TENDER REFERENCE: SAS/OP/2023/004/T

SCHOOL OF THE
ARTS SINGAPORE

TENDER FOR PROVISION OF BUSINESS PROCESS RE-ENGINEERING (BPR) CONSULTANCY AND IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM FOR SCHOOL OF THE ARTS, SINGAPORE

Name of Tenderer : ______________________________

Closing Date/Time : **27 June 2023 at 1400 hours**

Submit To :

Tender Submission Box 3
Office Of Procurement
School Of The Arts, Singapore
1 Zubir Said Drive
Administration Office #05-01
Singapore 227968

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/2023/004/T**

05 June 2023

Dear Sir/Mdm,

INVITATION TO TENDER (ITT) FOR PROVISION OF BUSINESS PROCESS RE-ENGINEERING (BPR) CONSULTANCY AND IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM FOR SCHOOL OF THE ARTS, SINGAPORE (ITT REFERENCE NO: SAS/OP/2023/004/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 Business Process Re-Engineering (BPR) Consultancy and Implementation of the Enterprise Resource Planning (ERP) System** at **1 Zubir Said Drive, Singapore 227968** as described in the attached documents.

2. You are required to submit your proposal and any accompanying information to our **Tender Submission Box 3** at 1 Zubir Said Drive, Administration Office #05-01, Singapore 227968 by **27 June 2023, 1400 hours Singapore Time**. All late and/or incomplete submissions will be disqualified.

3. The documents enclosed in this ITT includes:

(a)	Schedule 1	:	Instruction to Tenderers
(b)	Schedule 2	:	Form of Tender
(c)	Schedule 3	:	Price Schedule
(d)	Annex A	:	ERP Conditions of Contract
(i)	Appendix 1	:	Payment Terms
(ii)	Appendix 2	:	Intentionally left blank
(iii)	Appendix 3	:	Intentionally left blank
(iv)	Appendix 4	:	Undertaking to Safeguard Official Information
(v)	Appendix 5	:	Declaration
(e)	Annex B	:	Selection Criteria
(f)	Annex C	:	ERP Functional Requirement Specifications
(g)	Annex D	:	Detailed Business and Functional Requirements
(h)	Annex E	:	Project Schedule

(i)	Annex F	:	Proposed Project Team and Track Record
(j)	Annex G	:	ERP Technical Requirement Specifications
(k)	Annex H	:	Statement of Compliance
(l)	Appendix A	:	High-level current corporate system landscape

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

5. Before the submission of their Tenders, Tenderers must attend the 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.

6. The **Online Tender Briefing** for the tender requirements and documents submission will be held on **12 June 2023, 1030 hours Singapore Time** via Zoom video conferencing.

7. Tenderers are required to confirm their attendances for the Online Tender Briefing with **Ms Jacqueline Tan** through email no later than **09 June 2023, 1200 hours Singapore Time.**

8. Attendance is compulsory for the Tender Briefing participation in Tender.

9. All enquiries and clarifications regarding this Invitation to Tender must be made in writing and directed to no later than **16 June 2023, 1200 hours Singapore Time**:

(a) Tender Matters : Ms Jacqueline Tan, Direct line: 6342 5821 &
Email : procurement@sota.edu.sg

(b) Requirement Specifications : Mr Lee Yew Wah, Direct Line: 6342 5808 &
Email : yewwah.lee@sota.edu.sg

(c) Requirement Specifications : Ms Elizabeth Tay, Direct Line: 6342 5855 &
Email : otm@sota.edu.sg

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

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

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

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

TABLE OF CONTENTS

Schedule 1 :
INSTRUCTION TO TENDERERS

TENDER FOR
PROVISION OF BUSINESS PROCESS RE-ENGINEERING (BPR) CONSULTANCY AND IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM 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, E, F, G, and H
   c) Appendices 1, 4 and 5
   d) Company Profile
   e) Details of proposed Project Team
   f) Tender Proposal (Detailed proposal as set out in Annex C, Point 3.3 to 3.7)
   g) Client Track Records for past 5 years
   h) Latest Statement of Accounts or Audited Financial Statement of two (2) most recent financial years
   i) Proof of GSR at least meeting Financial Grade S6, as set out in Annex C, Point 3.1
   j) Proof of certified partner of the proposed ERP system, as set out in Annex C, Point 3.2
   k) Relevant Certification(s)

2. Tenderers must submit **2 full sets** of Tender documents in hardcopy. One set is to be marked “Original” and the other marked “Duplicate” and endorsed with **company stamp and authorised signatory on every page.**

3. Tender documents shall be submitted to the “**TENDER SUBMISSION BOX 3”** located at :

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

   by:

   27 June 2023 (1400 hours) in sealed envelope(s) with the following marked :

   “TO: OFFICE OF PROCUREMENT

   TENDER FOR PROVISION OF BUSINESS PROCESS RE-ENGINEERING (BPR) CONSULTANCY AND IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM FOR SCHOOL OF THE ARTS, SINGAPORE

   TENDER REFERENCE: SAS/OP/2023/004/T”

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

5. Any items which the Tenderer considers to have no value shall 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 shall be deemed to be of no value .

6. Incomplete tender submission or submission of which are found not meeting the full requirements as stated in the Annexes herein 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 to the lowest quotes of any proposal and any claims for expenses incurred in the preparation of this Tender will not be entertained. The Company may choose to award the Tender in whole or in parts.

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

10. Before the submission of their Tenders, Tenderers must attend a mandatory 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), ERP Functional Requirement Specifications (Annex C), Detailed Business and Functional Requirements (Annex D), ERP Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) attached herein must be strictly adhered to unless specified that SAS accepts alternative proposed.

12. A "NIL" return of the Tender submission on any required Schedules will not be accepted.

13. The Contract Sum submitted shall be exclusive of 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 LATEST Profit & Loss Statements of two (2) most recent financial years

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)– CONTRACTOR REGISTRATION SYSTEM INFORMATION

GSR Head (with date of expiry if applicable)	Head Title	Financial Category / 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/ACCOUNT MANAGER/PROJECT MANAGER

	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						
4 Project Manager						

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 5 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)	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 tender offer (including the prescribed forms) are correct and true.

I/We hereby undertake to inform SAS 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 DATE

(AUTHORISED REPRESENTATIVE)

____

COMPANY STAMP

IMPORTANT NOTES :

(a) All items in Schedules 1, 2 ,3, Annex 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 should 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

FOT/1

FORM OF TENDER

TO: SINGAPORE ARTS SCHOOL LIMITED

TENDER FOR PROVISION OF BUSINESS PROCESS RE-ENGINEERING (BPR) CONSULTANCY AND IMPLEMENTATION OF THE ENTERPRISE RESOURCE PLANNING (ERP) SYSTEM FOR SCHOOL OF THE ARTS, SINGAPORE

1 I/We, the undersigned having visited the site, hereby submit this Tender for **Provision of Business Process Re-Engineering (BPR) Consultancy and Implementation of the Enterprise Resource Planning (ERP) System for School of the Arts, Singapore** as specified in this tender document in accordance with the EPR Conditions of Contract (Annex A), ERP Functional Requirement Specifications (Annex C), Detailed Business and Functional Requirements (Annex D), ERP Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) as attached hereto to the entire satisfaction of the Company.

2 My/Our Total Tender for the Contract is for the Total Amount (“the Contract Sum”) of:

Singapore Dollars: ____

____(S$________________)

*(*Amount brought forward from Schedule 3. Price Schedule, S3/1, Total. 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, shall constitute a binding contract between us.

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

5 I/We further undertake that this offer shall not be retracted or withdrawn for a period of ninety (90) days from the date fixed for receiving the same and it shall 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 shall commence within ninety (90) days of the tender validity.

7 I/We understand that the actual commencement date of Service will be concluded upon the award of the Contract. The commencement date 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 – EPR Conditions of Contract, COC/10, Clause 4

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.

FOT/2

11 I/We have read and understood all Selection Criteria (Annex B), ERP Functional Requirement Specifications (Annex C), Detailed Business and Functional Requirements (Annex D), ERP Technical Requirement Specifications (Annex G) and Statement of Compliance (Annex H) and their relation to the Price Schedule (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 Material Works, Equipment, Goods and Services at the prices submitted in the Tender based on the terms and conditions as stated in the EPR Conditions of Contract (Annex A), ERP Functional Requirement Specifications (Annex C), Detailed Business and Functional Requirements (Annex D) and ERP 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 :
PRICE SCHEDULE

Price Schedule

Price Schedule - BPR consultancy and proposal, complete implementation, integration, data migration and user adoption of the ERP

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

BPR consultancy & implementation of ERP SaaS	Timeline (months)	Year 1 $	Year 2 $	Year 3 $	Remarks
A. BPR consultancy, proposal, complete implementation, integration, data migration and user adoption of ERP					
B. Annual software subscription (provide breakdown, if any)					
C. Interface with existing SAS systems (refer to Appendix A)					
D. Any other item (provide breakdown)					
E. Application maintenance service					
Total					
F. Optional items					

Annex A :
EPR CONDITIONS OF CONTRACT

ERP CONDITIONS OF CONTRACT

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 computer programs 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 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 Instructions to Tenderers, the Conditions of Contract, the General Requirements, Functional Requirements, the Schedules, the Tender Proposal, the 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 sum specified in the Contractor's Tender for design, supply, delivery, installation, testing and commissioning of the System 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, Form of Tender, Instructions to Tenderers, Conditions of

Contract, General Requirements, Functional Requirements, Evaluation Criteria and any other documents and forms enclosed.

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

"**network bandwidth connectivity**" refers to the interconnecting of users, devices and computers in different locations for information exchange and access. It includes –

Layer 2 network bandwidth connectivity which is connectivity at the "data link" layer of the OSI model and TCP/IP models, and which minimally includes Ethernet frame transmission; and

Layer 3 network bandwidth connectivity which is connectivity at the "network layer" of the OSI model and to the "network/Internet layer" of the TCP/IP model, and which minimally includes IP packet transmission.

"Next Generation National Broadband Network" or **"Next Gen NBN"** refers to the nationwide all-fibre communications network to be designed, built and operated by OpenNet Pte Ltd (pursuant to the award made by the Info-Communications Development Authority on 26 September 2008 for the Next Gen NBN NetCo Request for Proposal) which has been replaced by its succeeding entity CityNet Infrastructure Management Pte Ltd (in its capacity as the Trustee-Manager of the NetLink Trust) (the "NetLink Trust"), and Nucleus Connect Pte Ltd (pursuant to the award made by the Info-Communications Development Authority on 3 April 2009 for the Next Gen NBN OpCo Request for Proposal).

"Next Gen NBN Operators" refers to the NetLink Trust and Nucleus Connect Pte Ltd.

"Next Gen NBN Retail Service Providers" refers to the entities which provide network bandwidth connectivity over the Next Gen NBN to end-users at the retail service layer using the underlying bandwidth connectivity supplied by Nucleus Connect Pte Ltd and the underlying physical connectivity supplied by the NetLink Trust.

"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**" (Representative) refers to the person appointed by SAS pursuant to

Clause 12.1 and any persons appointed by the Representative to assist him or perform such duties or functions as may be delegated to him by the Representative.

"Requirement Specifications" and "**Functional Requirements**" refers to:

(a) the specifications issued by SAS to the Contractor for the purpose of inviting the Contractor to submit its Tender for Consultancy for Business Process Re-engineering, and Proposal for Implementation, Integration, Data Migration and User Adoption of an Enterprise Resource Planning Solution; 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.

"**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 representatives, 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 representatives, 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 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

2.1 All references to clauses, unless otherwise expressly stated, are references to clauses numbered in the 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 the SAS, forms the System which is capable of meeting or exceeding the requirements of this Contract;

(b) supply the Application Software to the Authority 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 the Authority, 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 Tender Offer.

3.3 The Contractor shall designate a common service location for the 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, the SAS shall pay to the Contractor the Contract Price in the manner prescribed in Appendix 1.

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

4.3 The 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 the Authority.

4.4 The Contract Price is exclusive of any GST chargeable on the supply of goods, services or works to the SAS by the Contractor under this Contract. If the Contractor is a taxable person under the GST Act, the 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 the 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 the SAS may subsequently so pay, any such taxes, fees, duties, fines, levies and assessments (“Taxes”), the Contractor agrees that the Authority 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 the 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

6.1 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 the Authority or not), the 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 the Representative in writing as those the 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 the 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 the SAS connected with the project until one (1) year after the completion of the Software Warranty Period.

8.4 If the Contractor delays progress on any part of this Contract, for any reason not attributable to the SAS, and thereby reduces any scheduled duration of activities to be carried out by the SAS under this Contract, the SAS shall be entitled to a corresponding time extension for completion of such activities at no additional cost to the 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

SAS shall appoint a person to supervise and liaise with the Contractor for the purpose of the Contract and such person may designate others to assist him in such matters.

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 the SAS, conform with the work programme submitted by the Contractor in its Tender Offer and shall not extend the time prescribed in Requirement Specifications.

12.5 Regular Progress Reports & Meeting

12.5.1 The Contractor shall deliver to the Representative regular written progress and status reports in a format approved by the Representative (the "Progress Reports"). Unless otherwise stipulated by the Authority 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 the Authority and its 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 the Authority 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 the 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 the Representative.

13.1.3 Except as approved by the Authority and subject to such conditions as the Authority 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 the Authority. The personnel shall, as part of the security clearance, submit such declaration as may be required by the Authority.

