SBM Bank (Mauritius) Ltd

Request for Proposal

Printing, Mailing & Franking Equipment

23rd January 2026

Disclaimer

The information contained in this Request for Proposal (RFP) document or information provided subsequently to service provider(s) or applicants whether verbally or in documentary form by or on behalf of SBM Bank (Mauritius) Ltd, is provided to the service provider(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by SBM Bank (Mauritius) Ltd to the interested parties for submission of proposals. The purpose of this RFP is to provide the service provider(s) with information to assist with the formulation of their proposals. This RFP does not claim to contain all the information each service provider may require. Each service provider should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. SBM Bank (Mauritius) Ltd makes no representation or warranty as to the correctness or completeness of the information contained herein and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP.

SBM Bank (Mauritius) Ltd may in its absolute discretion, but without being under any obligation to do so, update, amend the terms of, or supplement the information in this RFP. In addition, further information may be sought from all or any of the service provider(s) whether before or post the RFP deadline.

Contents

INTRODUCTION

This is a Request for Proposal (RFP) issued by SBM Bank (Mauritius) Ltd, referred to as 'the Bank' or 'SBM' throughout this document. SBM is hereby inviting your company to submit its written proposal with regards to products/services required under this RFP.

This Request for Proposal exercise aims at selecting a supplier with proven track record, experience, and capability in the **Supply, Installation, Configuration and Maintenance of a Statement Printing, Mailing and Franking Solution.**

It is part of a competitive procurement process to enable SBM to assess suppliers both in financial and qualitative terms. At the same time, it provides suppliers with a fair opportunity for their services to be considered. With this structured tender process in place, SBM aims at obtaining the best value from suppliers.

In addition to highlighting the best alternative for SBM, this evaluation will increase SBM's confidence in, and understanding of the product that will be implemented, and the effort required to perform the implementation.

For ease of reference, this RFP is structured as follows:

- Section 1 – Company Overview
  This section provides an overview of SBM company profile.

- Section 2 – SBM Bank (Mauritius) Ltd Requirements
  This section provides SBM's functional and technical service provider requirements. It also outlines the financial costing of this RFP.

- Section 3 – Service provider Response
  This section outlines the instructions to the service provider in responding to this RFP.

- Section 4 – General Information About this RFP
  This section provides general information on the RFP.

- Section 5 – Terms and Conditions
  This section highlights the normal terms and conditions along with the Service Level Agreement required by SBM.

- Section 6 – Evaluation and comparison of proposals
  This section highlights the method SBM will use to evaluate proposals.

1 COMPANY OVERVIEW

SBM Bank (Mauritius) Ltd (''Bank'' or ''Company'') is the flagship of SBM, a leading financial services Group in Mauritius. SBM's journey started in 1973, with the primary goal of making financial services accessible to a larger share of the population, both urban and rural, in Mauritius. It provides all services of a universal bank within a diversified business model. The lines of business include Retail Banking, Small and Medium Enterprises, Wealth Management & Private Banking, Corporate Banking and International Banking & Global Business, Treasury services, eBusiness, Fiduciary services, Asset Financing, Stockbroking and Asset Management.

The Bank makes use of Information Technology to meet its business objectives and strategies.

Further information on SBM can be obtained from our website: https://www.sbmgroup.mu

2 SBM REQUIREMENTS

2.1 *BACKGROUND*

SBM Bank (Mauritius) Ltd (SBM) operates critical printing and mailing facilities through its Medcor Unit and Operations Processing Centre (OPC). These facilities are responsible for the production and distribution of customer statements, PIN mailers, regulatory notices, and other high-volume communications essential to customer services and regulatory compliance.

The existing printing and mailing infrastructure is nearing the end of its contractual and operational lifecycle. In addition, the current solution will not be retained at its present site, as the Bank contemplates to relocate these operations to a new location. This transition provides an opportunity to modernize the Bank's printing and mailing platform, ensuring scalability, resilience, and compliance with evolving business and regulatory requirements.

In recent years, transaction volumes have increased significantly, driven in part by the adoption of SBM TAG and other digital payment channels. This has created added demand on printing and mailing operations. At the same time, the Bank is pursuing a progressive digital transformation strategy, with a focus on increasing adoption of e-Statements and reducing dependency on physical printing.

The Bank therefore requires an enterprise-grade, future-proof solution that addresses the dual imperatives of:

- Ensuring continuity of critical operations during the transition to the new location, including support and maintenance over the interim period; and
- Deploying a modern, secure, and scalable printing and mailing platform at the new site, with support for hybrid models (physical and electronic statements), integration with existing operational systems, and compliance with Bank of Mauritius guidelines.

2.2 *PROJECT OBJECTIVES*

The objective of this RFP is to engage with a qualified vendor to provide a complete, future-proof Printing and Mailing Solution that meets the Bank's operational, regulatory, and strategic needs.

The key objectives are:

1. High-Volume Capability
   - Ensure the solution can support peak workloads, including printing up to 1.1 million pages within 10 consecutive days and mailing up to 50,000 envelopes per day.
2. Secure and Compliant Operations
   - Provide tamper-proof workflows for PIN mailers and other sensitive communications.
   - Ensure compliance with Bank of Mauritius guidelines, data protection standards, and internal security requirements.
3. Automation and Efficiency
   - Automate end-to-end printing and mailing processes (folding, inserting, sealing, franking, handling returned mail).
   - Minimize manual intervention while ensuring operational accuracy and reliability.
4. Digital Transformation Alignment
   - Support a hybrid operating model with both physical printing/mailing and electronic statement delivery.
   - Provide tools to monitor and progressively increase adoption of e-Statements.
5. Service and Lifecycle Support
   - Provide a 10-year service contract with back-to-back OEM support for all equipment.
   - Deliver SLA-backed preventive and corrective maintenance, with local spare parts and consumables availability.
   - Ensure support coverage during critical operational windows (end-of-day, end-of-month, regulatory cut-offs).
6. Resilience and Availability
   - Deploy the solution in an active-active configuration with minimal single points of failure.
   - Provide clear room specifications and remediation requirements for the new facility.
7. Futureproofing
   - Present a clear 3–5 year roadmap for modernization, including franking machine upgrades and process optimization.
   - Provide a cost-based analysis comparing pre-printed vs. blank paper over a 10-year horizon.
   - Support modular scalability to accommodate growth in volumes and features.

2.3 *FUNCTIONAL REQUIREMENT*

The functional requirements outlined in this section represent the minimum capabilities expected of the proposed Printing and Mailing Solution. Bidders are required to provide a detailed response against each requirement, indicating whether their solution is Compliant, Non-Compliant, or Partially Compliant, and must supply supporting documentation, references, and clarifications where applicable.

The Bank expects the proposed solution to:

- Support end-to-end printing and mailing operations required by the Bank's Operations Teams.
- Ensure high-volume capacity, resilience, and consistent performance during peak periods.
- Provide secure workflows for sensitive communications, including customer statements, PIN mailers, and regulatory notices.
- Enable automation of mailing processes, including folding, inserting, sealing, franking, and handling of returned mail.
- Offer a modular and scalable design, capable of adapting to future growth and new business requirements.
- Deliver a complete, integrated solution covering printing, mailing, and franking, with operational dashboards and reporting tools.

All functional requirements have been captured based on the Bank's operational needs. Bidders must demonstrate how their proposed solution meets or exceeds these requirements and provide a clear mapping in their responses.

2.3.1 Printing Functional Requirements

The proposed solution must meet the following printing requirements:

- CMYK coloured heavy-duty printer.
- Ability to print 1,100,000 pages within 10 days for peak periods (10% growth factored over the years).
- Where multiple printers are proposed, vendors must provide a graphical representation showing the relationship between number of printers and number of days required to complete the printing workload. Separate graphs must be included for simplex and duplex printing.
- Capability to print high-quality colour marketing campaigns on statements (replacing inserts/flyers), including header printing and charts (e.g., customer product utilization).
- Support for printing cheque images in grey scale.
- Printer must support multiple paper types:
  - 11" x 9.5"
  - Letterhead
  - A4
  - A3
- Duplex printing supported (flip on Long Edge). Vendor must specify the impact on printing speed when duplex mode is used.
- Cut sheet feed only.
- Support for multiple formats including PDF, PCL, PostScript, Pictures, ASCII, and others.
- Expected print ratio: 20% colour, 80% mono.
- Printers are expected to remain in service for up to 10 years. Proposals must include full maintenance support for this period.
- Bidders must provide detailed technical specifications for the proposed equipment, including but not limited to:
  - Print speed (pages per minute)
  - Image resolution (dpi)
  - Average monthly print volume
  - Duty cycle
  - Media weight support
  - Machine uptime (hours of continuous operation per day)

(For reference: current equipment in use – Xerox 1000, 100 ppm, 2400 x 2400 dpi, 100k monthly volume, media weight up to 350 gms, 12-hour daily uptime.)

2.3.2 Mailing Functional Requirements

- The proposed solution must meet the following mailing requirements:
- Support for multiple envelope types: DL, DLE, C4, C5, and C6 (optional).
- Capability to process 50,000 envelopes in a single day during peak periods.
- Must support cut sheet input source.
- Folding capabilities: Z-fold, C-fold, and no-fold, depending on the number of pages and envelope size.
- Ability to split and merge multiple pages into envelopes, based on OMR marks, barcodes, QR codes, and 2D/3D codes.
- Operator must be able to select envelopes by:
  - Number of pages per customer
  - Envelope type
  - Envelope size
- Capability to insert up to two collaterals into envelopes (A4, A5, A6).
- Collaterals must be folded automatically according to envelope selection.
- Equipment Specifications (minimum):
  - Cycling speed: 3,000 – 5,000 envelopes per hour
  - Multisheet speed: 1, 2, or 3 sheets
  - Support for A3 feeders

  - Maximum sheets per envelope: 10 sheets
  - Maximum packing thickness: based on paper weight
  - Maximum insert thickness: based on collateral weight
  - Number of feeders: 3 (1 main feeder and 2 insert feeders)
  - Lifecycle: 10 years
  - A4 feeder capacity: 5,000 sheets
  - Envelope feeder capacity: 2,000 envelopes
- Data encryption for communication with Mauritius Post and any connected systems.
- User authentication to control access to franking operations and configuration.
- Audit trail and activity logs capturing all transactions, configuration changes, and user actions for traceability and compliance.

