; and

(d) Provide the following services even if after support hours:
   i. Resolution of Business Impact Level 1 problems (refer to Clause 7.6.8);
   ii. Restoration of System; and
   iii. Testing of System for OS, database and/or software upgrades and patches.

7.2 Service Request (SR) (On-demand)

7.2.1 Service Request (SR) refers to requests for modifications or enhancements to the System not previously defined in the project scope. The enhancements may also include requirements to support new user requirements or future growth and expansion, which is on-demand.

7.2.2. The Contractor shall clarify the requirements, make an assessment of the SR and submit a SR proposal detailing impact analysis such as performance, integration, availability as well as the scope of work for SAS's review and approval.

7.3 Service Request (SR) Procedure

7.3.1. The Contractor shall submit a SR procedure describing how all the proposed changes to the System are to be processed. The procedure shall cover the progress of a proposed change from its formal definition through its implementation in a released version of the software, or to its disposal for other reasons. This shall take into consideration the mutually agreed System change management standards with respect to prioritisation of such requests.

7.3.2. The aim of the SR procedure is to ensure that all proposals for changes to the System are properly evaluated in terms of their costs and benefits and their priority. Such changes include alterations to the System documentation and operational procedures. It shall also monitor progress of processing service requests.

7.4 Types of Service Request (SR)

7.4.1. Normal Request: Requests that are not urgent. SR Proposal shall be submitted within SEVEN (7) working days; and

7.4.2. Urgent Request: Requests that are urgently required. SR Proposal shall be submitted within THREE (3) working days.

7.5 Turnaround time (TAT) to implement Service Request (SR)

7.5.1 TAT is the total time taken from approving a SR proposal to its completion or resolution. All accepted change requests shall be completed and implemented within the specified turnaround time depending on the estimated man-days required in Table 5:

Table 5

Estimated Man-days	Turnaround Time
< = 3 man-days	One (1) calendar week
> 3 and < 10 man-days	Two (2) calendar weeks
= > 10 man-days	More than two (2) calendar weeks as mutually agreed between SAS and the Contractor

7.5.2 The Contractor shall provide the unit cost for SR in Price Schedules.

7.6 Problem Management

7.6.1. The Contractor shall set up the appropriate Problem Management channels and procedures with SAS.

7.6.2. The Contractor shall provide support and coordinate for all System related problems.

7.6.3. The Contractor shall provide a primary and secondary contact number and email accounts for the reporting of problems. The Contractor shall provide alternate contacts as and when the provided contacts are unavailable.

7.6.4. Any System operational issues, inadequacies or problems identified that are attributable to the Contractor's design, development or implementation of the System shall be rectified by the Contractor to SAS's satisfaction within TWO (2) calendar weeks upon the occurrence at no additional cost to SAS. For issues, inadequacies and problems which are not attributable to the Contractor, the Contractor shall work with all relevant parties to resolve the underlying issues and ensure that the System is secured against the identified vulnerabilities.

7.6.5 . The Contractor shall schedule problem reviews to track unresolved problems and provide rectification efforts to prevent problems from reoccurring. Frequency of such reviews shall be specified by SAS.

7.6.6. The Contractor shall perform a thorough analysis of the problem, which includes identification of the cause of the problem to its component level, the System affected, the data or any loss suffered, the recommended solution and the preventive measures.

7.6.7. When alerted by SAS of potential weaknesses, threats and vulnerabilities to the System, the Contractor shall assess the impact and recommend any necessary measures to mitigate or remove the risks to the System.

7.6.8. Unless otherwise specified by SAS, the classification of the defects or errors in the System during the Contract Period is as specified in Table 6 below. In the event that SAS and the Contractor could not agree on the assignment of a business impact level to a problem / defect, SAS shall have the final decision on the business impact level, and this shall be conclusive and binding to all parties involved in resolving the problem / defect.

Table 6

Business Impact Level	**Problem Impact (Any of the following conditions is met)**
1	Defects/Problems that affect the System such that required operational objectives cannot be achieved. These include: ● System unavailable, ● Problem that will weaken/breach the user of the System, and ● Disruption of services to more than FIFTY percent (50%) of the users.
2	Defects/Problems that affect a particular form of operation but does not affect any operational objectives, as there exists temporary workaround solutions. These also include failure to meet the System Response Time required.
3	Defects/Problems that have minimum or no impact on the operation.

7.6.9. The “Response Time” shall be the time between notification of the problem to the Contractor and the response by the Contractor to the problem.

7.6.10. The “Problem Resolution Time” shall begin upon notification of the problem until the problem is resolved and the defect is restored to a satisfactory working condition.