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 the 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 the 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 work on the Contract, the Contractor shall remove such person immediately and furnish a suitable and adequate replacement at no additional expense to the SAS. If the 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 the 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 the SAS's or the 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 the SAS or the Representative for the SAS's or the Representative's (as the case may be) consent. Replacement staff shall not commence work on the project unless approval is given in writing by the SAS.

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

14 INTENTIONALLY LEFT BLANK

15 INTENTIONALLY LEFT BLANK

16 INFORMATION AND ACCESS

16.1 The 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 The SAS shall, for the purposes of the Contract, afford to the authorized personnel of the Contractor 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

21.1 The Contractor shall deliver the Application Software to the 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 the Authority in relation to this Contract.

22.1.3 The Acceptance Tests shall comply with the Acceptance Test Procedures proposed by the Contractor in its Tender Offer and accepted by the SAS. The 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 Tender Offer shall be developed based on the Requirement Specifications or otherwise specified by the SAS in the Contract.

22.2 Notice of Commencement and Completion of Acceptance Tests

22.2.1 The Contractor shall give to the 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 Annex C - ERP Functional Requirement Specifications, Annex D - Detailed Business and Functional Requirements, Functional Requirements 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 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 Price 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

22.7.1 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 SAS reserves the right to charge interest for any delayed payment at the rate of five percent (5%) per annum.

23.5 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 one (1) calendar month.

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 - ERP Technical Requirement Specifications, - and render the System fully operational within the turn-around-time specified in Annex G - ERP Technical Requirement Specifications.

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

27.1 SAS shall be entitled to obtain Maintenance Services 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 maintenance and support services shall be valid for a period of twenty-four (24) months commencing after the expiry of System Warranty Period, with option to extend for up to an additional twelve (12) months.

27.3 This option, if exercised, shall be based on terms no less favourable to SAS than those contained in the Annex G - ERP Technical Requirement Specifications and any other terms that may be mutually agreed in writing.

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

31.1 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

32.1 If the Contractor is obtaining part(s) of the Application Software from a third party, the Contractor shall inform the Authority 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 or representatives, 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, representatives 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 representatives 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 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

43.1 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

44.1 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

45.1 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

47.1 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 the Appointing Authority;

(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

52.1 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

53.1 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)

56.1 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

60.1 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 Authorised signatory)
for and on behalf of [Contractor Name]
[Name / Designation]) ______________________________
)

in the presence of:)
)
______________________________) ______________________________
) Name:

APPENDIX

CONTENTS

.

APPENDIX 1

.

Reference: Clause 4 of Conditions of Contract

THE CONTRACT PRICE SHALL BE PAID AS FOLLOWS:-

Stage	% of Contract Price	Cumulative Total
Thirty (30) days from acceptance of contractor's high level Business Process Re-engineering (BPR) project plan	20	20
Thirty (30) days from completion of BPR plan and process workshops	20	40
Thirty (30) days from completion of prototype	20	60
Thirty (30) days from completion of System Integration Test (SIT)	25	85
Thirty (30) days from completion of User Acceptance Test (UAT)	5	90
Thirty (30) days from go-live	5	95
Thirty (30) days from completion of one-month support	5	100

Any GST payable for the supply of goods, services or works by the Contractor under this Contract shall be reimbursed by the SAS.

PROVIDED THAT if the SAS in the Letter of Acceptance accepts payment in accordance with the Contractor's alternative payment terms contained in the Tender Offer then such alternative payment terms shall apply.

APPENDIX 2

INTENTIONALLY LEFT BLANK

APPENDIX 3

INTENTIONALLY LEFT BLANK

APPENDIX 4: UNDERTAKING TO SAFEGUARD OFFICIAL INFORMATION

UNDERTAKING TO SAFEGUARD OFFICIAL INFORMATION

1. My attention has been drawn to the Official Secrets Act (Chapter 213) and 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 and consultancy with SAS in connection with this project is of a strictly confidential in nature and is not to be published or communicated by me to unauthorised person in any form at any time, without official sanction of the relevant Chief Executive Officer of SAS.

3. I shall ensure that any other person who is authorized 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 the SAS, any other copies made or reproduced from such document or part thereof whenever required by the SAS.

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

______________________ Signature	______________________ Full Name in BLOCKS (Authorised Representative)	______________________ NRIC/Passport No (last 4 alphanumeric characters, e.g. XXXXX567A)
______________________ Designation	______________________ Company Name and Company Stamp	______________________ Date
______________________ Signature of SAS Witness	______________________ Full Name in BLOCKS	______________________ 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)	NRIC/Passport No (last 4 alphanumeric characters, e.g. XXXXX567A)
____________________	____________________	____________________
Designation	Company Name and Company Stamp	Date
____________________	____________________	____________________
Signature of Witness	Full Name in BLOCKS	NRIC No
____		____________________
Address		Date

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 Provision of Business Process Re-Engineering (BPR) Consultancy and Implementation of the Enterprise Resource Planning (ERP) System shall be evaluated based on the following criteria:

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

✓ b) Compulsory attendance at Tender Briefing

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 EPU/SER/34 – Consultancy Services
✓ ii) **Financial Grade**	**:**	**S6 and above** Tendering Capacity up to S$3,000,000 and above

d) Valid certifications before the Tender registration open date. (where applicable)
i) Other relevant certifications (if any)

e) Compliance with list of required Tender Documents submission including :
✓ i) Tender Price Schedule (Schedule 3)

✓f) Tender Proposal (Detailed proposal as set out in Annex C, Point 3.3 to 3.7)

✓ i) Compliance with points in the Annex C , Point 3.1 to 3.7 are critical specifications that need to be adhered to

j) Financial capabilities of the Tenderer

k) Record of past and current contracts/ projects

l) Other relevant certifications

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

Note: Criteria marked with ✓are critical.

Annex C :
ERP FUNCTIONAL REQUIREMENT SPECIFICATIONS

ERP FUNCTIONAL REQUIREMENT SPECIFICATIONS

CONTENT

1. Background

1.1 The Singapore Arts School Ltd ("SAS") invites qualified Enterprise Resource Planning ("ERP") implementation partner to submit a proposal for providing consultancy, project management and system implementation services for its ERP project.

1.2 Due to evolving organisational needs, the SAS is undergoing transformation to improves its corporate processes and replace its current corporate systems. The main focus of the ERP project is as follow:

1.2.1 Business Process Re-engineering ("BPR") of current work processes; and
1.2.2 Implementation of a cloud-based ERP system.

1.3 The main scope of the ERP project includes the BPR consultancy and proposal, complete implementation, integration, data migration and user adoption of the ERP modules. The objectives of the ERP project are:

1.3.1 Conduct a comprehensive review and understanding of the existing structure, policies, processes and operations of SAS; and benchmark against public service and/or industry best practices;

1.3.2 Identify areas of improvement in corporate processes; and propose a roadmap to identify actions and activities to achieve the objectives;

1.3.3 Define, design and align the vision and objectives of the transformation project across key stakeholders in SAS;

1.3.4 Propose and implement a cloud-based ERP system that is suitable for SAS in order to achieve the objectives; and

1.3.5 Work with SAS on change management, including the new operating model for finance, human resource and procurement.

2. Current system landscape

2.1 Please refer to Appendix A for a high-level SAS system landscape with connectivity to the current corporate systems. For finance, SAS uses SAP ECC6.0. For HR and procurement, SAS uses custom-built applications, namely HRIS and ePR.

2.2 There are currently about 250 users of the HRIS.

2.3 The number of users for finance and procurement will be recommended upon completion of BPR and agreed by SAS in the future-state ERP.

3. Requirement Specifications

3.1 The tenderer shall minimally meet Financial Grade S6 under Government Supplier Registration (GSR).

3.2 The tenderer shall recommend an ERP system and be a certified partner of the ERP system.

3.3 The tenderer shall have an office located in Singapore. The consulting and implementation team should preferably be located in Singapore.

3.4 The tenderer shall provide a full-time project manager who is locally based, as the single point-of-contact between the tenderer and SAS in all matters relating to the ERP project.

3.5 The tenderer should be experienced in BPR transformation and be competent to achieve the objectives set out in Paragraph 1.3.

3.6 The tenderer shall provide a full proposal of the ERP project. The proposal should minimally include the following information:

3.6.1 Company profile

3.6.2 Detailed project team and structure, including names, qualification and experience.

3.6.3 The Project Manager shall have at least 5 years of experience in managing similar projects

3.6.4 Track record in similar projects

3.6.5 Detailed proposal and execution plan; including but not limited to the following:

BPR Phase

The BPR phase involves a systematic approach to redesigning and improving existing business processes and operation to achieve significant improvements in performance, efficiency, quality, and customer satisfaction. Below are the some of the key components:-

i. Process Mapping and Analysis: Map and analyze the current state of the processes to identify inefficiencies, redundancies, and opportunities for improvement. Also, it should include a comprehensive review and understanding of the existing structure, policies of SAS;

ii. Performance Measurement: Establish metrics and performance indicators to measure the effectiveness and success of the reengineered processes. Continuously monitor and track key performance indicators (KPIs) to assess the impact of the changes and identify areas for further refinement.

iii. Target operating model TOM: a blueprint or framework that defines how an organization will operate in the future to achieve its strategic objectives. It provides a clear vision of the desired state of the organization's structure, processes, capabilities, and technology to support the delivery of its products or services. The target operating model will serve as a roadmap for organizational transformation and guides decision-making in aligning resources, capabilities, and processes to achieve the desired outcomes.

Project Execution Phase

iv. Project management plan/Charter: A document that defines the project's purpose, objectives, scope, stakeholders, and high-level approach.

v. Project Plan: A comprehensive document outlining the project's schedule, tasks, dependencies, resources, and budget.

vi. Requirement and Gap Specification: Detailed specifications and documentation that describe the functional and non-functional requirements of the project. As for the GAP document, it outlines the gaps between the TOM and the ERP application, and the workarounds.

vii. Design specifications: Blueprints, wireframes, mock-ups, or technical specifications that outline the design of the project, such as system architecture, user interface, or database schema.

viii. Other documents to include are configuration setting, integration setup, testing result.

ix. All system development should include unit testing, system testing and integration and UAT activities; these include integrating all necessary for the proposed System.

x. Data conversion/migration plan and to carry out the cleansing, conversion, migration and verification of the data from the existing systems, that are required to supply data to the new System in order for it to fully fulfil its operational requirements;

xi. End user training, business, IT Admin and technical training sessions for various user roles and a comprehensive training package that includes training plan, training material, qualified trainers and setup of the training environment.

3.6.6 Propose a comprehensive Business Continuity Plan to ensure there is no disruption to the business operations in the event of disruptions that affect the availability of the System.

3.6.7 Provide ONE (1) Calendar month of Performance Guarantee Period (PGP) upon commissioning of the System.

3.6.8 Provide ONE (1) year of System Warranty Period after PGP period.

3.6.9 Provide Application Software Maintenance and Support Services for TWO (2) years after the Warranty Period.

3.6.10 Change Management: Develop a comprehensive change management plan to facilitate successful implementation of the reengineered processes. This involves effective communication, training, stakeholder engagement, and managing resistance to ensure a smooth transition.

3.6.11 Contact of at least two (2) completed projects, with whom SAS can verify through reference check

3.6.12 SAS envisages the project to complete between 9 and 15 months

3.6.13 Any other information that the tenderer considers relevant to its proposal

3.7 Point 5 - Business and functional requirements of ERP – forms part of the Requirement Specifications in Point 3. In its proposal, the tenderer should clearly set out the functionalities of the proposed ERP.

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 S6, as set out in 3.1;

4.1.2 Proof of certified partner of the proposed ERP system, as set out in 3.2;

4.1.3 Detailed proposal as set out in 3.3 to 3.7;

4.1.4 Schedule 3, Annexes D, E and F

5. Business and functional requirements of ERP

5.1 Please refer to “Annex D – Detailed Business and Functional Requirements”, form set out for the tenderer to list and explain features of the ERP system. While it is not mandatory to complete every item in the forms, every effort should be made to be as detailed as it is feasible for SAS to assess the system capabilities.

5.2 At a broad level, the ERP should comprise the following modules:

Finance functions:

5.2.1 Plan to perform
5.2.2 Procure to pay
5.2.3 Order to cash
5.2.4 Record to report
5.2.5 Acquire to retire
5.2.6 Inventory
5.2.7 Treasury
5.2.8 Project accounting

Procurement functions:

5.2.9 Purchase requisition or Approval of Requirement
5.2.10 Invitation to quotation
5.2.11 Invitation to tender
5.2.12 Purchase order
5.2.13 Goods receipt
5.2.14 Supplier maintenance
5.2.15 Contract management

HR functions

5.2.16 Organisation management
5.2.17 Position and staffing
5.2.18 Onboarding
5.2.19 Compensation and benefits administration
5.2.20 Payroll
5.2.21 Salary structure administration
5.2.22 Salary benchmarking
5.2.23 Employee/manager self service
5.2.24 Contingent labour management
5.2.25 Recruitment
5.2.26 Talent management
5.2.27 Performance ranking and calibration
5.2.28 Succession planning
5.2.29 Time and absence management
5.2.30 Learning and development
5.2.31 Insurance

Annex D :
DETAILED BUSINESS AND FUNTIONAL REQUIREMENTS

DETAILED BUSINESS AND FUNCTIONAL REQUIREMENTS

Note:

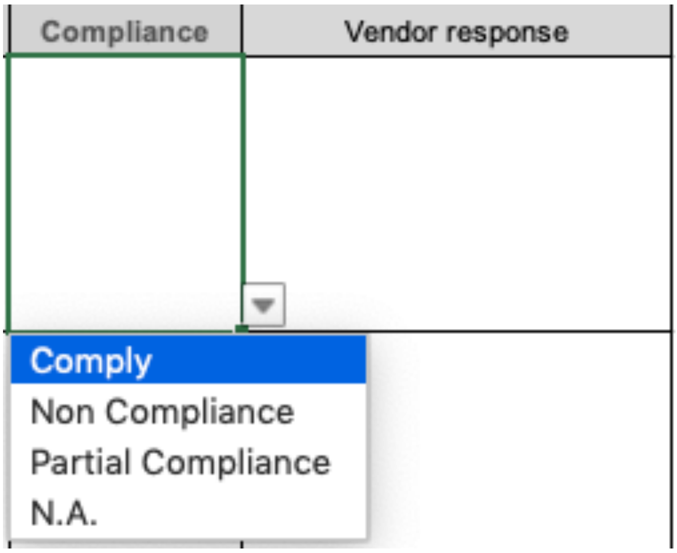
1. Tenderer to list and explain features of the ERP system. While it is not mandatory to complete every item in the forms, every effort should be made to be as detailed as it is feasible for SAS to assess the system capabilities.