2.3.3 Franking Machine Functional Requirements

The proposed solution must address the Bank's franking requirements and provide a modernized, scalable alternative to the current setup. Vendors must demonstrate compliance with the following:

- Current Setup
  - IJ140 – Attached to mailing machine; franks 3,000–5,000 letters per hour.
  - IJ80 – Standalone machine; franks up to 2,000 letters per hour, supporting:
    1. Envelope sizes from DL to A3.
    2. Envelope weights from 20 grams to 1,000 grams.
    3. Franking for different regions worldwide.
  - Both machines connect directly to the Mauritius Post server via telephone line.
  - Funds replenishment performed online.
- Functional Requirements
  - Must support automatic variable stamping based on envelope weight, size, and region.
  - Throughput must be equivalent or higher than the IJ80/IJ140 machines.
  - Must integrate with mailing machine workflows for high-speed runs.
  - Must support digital replenishment (minimum 7 digits) and be upgradeable to new online methods.
  - Must ensure full compliance with Mauritius Post standards and allow for future adaptability.
  - Expected lifecycle: 10 years, with OEM-backed support.

2.3.4 Overall Solution Requirements

The proposed solution must meet the following overall requirements:

- The complete printing and mailing process must be completed within 10 days.
- Option to streamline the printing and enveloping processes without manual intervention (optional feature).
- A central dashboard must be provided to track the overall process, display status, and allow for online reporting.
- The solution must be modular, with the ability to:
  - Add additional modules to accommodate increased printing and mailing requirements.
  - Switch modules between machines as required.
  - Scale horizontally or vertically to benefit from new features.
- Bidder must ensure availability of qualified resources for the maintenance of the proposed solution.
- The proposed solution must be a complete end-to-end system covering printing, mailing, and franking.

2.3.5 Infrastructure & Hosting (Virtualization) Requirements

- All solution servers must be deployed as virtual machines (VMs). Physical appliances are not allowed unless justified.
- Supported hypervisors: VMware vSphere/ESXi, KVM, Nutanix AHV.
- Bidder must confirm compatibility with at least one of the above and declare any platform dependencies.
- Solution must support:

  - High Availability (live migration, clustering)
  - Disaster Recovery (RTO/RPO, replication method)
  - Backup & restore via hypervisor APIs (e.g., VADP, AHV PD, KVM agents)
  - Network segmentation (management, app, data)
  - Security controls (OS hardening, TLS 1.2+, MFA admin, SIEM logging)
  - Monitoring metrics (CPU, RAM, storage, network, app KPIs) must integrate with SBM's monitoring tools – PRTG.
  - OS compatibility: Windows Server 2022 and RHEL 9.x
- Bidder to provide:
  - VM sizing specs (CPU, RAM, storage, IOPS)
  - DR/backup runbooks
  - Compliance mapping (BoM CTRM, ISO 27001, PCI DSS, CIS).

2.3.6 Non-Functional Requirement

The proposed solution must also meet the following non-functional objectives:

- The setup must cater for an active-active configuration, ensuring high availability and redundancy.
- Single points of failure must be minimized and clearly identified in the proposal.
- Latency must be reduced throughout the entire statement generation and combination process.
- Bidders should review the logic of the statement generation and combination process and propose improvements where applicable.
- Each bidder must provide a cost-based analysis comparing the use of pre-printed (with SBM logo) paper against blank paper for their proposed solution over a 10-year period.
- Each bidder must provide the throughput speed of the mailing machine and digital franking equipment.
- The solution will be a greenfield implementation in a new work environment. Bidders must:
  - Provide all necessary room specifications (power, space, HVAC, etc.) required to support the proposed equipment and committed service levels.
  - Document any room remediation requirements as part of their proposal.
- Bidders should address the Bank's sustainability objectives. Final requirements from the Sustainability Team will be shared and must be incorporated into the solution.

2.4 *SUPPLIER SCOPE OF WORK & SLA*

The selected vendor will be responsible for the full implementation, operation, and support of the Printing and Mailing Solution, including the following:

2.4.1 Solution Supply & Deployment

- Supply, delivery, installation, and commissioning of heavy-duty printers, mailing machines, and franking equipment.
- Capacity to print 1,100,000 pages within 10 days during peak demand periods.
- Capability to mail 50,000 envelopes per day, supporting DL, DLE, C4, C5, and C6 formats.
- Integration with statement generation processes and Bank systems (including 2D/3D code recognition).
- Compliance with Mauritius Post standards for franking.

2.4.2 Operational Capabilities

- Secure PIN mailer workflows, with tamper-proof sealing and full audit trails.
- Process dashboards for monitoring, tracking, and reporting of operations.
- Modular design allowing scaling and reconfiguration of modules between machines.
- Automation options to minimize manual intervention in print-to-mail workflows.

2.4.3 Service & Support

- Comprehensive 10-year service contract covering hardware and software.
- Back-to-back OEM support for all equipment.
- SLA-backed corrective and preventive maintenance, aligned to critical operational periods.
- Local spare parts and consumables availability.
- End-user and administrator training, including manuals and documentation.

2.4.4 Non-Functional Requirements

- Active-active deployment for high availability and redundancy.
- Minimal single points of failure, with clear risk documentation.
- Room specifications (power, HVAC, space, safety) and remediation requirements.
- Optimized statement generation and combination process, with reduced latency.
- Sustainability requirements (to be finalized with the Bank's Sustainability Team).

2.4.5 Roadmap & Futureproofing

- Roadmap for 3–5 year modernization and upgrades, including franking enhancements.
- Cost-based analysis comparing pre-printed vs. blank paper for 10 years.
- Support for hybrid operations (physical + e-Statements).

2.4.6 Application Hosting, Database & Maintenance

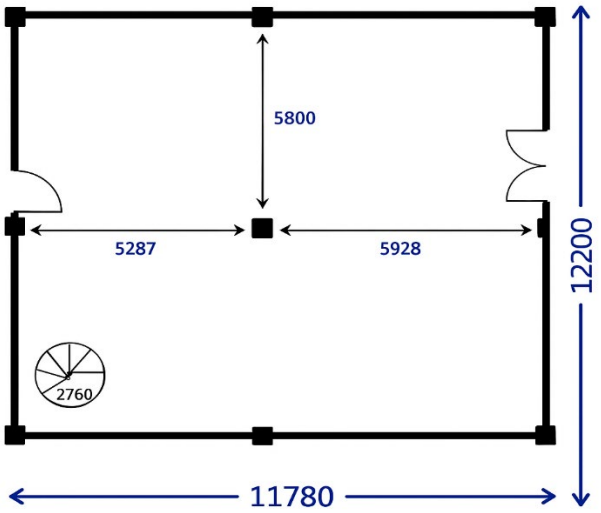
- All application and database components must be deployed on virtual machines (VMs) running on the Bank's supported hypervisors (VMware vSphere, KVM, Nutanix AHV).
- Selected bidder to perform installation, configuration, and commissioning of all solution software (application servers, middleware, and databases).
- Database setup must include:
- High availability design (clustering/replication)
- Backup/restore integration with Bank's enterprise backup systems
- Security hardening (access controls, encryption, audit logging)
- Selected bidder to provide ongoing software patching, upgrades, and preventive maintenance throughout contract duration, with alignment to the Bank's change management processes.
- Monitoring metrics (app availability, DB performance, error logs) must integrate with the Bank's existing monitoring/observability tools.
- Complete documentation and handover runbooks for VM builds, application services, and DB maintenance must be delivered.
- All databases must support patching, upgrades and compatible with CSI hardening up to bank's standard.

2.5 *SECURITY REQUIREMENTS*

The proposed solution must comply with the Bank's security policies, regulatory obligations, and industry best practices. Bidders must clearly demonstrate how their solution addresses the following requirements:

2.5.1 Site Location and Space Allocation

- The Bank has identified and allocated a new facility to host the Printing, Mailing, and Franking operations. The site plan and room dimensions of the new space are included in this RFP to assist bidders in assessing equipment placement, environmental requirements, and operational layout.



- Bidders shall design their proposed setup based on the provided site layout and measurements, ensuring proper equipment spacing, workflow efficiency, and compliance with power, HVAC, and safety standards. Any additional space or environmental requirements beyond those provided must be clearly indicated in the vendor's proposal.

2.6 *IT SECURITY REQUIREMENTS:*

Bidders are required to read the attached SBM's IT Security requirements and fill the different requirement forms and advise whether they comply to each requirement.

SBM - Application Onboarding Checkli

Cloud Risks and Security Checklist.xls

2.7 *SERVICE LEVEL AGREEMENT*

The following SLA to govern the agreement with the selected bidder.

Service Levels	**Response Time**	**Resolution Time**
Severity 1 A severity one (1) issue is a catastrophic production problem which may severely impact the production systems, or in which production systems are down or not functioning.	Within 30 minutes	Within 4 hours
Severity 2 A severity two (2) issue is a problem where the system is functioning but in a reduced capacity. The situation is causing significant impact to production and potential impact on service level.	Within 30 minutes	Within 8 hours
Severity 3 A severity three (3) issue is a medium-to-low impact problem which involves partial non-critical functionality loss. One which impairs some operations but allows the client to continue to function.	Within 4 hours	Within 3 business days
Severity 4 A severity four (4) issue is for a general usage question or recommendation for a future product enhancement or modification.	Within 4 hours	Within 5 working days

There is no impact on the quality, performance, or functionality of the product.		

Service Provider must provide the following evidence as part of its proposal submission: -

- **Manufacturer Tie-up:** Require proof of a formal, long-term partnership or distributorship with an established, enterprise-grade equipment manufacturer for both the high-speed printer and the enveloping/inserting and franking system.
- **Local Support:** Mandate a minimum 10-year service and support contract, detailing local spare parts inventory, certified technical team size, and guaranteed response/fix times.
- **High-Volume Experience:** Submit case studies or references for similar high-volume statement printing and enveloping solutions implemented and supported locally, in the region or globally.
- **Variable Data/Security:** Ensure the solution addresses variable data printing, integrity checking, and security/audit trails required for transactional documents.

Service Provider must submit a proposed Service Support and Service Level Agreement along with the submission.

2.8 *PROJECT MANAGEMENT*

The service provider will be required to setup a dedicated project team who will report to SBM Project Manager to drive this project end-to-end till stabilization period of the solution aligning to project management standards and who will be responsible to deliver the documentations listed below: -

Project Stage	Deliverables
• A. Signature of Agreement	Project Plan Project Schedule Project Approach Document Project team Constitution Work Breakdown Structure Responsibility Assignment Matrix Status Report
• B. Implementation	Architecture Diagrams or any other required documentations related to this implementation whenever requested Testing Approach Document Test Environment Setup End User & IT Training Data Migration Document Security vulnerabilities fix and release if any Production & Recovery environments Setup Status Report
• C. Closure	Status Report Project closure sign-off Minutes of meetings

2.9 *ADDITIONAL INFORMATION*

The service provider is welcome to provide any additional information that will help to provide a better understanding of its proposed solution and of its relevance to SBM's requirements. This information must be provided in the Solution Response in such a manner that it is easily understood in relation to the RFP. The service provider must be available to discuss the solution proposed by phone and/or email.