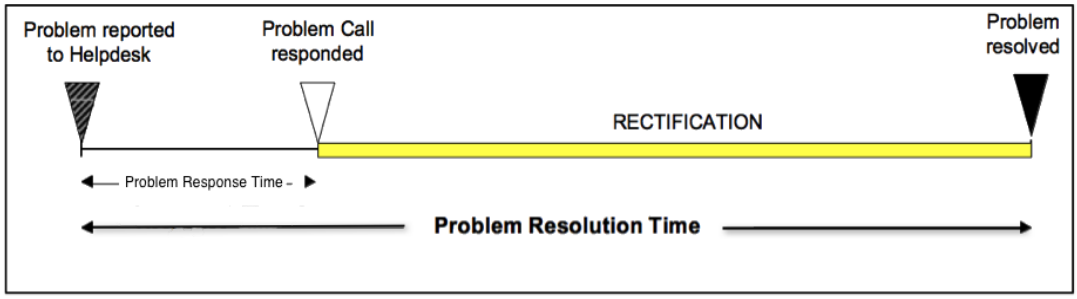


Illustration of Response Time and Problem Resolution Time

7.6.11. The Contractor shall work with all parties designated by SAS and take whatever actions necessary to resolve all problems. For problems classified as business impact level ONE (1), the Contractor shall also provide in writing a preliminary incident report to explain the incident by the following working day. Subsequently, the Contractor shall furnish SAS with a post-incident report to explain in detail the background of the problem, the impact of the problem, the cause of the incident, the corrective actions taken and the solutions / recommendations to prevent the incident from recurring

7.6.12. The Contractor shall comply with the service levels according to the business impact level classification in Table 7:

Table 7

Severity Level	Problem Response Time	Status Reporting	Problem Resolution Time
1	Within 4 hours	Every 4 hours	Within 1 day
2	Within 8 working hours	Daily	Within 4 working days
3	Within 1 working day	End of Problem Resolution	Within 7 working days

7.7 Problem Reporting Procedure

7.7.1. The Contractor shall propose both the incident and problem resolution support team structures and the escalation procedures for incident and problem resolution including the infrastructure and mechanism for reporting, management and escalation of problems, unsatisfactory restoration or services rendered. This shall include the process, procedures, contact persons and response time. The support team shall be based in Singapore.

Annex H :
STATEMENT OF COMPLIANCE

STATEMENT OF COMPLIANCE

* The indication of Compliance (C) or Non-compliance (NC) will be deemed to be applicable to each **main** section, unless it is clearly stated to be otherwise.

** Please indicate the specific items/points of non-compliance where applicable and proposed equivalent customisation or/and workable solutions.

Specification	Compliance (C/NC)*	Explanatory Remark**
ANNEX A - ERP CONDITIONS OF CONTRACT		
1.1		
1.2		
1.3		
1.4		
1.5		
2		
3.1		
3.2		
3.3		
3A Intentionally Left Blank		
4.1		
4.2		
4.2A		
4.3		
4.4		
4.5		
5.1		
5.2		
5.3		
6		
7.1		
7.2		
8.1		
8.2		
8.3		
8.4		
8.5		
8.6		
8.7		
9.1		
9.2		
9.3		
9.4		
9.5		
9.6		
10.1		
10.2		
11 Intentionally Left Blank		
12.1		
12.2		
12.3		
12.3.1		
12.3.2		
12.4		
12.4.1		
12.4.2		
12.5		
13.1		
13.1.1		
13.1.2		
13.1.3		
13.1.4		
13.2		

Specification	Compliance (C/NC)*	Explanatory Remark**
13.3		
13.4		
14 Intentionally Left Blank		
15 Intentionally Left Blank		
16.1		
16.2		
17 Intentionally Left Blank		
18 Intentionally Left Blank		
19 Intentionally Left Blank		
20 Intentionally Left Blank		
21		
22.1		
22.1.1		
22.1.2		
22.1.3		
22.2		
22.2.1		
22.2.2		
22.2.3		
22.3		
22.3.1		
22.3.2		
22.4 Intentionally Left Blank		
22.5 Intentionally Left Blank		
22.6		
22.6.1		
22.6.2		
22.6.3		
22.6.4		
22.6.5		
22.7		
22.8		
22.8.1		
22.8.2		
22.8.3		
23.1		
23.2		
23.3		
23.4		
24.1		
24.2		
24.3		
24.4		
24.5		
24.6		
24.7		
24.8		
25.1		
25.2		
25.3		
25.4		
25.5		
25.6		
26 Intentionally Left Blank		
27.1		
27.2		
28.1		
28.2		
28.3		
29 Intentionally Left Blank		
30.1		
30.2		