2. Tenderer is to indicate their reply clearly for each item in the “Compliance” column with below reply:

   - Comply
   - Non-Compliance
   - Partial Compliance
   - N.A

   Any items with no reply and without dashes or other suitable marks shall be deemed to be N.A.

3. Tenderer may indicate their remark in “Vendor response” column if any.



GENERAL

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	All	Is there a dashboard function in the ERP, configurable views available to user based on the role, department, level in hierarcy or other factors. Provide a demo of the dashboard.		
2	All	Is there a tool in the ERP to configure prebuilt processes to meet SASL needs. The tool should not require coding and should be configurable by user without need for IT intervention. Provide a demo on the tool.		
3	All	Is there a master subscription agreement of the software-as-a-Service(SaaS) model		
4	All	Is there cloud service provider and location of data centre etc		
5	All	Is there third-party independent assessment of the security of the SaaS e.g. CSA-STAR or ISOs: 27001, 27017 and 27018. Provide details		
6	All	Is there third-party independent audit of System and Organisation Controls (SOC) standards. Provide details.		

FINANCE - GENERAL LEDGER

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Allocation	Ability to configure business rules to automate allocations in General Ledger, e.g. distributes cost in one account to different cost centers based on the headcount in each cost center.		
2	Budgetary Control	Ability to support budgetary control & encumbrance acccounting requirement		
3	Enterprise Structure	Ability to provide chart of accounts structure with multiple dimensions e.g. entity, academic/corporate divisions, cost center, fund, project etc.		
4	Enterprise Structure	Ability to set up Chart of Accounts hierarchies		
5	Enterprise Structure	Ability to define chart of accounts security rules		
6	Financial Close	Ability to close periods at end of month, restrict access to select users to reopen for period adjustments		
7	Financial Close	Ability to provide dashboard to see closing status		
8	General Accounting & Rules	Ability to define Accounting calendar		
9	General Accounting & Rules	Ability to support accrual method of accounting		
10	General Accounting & Rules	Capability to handle different fiscal calendars		
11	General Accounting & Rules	Ability to support multi-currency requirement.		
12	General Accounting & Rules	Ability to always-on audit trail		
13	General Accounting & Rules	Ability to allow role based user access		
14	Journal Processing	Ability to process recurring journal entries		
15	Journal Processing	Ability to auto-post journal entries		
16	Journal Processing	Ability to auto-post journal entries from subledgers into General Ledger		
17	Journal Processing	Ability to post journal entries from external systems		
18	Journal Processing	Ability to support Journal entry approval workflow		
19	Reporting	Ability to drill down to granular level		
20	Reporting	Ability to support non-financial or statistical entry		
21	Reporting	Ability to prepare different reports for differenet settings e.g. boardroom level, management level, department levels, operational reports etc		
22	Reporting	Ability to integrate with Microsoft spreadsheet		
23	Reporting	Ability to display red flags		
24	Reporting	Ability to provide datawarehousing tool with prebuilt, AI-powered analysis and dashbords		
25	Journal Processing	Ability to upload excel file to post bacth GL entries		

FINANCE - ACCOUNT PAYABLE

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Invoice	Ability to harness Robotic Process Automation (RPA) in the AP process		
2	Invoice	Ability to auto-calculate GST on invoice		
3	Invoice	Ability to support multi-level invoice approval workflow		
4	Invoice	Ability to match invoice with multiple POs or multiple receipts against PO.		
5	Invoice	Anility to perform 3-way match (PO, invoice, receipt)		
6	Invoice	Ability to detect and prevent processing of duplicate invoice		
7	Invoice	Ability to record a credit or debit memo to adjust original invoice amount		
8	Invoice	Ability to record advance payment		
9	Invoice	Ability to handle various ways through which invoices can be processed in ERP e.g. RPA, einvoice etc		
10	Invoice	Ability to auto-generate invoice for recurring expenses		
11	Invoice	Ability to process invoices in multiple currencies		
12	Invoice	Ability to support multiperiod accounting e.g in prepaid expense		
13	Payment	Ability to create payment to multiple payees e.g. student assistance		
14	Payment	Ability to review and approve batch payment		
15	Payment	Ability to support multiple payment methods and integration with bank and other payment systems		
16	Period Close	Ability to auto generate accrual on good receipt		
17	Period Close	Ability to support AP closing		
18	Reporting	List the varous standard AP reports		
19	Payment	Ability too download AP payment advice as PDF		
20	Payment	Ability to handle petty cash		

FINANCE - EXPENDITURE MANAGEMENT

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response	
1	Expense Submission	Ability to fully auomate the process of exepnse submission by staff			
2	Expense submission	Ability to allow staff to submit claims and supporting documents via smartphone technologies e.g camera, app, cloud etc			
3	Expense submission	Ability of ERP to automate compliance of expense claim with policy e.g. claim beyond 30 days from receipt date is automatically rejected			
4	Expense submission	Ability to enforce policy compliance at multiple levels e.g. on nature of expense, on account level, on claim limit etc			
5	Expense Submission	Ability for ERP to display pop-up message for staff to declare the veracity of the claim before hitting the submit button			
6	Expense Submission	Ability to submit expenses from scanned digital images			
7	Expense Submission	Ability to process and submit expense claim via mobile or tablet with OCR technology			
8	Expense Submission	Ability to manage prevailing GST in expense			
9	Expense Submission	Ability support credit card purchase			
10	Expense Submission	Embedded Artifical Intelligence (AI) in expense processing			
11	Expense Submission	Ability to delegate or authorize another user to perform expense entry and expense management			
12	Cash Advance	Ability tto administer cash advance			
13	Integration	Ability to book travel process with travel partner			
14	Integration	Integration with corporate credit card where purchases automatically populate expense system			
15	Expense Approval	Ability to set up approval workflow process for expense claims			
16	Expense Approval	Ability to approve Expense reports on mobile device			
17	Expense Reimbursement	Ability to notify staff on status of expense claim			
18	Reporting	Ability to provide intelligence on spend analysis			

FINANCE - ACCOUNTS RECEIVABLE

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Master Data	Ability to inegrate master data of all funders, customers, students, hirers etc from other systems		
2	Billing	Ability to generate periodic statements of account (SOA) and sent via email		
3	Billing	Ability to import detailed billiing data e.g. venue hire details from external systems		
4	Billing	Ability to generate credit note from original invoice		
5	Billing	Ability to generate default prevailing tax rate		
6	Billing	Ability to support multi-currency receivables		
7	Billing	Ability to generate recurring billing		
8	Billing	Ability to recognise deferred revenue		
9	Billing	Ability to various output formats e.g. pdf, xml, edi		
10	Receipt	Ability to match receipts matching to invoices		
11	Receipt	Ability to support advance collection		
12	Receipt	Ability to generate reminder for payment		
13	Receipt	Ability to support payment by instalment		
14	Receipt	Ability to alert system user that payment due is missed		
15	Reporting	Ability to privide high level dashboard with drill-down capabilities		
16	Reporting	List the standard AR and aging reports available		

FINANCE - CASH MANAGEMENT

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Bank Account	Ability to create multiple bank accounts		
2	Bank Account	Ability to report bank account balances in local and transaction currency		
3	Bank Account	Ability to track fixed deposit placement, start date, maturity date, interest rate and other relevant parameters		
4	Bank Transaction	Ability to enter ad hoc cash transaction		
5	Bank Transaction	Ability to support adhoc payment		
6	Bank Transaction	Ability to perform bank transfer		
7	Bank Reconciliation	Ability to upload bank statement via auto or manual means		
8	Bank Reconciliation	Ability to automate bank reconciliation. Ability for user to define reconciliation rule.		
9	Bank Reconciliation	Ability to highlight different types of receipts and payments e.g. school fees, misc fee, sale, giro payments, cheque payments etc		
10	Bank Reconciliation	Ability to identify unreconciled bank transaction		
11	Bank Reconciliation	Ability to highlight anomaly & red flag e.g. long reconciling item, possible fraud etc		
12	Cash Forecast	Ability to support cashflow forecast & simulation. Describe how ERP performs forecast & simulation from multiple sources like AP, AR, grants, FD etc		
13	Cash Position	Ability to calculate and view cash flow, cash position with configurable alert triggers		
14	Reporting	Ability to generate standard reports, identify cash in transit, unreconciled items, bank statements		
15	Reporting	Ability to generate cash position report		

FINANCE - FIXED ASSET

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	General	Ability to handle the complete fixed asset life cycle, from acquisition, depreciation, transfer, disposal, gain or loss on disposal		
2	General	Ability to automate deferred capital grant entries		
3	General	Ability to perform mass asset creation and disposal		
4	General	Ability to handle non-capitalised assets ie items below asset threshold, and the tracking and tagging of such low value assets		
5	General	Ability to handle single or multiple assets, parent and chiild assets relationships		
6	General	Ability to asset funded by multiple funding sources		
7	General	Ability to track and tag assets		
8	General	Ability to increase or decreas cost of existing asset		
9	General	Ability to search asset by query		
10	General	Ability to track and tag assets		
11	General	Ability to handle work in progress of asset capitalisation based on milestone payment		
12	General	Ability to perform partial retirement or disposal		
13	General	Ability to perform CAPEX budgeting		
14	General	Ability to forecast or project depreciation in the future by asset class, project, funding source etc		
15	Reporting	List the standard fixed asset reports		
16	General	Ability to recognize asset upon invoicing		
17	General	Ability to capitalize asset with tax amount		
18	General	Ability to track non-depreciated asset (ie: item expensed-off but trackable)		

FINANCE - TAX

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Configuration	Ability to fully comply with local and international tax across multiple entities and countries		
2	Configuration	Ability to fully comply with prevailing GST and WHT regulations		
3	Configuration	Ability to set up tax tables and update when rates change		
4	Configuration	Ability to allocate applicable tax code to invoice		
5	Configuration	Ability to classify taxable and non-taxable supplies		
6	Configuration	Ability to generate various GST Returns, including but not limited to GST F5 Return		

FINANCE - BUDGETING & PLANNING

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	General	Ability to provide budget utilisation via a dynamic budgeting module		
2	General	Ability to support forecast using advanced algorithms and/or machine learning. Describe further how these multi year prjects are rolled over abd tracked from one FY to another.		
3	General	Ability to support multi-year projects (both operating and capital in nature) and uploading of budget across FYs		
4	General	Ability to support optimisation of funding for various programmes		
5	General	Ability to produce key reports and presentation slides including dashboards/charts		
6	General	Ability to build/download/print standard reports and subscribe to them by email		
7	General	Ability to produce ad-hoc reports on planned data - including analysis of multiple plan scenarios/versions		
8	General	Ability to define allocation formula based on actual & budgeted balances as well as statistical balances		
9	General	Ability to integrate operational plan with forecast		
10	General	Out-of-the-box planning for workforce (plan headcount and related expenses)		
11	General	Out-of-the-box planning for projects and capital expenditure		
12	General	Ability to support project accounting		
13	General	Out-of-the-box planning for multi-year project related expenditure		
14	General	Ability of ERP to prepare budget on various basis e.g. historical budget, actual result, zero-based, percentage-based		
15	General	Ability to set prepare at any hierarchical level of the organisational structure		
16	General	Ability to support rolling budget and forecast		
17	General	Ability to upload data from different sources		
18	General	Ability to create multiple scenarios and versions of budgets and forecast		
19	General	Ability to support What-If modelling		
20	General	Ability to configure workflow process		
21	General	Ability to support different versions of budget		
22	General	Ability to allocate and track expenses by project for budgeting and reporting purposes		
23	General	Ability to return balance budget in cases of PO cancelled or partially delivered		