2.10 *EOSL*

- Solution proposed within the scope of this RFP should not have any end of support announced at the time of commissioning.
- Solution should have full active support for at least 10 years at the time of commissioning.

2.11 *COST REQUIREMENTS*

The proposed quote should include software, license, installation, configuration, customization, development of new interfaces, testing, training, commissioning, operation, and any other items required. The service provider should provide a complete solution either based on an OPEX or CAPEX model, with maintenance and support cost over 5 years.

The quote should be in MUR and fixed for the period the proposal is valid and should not be affected by any fluctuations for a period of 6 months. Bidders to use the template spelt out below for formulating their financial offer. Detailed cost breakdown to be provided under each subtitle.

		Year 1		Recurring cost								
Item	**Qty**	**Unit cost**	**Total Cost**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Year 6**	**Year 7**	**Year 8**	**Year 9**	**Year 10**
A. Software License												
B. Hardware												
C. Implementation Fee												
D. Professional Services												
Total:												
VAT												
Total VAT Included:												

The following details need to be provided: -

- The Service Provider to provide full cost requirements as regards hardware, software, license, installation, testing, commissioning, and any other items required.
- Costing should be broken down yearly under Initial Costs and Maintenance Costs before VAT, and after VAT, if applicable
- List of consumables, respective yield and associated pricing to be submitted.
- The terms of payment & Warranty period
- Applicable taxes
- Cost schedules should specify the total amount and terms/schedule of payment.
- It should follow a tabular format and in the same sequence as the stated requirements and supported by an Excel document as far as possible.

Initial Costs

Initial costs should include one-time cost that will not be re-incurred in the future as follows: -

- Hardware
- Software license if any
- Implementation fee
- Training
- Any requirement of 3rd party License
- Any other additional items required

Maintenance Costs

SBM expects that the annual cost includes all the minor, major upgrades, versions upgrades of the software. Unforeseen costs will not be accepted.

The service provider is expected to elaborate on its upgrade process to demonstrate the benefit of such upgrades to the bank.

Bidders should submit their offer alongside a proposal for maintenance and support services for a period of ten (10) years during and post the warranty period.

Licensing Requirements

The service provider must disclose all licenses used on the project, if any. Any licenses procured are owned by the bank. In case the service provider is the vendor of the solution, the licensing details must be specified and include any upgrades, minor as well as major for future compatibility.

The following details should be provided for each product: -
- Licensing structure (Cost structure and dependencies).
- Any other relevant information

Confirmation of the above is expected in writing in the response to the RFP.

All licensing requirements will be done to include the parent company of the bank (currently called SBM Holdings Ltd) as well as all Group entities.

Other Requirements

In addition, the proposal should include the following:
- The guarantees given by your company against substantial future price increase, particularly in relation to support, upgrade to new releases/ versions, and increase in the number of sites.
- Protection offered by your company in the event of inadequate support or withdrawal of your company from the market.
- Maximum increase % in support/product maintenance after duration of initial contract.
- Solution version lifetime and duration of support of previous versions.

Supplier Eligibility:-

To ensure participation from competent and experienced service providers, only suppliers meeting the following minimum eligibility criteria will be considered for technical evaluation. Bidders failing to meet any of the requirements below shall be disqualified without further assessment.

Eligibility Criteria	Requirement	Supporting Documents Required
Manufacturer Authorization	The bidder must provide a valid Manufacturer Authorization Form (MAF) for all proposed hardware and software components, confirming OEM backing for supply, warranty, and post-sales support.	OEM-issued MAF covering all proposed components.
Relevant Experience	The bidder must have successfully completed at least two (2) similar large-scale printing, mailing, and franking solution implementations, preferably in the banking or financial sector within the last five (5) years.	Reference letters or completion certificates with client contact details.
Certified Personnel	The bidder must have a minimum of three (3) certified engineers or technicians trained on the proposed equipment and solution stack.	CVs and valid certification copies.
Financial Stability	The bidder must demonstrate financial soundness and profitability over the last three (3) financial years.	Audited financial statements for the last three (3) years.
Local Presence and Support	The bidder must maintain a local service and support presence in Mauritius with access to spare parts and on-site intervention capability.	Address and structure of local service/support centre.

3 SERVICE PROVIDER RESPONSE

3.1 RESPONSE CONTENT

By responding to the RFP, the applicant agrees and will commit in writing.

The response should be as clear and concise as possible while providing all information necessary to understand the feature or procedure being described.

Applicant(s) are requested to carefully examine the RFP Documents and the terms and conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy between any of the RFP documents, they should forthwith refer the matter to SBM for necessary clarifications.

To facilitate consistent evaluation and understanding of the response, we request that the following guidelines be adhered to:

- It should follow a tabular format and in the same sequence as the stated requirements and supported by an Excel document as far as possible
- Response should indicate for each of SBM's requirements, whether the proposed solution complies with the requirement and to what degree.
- More detailed explanations and Cross-references must be provided to support the response wherever appropriate.
- The proposal must be signed by an authorized person.
- All pages must be signed.

3.2 SOLUTION RESPONSE

This response should be structured into the following sections:

Section I: Executive Summary - This section is an overview of the response and is provided by your company's senior management. The summary should contain a statement of the relative strengths of your

company and a brief description of your proposed solution, clearly identifying the main benefits, overall indicative cost and time frames.
In addition, the following details shall be required:

1. Registered company name
2. Business Registration Number
3. Registered Address
4. Contact details of authorized person to discuss on proposal
5. Date of incorporation of company
6. Nature of Organization (Proprietary / Partnership / Pvt. Ltd. Co / Public Ltd. Co)
7. Number of Employees experienced on the systems provided
8. Support Centre details
9. Any affiliates / associated businesses
10. Company's balance sheet
11. Number of persons to be assigned to this project
12. CVs of Project Manager and team members
13. Brief history of the company
14. A reference document
    i. Showing the trust that other flagship clients have granted you for similar products
    ii. Showing your best / impressive achievements
    iii. Honestly explaining your responsibility in each of these projects.
15. A list of customers where your solution with regards to similar products has been successfully implemented and working.
16. Valid Manufacturer Authorization Form (MAF) for all proposed hardware and software components, confirming OEM backing for supply, warranty, and post-sales support.
17. Proof of successful completion at least two (2) similar large-scale printing, mailing, and franking solution implementations, preferably in the banking or financial sector within the last five (5) years.
18. Evidence of a minimum of three (3) certified engineers or technicians trained on the proposed equipment and solution stack.
19. Demonstrate financial soundness and profitability over the last three (3) financial years.
20. Address/structure/details of local service and support presence in Mauritius with access to spare parts and on-site intervention capability.

Section II: Response to Service Provider's Technical Proposal. A full fledge technical proposal addressing SBM's needs under this RFP particularly section 2 should be submitted under this section. Bidders to advise how far they comply to each of the requirements and, if possible, in a tabular format. Bidders to also submit the specifications/features of any equipment proposed. Bidder to submit the following annexes duly filled and with the requirement supporting documents as applicable.

(a) Annex 1 - Compliance to the General and Functional Requirements
(b) Annex 2 - Compliance to the IT Security Requirements
(c) Annex 3 - Other requirements and documents to be submitted in relation to same.

Section III: Response to Support Structure and conditions – This section should contain your response to the support and maintenance requirements as applicable.

Section IV: Response to Additional Information Requirements - This section should contain any additional information that you wish to provide about your support structure that you view as being beneficial to SBM

Section V: Non-Disclosure Agreement
This section should contain the **Non-Disclosure Agreement** executed by service provider on its behalf and those of its employees, consultants, agents, subcontractors or other third parties who are involved (directly and indirectly) with this RFP.

3.3 FINANCIAL RESPONSE

This response documents the costing of your solution, and essential contract terms.

This response should consist of three sections:

Section I: Solution Costing Requirements - This section sets out your detail costing for the supply and after-sales services as per our request as applicable. The costing should be as per template spelt out in section 2.11 above.

Section II: Licensing Structure Requirements - This section provides details of the licensing structure for each of the proposed products

Section III: Contract Requirements – This section sets out your proposed contract terms and conditions, including your ability to comply with the contract requirements of SBM. SBM would expect that part of the contract to be performance based to give SBM the comfort on the service provider's ability to deliver its services as per its Service Agreement.

This section should also include any disengagement level costs and coverage of support to migrate out of the proposed solution.

4 GENERAL INFORMATION ABOUT THIS RFP

4.1 RESPONSE SUBMISSION

Proposals must be signed by duly authorized person(s) and submitted in English language. Each proposal must include all information as outlined in this RFP document and must be sent in PDF format **exclusively** to our secured electronic tender email address:

tender2@sbmgroup.mu **at latest by Friday 13th February 2026 at 14:00 Mauritius Time.**

Technical proposal and financial/commercial proposals to be submitted in separate emails with following reference in the subject line of your emails:

Technical Proposal: **"RFP – Printing Mailing & Franking Equipment – Technical Proposal"**
Financial Proposal: **"RFP – Printing Mailing & Franking Equipment – Financial Proposal"**

The maximum receiving capacity of the mailbox is **10 MB** per e-mail. Should your proposal exceed this size limit, you are requested to send same in two or more parts.

Proposals received after the closing date and time will not be considered. Proposals shall be considered to have been received within the closing date and time when it has been successfully opened by SBM. The burden of proof for the successful sending and time of sending of such proposals shall be on the party sending such proposals.

Once proposals are submitted at the above-mentioned electronic tender email address, applicants are advised to notify the contact person stipulated in Section 4.2 below of the submission of the bid **(WITHOUT ATTACHING THE PROPOSAL)**.

All queries on this RFP should be compiled and sent to the respective contact persons by **Friday 30th January 2026** latest**.**

Each applicant must include in its proposal all requirements and should not assume that another opportunity will be available to add any such matter after the proposal is submitted.

SBM reserves the right to request for any further information required at any time where RFPs' proposals are incomplete or SBM is of the view that further information is required from an applicant.

In addition, SBM reserves the right neither to accept the proposal or any proposal or any part of the proposal nor to assign any reason whatsoever for the non-acceptance or rejection of any proposal.