Specification	Compliance (C/NC)*	Explanatory Remark**
30.3		
30.4		
31		
32		
33.1		
33.2		
33.3		
33.4		
33.5		
33.6		
33.7		
33.8		
33.9		
34.1		
34.2		
34.3		
34.4		
35.1		
35.2		
36.1		
36.2		
37.1		
37.2		
37.3		
38 Intentionally Left Blank		
39.1		
39.2		
39.3		
39.4		
39.5		
39.6		
39.7		
39A		
39A.1		
39A.2		
40.1		
40.2		
41.1		
41.2		
42.1		
42.2		
42.3		
42.4		
42.5		
43		
44		
45		
46 Intentionally Left Blank		
47		
48.1		
48.2		
48.3		
48.4		
48.5		
48.6		
48.7		
48.8		
48.9		
48.10		
48.11		
49.1		
49.1.1		

Specification	Compliance (C/NC)*	Explanatory Remark**
49.1.2		
49.1A		
49.1A.1		
49.1A.2		
49.2		
49.2.1		
49.2.2		
49.2.3		
49.2.4		
49A		
49A.1		
49A.2		
49A.3		
49A.4		
49A.5		
49A.6		
50.1		
50.2		
50.3		
50.4		
50.5		
50.6		
50.7		
51 Intentionally Left Blank		
52		
53		
54.1		
54.2		
54.3		
54.4		
55.1		
55.2		
55.3		
56		
57 Intentionally Left Blank		
58.1		
58.2		
58.3		
59.1		
59.2		
59.3		
60		
61.1		
61.2		
ANNEX C - GENERAL REQUIREMENT SPECIFICATIONS		
1.1		
1.1.1		
1.1.2		
1.2		
1.2.1		
1.2.2		
1.3		
1.3.1		
1.3.2		
1.3.3		
1.3.4		
1.3.5		
2.1		
2.1.1		
2.1.2		
2.1.3		
2.1.4		

Specification	Compliance (C/NC)*	Explanatory Remark**
2.1.5		
3.1		
3.1.1		
3.2		
4.1		
ANNEX D - COMBINED FUNCIONAL REQUIREMENTS		
D1 - PRO 1.0		
D1 - PRO 2.0		
D1 - PRO 3.0		
D1 - PRO 4.0		
D1 - PRO 5.0		
D2 - FIN 1.0		
D2 - FIN 2.0		
D2 - FIN 3.0		
D2 - FIN 4.0		
D2 - FIN 5.0		
D2 - FIN 6.0		
D2 - FIN 7.0		
D2 - FIN 8.0		
D3 - OHR 1.0		
D3 - OHR 2.0		
D3 - OHR 3.0		
D3 - OHR 4.0		
D3 - OHR 5.0		
D3 - OHR 6.0		
D3 - OHR 7.0		
D4 - IT 1.0		
D4 - IT 2.0		
ANNEX G - TECHNICAL REQUIREMENT SPECIFICATIONS		
1.1		
1.1.1		
1.1.2		
1.1.3		
1.2		
1.2.1		
1.2.2		
1.3		
1.3.1		
1.3.2		
1.3.3		
1.3.4		
1.3.5		
1.3.6		
1.3.7		
1.4		
1.4.1		
1.4.2		
1.4.3		
1.4.4		
1.4.5		
1.4.6		
1.4.7		
1.4.8		
1.4.9		
1.4.10		
1.4.11		
1.5		
1.5.1		
1.5.2		
1.5.3		
1.6		
1.6.1		

Specification	Compliance (C/NC)*	Explanatory Remark**
1.6.2		
1.7		
1.7.1		
1.7.2		
1.7.3		
1.8		
1.9		
1.9.1		
1.9.2		
1.9.3		
1.10		
1.10.1		
1.10.2		
1.10.3		
1.10.4		
1.10.5		
1.10.6		
1.11		
1.11.1		
1.11.2		
1.11.3		
1.11.4		
1.11.5		
1.11.6		
1.11.7		
1.11.8		
1.11.9		
1.11.10		
1.12		
2.1		
2.1.1		
2.1.2		
2.1.3		
2.1.4		
2.1.5		
2.2		
2.2.1		
2.2.2		
2.2.3		
2.2.4		
2.2.5		
2.2.6		
2.3		
2.3.1		
2.3.2		
2.3.3		
3.1		
3.1.1		
3.1.2		
3.1.3		
3.1.4		
3.1.5		
3.1.6		
3.1.7		
3.1.8		
3.1.9		
3.1.10		
3.1.11		
3.2		
3.2.1		
3.2.2		
3.2.3		