PROCUREMENT

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	General	Capability of the ERP system in supporting different public sector procurement approaches based on values setting. Following are the procurement approaches: - Invitation-to-Tender; - Invitation-to-Quote (ITQ); or - Small Value Purchase (SVP)		
2	General	Ability to support different sourcing methods. Following are sourcing methods commonly used in public service procurement: - Open quotation or tender; - Limited quotation or tender; - Period contract; - Framework agreement; - Request for proposal - verbal or written quote; - online or off the shelf purchase		
3	General	Ability to support evaluation process of various proposals in an ITT, ITQ or SVP process, through automation and digitalisation		
4	General	Ability to perform budgetary control checks at various stages eg. enquiry, PR, PO etc		
5	General	Ability to intergrate procurement with budgeting module and provide dynamic budget utilisation		
6	General	Ability to maintain system log and error log		
7	General	Ability to for system to appoint Approving Officers and to set up covering officer with validity period while AOs are away		
8	Requisition	Ability to Attach documents to requisition		
9	Sourcing	Ability to create custom templates		
10	Supplier Management	Ability to have supplier portal page		
11	Supplier Management	Ability for workflow approval process for vendor creation		
12	Procurement Contract	Ability to Store, Maintain and update existing contracts and create new contract		
13	Procurement Contract	Ability to manage contract approvals throug workflow		
14	Procurement Contract	Ability to sign contracts electronically		
15	Procurement Contract	Ability to have reminders and email alerts for contract expiry and other key events		
16	Procurement Contract	Ability to have Integrated functionality between eProcurement and Contract Management		
17	Procurement Contract	Ability to have always-on audit		
18	Procurement Contract	Ability to create and modify templates for contract creation		
19	Procurement Contract	Ability to generate standard and management reports and have real time reporting abilities		
20	Procurement Contract	Ability to have procurement dashboard with complete overview of contract		
21	Procurement Contract	Ability to have include KPI in contract performance		
22	Procurement Contract	Ability to track conract balance in real time i.e deducting original contract value by payments made to date		
23	Procurement Contract	Ability to release budget for PR/PO created by user who subsequently leaves SASL		
24	Purchase Requisition	Ability for system to link cost centre/project code/ GL account		
25	Purchase Requisition	Ability to allow more than 200 users in various procurement roles		
26	Purchase Requisition	Ability to have create separate approval workflows for different levels of procurement e.g. ITQ, ITT, SVP etc		
27	Report	Ability to export report to excel		
28	PO Creation	Ability for system to display correct tax code upon PO creation and buyer should. have ability to change tax code during PO creation		
29	Purchase Order	Ability to handle multi currency		

FINANCE CLOSING & REPORTING

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	General	Ability to maintain a financial calendar of events relating to closing schedule and tasks to be performed		
2	General	Ability for always-on audit		
3	General	Ability for dashboard to track closing process and status		
4	General	Ability to support IFRS and other local statutory requirements		
5	General	Ability to support reporting to different stakeholders through user-defined report e.g. Commissioner of Charities annual report format		
6	General	Ability to Integrate with MS Office		
7	General	List the standard financial and management reports available in the ERP		
8	General	Ability for ERP to handle audited financial statement narrative disclosure. Describe if and how this can be done		
9	General	Ability to generate report at various levels e.g. company level, academic/corporate level, department level, cost centre level, fund level, project level etc		
10	General	Ability for ERP to perform variance analysis against approved budget, forecast, including mult-period trend analysis		
11	General	Ability to import and export budget in excel or other format		

HUMAN RESOURCES

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1	Talent acquisition	Ability to auto populate the vacancy information (e.g. position title, department, FTE, Perm/Contract/Temp Status etc) from the requisition template		
2	Talent acquisition	Ability to check whether the requisition is within approved manpower budget and route for approval accordingly. If requisition is beyond approved manpower budget, system will alert requestor to seek approval before proceeding.		
3	Talent acquisition	Ability for administrator to define approval workflow for different types of requisition e.g. academic, corporate, leadership etc.		
4	Talent acquisition	Ability for approvers/reviewers etc to access the module on the go?		
5	Talent acquisition	Ability to post vaancy internally first for a predefined period before posting externally		
6	Talent acquisition	Ability to host internal and external job sites and social media e.g. jobstreet, linkedin		
7	Talent acquisition	Ability to create and manage referral campaign in the system		
8	Talent acquisition	Ability to view and track progress of end to end requisition process e.g. from approval to shortlisting, interview, selection and onboarding		
9	Talent acquisition	Ability for recruiters to filter CVs by selected criteria.		
10	Talent acquisition	Ability to include prescreening questions and set rules for screening applicants		
11	Talent acquisition	Ability to upload attachments (e.g. educational certs, CV) in job portal to ERP		
12	Talent acquisition	Ability to black-list candidates		
13	Talent acquisition	Provide a unified experience through bringing the LinkedIn “search and match” experience into recruiting solution		
14	Talent acquisition	Ability to leverage a one-click export of profiles from LinkedIn into recruiting solution		
15	Talent acquisition	Ability to score, rank and match applicants to the right roles.		
16	Talent acquisition	Ability to follow up and communicate result of the screening directly to the applicant to engage and improve applicant experience		
17	Talent acquisition	Ability for interviewers to update their availability for interviews online		
18	Talent acquisition	Features to improve applicant experience. Please elaborate.		
19	Talent acquisition	Ability to trigger email communication based on predefined milestones to keep candidates engaged throughout the recruitment process		
20	Talent acquisition	Ability for recruiter to view the progress of the job applications per candidate (e.g. in situations where a candidate is concurrently considered for multiple roles) as well as candidates per job application		
21	Talent acquisition	Ability to capture and organize all interview results and feedback into the central database/recruitment tool.		
22	Talent acquisition	Ability to automatically close job postings post expiry date or when the position(s) in the requisition has been filled.		
23	Talent acquisition	Ability to integrate results from 3rd party solutions e.g. behavioral assessments, profiling etc		
24	Talent acquisition	Ability to capture candidate’s salary requests and compare with salary benchmarks for similar roles within and outside the organization		
25	Talent acquisition	Ability for salary recommendations to be routed for online approvals in case salary offered is outside the budgeted range		
26	Talent acquisition	Ability to model and predict optimum compensation range for a candidate based on candidate's profile and external pre-defined factors.		
27	Talent acquisition	Ability to send offer to the candidate through an automated process and track all subsequent communication / negotiation within the system		
28	Talent acquisition	Ability to create and store multiple offer templates on the basis of the type of hire		
29	Talent acquisition	Ability for candidate to view and accept an offer online		
30	Talent acquisition	Ability to automatically generate appointment letter creation upon acceptance of letter of offer (whether in system or offline) using information captured from candidate application form with standard Letter of Appointment template		
31	Talent acquisition	Ability to generate mass Letters of Appointment		
32	Talent acquisition	Ability to capture feedback from candidates and new joiners to identify potential areas for improvement		
33	Talent acquisition	Ability to churn reports and perform data analytics on the talent acquisition process.		
34	Talent acquisition	Report/Analytics with ability to predict lead time for an open position based on market conditions and historical trends.		

HUMAN RESOURCES

35	Talent acquisition	Report/Analytics to automatically identify most suitable talent source based on based on historical data (i.e. hit rate of similar jobs across sourcing channels as per predefined criterias such as time period, job levels etc).		
36	Talent acquisition	Report/Analytics to analyze sourcing channel effectiveness and cost to aid decision making.		
37	Talent acquisition	Ability to track budgeted/ approved headcount vs total staff (including short term Contractors)		
38	Talent acquisition	Ability for administrators to create multiple onboarding forms and multiple onboarding workflows based on job type.		
39	Talent acquisition	Ability for straight through processing from candidate application in job portal to employee central		
40	Onboarding	Ability to handle new staff orientation. Please elaborate.		
41	Onboarding	Employee administration e.g. allocation of laptop, staff pass, work desk, phone number etc before date of joining.		
42	Onboarding	Automatically enrolling new joiners to a compliance program e.g. conflict of interest declaration, training plans, staff handbook etc		
43	Onboarding	Ability to send notification to relevant parties (e.g. IT, Facilities management, Finance, to complete necessary processes prior to new joiner's first day		
44	Onboarding	Ability to automatically track and send email reminders to new joiners of necessary forms based on predefined criteria		
45	Onboarding	Availabilty of Reports/Analytics to measure and assess the effectiveness of onboarding. Please elaborate.		
46	Onboarding	Ability to integrate onboarding site and activities with learning management system		
47	Onboarding	The system must have an integrated onboarding process from recruitment to acceptance of the offer. Upon employee acceptance of the job offer, the application must have the capability to notify relevant parties, such as facility and IT, for		
48	HR management	Ability to add, modify, remove benefits plans on the system		
49	HR management	Ability to calculate monetary value of cash and non cash components		
50	HR management	Ability to interface with external parties (3rd party providers / government)		
51	HR management	Ability to generate report indicating the employee’s current participation levels in all benefit plans		
52	HR management	Ability for the employee to submit benefit claims		
53	HR management	Ability to define / edit claims approval workflow		
54	HR management	Ability to maintain record of employee plan history		
55	HR management	Ability to access external sites to benchmark benefits		
56	HR management	Ability to flag employee approaching retirement and re-employment age		
57	HR management	Ability to capture information regarding dependents		
58	HR management	Ability for employees to view their salary related information data via self service and on mobile		
59	HR management	Ability to interface in and view payslips and statutory forms (IR8, IR8A, IR8B, SRS declarations)		
60	HR management	Ability to capture details of contract staff and notify when contract is due		
61	HR management	Ability to perform renewal, extension or conversion for contract staff		
62	HR management	Ability to maintain grievance data and support tracking		
63	HR management	Ability to maintain and track non-compliance or misconduct		
64	HR management	Ability to maintain the disciplinary action types		
65	HR management	Ability to support whistle-blowing policy		
66	HR management	Ability for employee to enter and update personal data via self service and on mobile		
67	HR management	Ability to mass upload employee data via template		
68	HR management	Ability to maintainposition information e.g. isecondary positions, concurrent appointment, committee & taskforce etc		
69	HR management	Ability to capture personal information such as qualifications, educations, military service, external directorship, bank accounts for each employee		
70	HR management	Ability to upload documents		

71	HR management	Ability to maintain employee history		
72	HR management	Ability to report on employee data		
73	HR management	Ability to define / update approval workflow for employee data change		
74	HR management	Ability to store and access electronic P-file		
75	HR management	Ability to generate headcount report		
76	HR management	Ability to auto generate letter of employment		
77	HR management	Ability to capture additional organisation defined information such as security clearance level, office location, office phone number, organisational roles, government positions, potential ratings, referral source		
78	HR management	Ability to maintain non-employee and relationship with the organization e.g. board director		
79	HR management	Ability to view staff' information such as education, past employment & job history in a single view		
80	HR management	Ability to support annual declaration eg. Conflict of interest		
81	HR management	Ability to configure letter templates and automatically generate the template upon request.		
82	HR management	Ability to build adhoc requests for information and design reports with ease. Please elaborate.		
83	HR management	Ability to track employee's probation period and trigger confirmation workflow		
84	HR management	Ability to auto geneate Long Service Award and integrate to payroll		
85	HR management	Ability for each department/team/committee to customise and publish survey		
86	HR management	Ability to access HR policies on mobile platforms (Android, iOS app)		
87	HR management	Ability to broadcast information to staff		
88	HR management	Ability to integrate with external mobile applications with gamification e.g. health apps		
89	HR management	Ability for staff to personalise homepage view or dashboard		
90	HR management	Ability to foster collaboration and knowledge management		
91	HR management	Ability to support various types of time entry for both staff and contingent workforce (adjunct staff). Please elaborate.		
92	HR management	Ability to support time clocking of adjunct staff in order to calculate payroll. Please elaborate.		
93	HR management	Ability to raise exit requesst e.g. resignation		
94	HR management	Ability to notify relevant stakeholders in employee’s resignation to kickstart exit clearance process		
95	HR management	Ability to allow managers to manage/approve the exit checklist and for HR to view the approved checklist for processing		
96	HR management	Ability to define and manage workflows for different types of exits (e.g. voluntary, involuntary, death, retirements etc)		
97	HR management	Ability to create an online exit questionnaire for exiting employees to complete online exit questionnaire.		
98	HR management	Ability report and analyse various types exit reasons as captured during exit interviews. Ability to support various types of time entry for both staff and contingent workforce (adjunct staff). Please elaborate.		
99	HR management	Ability notify alumni database administrator of ex employees who have completed their exit clearance for alumni database registration purposes.		
100	HR management	Ability to calculate leave balance based on termination date		
101	HR management	Ability to maintain country specific public holiday calendars		
102	HR management	Ability to support evolving working needs to staff e.g. flexible work arrangements. Please elaborate.		
103	HR management	Ability to upload supporting documentation for leave application (medical, marriage etc.)		
104	HR management	Ability to notify employees when leave balance is expiring.		
105	HR management	Ability to auto add leave balance if the Public Holiday is on a Sunday/ non-working day		
106	HR management	Ability to pro-rate leave balances based on predefined rules (e.g. hire date, FTE ratio, termination dates etc.)		