4.2 RESPONSE CONTACT PERSON

Any queries or clarifications with regards to the RFP should be sent to the following address:

Name of Company	SBM Bank (Mauritius) Ltd
Contact for proposal submission	Mr. Sailendra Kumar Booluck and Mrs. Shanita Bussawon Finance Division, SBM Tower, 1 Queen Elizabeth II Avenue, Port Louis Mauritius. Email : sailendrakumar.booluck@sbmgroup.mu Email : shanita.bussawon@sbmgroup.mu Tel : (230) 202-3490/ 202-1024

4.3 CONDITIONS

RFP & Response Validity

This RFP is not an offer to contract. Instead, it represents a definition of specific requirements and an invitation to submit a response addressing such requirements.

Your formal response shall constitute an offer to SBM and shall be deemed to be valid for a period of 6 months from the response due date.

Misrepresentation of any fact during the RFP process, inaccurate or misleading information in whatever form shared by the applicant with the Bank, will lead to the disqualification of the applicant without prejudice to other actions that the Bank may take.

The responses to this RFP and any accompanying documents will become the property of the Bank and the Bank shall be free to reproduce the whole or part of any response, for evaluation purposes, to disclose the contents of submitted responses to other applicants and/or to disclose and/or use the contents of submitted responses as the basis for the RFP process. Applicants must advise the Bank immediately in writing of any material change to the information contained in their RFP, including any substantial change in their ownership or their financial or technical capacity. Copies of the relevant documents must be submitted with their advice.

The Bank reserves the right to not accept the lowest or any quotation and shall not have to assign any reason for the rejection of the quotation. The Bank also reserves the right to annul the bidding process and reject all quotations, even the lowest, at any time prior to award of contract without thereby incurring any liability towards any bidder and any obligation to inform any bidder of the grounds for the Bank's action.

The Bank reserves the right, at any time, to make any amendment or waive any of the requirements of this RFP document.

During the RFP evaluation process, applicants may be asked to make a presentation of the solution, including a demo and demonstrate proof of concepts. Applicants shall bear all costs associated therewith.

SBM shall be under no obligation to consider, evaluate or accept your response notwithstanding that the requirements in the RFP have been met in your formal response. Should a contract be awarded, SBM may, at its option, incorporate all or any part of your offer in the formal response to this RFP in the contract. SBM's acceptance thereof shall be valid only upon the execution of a written contract and shall be subject to SBM's standard contracting terms and conditions.

Incomplete responses may be a reason for **outright rejection** of the proposal. However, SBM reserves the right to seek further information or clarification from you in the event your proposal is incomplete.

Any deviations from the specifications, terms, and conditions of this RFP and/or alternative proposals must be distinctly pointed out by the applicant.

The applicant shall bear all costs associated with submission of RFP, presentation / Proof of Concept / additional information as designed by the Bank.

Confidentiality

You will be required to execute the Non-Disclosure Agreement, which will form part of your formal response to this RFP. Please read the terms thereof carefully and note that the obligation of confidentiality contained therein is to extend to all your employees, agents and third parties involved (directly or indirectly) with this RFP.

All responses to this RFP shall become the property of SBM. All materials contained within your formal response, as well as the materials and information distributed during the service provider presentations, if any, will be made available to all project team members including external parties appointed by SBM to assist in the evaluation process. This group of people will be bound by the same confidentiality obligations.

You should not announce, discuss or disclose to any third party the existence of this RFP or any information contained therein, other than a third party or parties selected by your company to assist you in the preparation of your proposal. Such third parties should be bound equally by the confidentiality obligations of the confidentiality agreement. Failing to abide to the above will lead to automatic disqualification and could even jeopardize the existing and future business relationship between your company and SBM.

Correct and Complete Requirement Interpretation

It is the responsibility of the service provider to properly interpret and understand all SBM's requirements prior to submission of the response. During preparation of the response to the RFP, the applicant may contact SBM for clarification, from the contact persons specified under Section 4.2.

Potential service providers shall notify SBM in writing for clarification of any inconsistency, discrepancy or conflict within the content thereof or any figures and wording, or any ambiguity regarding any part of this RFP document.

Sub-Contracting

The service provider must identify and describe the role of any subcontractor employed in providing a solution to SBM. These roles include subcontracting for specific tasks, partnering with other tool service providers to provide solutions, and the roles of all third-party tool service providers where there are services

or procurements made during the implementation of the solution. The payment and management responsibilities of SBM should be clearly delineated with regard to each of the planned subcontractors. SBM will need to approve the hiring of all subcontractors. Such subcontractors will be bound by the same contractual obligations of the selected service provider to SBM. However, the service provider will remain liable for any non-performance by the sub-contractor.

The service provider should disclose all proposed subcontractors for SBM's approval by: -

at latest by Friday 13th February 2026 by 14:00 Mauritius Time (GMT+4)

No information to be disclosed to any third party, without the prior consent of SBM.

Project Materials

Any material prepared by SBM, the service providers, or the subcontractors in connection with the development and/or delivery of the project will be the sole property of SBM. The service provider may not use such materials for any purpose other than for the Bank solution. Response to the RFP and other supporting documentation submitted by service providers will become the property of SBM and will not be returned.

Incurred Costs

SBM is not responsible for the costs of preparing, presenting and attending the RFP. All expenses incurred by the service provider, whether selected or not, for the preparation and submission of the RFP, presentation and product demonstration is the responsibility of the service provider and will not be reimbursed by SBM. All equipment required during the presentation, demonstration and/or prototyping will be provided by the service provider, unless specifically agreed to by SBM prior to the presentation.

Misrepresentation

The answers given in your response to the questions raised in this RFP and the information provided and/or obtained in discussions, presentations, further clarification and site visits will be accepted in good faith by SBM, and SBM's decisions will be based on the same.

Should SBM have reason to believe that you have misrepresented, fabricated, exaggerated or lied about any information contained in your response, you will be immediately disqualified from the process.

Bank Obligations

SBM reserves the right to accept **whole or part of any proposal**, which could under certain circumstances lead to the service provider being asked to consider an alternative provider as part of their total solution. In which case, options and terms of any engagement will be discussed with the appropriate service providers in order to achieve an acceptable conclusion.

SBM is under no legal obligation to accept the response of the RFP as a binding contract with the applicant.

SBM reserves the right to accept, split or reject any or all proposals received or cancel the tendering exercise without incurring any liability towards any service provider and/or any obligation to inform any applicant of the grounds of its action.

Non-acceptance of a service provider's proposal will mean that other proposal(s) were deemed more advantageous to SBM or that all proposals were rejected. Applicants whose proposals are not accepted, will be notified after the issuance of a letter of offer to the selected applicant and its acceptance thereof or in the event SBM rejects all proposals.

Amendment of RFP Document

a) SBM reserves the right to amend the RFP process by notice to the applicant.
b) At any time before the deadline for submission of proposals, SBM may, for any reason, whether at its own initiative or in response to a clarification requested by prospective bidders, modify or amend the conditions of this RFP Document.
c) All applicants who have received this RFP shall be notified of the amendment in writing by e-mail or fax or post, and all such amendments shall be binding on them.
d) If required in order to allow applicants reasonable time in which to take the amendment into account in preparing their bids, SBM reserves the rights to extend the deadline for the submission of proposals. Any request to extend the said deadline shall be entertained at SBM's sole discretion.

Legal

It is hereby agreed that this RFP, and all matters arising there from, shall be governed by the laws of Mauritius, and it is agreed that the applicant and SBM shall submit to the non-exclusive jurisdiction of the courts of Mauritius.

Access control

Access by the service provider or any of the service provider's employees, subcontractors, officers, auditors and officials of any regulatory or supervisory authority, to the Bank's servers and computing environment (consisting of hardware, firmware and software) shall at all times be subject to the Bank's prior approval and access shall be on such terms as the Bank, in its sole discretion, may require.

Warranty

All service providers are required to **include the following warranty** as part of their formal response to this RFP:

"I/We hereby warrant and represent to SBM Bank (Mauritius) Ltd that: -

1. All my/our statements herein are true, correct and complete, and shall remain so for 9 months from the response due date;

2. The product and services package described, proposed and presented herein is the latest operational and stable release of the same;

3. All my/our services described, proposed and presented shall be conducted in accordance with good industry practice, and I/we are willing, ready and able to perform the same; and

4. I/we will inform SBM in writing within seven (7) days of our receipt of notice of any litigation, arbitration or administrative or bankruptcy/insolvency proceedings threatened or instituted against us, and which may adversely affect the use, delivery or performance of any deliverable set out herein."

Service Provider Selection Criteria

The Service Provider will be selected according to a set of criteria.

a. Its capabilities to fulfill the mission.
b. Its ability to demonstrate its "fair play" spirit where the result goes before the administrative bottlenecks.
c. Its ability to encompass the entire project in a reasonable overall budget.
d. Its ability to demonstrate a strong expertise in this field.

e. Its ability to demonstrate successful and satisfactory customer references.
f. Its ability to demonstrate its delivery commitment with penalty-backed service levels.

5 TERMS AND CONDITIONS

The terms listed below represents SBM's Standard Service Requirements. These requirements are not exhaustive and will be supplemented and/or by the final contractual documents. Please tick as appropriate to indicate your compliance to these requirements. In case of a 'No' or 'Partly' answer, please specify the alternative arrangements provided by your organization, or your comments in case you feel that such an arrangement is not required.

	5.1 TERMS OF SERVICE CONTRACT – GENERAL	**YES**	**NO**	**Partly**
1.	Coverage up to 24:00 hours 7/7 with a maximum of 1 hr. call out response for onsite intervention			
2.	Service effort to be paid after satisfactory defined milestone as per schedule of payment in conjunction to the roadmap			
3.	SBM may terminate service contract with 30 days written notice to the Service provider.			
4.	The service provider will provide a report detailing possible causes of failure and recovery procedures in case of attendance to a problem.			
5.	Service premium rate to be fixed for a period of 10 years and to be calculated on cost of each individual product excluding VAT.			
6.	The Letter of Credit for the purchase of the solution should be done via SBM.			
7	All payments will be done in MUR and will be fixed for the initial and maintenance costs. These costs will not be negotiated for any exchange rate fluctuations.			
8.	A penalty of 0.5% of the value of contract will be charged per day for non-compliance with delivery dates.			
9.	Any system introduced for SBM must be virus free and free of malicious codes. The service provider will be liable, accountable and contribute to the cost of recovering from the harm caused by the software provided which includes cash payment for any documented expenses incurred by SBM in removing virus, any costs of rebuilding machines or restoring things to their original condition, and any costs for lost productivity during cleanup.			
10.	In the event the commissioning of the proposed solution/hardware/software/accessories is not successful, as per specifications and to the satisfaction of SBM, SBM reserves the right to cancel the whole order and the supplier should refund any part payment effected after confirmation of order and any costs borne by SBM.			
11	The service provider shall commit in writing that the licenses for the proposed solution will be provided at enterprise level based only for unrestricted use across organization, irrespective of locations.			