Specification	Compliance (C/NC)*	Explanatory Remark**
3.2.4		
4.1		
4.1.1		
4.1.2		
4.1.3		
4.1.4		
4.2		
4.2.1		
4.2.2		
4.2.3		
5.1		
5.1.1		
5.1.2		
5.1.3		
5.1.4		
5.1.5		
5.1.6		
5.1.7		
5.1.8		
5.1.9		
5.1.10		
5.1.11		
5.1.12		
5.1.13		
5.1.14		
5.1.15		
5.1.16		
5.2		
5.2.1		
5.2.2		
5.2.3		
5.2.4		
5.2.5		
5.2.6		
5.2.7		
5.3		
5.3.1		
5.3.2		
5.3.2.1		
5.3.2.2		
5.3.2.3		
5.3.3		
5.3.4		
5.3.5		
5.3.6		
5.3.7		
5.3.8		
5.3.9		
5.3.10		
5.3.11		
5.3.12		
5.3.13		
5.3.14		
5.3.15		
5.3.16		
5.3.17		
5.3.18		
5.3.19		
5.3.20		
5.4		
5.4.1		
5.4.2		

Specification	Compliance (C/NC)*	Explanatory Remark**
5.4.3		
5.4.4		
5.4.5		
5.4.6		
5.5		
5.5.1		
5.5.2		
5.5.3		
5.5.4		
5.5.5		
5.5.6		
5.5.7		
5.5.8		
5.5.9		
5.5.10		
5.5.11		
5.5.12		
5.5.13		
5.5.14		
5.5.15		
5.6		
5.6.1		
5.6.2		
5.6.3		
5.6.4		
5.6.5		
5.6.6		
5.6.7		
5.6.8		
5.6.9		
5.6.10		
5.6.11		
5.6.12		
5.7		
5.7.1		
5.7.2		
5.7.3		
5.7.4		
5.7.5		
5.7.6		
5.7.7		
5.7.8		
5.7.9		
5.7.10		
5.7.11		
5.7.12		
5.8		
5.8.1		
5.8.2		
5.8.3		
5.8.4		
5.8.5		
5.8.6		
5.8.7		
5.8.8		
5.8.9		
5.8.10		
5.8.11		
5.8.12		
5.8.13		
5.8.14		
5.8.15		

Specification	Compliance (C/NC)*	Explanatory Remark**
5.8.16		
5.8.17		
5.8.18		
5.8.19		
5.8.20		
5.8.21		
5.8.22		
5.8.23		
5.8.24		
5.8.25		
5.8.26		
5.8.27		
5.8.28		
5.8.29		
5.8.30		
5.9		
5.9.1		
5.9.2		
5.9.3		
5.9.4		
5.9.5		
5.9.6		
5.9.7		
5.9.8		
5.9.9		
5.9.10		
5.9.11		
5.9.12		
5.10		
5.10.1		
5.10.2		
5.10.3		
5.10.4		
5.10.5		
5.11		
5.11.1		
5.11.2		
5.11.3		
5.11.4		
5.11.5		
5.11.6		
5.11.7		
5.11.8		
5.11.9		
5.11.10		
5.11.11		
5.11.12		
5.11.13		
5.11.14		
5.11.15		
5.11.16		
5.11.17		
5.11.18		
5.11.19		
5.11.20		
5.11.21		
5.12		
5.12.1		
5.12.2		
5.12.3		
5.12.4		
5.12.5		

Specification	Compliance (C/NC)*	Explanatory Remark**
5.12.6		
5.12.7		
5.12.8		
5.13		
5.13.1		
5.13.2		
5.13.3		
5.13.4		
6.1		
6.1.1		
6.1.2		
6.1.3		
6.1.4		
6.1.5		
6.1.6		
6.1.7		
6.1.8		
6.1.9		
6.1.10		
6.1.11		
6.1.12		
6.1.13		
6.2		
7.1		
7.1.1		
7.2		
7.2.1		
7.2.2		
7.3		
7.3.1		
7.3.2		
7.4		
7.4.1		
7.4.2		
7.5		
7.5.1		
7.5.2		
7.6		
7.6.1		
7.6.2		
7.6.3		
7.6.4		
7.6.5		
7.6.6		
7.6.7		
7.6.8		
7.6.9		
7.6.10		
7.6.11		
7.6.12		
7.7		
7.7.1		

We fully understand and agree that notwithstanding the fact that the Statement of Compliance as herein declared is subjected to the Company's acceptance.

Dated this _____ day of _____ 202_.

NAME AND SIGNATURE (AUTHORISED REPRESENTATIVE)	:	NAME (WITNESS)	:
DESIGNATION (AUTHORISED REPRESENTATIVE)	:	DESIGNATION (WITNESS)	:
DATE	:	DATE	:
COMPANY STAMP (AUTHORISED REPRESENTATIVE)	:	COMPANY STAMP (WITNESS)	:
COMPANY NAME (AUTHORISED REPRESENTATIVE)	:	COMPANY NAME (WITNESS)	:

Appendix A :
HIGH-LEVEL CURRENT CORPORATE SYSTEM LANDSCAPE

High-level current corporate system landscape