107	HR management	Ability to track employees required to take Mandatory Block Leave and automatically send reminders if not taken		
108	HR management	Ability to encash unutilised leave during termination process and integrate to payroll for payout.		
109	HR management	Ability to support many levels of organisation structure e.g. company, division, department etc. Please elaborate.		
110	HR management	Ability to mass upload / update all organizational data		
111	HR management	Ability to display staff directory		
112	HR management	Ability to support singapore payroll administration, including statutory requirements such as CPF, tax reporting		
113	HR management	Ability to interface with payroll for leave related pay calculation (e.g. unpaid leave, childcare leave, encashed leave balances for employees who are leaving)		
114	HR management	Ability to interface with payroll for compensation data (salary, bonus, allowances, deductions)		
115	Performance management	Ability to support the schools ranking, cross-ranking process. Please elaborate.		
116	Performance management	Ease of change of performance management criteria such as rating, ranking by the business administrator. Please elaborate.		
117	Performance management	Ability to define and launch multiple performance appraisal cycles		
118	Performance management	Ability to define employee groups for the performance appraisal cycle		
119	Performance management	Ability to set goals/targets and weightages		
120	Performance management	Ability to upload goals / target via excel template		
121	Performance management	Ability to support school's strategic goals and cascade to goals to departmental and staff levels. Please elaborate.		
122	Performance management	Ability to define multiple performance assessment templates based on job roles e.g. one template for teaching staff and another for corporte staff		
123	Performance management	Ability to define weights for each performance appraisal sections (e.g. KPIs, Competencies, Values etc)		
124	Performance management	Ability to display and track the progress of performance appraisal at various levels e.g. department, staff level. Please elaborate.		
125	Performance management	Ability to highlight and direct staff to incomplete items in the performance appraisal form		
126	Performance management	Ability for Reporting Officer to stack rank managers to stack rank staff based on ranking within job grade and ranking within department. Describe the ability to present a consolidated view.		
127	Performance management	Ability for ROs to view the gap between their ratings and staff ratings		
128	Performance management	Ability to seek feedback from staff participation in committees and taskforce		
129	Performance management	Ability to highlight the incomplete items in the performance appraisal forms to staff and managers		
130	Performance management	Ability to seek further clarifications / inputs from the employee		
131	Performance management	Ability to view status of completion of self input and manager feedback during the periodic performance review (mid year / quarterly)		
132	Performance management	Ability for the manager to view employees status on achievement against goals / targets throughout the year		
133	Performance management	Ability for employees/managers to view the overall calculated performance ratings in the performance appraisal form		
134	Performance management	Ability for the employee to provide self inputs during the final review against goals / targets		
135	Performance management	Ability to attach documents (in defined format) while providing self inputs		
136	Performance management	Ability for employees to select persons (e.g manager, peers, subordinate, etc.) to seek performance feedback from.		
137	Performance management	Ability for the manager to provide performance rating, potential and feedback (qualitative and quantitative) against goals / targets		
138	Performance management	Ability for managers to view past performance ratings and feedback of employees who were in their teams		
139	Performance management	Ability to highlight developmental areas for the employee		
140	Performance management	Ability to interface with the learning system to suggest / identify training programs against development areas		
141	Performance management	Ability for 360 feedback exercise		
142	Performance management	Ability to set and define bell curve distribution and quota for each performance review cycle		

143	Performance management	Ability for managers/facilitators to compare and rank employees within his / her team		
144	Performance management	Ability for Counter-signing Officer (CO) to provide final rating and comments		
145	Performance management	Ability to roll-up rating and rankings for next level calibration session		
146	Performance management	Ability to auto-update the final approved ratings into the employees performance appraisal form.		
147	Performance management	Ability for employees to acknowledge the final rating/performance feedback provided to complete the process		
148	Performance management	Ability for employees/managers/administrators to view and track where the progress of the individual employee's performance appraisal forms		
149	Performance management	Ability for HR to view, track the submission of performance forms and trigger reminder emails to Reporting Officers		
150	Performance management	Ability to define competencies by role, department / function and level		
151	Performance management	Ability to use competency assessment as part of Recruitment, Succession Planning, Performance Management and Learning and Development		
152	Performance management	Ability to identify eligible hi-potentials / talent pool based on competencies, performance rating etc.		
153	Performance management	Ability to compile scores from various assessment tools like psychometric test, 360 feedback and Assessment Center		
154	Performance management	Ability to create and download customizable grid (eg. 9 Box grid for performance potential) to identify and position hi-pos		
155	Performance management	Ability to view and download results / report of various assessment tools (eg. 360 degree feedback)		
156	Performance management	Provide AI driven skills repository to enable employees to upskill or crossskill in their career		
157	Performance management	Ability to identify critical roles within company/organization to plan succession		
158	Talent Review & Succession	Ability to use technologies e.g. analytics, machine learning and dashboards to help organisation optimise talent attraction and retention. Please elaborate.		
159	Learning and development	Ability for employees to upload learning content (e.g. videos, documents) and add links to content within or outside the intranet.		
160	Learning and development	This is a place holder for PD process to be incorporated into the ERP		
161	Learning and development	Ability to create online assessment and feedback forms		
162	Learning and development	Ability to integrate content from third party course content providers on the system		
163	Learning and development	Ability to link courses to organization’s competency framework		
164	Learning and development	Ability to link courses to different levels / roles at company		
165	Learning and development	Ability to create a dedicated learning portal for different programs (leadership, functional, flagship programs, etc.)		
166	Learning and development	Ability for employee to view learning courses based on the development needs identified		
167	Learning and development	Ability submit request for external learning courses for manager's approval by entering relevant details (name of course, location, cost etc)		
168	Learning and development	Ability to build approval workflow for application for training		
169	Learning and development	Ability to enable gamification of learning activities e.g. points or rewards for completion of learning courses that can be redeemed		
170	Learning and development	Ability to generate training completion reports		
171	Learning and development	Ability to build custom reports (as per defined criteria) to analyze learning results		
172	Learning and development	Ability to integrate with different HR systems to capture employee data such as attrition, employee engagement etc. for a holistic effectiveness of the learning courses		
173	Learning and development	System should be able to interface with content management system organization to share content related to coaching and mentoring (techniques, best practices, templates, links to external certification programs)		
174	Learning and development	Ability to assess coaching / mentoring skills of individuals based on defined parameters and scale		
175	Learning and development	Ability to embed contextual learning in HR and talent management processes		
176	Learning and development	Ability to configure course surveys to allow staff to feedback after attending the course		
177	Learning and development	Ability to tag the training dates to the leave calendars and block staff from taking leaves during these training dates?		
178	Learning and development	Ability to configure the training budget for each faculty/department with respective GL account		

179	HR reporting & analytics	Due to the sheer number of reports avaialbe in ERP, it is not possible to full list the reports. Please provide demo during tender interview on ERP features on reports and anlytics		
180	HR reporting & analytics	Ease to build and deploy reports and analytics tools. Please elaborate.		
181	HR reporting & analytics	Ability to perform multi-dimensional analysis and ability to drill-down to transactional level. Please elaborate.		
182	HR reporting & analytics	Ability to empower ERP user and reduce dependency on IT support. Please elaborate.		
183	HR reporting & analytics	If requested, to provide a demo of the system capabilities		
184	General Requirements	Ability to configure comprehensible and informative error messages with clear instructions for the user to recover from the error condition in order to proceed.		
185	General Requirements	Ability to have the notifications feature to send out the alerts or reminders		
186	General Requirements	Ability to run on both Microsoft Windows and Apple macOS and the mobile app shall be able to run on Andriod or IOS		
187	General Requirements	Ability to provide a mobile application to allow users to access certain modules		
188	General Requirements	Ability to create or edit User Roles and assign access right based on the Access Right Matrix		
189	Personal Module	Ability to maintain employees' personal information		
190	Personal Module	Ability to auto granting of self-service access rights and the setting up of approving workflow based on employee type and information keyed in		
191	Personal Module	Ability to capture the no-pay leave period and compute the length of service readily		
192	Personal Module	Ability to store the key documents linked to individual employee records with the option to grant "View" access rights to employees. E.g. bonus letters, disciplinary letters and so on.		
193	Personal Module	Ability to allow future effective dates on career progression details to be keyed in advanced		
194	Personal Module	Ability to provide the mass upload features such as mass annual increment data, photo udpates and so on		
195	Personal Module	Ability to allow Business Administrators to search employee's records by employee code,employee name,department,designation and so on in the search bar		
196	Personal Module	Ability to allow HR managers to generate the recommendation list based on SAS's promotion guidelines and rules.		
197	Personal Module	Ability to allow HR managers to key in salary proposal,to-be job title, and to-be job grade for each staff in the promotion report		
198	Personal Module	Ability to allow business administrator to update/edit/add promotion business rules		
199	Personal Module	Ability to allow business administrators to confiture the acting allowance based on the job roles		
200	Personal Module	Ability to automatically populate the acting allowance if the acting role filed indicates with "Yes"		
201	Personal Module	Ability to schedule or configure batch jobs to update the corresponding staff employee profiles and organizational charts based on the final approved promotion list once the organisational charts for promotion workflow is verified		
202	Leave Module	Ability to configure different leave codes and entitlements for different employee types		
203	Leave Module	Ability to configure different leave policies		
204	Leave Module	Ability to configure different approving workflow processes for different leave types		
205	Leave Module	Ability to auto approved sick leave once staff submit it		
206	Leave Module	Ability to display a Leave Calendar with all employee's leave entries indicating their name/alias with surname and leave type		
207	Leave Module	Ability to alert Business Administrators on the approval of no-pay leave and auto import to Payroll module for payroll purposes		
208	Leave Module	Ability to automatically grant the necessary Parenthood Leave to eligible employees when Business Administrators update the employee's record		
209	Leave Module	Ability to allow a fuss-free year-end leave initialization process to a new year with no downtime		
210	Leave Module	Ability to configure the parameters for special leaves such as childcare leave, child sick leave,family care leave and parent care leave		
211	Leave Module	Ability to not allow staff to submit any leave applications if the selected dates are tagged with any approved or paid training.		
212	Claim Module	Ability to automatically tag to corresponding GL accounts for different types of claims		
213	Claim Module	Ability to indicate the corresponding budget owner and final approval officers for different type of claims		
214	Claim Module	Ability to pop up messages to remind budget owners or approving officers if the budget under the particular GL account is not sufficient for the claim		

215	Claim Module	Ability to allow employees to upload supporting documents		
216	Claim Module	Ability to build different approval workflows for the different claim processes		
217	Payroll Module	Ability to perform calculations of payroll with inbuilt formulas as determined by statutory regulations.Such as regular monthly payroll for different groups of employees,allowances,payments and deductions, bonuses and other pay items		
218	Payroll Module	Ability to mass upload data like adjuncts's fees		
219	Payroll Module	Ability to multiple pay runs in a month such as festive advance payroll run and main payroll run in a month		
220	Payroll Module	Ability to define pay rules,pay items,pay types		
221	Payroll Module	Ability to release payslips on self-service modules based on the payday indicated		
222	Payroll Module	Ability to generate payroll-related files such as Inter-Bank GIRO file, IR8A,IR21, CPF,etc in the format required by the relevant authorities		
223	Payroll Module	Ability to configure the pay rate matrix for different groups of staff		
224	Payroll Module	Ability to export a range of reports related to payroll in excel/pdf format		
225	Organisational Chart	Ability to create organizational chart to identify seniority and lines of authority that ought to be followed		
226	Organisational Chart	Ability to display the organisational chart filtered by faculty/department		
227	Organisational Chart	Ability to depict the organization's hierarchy with more senior positions at the top. Underneath each potion should be subordinate positions and roles, which may be segregated by department or faculty.		
228	Organisational Chart	Ability to mass upload the data by importing excel or CSV file		
229	Organisational Chart	Ability to link to the employee's personal profile when clicking the hyperlink of the employee's name in the organisational chart		
230	Off-Boarding	Ability to build the off-boarding process		
231	Off-Boarding	Ability to automatically compute employee balance pay,leave,claim,etc		
232	Off-Boarding	Ability to build a checklist for resignation or end-contract		
233	Off-Boarding	Ability to allow users to view stage of the off-boarding process		
234	Off-Boarding	The system must have an integrated offboarding process from the resignation to the employee's exit. Upon an employee's resignation, the application must notify relevant parties, such as facility and IT, for off-boarding preparation.		

TECHNICAL

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
1.1.3	Ease of Maintenance	Ability to provide a set of comprehensive application related standards and guidelines (e.g. no duplication of codes without good reasons) to ease maintenance of the System.		
1.2.1	Up-to-date Technology	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.		
1.3.3	System Performance	Ability to provide the application performance testing benchmark results on meeting the defined set of standard benchmarked performance of the System		
1.4.1	System Availability	The System shall minimally achieves 99.5% availability		
1.4.2	System Availability	The vendor shall ensure the system maintenance activities (e.g. backup jobs) shall not impact the availability of the System.		
1.4.5	System Availability	Ability to provide SAS the planned activities at the beginning of the calendar year. Ability to inform SAS on the ad-hoc maintenance 1 month before the executions.		
1.4.6	System Availability	The vendor shall provide the required scheduled service downtime and planned total service uptime per calendar month with SAS to avoid unnecessary disputes later.		
1.4.7	System Availability	Ability to implement auto-scaling based on conditions that are predefined with SAS. (e.g. scale up x% and scale down at y%).		
1.5.2	System Reliability/Integrity	Ability to provide suitable performance monitoring and analysis procedures to enable proper capacity planning,tuning and maintenance.		
1.6.2	System Readiness	Ability to provide the necessary documentations required for system readiness		
1.7.2	Service Administration	Remote administrative access shall only be granted to authorised personnel who need to perform administration on the system remotely.		
1.9.1	Disaster Recovery (DR)	The vendor shall provide SAS with the documentation required for the Disaster Recovery Plan, including the Business Continuity Plan (BCP)		
1.9.3	Disaster Recovery (DR)	Ability to work with SAS to ensure the System's availability in a disaster.		
1.10.3	Data Archival	Can the vendor comply with the Technical Requirement Section 5 - IT Security for the archived data to prevent malicious or accidental deletion or modification of records even where access credentials are granted.		
1.10.4	Data Archival	Ability to provide the cost-optimization design/solution of the data archival based on SAS needs.		
1.10.5	Data Archival	Ability to 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	Data Archival	Ability to implement auto-scaling for archival storage solutions with pay-as-you-go pricing.		
1.10.8	Data Archival	Ability to provide the best industry design solution for data archival (e.g., transactional data,metadata and etc) of the System.		
1.11.1	Data Migration	Can the vendor to 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	Data Migration	Ability to implement the transform and load processes to move data from the database on-premise to the commercial Cloud.		
1.11.3	Data Migration	Ability to convert the historical data from the existing relational database to the Cloud database.		
1.11.4	Data Migration	Ability to 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	Data Migration	Ability to implement a backup plan to rollback in case the first attempt of data migration fails.		
1.11.6	Data Migration	The vendor to propose an appropriate migration tool from premise to cloud. Please elaborate.		
1.11.7	Data Migration	The vendor to provide the data reports and checklist of the whole data migration activities to SAS.		
1.11.8	Data Migration	The vendor to share the issue logs and audit logs of the operational migration process to SAS.		
1.11.9	Data Migration	The vendor to propose the solutions on the issue logs of the operational migration process for SAS approval.		