	5.2 TERMS OF SERVICE CONTRACT – SOFTWARE	**YES**	**NO**	**Partly**
1.	Undertakes to provide support services up to 24:00 hours 7/7.			
2.	Guarantee to have engineers available at all times specialized in the supplied software.			

3.	Throughout the duration of the contract, SBM will receive all product updates (both major and minor), maintenance releases, and any patches, fixes and error corrections for the product for which customer purchased the solution. The service provider undertakes to inform the customer about the availability of any updates, deliver and install all software updates.			
4.	All upgrades and updates should be installed after office hours (time to be communicated by SBM) at no additional cost.			
5.	Undertakes to schedule frequent (at least once every month) preventive maintenance visits to help in fine-tuning of software performance including security aspects, analysis of usage logs, error logs, etc. and capacity planning and taking remedial / preventive measures thereon, if required			

6 EVALUATION AND COMPARISON OF PROPOSALS

a. A screening committee will be constituted by SBM for the purpose of selection of the best proposal/alternatives.

b. The company profile, past experience of the bidder in the area of supply, installation, training and operationalization of the solution, technical features, hardware/software requirements, delivery schedule, service, support, price, etc. shall be some of the important criteria in selecting the bidder.

c. During the period of evaluation, applicants may be asked to provide more details and explanations about information they have provided in the proposals. Service providers should respond to such requests within the time frame indicated in the letter/fax/e-mail seeking the explanation. Service providers will be required to make a presentation of the proposals to the screening committee.

d. SBM reserves the right to modify/amend the evaluation process at any time during the process, without assigning any reason, whatsoever, with notice to the applicant.

e. SBM will adopt the evaluation methodology as given below:

i. The functional and technical requirement
ii. The applicants should provide their response to the questionnaire and enter their remarks in the last column, if any.

Scale	Description
3	Supplier exceeds the Bank's expectations
2	Supplier meets the Bank's expectations
1	Supplier meets partly the Bank's expectations. Customization/Feature in roadmap
0	Supplier fails to meet the Bank's expectations

f. Marks will be allocated to the responses provided in the questionnaire and also to the following:
- Formatting and clarity of the proposal
- Acceptance to the terms and conditions
- Deadline for submission of the proposal
- Response to all information requested as per this RFP
- Documentation provided to evidence responses among others

g. SBM shall notify the successful applicant by email. The applicant shall acknowledge receipt of the email notification.

h. The acknowledgment by the applicant shall be followed by execution of the services agreement. The applicant accepts and acknowledges that its appointment is subject to the execution of a binding services agreement, on such terms and conditions as may be acceptable to SBM. SBM reserves the right to withdraw from the negotiations at any time, should the parties not be successful in reaching a mutual agreement on the final terms and conditions.

……..

		Rating	Comply Yes/No
1	**BUSINESS PROCESS AND ENVIRONMENTAL CONSIDERATIONS**		
1.1	Application		
	The application should not include Functions, stored procedures, packages, routines, libraries, data types or any other resources that are never invoked or used by the application.	Medium	
	Application should not have any hard-coded or embedded passwords,Encryption Keys	High	
	Application should not have any backdoors that could allow someone to access the application functions without authenticating through the normal login process	High	
	All tasks should be automated as far as possible to prevent data manipulation. Vendor should specify instances where tasks are manual or semi automated such as diskette transfers, etc. and provide their suggestions/ recommendations for appropriate controls.	High	
	Minimum data entry: Makes use of combo boxes, list boxes, check boxes, and radio button, etc to minimize input	Medium	
	Process Flow Control: System should prevent an activity from being performed in case a prior activity remains outstanding. Alternatively Alert message is displayed to indicate when a prior activity remains to be performed before the next activity can be performed	Medium	
1.2	Operating System		
	Client side application should be able to run with non-administrative privilege	High	
	Client side application should NOT make use of shared id	High	
	Application should be able to run on OS hardened according to SBM's security configuration standards or to best practice security configuration standards as published by NIST, NSA or OS vendor	High	
	Any service accounts required by the application should not require any priviledged rights such as root or adminstrator	High	
	Any shares required should not be accessible to everyone group and should be restricted to minimum number of users on a need to basis with the minimum access required on the shares	High	
	Application should not require any risky ports to be opened	Medium	
	Vendor must provide guidelines for securing any risky ports if same is required	High	
1.3	Database		
	Application should be able to run on Database hardened according to SBM's security configuration standards or to best practice security configuration standards as published by NIST, NSA or OS vendor	High	
	Application should not require the application users to have direct access to the database	High	
	Any user ids required on the database in order for the application to run properly should not have any 'write' access to the database	High	
	The application should allow sensitive data (such as password or other sensitive data such as personal data or cardholder number) to be stored in encrypted format.	High	

	Application should support the physical segregation of database server from any web server required	High	
1.4	Network		
	Only network ports and accesses (source and target) required for the smooth running of the application should be opened on the firewall or any other filtering device Vendor must supply a list of all such ports required	High	
	Card/payment application should be compatible with a secure network environment. Application should not interfere with use of network address translation (NAT), port address translation (PAT), traffic filtering network devices, antivirus protection, patch or update installation, or use of encryption.	High	
1.5	Hardware		
	Hardware must be sized to take into consideration Forecasted Transaction Volumes	High	
	Hardware must be sized to take into consideration Forecasted Transaction Volumes	High	
	Hardware must be sized to take into consideration Forecasted volume of static data	High	
	Hardware must be sized to take into consideration Audit trail History	High	
	Hardware must be sized to take into consideration Endpoint protection system	High	
	Hardware must be sized to take into consideration Host Intrusion Prevention system	High	
	Hardware must be sized to take into consideration Log retrieval agent (SIEM) for log collection	High	
	Hardware must be sized to take into consideration File Integrity checker agent	High	
1.6	Robustness & Resiliency		
	Capability to detect duplicate transactions and corrupted / invalid transactions	High	
	Error Correction Capabilities	High	
	Graceful exits and error dumps in case of problems	Low	
	Application has Restore points for both system state and transaction in case of system crash following system configuration change or corruption of configurations	High	
	Restart point in case of crash during batch process	High	
	Roll back of incomplete transactions	High	
1.7	Purging of Historical Transactions		
	Complies with SBM's policies and applicable regulatory requirements such as PCI DSS requirements.	High	
	Application has Automated/scheduled as well as user triggered purging with the ability to define the period for purging	Medium	
	Application provides the capability to archive data	High	
	Supports user-friendly interface to view archived data	Low	
	Application should provide the facility to check the reliability of backed up or archived data	Low	
1.8	**Card Applications -** Comply with the latest version of Visa / MasterCard Rules		
	Account Information Security Best Practices Guide	High	
	Account Information Security Standards	High	
	Operating Regulations	High	

	CEMEA Risk Management – Acquirer Best Practice Guide	High	
	Latest version of PA-DDS and PCI DSS	High	
	Other standards and regulations as applicable	High	
1.9	Non-repudiation & confidentiality		
	Supports 3D secure for secure online transaction	High	
	Supports One time password for sensitive transactions	High	
	Supports PKI – digital certificates & digital signatures	High	
	Maintain audit log for sensitive operations	High	
1.10	Customer Data Protection		
	Display card number only partially to merchant (to prevent utilization of past transaction details to perform unauthorized transactions)	High	
	Where customers are provided with purchase details, apply the same principle of displaying only part of the card number as mandated by PCI DSS	High	
	Application should provide for cardholder information to be stored only at the acquirer database (unless otherwise stated by VISA Regulations)	High	
	Cardholder data should be encrypted with strong encryption (at least 128 bit), anywhere it is stored (including database, removable media, and logs).	High	
	Cardholder data must never be stored on a server connected to the Internet.	High	
1.1	Handling of card-verification code		
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in Incoming transaction data	High	
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in All logs (for example, transaction, history, debugging, error)	High	
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in History files	High	
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in Trace files	High	
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in Database schemas and tables	High	
	Ensure that the contents of any track from the magnetic stripe on the back of the card (CVV data) is not stored under any circumstance in Database contents	High	
1.1	Handling of the PIN Verification Value (PVV)		
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in Incoming transaction data	High	
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in All logs (for example, transaction, history, debugging, error)	High	
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in History files	High	
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in Trace files	High	
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in Database schemas and tables	High	
	Ensure that the PIN verification Value (PVV data) is not stored under any circumstance in Database contents	High	

2	**VENDOR CONSIDERATIONS**		
2.1	International best practices		
	Application should support best practice configuration standards such as SANS, NIST, PCI DSS, OWASP etc.	High	
	Application should have been developed using best practice secure coding standards such as PA-DSS, OWASP etc.	High	
	Vendors will ensure that their application is compatible with the latest version of the applicable industry standard (such as PA-DSS for card-related applications)	Medium	
	Vendors will provide a yearly certification of compliance with the applicable industry standard (such as PA-DSS for card-related applications)	Low	
2.2	Security Configuration standards		
	Vendor should provide SBM with the appropriate security configuration standards document based on International Best Practices for securing the application.	High	
	Additionally, SBM has got its own security standards for OS and databases, based on International Best practices. Vendor is required to review SBM's standards and to officially confirm compatibility with the application. In case application does not support any of SBM's standards, it is the responsibility of the vendor to propose mitigating controls to eliminate/ reduce the risk(s) identified.	High	
2.3	Services and Ports		
	Vendor should provide SBM with a list of services and protocols that are required by the application.	High	
	The list should be accompanied by justification for enabling these services and protocols.	High	
2.4	Protocols		
	Vendor should provide a list of required services and should ensure that services that are generally prone to attack such as ftp, telnet, messenger, snmp, etc are not used as far as possible.	High	
	Where services prone to attacks are used, vendor should provide their views on the risk factor, and provide suggestions/ recommendations for mitigating the risk.	High	
2.5	Backdoors and Hard Coded passwords		
	Vendor should provide assurance that there are No Backdoors to the application	High	
	Vendor should provide assurance that there are No Hard coded passwords in the application / scripts / interfaces	High	
2.6	Security patches		
	Vendor is responsible for the compatibility of the application with the OS and Database security patches and should provide assistance when deploying security patches.	High	
	Vendor is responsible to issue security patches for known vulnerabilities in the application.	High	
	Vendor is responsible for informing SBM for any vulnerability in the application and provides workaround until a security patch is released.	High	
2.7	Penetration Testing		