TECHNICAL

1.11.10	Data Migration	The vendor 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)	Ability to provide the design solution of the System with SSO features		
1.13.1	Notifications/Reminders	Ability to implement thresholds that are set to trigger alerts.		
1.13.2	Notifications/Reminders	Ability to turn on the notification features by email and/or sms for the System.		
3.1.4	Infrastructure- Commerical Cloud Service	Ability to 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	Infrastructure- Commerical Cloud Service	Ability to adopt best practices and open standards available in the cloud environment so as to optimise the in-built system capabilities and to minimise customization, system deployment time and cost.		
3.1.6	Infrastructure- Commerical Cloud Service	The vendor shall propose a commercial CSP that is Multi-Tier Cloud Security (MCTS) certified.		
3.1.8	Infrastructure- Commerical Cloud Service	The vendor shall ensure that SAS's data is isolated from other tenants in the multi-tenant cloud?		
3.1.9	Infrastructure- Commerical Cloud Service	The vendor to ensure that the performance of the System deployed for SAS does not interfere with other tenants' overloads in the multi-tenant cloud. Please elaborate.		
3.1.10	Infrastructure- Commerical Cloud Service	Ability to adequately configure the infrastructure to ensure no corrupted data from other tenants could spread to SAS.		
3.1.11	Infrastructure- Commerical Cloud Service	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. Please elaborate.		
3.2.2	Transition Management to a new commercial CSP	The tenderer shall ensure the accuracy and completeness of information documented and handed over to the new commercial CSP. Effort of migration is required.		
4.1.2	Service Management and Operations	Ability to itemize and state all Managed Services charges for implementing and maintaining the System.		
6.1.4	Logging and Monitoring	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).		
6.1.7	Logging and Monitoring	The tenderer shall ensure security-related logs are available to facilitate event reconstruction and incident investigation. CSP shall support the incident investigation without extra cost.		
6.1.10	Logging and Monitoring	Ability to implement that log information is accessed by authorized personnel only; operations personnel should not have access to logs to prevent the risk of tampering or deletion.		
6.1.11	Logging and Monitoring	The tenderer shall ensure that log files do not contain sensitive information.		
6.1.13	Logging and Monitoring	Ability to implement the auto-scaling feature turns on to provide sufficient capacity to store the log files.		
6.1.14	Logging and Monitoring	Ability to provide the design solutions for the logs for audit purposes.		
6.2	User Access Logging	Ability to 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	Ability to provide support services during the User Acceptance Testing Period, Performance Guarantee Period (PGP), System Warranty Period, and Application Software Maintenance and Support Period for the System, processing service requests, managing problems, and proposing incident and problem resolution support structures and procedures. Refer to the ANNEX D- ERP Technical Requirements Specification Section 7		

CYBER SECURITY

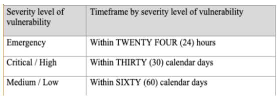
Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

S/N	Process Area	Requirement	Compliance	Vendor response
5.1.2	General Compliance	Ability to provide evidence of due diligence to relevant IT security standards (e.g. ISO 27001,Multi-Tier Cloud Security Standard)		
5.1	General Compliance	Ability to provide all information pertaining to the technical details and security limitations of the system		
5.1.4	General Compliance	Do you provide sufficient security controls to protect the System against unauthorised access, data loss, intrusion, malicious software infection, software vulnerability attacks, and hardware attack.		
5.1.5	General Compliance	Do you have adequate security controls to protect the System from unauthorized access, data loss, intrusion, malware infection, software vulnerability attacks, and hardware attacks?		
5.1.6	General Compliance	The tenderer shall ensure that are no security backdoors and loopholes exist in the system.		
5.1.7	General Compliance	The tenderer shall ensure that no unauthorised software or systems exist within the environment.		
5.1.8	General Compliance	Fully responsible for any security breaches resulting from insecure implementations, configurations, missing patches, negligence, insider attacks, or solution loopholes. Also responsible for rectification and all associated activities without any cost to the school.		
5.1.9	General Compliance	Do you implement controls to protect data at rest, data in motion and data in use		
5.1.10	General Compliance	Do you document the process, procedures and control measures		
5.1.11	General Compliance	Systems are resilient against known cyber-attacks and easily reconfigurable to respond to new and zero-day security threats that may arise.		

5.1.12	General Compliance	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 System.		

5.1.13	General Compliance	Do you maintain information system documentation and ensure these documentations are made avaialble during security risk analysis, security standards and policy implementation specific to the System.		
5.1.14	General Compliance	Only approved commercial cloud and SaaS providers shall be used if SaaS is proposed. Perform risk assessment on the proposed SaaS		
5.1.15	General Compliance	Do you have policy, procedures established and implemented to have versioning control for all related documentation?		
5.2.1	Responsibilities	The tenderer shall 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 approver.		
5.2.2	Responsibilities	The tenderer shall ensure that no unauthorised software or libraries are installed within the System.		
5.2.3	Responsibilities	The tenderer shall ensure that no security backdoors, loopholes or any form of mechanisms that allow unauthorised access are built into the System.		
5.2.4	Responsibilities	The tenderer shall ensure all software implemented is the latest most stable version. In the course of implementation, any patches or fixes shall be implemented. Any deviation will require further discussion with SAS		
5.2.5	Responsibilities	Do you have policy and procedures established and implemented to track, detail and rectify any security vulnerabilities affecting all System components (including but not limited to open-source products/libraries, commercial-off-the-shelf (COTS) products, underlying technologies and libraries).		
5.2.6	Responsibilities	The tenderer shall ensure that any login to the System for administrative or deployment purposes are only allowed from authorized source IP addresses in Singapore. All overseas logon and unauthorized IP addresses to the System for administrative or deployment purposes shall be denied.		
5.2.7	Responsibilities	Do you have policy and procedures established and implemented to ensure only necessary roles and responsibilities are able 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.		
5.3.1	Data Security	The tenderer 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 Tenderer shall propose and provide details on the encryption to be implemented for approval by SAS.		
5.3.2.1	Data Security	The tenderer 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	Data Security	Cryptographic implementations that have been certified (e.g. FIPS certification). The tenderer shall submit proof of such certifications (e.g.FIPS certification) as part of the Tender submission for evaluation, if available.		
5.3.2.3	Data Security	The Tenderer shall propose supported encryption standards.		
5.3.3	Data Security	The tenderer 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	Data Security	All digital certificates implemented within the System shall be digitally signed by a trusted and recognized Certificate Authority (i.e. no self-signed certificates).		
5.3.5	Data Security	Do you have policy and procedures established and implemented the security measures for the protection of cryptographic keys throughout its lifecycle, starting from key creation/generation, usage, backup, recovery, revocation to key destruction.?		

5.3.6	Data Security	Do you have policy and procedures established and implemented 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	Data Security	Ability to provide detailed description of the security measures and processes, including the storage and transmission encryption software to be used		
5.3.8	Data Security	The tenderer shall ensure that encrypted data will continue to be usable if the production System becomes unavailable or unusable.		
5.3.9	Data Security	Ability to segregate the production environment from non-production environments.		
5.3.10	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.		
5.3.11	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.		
5.3.12	Data Security	The tenderer 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	Data Security	Ability to work work with SAS to ensure 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	Data Security	The tenderer 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	Data Security	The tenderer shall ensure that data is accorded access rights based on the principle of least privilege throughout its life cycle.		
5.3.16	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.		
5.3.17	Data Security	Ability to propose data centres designed for the System with fully redundant subsystems and compartmentalized security zones.		
5.3.18	Data Security	The tenderer shall ensure data centres adhere to the strictest physical security measures: Multiple layers of authentication are required before access is granted to the server area; Critical areas require two-factor biometric authentication; Camera surveillance systems are located at critical internal and external entry points; Security personnel monitor the data centres 24/7; Unauthorised access attempts are logged and monitored by data centre security.		
5.3.19	Data Security	Ability to encrypt data at rest, data in motion and data in use.		
5.3.20	Data Security	Ability to 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.		
5.4.2	Security Hardening	Ability to 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	Security Hardening	Ability to 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; 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	Security Hardening	The tenderer shall ensure security hardening 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	Security Hardening	The tenderer shall ensure the packaging hardening is completed before the Commissioning Date.		
5.4.6	Security Hardening	Ability to 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.		
5.5.1	Vulnerability and Patch Management	Ability to 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	Vulnerability and Patch Management	Ability to implement tracking of expiry dates for all digital assets such as certificates,software licences, etc for renewal.		
5.5.3	Vulnerability and Patch Management	Do you sure any changes does not alter compliance to the security requirements?		
5.5.4	Vulnerability and Patch Management	The tenderer shall ensure developers and third-party Tenderers follow the established software development lifecycle and release management process to control the implementation of major changes.		
5.5.5	Vulnerability and Patch Management	Do you document and provide vulnerability and security patch management process to track of security vulnerabilities or all IT assets within the System, which include: Maintain and use the IT asset inventory as a source of truth for vulnerability tracking. Tracking of vulnerability alerts and assessing their applicability monthly or as required by SAS. Performing criticality review and testing. Conducting change management review. Planning for contingency or roll back. Implementing patches.		
5.5.6	Vulnerability and Patch Management	Ability to 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 patches and critical patches.SAS may inform the Tenderer of any advisories when available.		

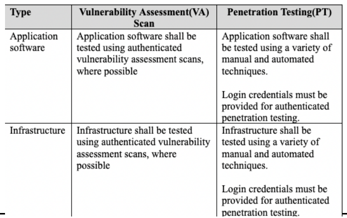
<table>
<tr><td>5.5.7</td><td>Vulnerability and Patch Management</td><td>Ability to notify and submit a request for change in a major security incident to deploy the fix</td><td></td><td></td></tr>
<tr><td>5.5.8</td><td>Vulnerability and Patch Management</td><td>Ability to remediate any vulnerabilities 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 ANNEX D- ERP Technical Requirement Specifications 5.5.8
<table><tr><th>Severity level of vulnerability</th><th>Timeframe by severity level of vulnerability</th></tr><tr><td>Emergency</td><td>Within TWENTY FOUR (24) hours</td></tr><tr><td>Critical / High</td><td>Within THIRTY (30) calendar days</td></tr><tr><td>Medium / Low</td><td>Within SIXTY (60) calendar days</td></tr></table></td><td></td><td></td></tr>
<tr><td>5.5.9</td><td>Vulnerability and Patch Management</td><td>The tenderer shall ensure that vulnerability assessment using industry recognised tools is performed on the System on a quarterly basis. (E.g. OWASP top 10)</td><td></td><td></td></tr>
<tr><td>5.5.10</td><td>Vulnerability and Patch Management</td><td>The tenderer shall ensure that Penetration Testing (PT) using industry recognised tools is performed on the System on a yearly basis.</td><td></td><td></td></tr>
<tr><td>5.5.11</td><td>Vulnerability and Patch Management</td><td>Ability to provide the Vulnerability Assessment and Penetration Testing (VAPT) post-assessment reports in detail for the System to SAS after every scanning.</td><td></td><td></td></tr>
<tr><td>5.5.12</td><td>Vulnerability and Patch Management</td><td>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.</td><td></td><td></td></tr>
<tr><td>5.5.13</td><td>Vulnerability and Patch Management</td><td>The Tenderer shall ensure that vulnerabilities identified through the VAPT are remediated before deploying the change to production of the System.</td><td></td><td></td></tr>
<tr><td>5.5.14</td><td>Vulnerability and Patch Management</td><td>Ability to perform the security scanning again after the remedial actions are taken to ensure all the vulnerabilities are resolved.</td><td></td><td></td></tr>
<tr><td>5.5.15</td><td>Vulnerability and Patch Management</td><td>Ability to implement measures to protect endpoint devices used for software deployment to mitigate risks of transferring malicious software (e.g. HIPS,EPP,EDR).</td><td></td><td></td></tr>
<tr><td>5.6.1</td><td>Authentication and Password Security</td><td>Ability to put in place strong authentication and access control mechanisms to ensure that only authorized users are granted access to controlled features (e.g. personalized views).</td><td></td><td></td></tr>
<tr><td>5.6.2</td><td>Authentication and Password Security</td><td>Ability to establish a 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.</td><td></td><td></td></tr>
<tr><td>5.6.3</td><td>Authentication and Password Security</td><td>Ability to implement the following features when using passwords (including service accounts):
Passwords to be made up of at least TWELVE (12) characters.
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.</td><td></td><td></td></tr>
<tr><td>5.6.4</td><td>Authentication and Password Security</td><td>The tenderer shall ensure generic authentication responses for login errors</td><td></td><td></td></tr>
<tr><td>5.6.5</td><td>Authentication and Password Security</td><td>Ability to implement strong multifactor authentication for all remote access and all administrative access 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).</td><td></td><td></td></tr>
<tr><td>5.6.6</td><td>Authentication and Password Security</td><td>Security measures in place to protect and ensure 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</td><td></td><td></td></tr>
<tr><td>5.6.7</td><td>Authentication and Password Security</td><td>The Tenderer shall ensure access to secrets is accorded the least privilege.</td><td></td><td></td></tr>
<tr><td>5.6.8</td><td>Authentication and Password Security</td><td>The tenderer shall ensure secrets used in production environments are not reused in non-production environments (such as development or test environments).</td><td></td><td></td></tr>
<tr><td>5.6.9</td><td>Authentication and Password Security</td><td>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.</td><td></td><td></td></tr>
<tr><td>5.6.10</td><td>Authentication and Password Security</td><td>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);
(d) Request Description;
(e). Request Reason/s.</td><td></td><td></td></tr>
<tr><td>5.6.11</td><td>Authentication and Password Security</td><td>The Requestor from the Tenderer who has the password of the root/administrator should not share with others.</td><td></td><td></td></tr>
<tr><td>*</td><td>Authentication and Password Security</td><td>Do you implement centralized security monitoring on privileged IDs to detect misuse of privilege and centralized logging to facilitate periodic review of privilege ID usage?</td><td></td><td></td></tr>
<tr><td>5.7.1</td><td>Infrastructure Security</td><td>Ability to 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.</td><td></td><td></td></tr>
<tr><td>5.7.2</td><td>Infrastructure Security</td><td>The Tenderer shall implement security control measures and procedures to prevent unauthorised access to system management consoles.</td><td></td><td></td></tr>
</table>