	Vendor should contract reputable and independent Ethical Hacking Firm to conduct WAPT (Web application Penetration testing) on the application & source code to be delivered to SBM and ensure that any vulnerability or weakness observed during the WAPT are corrected by vendor before release to SBM.	High	
	A copy of the PT Report before and after resolution of the vulnerabilities should be submitted to SBM before sign off is obtained.	High	
2.8	Vendor-supplied defaults		
	Vendor should provide SBM with a list of default user id, passwords, scripts, subsystems, drivers, error messages, keys and other default configuration and help SBM to disable/restrict such defaults settings.	High	
2.9	Critical application binaries		
	For Integrity purpose: Vendor should provide SBM with a list of critical application binaries and parameter files that require integrity monitoring.	High	
2.10	Database encryption		
	Vendor should confirm that application support encryption at database level (such as Oracle Advanced Security Option, etc.)	High	
2.1	Certificate of Assurance		
	Vendor should provide an assurance to SBM from an independent and qualified IT Security or IT audit organization regarding the development practices and security of the application.	High	
2.1	On-site Demo/ Training		
	On-site demo (including simulation and validation of all functions of the application) at the bank should be provided by vendor	Medium	
	Vendor/ third-party should provide training on system.	Medium	
3	**INTEGRATION CONSIDERATIONS**		
3.1	ID and Access Management		
	Application should support LDAP or other industry standard technology associated with ID and access management	High	
3.2	Interfaces		
	Interfaces between systems should be secure/encrypted Interfaces between systems (like webservices) should be secure/encrypted.	High	
	For file transfers, secure channel should be used	High	
	Connections between interfacing systems must be closed at all times except when required for uploads or downloads	High	
	There should be appropriate authentication between interfacing systems	High	
	The use of digital signature is required for system to system authentication.	High	
	Batch Interfaces: Data transferred must be output to a staging environment (e.g. flat file, intermediary staging table, etc) before transformation, data validation and upload to the production environment	Low	
	Minimum access rights must be applied to the folder on the staging environment in order for the functioning of the interface	Low	
	Data downloaded through interfaces from non SBM systems must be pulled by SBM instead being pushed by external systems	High	
	Data uploaded to non-SBM systems must be pushed by SBM instead of being pulled by external systems	Low	

	Data pulled from non SBM systems must be adequately secured in the external party's environment through the security obligations embodied in the contractual arrangements	Low	
4	**ACCESS CONTROL CONSIDERATIONS**		
4.1	User Authentication		
	Requires combination of user id and strong password as a minimum in order to access the application	High	
	Support strong authentication such as 2-Factor authentication for remote access to application over the Internet	High	
	Keep track of all login attempts (successful and unsuccessful)	High	
4.2	Server Authentication		
	Adequate authentication mechanism should be in place between servers in case of a tiered architecture	High	
4.3	Account Management		
	Account uniqueness: Prohibit 2 users from having the same user id	High	
	Automatically terminates temporary and emergency accounts after pre-defined time period for each type of account	High	
	Automatically disables inactive accounts after pre-defined time period	High	
	Determines normal time-of-day and duration usage for information system accounts	Low	
	Automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals	High	
	Dynamically manages user privileges and associated access authorizations	High	
	Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles	High	
4.4	Concurrent Log in		
	Application should prevent the same user id from concurrent log ins	High	
	Concurrent log in attempts must be logged and generate real time alerts	Medium	
4.5	Previous Logon Notification		
	Display the date and time of the previous successful log-on on completion of a successful logon:	Medium	
	Display the details of any unsuccessful log on attempts since the last successful log on	Medium	
4.6	Session Control		
	Inactive sessions should be disconnected automatically after a predefined and customizable period.	High	
	The application administrator should be able to configure the default time-out.	High	
	After invoking time-out facilities his screen should be cleared and he must be forced to re-authenticate.	High	
	User session must also be terminated after user log off i.e. user should not be allowed to access the application without re-authentication.	High	
	User session should be terminated if the user tries to attempt unauthorized access or escalate his privileges. This attempt must be logged as a security incident within the application.	High	
4.7	Access Control Granularity		
	Support role based access control	High	

	Support granular definition of roles based upon menus, screens, tasks and upon functions such as view, print, add, modify, etc	High	
	Support segregation of tasks between normal users, administrators, password administrators and parameter administrators	High	
	Support maker/ checker concept for all sensitive tasks such as user administration, password admin, parameter admin and for any sensitive user activities including transaction and maintenance activities	High	
4.8	User id Structure		
	Must support user ids up to at least 8 characters in length	Low	
	Must support alphabetic characters	Low	
	Application must allow System Owners to assigned pre-arranged naming conventions for user ids to ensure consistency throughout the environment (e.g. Surname & first initial of first name)	Medium	
4.9	User Administration		
	Application should have a separate User Administration Module such that Administration tasks are not combined with user tasks.	Medium	
	Should support role based access control.	High	
	All non-console administrative access (web-based management) should be encrypted using technologies such as SSH version 2, or SSLv3/TLS.	High	
	SSHv1 and SSLv2 are not acceptable.	High	
4.10	Merchant Management		
	Supports Automatic disabling of merchants not transacting for an extended period (period of inactivity to be determined)	High	
	Re-enabling of 'inactive' merchants require supervisor override.	High	
4.1	Account Lockout		
	Support different locking policies based on the respective user groups, i.e. locking for normal users and no locking for administrators	High	
	Lock out user ids of normal users after a predefined number of consecutive failed log in attempts	High	
	Prevent users from using the locked ids without administration intervention	High	
	Application should ensure that all user accounts that are not used for x number of consecutive days are automatically locked.	High	
4.1	Exits		
	Should only allow exit from the application through application commands	Low	
5	**CRYPTOGRAPHY CONSIDERATIONS**		
5.1	Confidentiality		
	Application should support database encryption.	High	
	Strong cryptography, such as 3DES 128-bit, AES 256-bit or higher should be used.	High	
	Confidential information should be encrypted on the database and should be viewed only through the application.	High	
5.2	Encryption		
	All sensitive data such as personal data, cardholder data, etc must be encrypted	High	
	Password must not to be stored in clear text. It should be stored in Hashed format.	High	
	Use standard encryption (e.g. 3DES and AES) as opposed to proprietary algorithm.	High	

	Application should protect encryption keys against disclosure and misuse.	High	
	Connection strings are encrypted in configuration files through implementing appropriate controls.	High	
	Connection string information is encrypted using strong encryption (for example, 3DES).	High	
	If possible, developer must ensure that appropriate authentication/ encryption is used when connecting to DB Server.	High	
	Sensitive data like passwords are not used in configuration files and scripts unless it is encrypted	High	
6	**OPERATIONS CONSIDERATIONS**		
6.1	Integrity Controls		
	Proper controls should be supported to Avoid duplicate transactions	High	
	Proper controls should be supported to Ensure that Activity such as batch runs, file transfers, end of day process, etc is not performed more than once	High	
	Proper controls should be supported to Handle incomplete transaction	High	
	Proper controls should be supported to Ensure completeness and integrity of transaction data	High	
	Proper controls should be supported to Allow easy detection of incomplete or incorrect transaction data	High	
	Proper controls should be supported to Allow easy detection of altered transaction	High	
6.2	Processing Controls		
	Has Control Totals/ Checksums (settlement file) mechanism to ensure completeness and integrity of transactions	High	
	Supports Reconciliation mechanism to ensure completeness and integrity of file transfers and batch uploads	High	
	Supports Identification of reject transactions	High	
	Supports Automated interface for file upload / and to edit file with appropriate audit trail feature	High	
	All sensitive tasks should be prompted for confirmation and require maker/ authoriser	High	
6.3	Downloading of Data		
	Prevent download of card information by merchant (Applies to card applications).	High	
	Prevent download of sensitive card related or customer information to local disk of user.	High	
6.4	Sensitive Data		
	Sensitive data transferred must be encrypted when in transit,storage and at rest.	High	
	Sensitive data must be at rest for the minimum amount of time possible during the staging phase	High	
6.5	Application Partitioning		
	User functionality should be separate from information system management functionality	High	
6.6	Security Function isolation		
	There should be separate console for security functions	High	
6.7	Output Distribution		

	System should provide the capability of defining distribution outputs based on a need to know basis	High	
	System should provide capability to restrict printing of documents to only authorized users.	High	
	Printout of scanned documents generated from the system should indicate source of the document and mark as scanned copy of the original document, e.g. header or watermark on the document.	High	
6.8	Output Storage		
	System should have built-in compression mechanism to optimize on storage utilization and provide fast retrieval of the stored information.	Medium	
6.9	Audit trails		
	Interface audit trails: Adequate audit trails should be available to indicate What data was transferred through the interface, such as what files were uploaded or down loaded	High	
	Interface audit trails: Adequate audit trails should be available to indicate Who or which process initiated the transfer	High	
	Interface audit trails: Adequate audit trails should be available to indicate Number and integrity of records transferred	High	
	Interface audit trails: Adequate audit trails should be available to indicate Success or Failure status	High	
6.10	Control Reports		
	File transfer Controls: Reports should be available on screen and in hard copy for all upload or download activities to ensure the completeness and integrity of records transferred.	Medium	
	The following details should be provided among other things:		
	Date, time, Person or process initiating the activity, Total number of records to be transferred and the total number of records actually transferred	High	
	Integrity of the records transferred	High	
	Details on the records transferred	High	
6.1	Security Access Violation reports		
	Adequate security reports should be available in the system in order to:		
	Determine security access violation	High	
	Enable monitoring of critical activities being performed by the system administrators	High	
	Enable monitoring of critical activities being performed by the end users	High	
	Successful Login Attempts:	High	
	Repeated failed login attempts including privileged accounts	High	
	Inactive ids	High	
	Inactive merchants (for card applications)	High	
	Sensitive User administration activities:	High	
	Parameter administration	High	
	All user account maintenance activities	High	
	Password administration activities	High	
7	**CONFIGURATION CONSIDERATIONS**		
7.1	Password Length		
	Minimum password length = 8	High	
7.2	Password Complexity		

	Enforce combination of numbers, alphabetic characters and of special characters	High	
	Enforce combination of lower and upper case characters	High	
7.3	Disallowed Passwords		
	Dictionary words	High	
	User id	High	
	User name	High	
7.4	Password History		
	Prevent reuse of 15 previous passwords as a minimum	High	
7.5	Password age		
	Minimum password age = 0 for administrators and 5 for normal users	High	
	Maximum password age = 30 days for administrators and 60 for normal users	High	
7.6	PIN		
	PINs must be randomly generated and contain at least four digits. (if you are implementing PINs within your application)	High	
7.7	Invalid Login Counter		
	Reset invalid log in count to zero after an administrator-defined period	High	
7.8	Password Change		
	Force password change upon first log in, following allocation of a new password by the administrator	High	
	Support different password expiry policies for different user profiles	High	
	Password Expiry = 30 days for System administrators and 60 days for normal users	High	
	Application must ensure that, users are able to change their own passwords at any point after they have successfully authenticated themselves.	High	
7.9	Expiry Notification		
	Minimum = 7 days	High	
7.10	Unique Password		
	Enforce unique combination of user id and password	High	
7.1	Null password		
	Prevent use of null password or of null user id	High	
7.1	Encryption		
	Passwords should be encrypted using strong encryption during transmission	High	
	Passwords should be encrypted using strong encryption or hashed using irreversible hashing function, when stored	High	
	Encryption algorithm must not be stored in clear	High	
7.1	Embedded Passwords		
	Should not include any hard coded or embedded passwords	High	
7.1	Disallowed Features		
	Should have the flexibility to disallow Auto Logon feature	High	
	Should have the flexibility to disallow 'Remember my password'	High	
7.2	Application Password		
	Application generated passwords must not be predictable or sequential.	High	
7.2	Flushing of sensitive information.		
	At the application side, no sensitive information is to stay in memory once a transaction is completed. When a transaction is completed, the application should flush all information residing in memory.	High	

7.2	Data Access		
	Trusted service accounts should be used to connect to DB Server.	High	
	Credentials in SQL connection strings should be protected and masked in configuration files.	High	
	Sensitive data like plain text passwords must not be used in configuration files.	High	
	Sensitive data that is stored in configuration files are encrypted using SBM approved encryption algorithms	High	
	Sensitive data is not passed across pages; it is maintained using server-side state management.	High	
	Sensitive data is not stored in cookies, hidden form fields, or query strings.	High	
	Sensitive data like customer sensitive information and credentials are encrypted in the database.	High	
8	**AUDIT/LOGGING CONSIDERATIONS**		
8.1	Accountability		
	Application should implement an automated audit trail to track and monitor access.	High	
8.2	Format		
	Application should support SysLog format or any other standard format (CSV, Flat text file)	High	
	Application log format should be compatible with the selected Security Event and Log Monitoring system (SIEM)	High	
8.3	Logging location		
	Application should provide the flexibility to log events to OS and to DB so as to enforce segregation of duties	High	
	Log files should be stored on separate server	High	
	Implement ACL on log files	High	
8.4	Auditable Events		
	Application should log all sensitive events and access by individual users (especially those with administrative privileges)	High	
	Application should log all User administration activities such as user account creation, user profile administration	High	
	Application should log all Password reset	High	
	Application should log all Parameter administration	High	
	Application should log all Log in	High	
	Application should log all Log out	Medium	
	Application should log all All sensitive user activities	High	
	Application should log all Access to sensitive data	High	
	Application should log all Printing of sensitive documents	High	
8.5	Contents		
	Should provide details on Who initiated(User id), Who authorised (User id), When (date & Time), Where (Terminal id), What (Function accessed), and action status (whether action was successful of not), filenames involved, and access control or flow control rules invoked	High	
	Audit trails should be supported by adequate transaction logs with details on the transaction performed	High	
	Audit trails for Maintenance activities should include details on the data before the change as well as data after the change	High	

8.6	User Interface		
	Provides a user- friendly interface for viewing audit trails	Medium	
8.7	Audit Storage Capacity		
	Should support minimum of 1 year on-line storage	Medium	
8.8	Protection of Audit Information		
	Application should be configured to provide only View access to audit trails to Application admins	High	
	Application must use cryptographic mechanisms to protect the integrity of audit information and audit tools	High	
	Application admins should not be able to delete audit trail	High	
	Application should support access controls to audit trail data	High	
	Deletion of audit trails should be logged as an auditable event	High	
9	**SECURE PROGRAMMING CONSIDERATIONS**		
9.1	Session security and session IDs		
	Assign random, non-sequential session Ids	High	
	Requires Re-authentication when accessing additional records.	High	
	Account credentials and session tokens should be protected.	High	
	Require all cookies to expire after a predetermined period following the user's last request.	High	
	Session tokens must change when the user moves from an SSL-protected resource to a non-SSL-protected resource.	High	
	Session token at the server side must be invalidated when the user logs out.	High	
	Session token must be non-persistent	High	
	Session token must never be written to the browser's history or cache	High	
	Sensitive pages of the website should not be cached in the user browser	Medium	
	Session token must be updated after the user logs in	Medium	
	Sessions token should be used to avoid multiple active logins	Low	
	Cookies should always be marked as HTTPOnly and Secure (when using HTTPS)	Medium	
	Sessions tokens should not be passed in the GET Reuqest	Low	
	Sesitive session related data should not be stored in cookies	Medium	
9.2	SQL Injection		
	User parameterized queries to construct and process SQL Statements	High	
	Use Store Procedures for processing SQL (DML) statements	High	
	Avoid using extended stored procedures (like xp_cmdshell)	High	
	Validate user input on server side for its type, length, range etc.	High	
9.3	Cross-site scripting (XSS)		
	Make use of HTML and URL Encoding	High	
	Make use of framekwork specific libraries like Anti XSS Libraries to protect against XSS	High	
	Validate user input on server side for its type, length, range etc.	High	
9.4	Buffer overflow		
	Prevent code insertion by unauthenticated source.	High	
	Validate the input field length.	High	
9.5	Denial of Service		

	Application should function properly when presented with large volumes of transactions, requests or traffic.	High	
	Block repeated requests from a single URL.	High	
	The application code must not include bugs, errors or exploitable vulnerabilities that could be used by a malicious user or program to launch a successful DoS attack against the application.	High	
9.6	Error Handling		
	All error messages should be generic and non-descriptive	High	
	Ensure that error messages do not reveal sensitive information(such as physical paths and platform architecture, etc), which can be used to facilitate an attack against the organization.	High	
	Ensure error conditions are not reported to the end user.	High	
	Filter message for any malicious behavior like XSS before displaying error pages.	High	
	Use try catch finally block to catch exceptions/error occurred in the application.	Medium	
	Log the exception/error occurred in the application.	Medium	
	Define custom error pages in the application.	Medium	
9.10	Parsing of sensitive information		
	Use Post method instead of Get method when parsing sensitive data to web server to prevent the information from being disclosed to onlookers in the address bar.	High	
9.1	Anonymous logins		
	Use proper authentication rather than anonymous authentication for all functionality aspects	High	
9.1	Application logins		
	Code should not require using the suid root/ administrator account in order to run.	High	
	The application should not require the database administrator account e.g. SQL sa account in order to run	High	
9.1	Client keeping important data		
	The application must not rely on the client keeping information such as hidden form fields, parameters.	High	
	Any information which is capable of being changed by the client, must be stored on the server side.	High	
9.1	Directly-entered URLs		
	The application must not allow users to access Web pages/resources not explicitly allowed by links on the WEB site by directly typing the URLs of the forbidden pages/resources into their browser's address bar	High	
9.2	Validation & reasonableness checks		
	All incoming data must be validated for consistency with rules applicable in the target system	High	
	Vendor must ensure that appropriate data validation practices are followed while developing the application. Some of them include:	High	
	Free form input is sanitized to clean malicious data.	High	
	Application does not rely only on request validation.	High	

	All the input is validated for length, range, format, and type. Input is checked for known valid and safe data and then for malicious, dangerous data.	High	
	Input from all the sources including query strings, cookies, and HTML controls is validated using the appropriate code validation.	High	
	Application does not rely on only client-side validation.	High	
	Application avoids file name and path input from user where possible.	High	
	If input file names are required, they are well formed and are verifiably valid within the application context.	High	
	Untrusted output is not directly echoed back to the user.	High	
	Output that contains untrusted data is encoded with HtmlEncode and UrlEncode.	High	
	The application must validate all data / parameter, input and must ensure the data complies with the following:		
	Contains correct syntax	Medium	
	Falls within the expected bounds (e.g., length, range, etc.)	Medium	
	Contains parameters or characters with valid values	Medium	
	Contains a numeric value that would not cause a routine or calculation in the application to divide any number by zero	High	
	Cannot induce a buffer overflow	High	
	Does not contain direct SQL queries	High	
	Does not contain HTML tags	High	
	Does not contain a truncated pathname reference	High	
	Performs Data Reasonableness Checks (e.g. transaction amount against average daily transaction amount)	High	
	All inputs should bee validated by the server application, even if some input validation has already been validated by the client application	High	
9.2	Hidden fields		
	The application must validate the source of all HTML updates to hidden fields	High	
	The application must reject any HTML field changes from unvalidated sources	High	
9.2	File Upload		
	The application should validate all the files to be uploaded on the server for its type, size and content type.	High	
10	**DISTRIBUTED COMPUTING AND WEB SERVICES CONSIDERATIONS**		
10	Authentication		
	Employ strong authentication, such as HTTPS, with encrypted credentials.	High	
	Require re-authentication at specified time intervals	High	
	Require re-authentication when moving between web pages.	High	
10	Log out users as soon as they leave the site.		
	User should be required to log in again in case user hops from the application to another site, and then tries to go back to the previous page using the back button	High	
10	Clearing of logon information		
	Application should not use persistent cookie at the client side.	High	
	Non-persistent cookies reside in memory of the client computer only as long as the browser is open.	High	
10	Transmission of Data		
	Encrypt data to protect against eavesdropping during transit on public network.	High	

	Public Key Encryption or Secure Socket Layer should be supported by the application.	High	
11	Maker/ Checker		
	maintenance activity reports, reports for all sensitive tasks, including maintenance activities, sensitive transactions	High	
11	Segregation of duties		
	Support segregation of tasks between normal users, administrators, password administrators and parameter administrators	High	
	Support maker/ checker concept for all sensitive tasks such as user administration, password admin, parameter admin and for any sensitive user activities including transaction and maintenance activities	Medium	

Description	Scale
Not available and will not be provided by the vendor.	N
Available and will be provided by the vendor.	Y
Currently not available but will be available in the future	F

Information Security Risk of hosting in Cloud

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
1	LOCK-IN	Currently, there is very little available in terms of tools, procedures or other offerings to facilitate data or service portability from CSP to CSP. This can make it very difficult for the enterprise to migrate from one CSP to another or to bring services back in-house. It can also result in serious business disruption or failure should the CSP go bankrupt, face legal action, or be the potential target for an acquisition (with the likelihood of sudden changes in CSP policies and any agreements in place). If the customer-CSP relationship goes sour and the enterprise wants to bring the data back in-house, the question of how to securely render the data becomes critical because the in-house applications may have been decommissioned or "sunsetted" and there is no application available to render the data.	Unavailability, loss	– Ensure contract with the CSP contain an exit strategy that specifies the terms that should trigger the retrieval of the enterprise's assets in the time frame required by the enterprise. – Implement a DRP/BCP, taking into account the possibility of complete CSP disruption.	
2	NETWORK UNAVAILABILITY	The value of cloud computing can only be realized when the network connectivity and bandwidth meet the company's minimum needs: The cloud must be available whenever you need it. If it is not, then the consequences are no different than a denial-of-service situation. There is a complete dependency on permanent and stable Internet connectivity to access Cloud system. Internet connectivity is beyond the control of the CSP and also the Bank. In case internet link is down, the whole organization may come to a halt.	Unavailability	– Have redundant Internet route and high resiliency network, with multiple vendors/ telcos.	