5.7.3	Infrastructure Security	Ability to implement controls to ensure that remote access to the System and network are not allowed by default unless it is justified and approved. Ability to 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. 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	Infrastructure Security	Ability to implement physical security control measures and procedures to prevent any unauthorised access to the System.		
5.7.5	Infrastructure Security	Ability to 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	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.		
5.7.7	Infrastructure Security	The tenderer shall ensure 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	Infrastructure Security	The tenderer shall ensure the latest definition files are installed into the System on a daily basis.		
5.7.9	Infrastructure Security	The tenderer shall take actions to prevent the spread of unauthorized codes and resolve incidents related to a virus outbreak, execution of malicious codes and recovery actions without additional cost to SAS.		
5.7.10	Infrastructure Security	Ability to 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	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.		
5.7.12	Infrastructure Security	Ability to implement Network Address Translation (NAT) to hide the internal IP addresses.		
5.8.2	Web 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 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	Web Application Security	Ability to 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	Web 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.		
5.8.5	Web Application Security	Ability to 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.		
5.8.6	Web 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.		
5.8.7	Web 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.		
5.8.8	Web 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..		
5.8.9	Web 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.		
5.8.10	Web Application Security	Ability to 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 authorized. The measures shall minimally include the following: Check access control permissions, whenever performing direct object references; Disable directory browsing; Authentication and authorization for each private page; Use of role-based authentication and authorization; Deny all access by default.		
5.8.11	Web Application Security	The tenderer 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	Web Application Security	The tenderer 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	Web Application Security	The tenderer shall ensure that all administration modules of the System are accessible only from pre-identified network addresses.		
5.8.14	Web Application Security	Ability to implement appropriate security mechanisms to protect the confidentiality and integrity of data transmitted from SAS's officers to the System, and within the System.		
5.8.15	Web 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.		

5.8.16	Web Application Security	The tenderer shall ensure that the System is secured and well protected against security attacks, including but not limited to the following: implement appropriate security mechanisms to protect the confidentiality and integrity of data transmitted from SAS's officers to the System, and within the System. Unauthorised access. Insecure API interfaces. Hijacking of accounts, services or traffic.		
5.8.17	Web Application Security	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	Web Application Security	The tenderer 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. Tenderer should propose the optimum approach.		
5.8.19	Web Application Security	The tenderer 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	Web 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 System development commences. If any attack is detected in the data, the incident shall be logged and communicated to SAS.		
5.8.21	Web 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 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	Web 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.		
5.8.23	Web Application Security	Ability to 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	Web Application Security	The tenderer shall ensure that the design of the System does not impose risks to the operations of SAS's existing computer networks.		
5.8.25	Web Application Security	Ability to 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	Web 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:
		
		Injection vulnerability flaws (e.g. SQL injection, command of injection etc);
		Cross Site Scripting (XSS);
		Broken access control;
		Broken authentication and session management (i.e. use of account credentials and session cookies);
		Insecure direct object references;
		Cross Site Request Forgery (CSRF);
		Security mis-configuration;
		Insecure cryptographic Storage;
		Failure to restrict URL access;
		Insufficient transport layer protection;
		Unvalidated redirects and forwards;
		Non-validated input;
		Buffer overflows;
		Improper error handling;
		Race conditions;
		Improper error/exception handling;
		Insecure storage;
		Denial of Service (DoS); and
		Insecure configuration management.		

5.8.27	Web Application Security	The tenderer shall ensure that the Application Software does not contain any hidden functionalities that SAS is not aware of.		
5.8.28	Web Application Security	The tenderer shall ensure all test data, test accounts and test credentials are removed from the System before commissioning.		
5.8.29	Web Application Security	Aibility to implement the notification message or banner displayed to user and CSP operation personnel before granting access to the System.		
5.8.30	Web Application Security	System shall display the key points equivalent to the following: Usage of service/system may be monitored, recorded, and subject to audit; Unauthorised use of the service/system is prohibited and subject to criminal and civil penalties; Use of the service/system indicates consent to monitoring and recording.		
5.9.1	Deployment Security	The tenderer 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 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.		
5.9.2	Deployment Security	Ability to 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.		

5.9.3	Deployment Security	The Tenderer shall conduct source code reviews using automated tools or peer reviews to uncover vulnerabilities.		
5.9.4	Deployment Security	Tenderer shall ensure any automated tools used include the following: Detection of Open Web Application Security Project (OWASP) Top 10 web application security risks; Scanning for Common Vulnerabilities and Exposures (CVEs) in libraries and open source codes; Highlighting areas that pose vulnerabilities and include possible resolutions; and Only allow deployments when security findings rated Medium and above are resolved.		
5.9.5	Deployment 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.		
5.9.6	Deployment Security	The tenderer shall perform automated testing of APIs before every release. (e.g. tools like Postman,SOAPUI).		
5.9.7	Deployment Security	Aiblity to integrate automated testing of APIs into the pipeline to ensure any code change won't break APIs in production.		
5.9.8	Deployment Security	The tenderer shall limit access to APIs to authorized users and systems only (e.g. IP whitelisting,machine whitelisting).		
5.9.9	Deployment Security	The tenderer shall provide documentation and publish a list of all Application Program Interfaces (APIs) utilized in the system and/or made available in the service and ensure best practices based on industry standards		
5.9.10	Deployment Security	The tenderer 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	Deployment Security	The tenderer shall implement a deployment pipeline for code release.		
5.9.12	Deployment Security	The tenderer shall integrate automated security testing into the code release process (e.g. IAST,SAST,DAST).		
5.10.1	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. Tenderer 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	Security Assurance	Ability to 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	Security Assurance	The tenderer shall seek SAS's approval where any deviations exist from the review. The Tenderer 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	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, VAPT is addressed before the Commissioning Date, at no additional cost to SAS.		
5.10.5	Security Assurance	The tenderer shall perform security tests on the System with the scope described in the table below: 		

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.

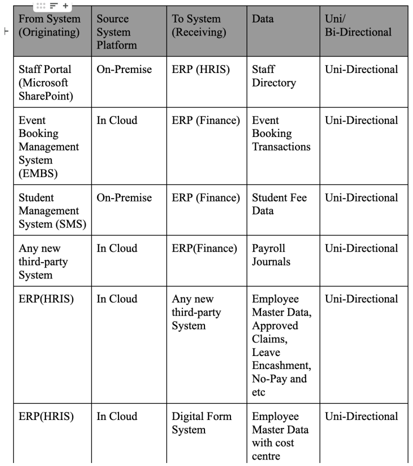
5.11.1	Access Management	Ability to implement Identity and Access Management for user account management.		
5.11.2	Access Management	The Tenderer shall propose an access control matrix for authorized users to the System for approval by SAS.		
5.11.3	Access Management	The tenderer shall ensure that access 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 system or user account not needed shall be deleted.		
5.11.4	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.		
5.11.5	Access Management	The tenderer shall disable login to multiple sessions using the same credentials		
5.11.6	Access Management	The tenderer shall implement account lockout after specific number of unsuccessful attempts as determined by SAS		
5.11.7	Access Management	The tenderer shall implement timeout or automatic logout feature to the System for non-active sessions.		
5.11.8	Access Management	The tenderer sall ensure that all system administrative or functional accounts are not shared.		
5.11.9	Access Management	The tenderer shall implement security controls to monitor privileged access and processes to ensure that system administrators, database administrators or other privileged users shall access SAS' system with approval. Ensure logs are reviewed to identify such unauthorised access		
5.11.10	Access Management	The tenderer shall ensure all successful and failed authentication events for access are logged.		
5.11.11	Access Management	The tenderer shall disable remote administrative access to the System if such access is not required.		
5.11.12	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 System.		
5.11.13	Access Management	The tenderer 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	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.		

5.11.15	Access Management	The tenderer shall implement ABAC using multiple attributes such as role,location,authentication method,IP address and mutual authentication.		
5.11.16	Access Management	The tenderer 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	Access Management	The tenderer shall ensure that the access control matrix for the system is established, roles and responsibilities are clearly documented.		
5.11.18	Access Management	Ability to implement an approval process and tracking mechanism for granting user access to the System.		
5.11.19	Access Management	Ability to 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	Access Management	The tenderer shall implement all of the following security measures if remote administration to server or applications is required: Remote administrative access shall only be granted to authorised personnel who need to perform administration on servers or applications remotely; Remote administrative access shall only be done by authorised personnel from specific systems and filtering based on IP address shall be implemented; 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; 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	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 System must be enforced.		
5.12.1	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.		
5.12.2	Incident Management	Provide technical SOPs 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 Technical SOP shall be reviewed minimally on an annual basis and approved by SAS.		
5.12.3	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.		
5.12.4	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 Technical 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.		
5.12.5	Incident Management	The tenderer shal inform SAS IT Security Incident Response (SITSIR) and personnel appointed by SAS required to deal with the IT security incidents.		
5.12.6	Incident Management	The Tenderer shall respond and report all security-related incidents and their status to SAS. In addition, the Tenderer 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	Incident Management	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	Incident Management	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.		
5.13.1	Security and Training Awareness	The tenderer shall ensure that all personnel assigned to this project are equipped with the relevant skills and experience to operate the System.		
5.13.2	Security and Training Awareness	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	Security and Training Awareness	The tenderer shall ensure that all employees are informed of their security responsibilities and accountability before assigning the person to their area of work before putting the person in his/her assigned areas of work.		
5.13.4	Security and Training Awareness	Ability to demonstrate that they have a comprehensive security program to train its personnel in security and their assigned role.		

ARCHITECTURAL

Due to the sheer number of functions in an ERP, it is not feasible, nor desirable, to exhaustively list all in the table below. This serves as a guide for a tenderer to provide more information.

<table>
<tr><th>S/N</th><th>Process Area</th><th>Requirement</th><th>Compliance</th><th>Vendor response</th></tr>
<tr><td>2.1.1</td><td>General Architecture Requirements</td><td>Ability to leverage the benefits of adopting cloud to fulfil business expectations such as availability, security, flexibility, scalability, performance, compliance and cost.</td><td></td><td></td></tr>
<tr><td>2.1.2</td><td>General Architecture Requirements</td><td>Ability to provide a loose coupling architecture design for the System.</td><td></td><td></td></tr>
<tr><td>2.1.3</td><td>General Architecture Requirements</td><td>Where there is a need for additional controls and governance to safeguard the integrity of the System, Ability to 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.</td><td></td><td></td></tr>
<tr><td>2.1.4</td><td>General Architecture Requirements</td><td>The System shall meet system availability requirements and recover any disruptions gracefully and on a timely basis</td><td></td><td></td></tr>
<tr><td>2.1.5</td><td>General Architecture Requirements</td><td>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.</td><td></td><td></td></tr>
<tr><td>2.1.6</td><td>General Architecture Requirements</td><td>The tenderer shall propose a To-Be System architecture design based on the functionalities of the proposed System?</td><td></td><td></td></tr>
<tr><td>2.2.1</td><td>Backup & Recovery Plan</td><td>Ability to 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.</td><td></td><td></td></tr>
<tr><td>2.2.2</td><td>Backup & Recovery Plan</td><td>Ability to provide a backup strategy with best industry practices for each type of data and the recommended retention and archival strategy to be used</td><td></td><td></td></tr>
<tr><td>2.2.3</td><td>Backup & Recovery Plan</td><td>Ability to conduct data recoverability testing to verify the effectiveness of backup and recovery plans.</td><td></td><td></td></tr>
<tr><td>2.2.4</td><td>Backup & Recovery Plan</td><td>Ability to 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.</td><td></td><td></td></tr>
<tr><td>2.2.5</td><td>Backup & Recovery Plan</td><td>The tenderer shall implement the same security safeguards in the alternative site as the primary site.</td><td></td><td></td></tr>
<tr><td>2.2.6</td><td>Backup & Recovery Plan</td><td>The tenderer shall ensure that backup data is protected through encryption and access controls.</td><td></td><td></td></tr>
<tr><td>2.3.1</td><td>System Integration</td><td>limited to:-

(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) DocHub for e-signature;
(e) Digital Form System (Using OutSystem)
(f) Google Authentication for user authentications.</td><td></td><td></td></tr>
<tr><td>2.3.2</td><td>System Integration</td><td>The System shall be able to integrate with third-party systems using APIs or connectors in the Cloud.</td><td></td><td></td></tr>
<tr><td>2.3.3</td><td>System Integration</td><td>Ability to assess and propose an appropriate interface design for implementation to facilitate integration and seamless end-to-end business process. Refer to 03 Part 2 ERP Technical Requirements Specification 2.3.3

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

Annex E :
PROJECT SCHEDULE

Project Schedule

Per Annex C, Point 3.6.7, SAS envisages the project to complete between 9 and 15 months.