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
3	RESOURCE REALLOCATION	One of the primary benefits of the cloud is the ability to perform dynamic allocation of physical resources when required. Different entities share a pool of resources, including storage, hardware and network components. All resources allocated to a particular tenant should be "isolated" and protected to avoid disclosure of information to other tenants. However, there is a risk that data be visible to other tenants when resources are allocated dynamically. When allocated storage or memory is no longer needed by a client it would be freely reallocated to another enterprise on the cloud. The data can be recovered by other entities sharing the cloud by using forensics techniques.	Theft, disclosure	– Encrypt all sensitive data that are being migrated to the CSP, and ensure that proper key management processes are in place. – Request the CSP's technical specifications and controls to ensure that the data are properly wiped when requested and isolated when in use. – Use a private cloud deployment model (no multitenancy).	
4	COLLATERAL DAMAGE	If one tenant of a public cloud is attacked, there could be an impact to the other tenants of the same CSP, even if they are not the intended target (e.g., DDoS). Another possible scenario of collateral damage could be a public cloud that is affected by an attack exploiting vulnerabilities of software installed by one of the tenants.	Unavailability, loss, theft, disclosure	– Use a private cloud deployment model (no multitenancy). If Private Cloud is not possible, then: – Ask the CSP to include the enterprise in its incident management process that deals with notification of collateral events. – Include contract clauses and controls to ensure that the enterprise's contracted capacity is always available and cannot be directed to other tenants without approval.	
5	VULNERABLE ACCESS MANAGEMENT	Information assets could be accessed by unauthorized entities due to faulty or vulnerable access management measures or processes. This could result from a forgery/theft of legitimate credentials or a common technical practice (e.g., administrator permissions override).	Identity theft, Theft, Disclosure	– Request that the CSP provide detailed technical specifications of its IAM system for the enterprise authorized department to review and approve. If necessary, include additional controls to ensure robustness of the CSP's IAM system such as Two-Factor authetication for critical operations. – Use corporate IAM systems instead of CSP's IAM systems. The IAM remains the responsibility of the enterprise, so no access to assets can be granted without the knowledge of the enterprise. It requires the approval of the CSP and the establishment of a secure channel between the CSP infrastructure and the corporate IAM system.	

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
6	DATA DISPOSAL	In the event of a contract termination, the data fed into the CSP's application must be erased immediately. When data is slated for destruction, the main challenge is ensuring that it is completely sanitized to meet policy and regulatory guidelines. In a cloud, the physical destruction of media is not possible compared to traditional server model. using the necessary tools to avoid disclosures and confidentiality breaches (forensic cleaning may be required for sensitive data).	Theft, disclosure	– Request CSP's technical specifications and controls that ensure that data are properly wiped and backup media are destroyed when requested. Software mechanisms for overwriting or cryptographic erasure of disk will be required – Include terms in the contract that require, upon contract expiration or any event ending the contract, a mandatory data wipe carried out under the enterprise's review.	
		Proper disposal of data is imperative to prevent unauthorized disclosure. If appropriate measures are not taken by the CSP, information assets could be sent (without approval) to countries where the data can be legally disclosed due to different regulations concerning sensitive data. Disks could be replaced, recycled or upgraded without proper cleaning so that the information still remains within storage and can later be retrieved.	disclosure		
7	INCOMPLETE DATA DELETION	Adequate or timely data deletion may be impossible, either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients.	Theft, disclosure	– Use a private cloud deployment model (no multitenancy). – Request for dedicated hardware	
8	MULTIPLE JURISDICTIONS	Mirroring data for delivery and redundant storage without actualized information as to where the data is stored. This may create legal issues and may infringe Data Protection Regulations.	non-compliance, legal	– Request the CSP's list of infrastructure locations and verify that regulation in those locations is aligned with the enterprise's requirements. – Include terms in the service contract to restrict the moving of enterprise assets to only those areas known to be compliant with the enterprise's own regulation.	
9	COMPLIANCE RISKS	Investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud: > if the CSP cannot provide evidence of their own compliance with the relevant requirements > if the CSP does not permit audit by the cloud customer (CC). ***In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS (4)).***	non-compliance	– Cloud Solution should be compliant with local laws and regulations – Avoid Cloud for systems requiring adherance to strict compliance requirements such as PCI DSS for systems processing, transmitting and storing card holder data.	

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
10	DATA OWNERSHIP	The CSP provides the applications and the customer provides the data. If data ownership is not clearly defined, the CSP could refuse access to data when required or even demand fees to return the data once the service contracts are terminated.	Unavailability, loss, disclosure	– Include terms in the contract with the CSP that ensure that the enterprise remains the sole legal owner of any asset migrated to the CSP. – Encrypt all sensitive assets being migrated to the CSP prior to the migration to prevent disclosure and ensure proper key management is in place.	
11	DATA PROTECTION	It may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud service provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds.	Theft, disclosure	– Request for certified CSP having SAS70 certification. – In the absense of certification, insist on having information on CSP data handling practices.	
12	LACK OF TRANSPARENCY	For any infrastructure, intrusion detection and prevention systems (IDPS), Firewalls and event management (SIEM) capabilities must be in place. It is the responsibility of the CSP to provide these capabilities to its customers. When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider's security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.	Unavailability, loss, theft, disclosure	To ensure that there are no security gaps, the security policy and governance of the CSP should match those of the enterprise. – Request the CSP's detailed schemes of the technical security measures in place and determine whether they meet the requirements of the enterprise. – Request that the CSP provide proof of independent security reviews or certification reports that meet the enterprise's compliance requirements (e.g. PCI DSS, ISO 27001). – Include in the contract, clauses that requires the CSP to provide the enterprise regular reporting on security (incident reports, IDPS logs, etc.) and rights to audit clause.	
13	POOR PROVIDER SELECTION	Selection of technology or service provide sub-optimal, resulting in system operational degradation		– Selection of best-of-breed solution service provider should be considered – Due dilligence to be conducted, especially the financial soundness of the company before contracting any vendor – Check the client references – Audit the CSP Data Center	
14	APPLICATION ATTACKS	Due to the nature of Cloud, the applications offered by a CSP are more broadly exposed. Because they can be the target of massive and elaborate application attacks, additional security measures (besides standard network firewalls) are required to protect them.	Theft, Unavailability	– Request that the CSP implements application firewalls, antivirus and antimalware tools. – The SLA must contain detailed specifications about vulnerability classification and actions taken according to the severity level, which must align with corporate policies and procedures for similar events.	

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
15	PHYSICAL SECURITY	In cloud, physical computer resources are shared with other entities in the cloud. If physical access to the CSP's infrastructure is granted to one entity, that entity could potentially access information assets of other entities.	Theft, disclosure	– Request the CSP's physical security policy and ensure that it is aligned with the enterprise's security policy. – Include in the contract clauses that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it. – Request that the CSP provide proof of independent security reviews or certification reports that meet the enterprise's compliance requirements (e.g., SOX, ISO certification). – Request the CSP's disaster recovery plans and ensure that they contain the necessary countermeasures to protect physical assets during and after a disaster.	
16	MALICIOUS INSIDER	Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CSP system administrators and managed security service providers. Privileged users (e.g. Administrator) performing unauthorized activities on the system (data theft, tampering…)	Theft, disclosure, Tampering	– Implement below Security tools and controls > Two Factor authentication > SIEM solution > Privilege User Management and Identity Access Management > VPN access	
17	LEGAL TRANSBORDER REQUIREMENTS	CSPs are often transborder, and different countries have different legal requirements, especially concerning personal private information. The enterprise might be committing a violation of regulations in other countries when storing, processing or transmitting data within the CSP's infrastructure without the necessary compliance controls. Furthermore, government entities in the hosting country may require access to the enterprise's information with or without proper notification.	Disclosure	– Encrypt all sensitive assets being migrated to the CSP prior to the migration to prevent disclosure and ensure proper key management is in place. – Include contract clauses to ensure that the CSP cannot share enterprise information, even to government entities without explicit approval from us.	
18	PROPAGATION OF FLAWS	An attacker might be able to analyze configuration, patch level, and code in detail using administrative rights by renting a virtual server as a service customer, and thereby gaining knowledge helpful in attacking other customers images in the same cloud. An attack against a VM may lead to an attack against a hypervisor of a physical server hosting the VM, subsequent attacks against other VMs hosted on that server, and eventually, all VMs sharing that server	Unavailable, Theft	– Use a private cloud deployment model (no multitenancy). – Ensure that all VMs are kept up to date in terms of patches	

SN	RISKS	DESCRIPTION	IMPACT	RECOMMENDATIONS	COMMENTS
19	POOR INCIDENT RESPONSE	Failure for the provider to detect, handle incidents and report them with data that can be analyzed easily to satisfy legal requirements in case of forensic investigations	non-compliance	– Include in the contract, clauses that requires the CSP to provide the enterprise regular reporting on security (incident reports, IDPS logs, etc.) – Ensure that the systems are under SIEM monitoring and all alerts are copied to the Bank as well. – Put strict SLA for identifying, reporting and closing incidents, and the requirements for timely root cause analysis (RCA) report.	