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

Task	Duration (month)	2023					2024											
		Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Annex F :

PROPOSED PROJECT REAM 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. 2018 to 2022 (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

Annex G :
ERP TECHNICAL REQUIREMENT SPECIFICATIONS

ERP 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 Maintenance 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.

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:

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 in Clause 2.7.11.

1.8 Supported File Formats

1.8.1. 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 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-optimization design/solution of the data archival based on SAS needs. e.g.,the Contractor shall recommend 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 implement auto-scaling for archival storage solutions with pay-as-you-go pricing.

1.10.7. 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)

1.12.1 The System shall have the SSO feature to turn on to enable SAS to Single Sign On in multiple applications and systems using 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) DocHub for e-signature;
(e) Digital Form System (Using OutSystem)
(f) 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 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.

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	Uni-Directional

			Encashment, No-Pay and etc	
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 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.

(c) The complete itemised charges for all components of the proposed System including components that are not required immediately but may be needed to support service requests in the future.

3.1.2. 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 System 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”.

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 customization, 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 Managed Services 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:

(a) patch management process to be approved by SAS and patch management team.

5 IT SECURITY

5.1 General Compliance

5.1.1. The Contractor and/or 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-off-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 recognized 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 authorization 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 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;
(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 below:

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. 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 authorization for each private page;
(d) Use of role-based authentication and authorization;
(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 below:

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 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.

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

6.2.1 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 to implement Service Request (SR)

7.5.1 All accepted change requests shall be completed and implemented within the specified turnaround time depending on the estimated man-days required:

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 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.

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.

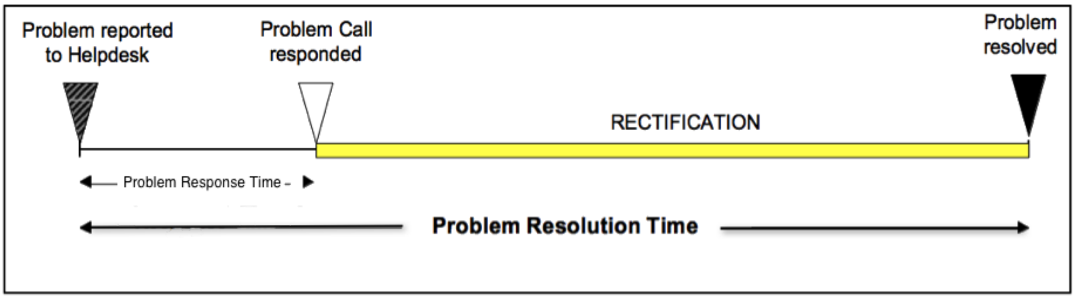


Illustration of Response Time and Problem Resolution Time

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:

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 days	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 will be deemed to be applicable to each **main** section, unless it is clearly stated to be otherwise, where C is for Compliance and NC is for Non-Compliance.

** Please indicate the specific items/points of non-compliance where applicable.

Specification	Compliance (C/NC)*	Explanatory Remark**
ANNEX A – ERP CONDITIONS OF CONTRACT		
1		
1.1		
1.2		
1.3		
1.4		
1.5		
2		
2.1		
3		
3.1		
3.2		
3.3		
4		
4.1		
4.2		
4.2A		
4.3		
4.4		
4.5		
5		
5.1		
5.2		
5.3		
6		
6.1		
7		
7.1		
7.2		
8		
8.1		
8.2		
8.3		
8.4		
8.5		
8.6		
8.7		
9		
9.1		
9.2		
9.3		
9.4		
9.5		
9.6		
10		
10.1		
10.2		

Specification	Compliance (C/NC)*	Explanatory Remark**
11		
12		
12.1		
12.2		
12.3		
12.3.1		
12.3.2		
12.4		
12.4.1		
12.4.2		
12.5		
12.5.1		
13		
13.1		
13.1.1		
13.1.2		
13.1.3		
13.1.4		
13.2		
13.3		
13.4		
16		
16.1		
16.2		
21		
21.1		
22		
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		
22.5		
22.6		
22.6.1		
22.6.2		
22.6.3		
22.6.4		
22.6.5		
22.7		
22.7.1		
22.8		
22.8.1		
22.8.2		
23		
23.1		
23.2		
23.3		
23.4		

Specification	Compliance (C/NC)*	Explanatory Remark**
23.5		
24		
24.1		
24.2		
24.3		
24.4		
24.5		
24.6		
24.7		
24.8		
25		
25.1		
25.2		
25.3		
25.4		
25.5		
25.6		
27		
27.1		
27.2		
27.3		
28		
28.1		
28.2		
28.3		
30		
30.1		
30.2		
30.3		
30.4		
31		
31.1		
32		
32.1		
33		
33.1		
33.2		
33.3		
33.4		
33.5		
33.6		
33.7		
33.8		
33.9		
34		
34.1		
34.2		
34.3		
34.4		
35		
35.1		
35.2		
36		
36.1		
36.2		
37		

Specification	Compliance (C/NC)*	Explanatory Remark**
37.1		
37.2		
37.3		
39		
39.1		
39.2		
39.3		
39.4		
39.5		
39.6		
39.7		
39A		
39A.1		
39A.2		
40		
40.1		
40.2		
41		
41.2		
42		
42.1		
42.2		
42.3		
42.4		
42.5		
43		
43.1		
44		
44.1		
45		
45.1		
47		
47.1		
48		
48.1		
48.2		
48.3		
48.4		
48.5		
48.6		
48.7		
48.8		
48.9		
48.10		
48.11		
49		
49.1		
49.1.1		
49.1.2		
49.1A		
49.1A.1		
49.1A.2		
49.2		
49.2.1		
49.2.2		
49.2.3		

Specification	Compliance (C/NC)*	Explanatory Remark**
49.2.4		
49A		
49A.1		
49A.2		
49A.3		
49A.4		
49A.5		
49A.6		
50		
50.1		
50.2		
50.3		
50.4		
50.5		
50.6		
50.7		
52		
52.1		
53		
53.1		
54		
54.1		
54.2		
54.3		
54.4		
55		
55.1		
55.2		
55.3		
56		
56.1		
58		
58.1		
58.2		
58.3		
59		
59.1		
59.2		
59.3		
60		
60.1		
60.2		
ANNEX C – ERP FUNCTIONAL REQUIREMENT SPECIFICATIONS		
1.		
1.1		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
2.1.		
2.2		
2.3		
3		
3.1		
3.2		
3.3		
3.4		
3.5		
3.6		
3.6.1		
3.6.2		
3.6.3		
3.6.4		
3.6.5		
BPR PHASE		
i		
ii		
iii		
Project Execution Phase		
iv		
v		
vi		
vii		
vii		
ix		
x		
xi		
3.6.6		
3.6.7		
3.6.8		
3.6.9		
3.6.10		
3.6.11		
3.6.12		
3.6.13		
3.7		
4		
4.1		
4.1.1		
4.1.2		
4.1.3		
4.1.4		
5		
5.1		
5.2		
5.2.1		
5.2.2		
5.2.3		
5.2.4		
5.2.5		
5.2.6		
5.2.7		
5.2.8		
5.2.9		

Specification	Compliance (C/NC)*	Explanatory Remark**
5.2.10		
5.2.11		
5.2.12		
5.2.13		
5.2.14		
5.2.15		
5.2.16		
5.2.17		
5.2.18		
5.2.19		
5.2.20		
5.2.21		
5.2.22		
5.2.23		
5.2.24		
5.2.25		
5.2.26		
5.2.27		
5.2.28		
5.2.29		
5.2.30		
5.2.31		
ANNEX G – ERP TECHNICAL REQUIREMENT SPECIFICATIONS		
1		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
1.6		
1.6.1		
1.6.2		
1.7		
1.7.1		
1.7.2		
1.7.3		
1.8		
1.8.1		
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		
1.10.7		
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		
1.12.1		
2		
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		
3.1		
3.1.1		
3.1.2		

Specification	Compliance (C/NC)*	Explanatory Remark**
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		
3.2.4		
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		
5.1		
5.1.1		
5.1.2		
5.1.3		
5.1.4		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
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		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
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		
5.7.2		
5.8		
5.8.1		
5.8.2		
5.8.3		
5.8.4		
5.8.4		
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		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
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		
5.12.6		
5.12.7		
5.12.8		
5.13		
5.13.1		
5.13.2		
5.13.3		
5.13.4		
6		
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		

Specification	Compliance (C/NC)*	Explanatory Remark**
6.2.1		
7		
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 ________________ 2022.

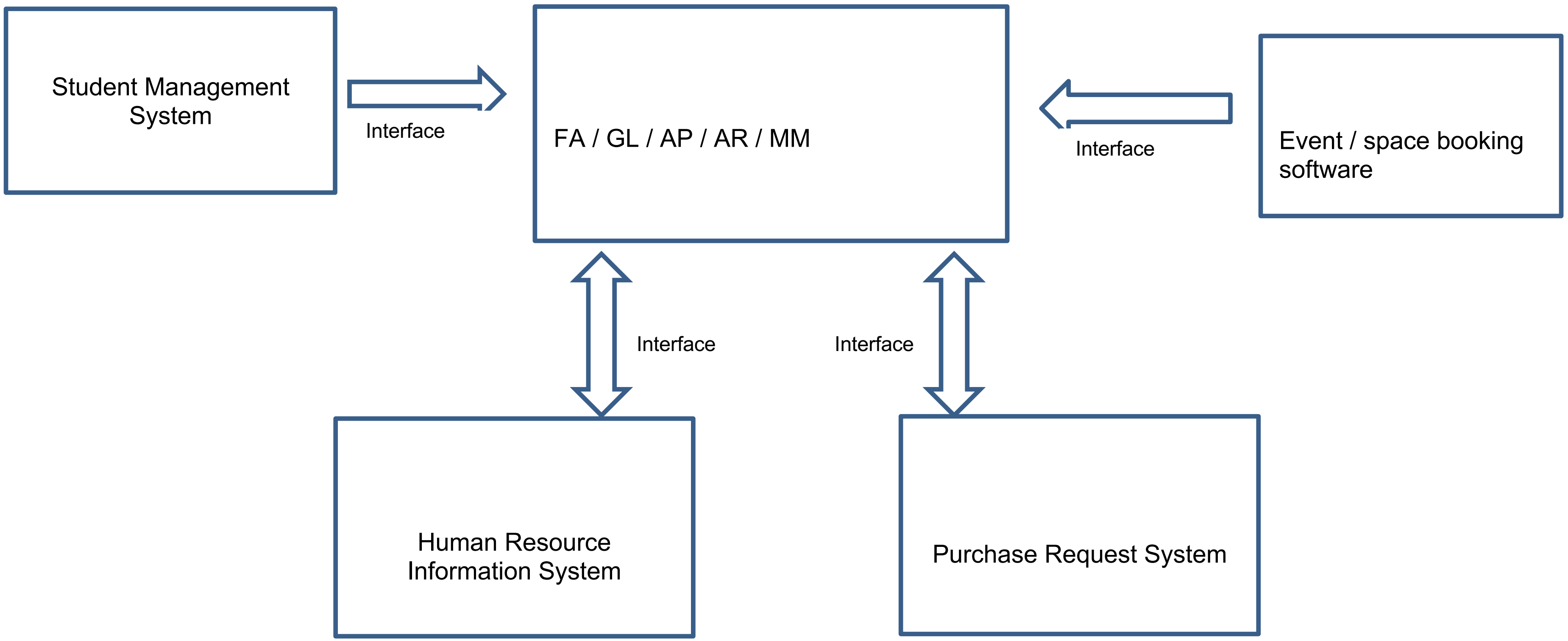
NAME AND SIGNATURE (AUTHORISED REPRESENTATIVE)	: ______________________	NAME (WITNESS)	: ______________________
DESIGNATION (AUTHORISED REPRESENTATIVE)	: ______________________	DESIGNATION (WITNESS)	: ______________________
DATE	: ______________________	DATE	: ______________________

COMPANY STAMP : ____

COMPANY NAME : ____

APPENDIX A:
HIGH-LEVEL CURRENT CORPORATE SYSTEM LANDSCAPE

High-level current corporate system landscape


Student Management System
Interface
FA / GL / AP / AR / MM
Interface
Event / space booking software
Interface
Interface
Human Resource Information System
Purchase Request System