Virgin Islands
Shipping & Maritime
Authority

VIRGIN ISLANDS SHIPPING AND MARITIME AUTHORITY
(VISMA)

REQUEST FOR PROPOSAL
FOR THE PROVISION OF
INFORMATION TECHNOLOGY (IT) SERVICES
FOR THE
VIRGIN ISLANDS SHIPPING & MARITIME AUTHORITY

RFP REF# — VISMA/IT-01/2026
RFP Date: 17th April 2026 Closing Date: 17th May 2026

TABLE OF CONTENTS

1.0 REQUEST FOR PROPOSAL (RFP)

Our Ref: RFP (VISMA/IT-01/2026)

The Virgin Islands Shipping and Maritime Authority (VISMA), a statutory body established under the Virgin Islands Shipping & Maritime Act, 2023, hereby invites proposals from qualified and experienced firms for the provision of comprehensive Information Technology (IT) Services.

This procurement is being conducted in accordance with the Virgin Islands Public Procurement Act, 2021 and any other applicable public procurement rules, policies, and internal procedures of VISMA.

VISMA is seeking to appoint a suitably qualified IT Services Provider to deliver structured, secure, responsive, and forward-looking IT services that support VISMA's operational continuity, regulatory obligations, service delivery requirements, and digital transformation priorities.

The selected Proponent will be expected to provide a proactive managed service model which includes not only day-to-day support and technical administration, but also governance, cybersecurity oversight, reporting, service level management, and continuous improvement.

VISMA does not bind itself to accept the lowest-priced proposal or any proposal and reserves the right to reject any or all submissions, amend the RFP, cancel this procurement, or reissue the RFP at any time without liability.

2.0 CHECKLIST TO ACCOMPANY PROPOSAL

Proponents are to place a tick in the checkbox for each item that is included in the Proposal.

- ☐ Title Page
- ☐ Table of Contents
- ☐ Letter of Transmittal
- ☐ Form 1A: Technical Proposal Submission Letter
- ☐ Form 2A: Methodology, Workplan, and Deliverables
- ☐ Form 3A: Proposed Team – CV Summary Table
- ☐ Form 4A: Team Composition and Task Assignments
- ☐ Form 5A: Professional Qualification Certificates
- ☐ Form 6A: Proposed Project Plan / Time Schedule
- ☐ Form 7A: Confidentiality Agreement
- ☐ Form 8A: No Conflict of Interest Declaration
- ☐ Form 9A: Form of Contract
- ☐ Form 10A: Proponents Declaration Form
- ☐ Form 1B: Commercial Proposal Submission Letter
- ☐ Form 2B: Summary of Costs
- ☐ Form 3B: Detailed Cost Breakdown
- ☐ Form 4B: Reimbursable and Miscellaneous Expenses
- ☐ Evidence of Insurance (Professional Indemnity, Cyber Liability, General Liability, and other applicable insurance coverage)

- ☐ Any additional schedules or annexes required by this RFP

Failure to submit mandatory forms and required supporting documentation may result in disqualification.

3.0 INTRODUCTION & BACKGROUND

The Virgin Islands Shipping and Maritime Authority (VISMA) is responsible for the oversight, regulation, and development of maritime transportation, shipping operations, vessel registration, seafarer services, and related maritime activities within the Virgin Islands.

In order to effectively fulfil its mandate, VISMA requires secure, resilient, responsive, and well-governed information technology services that support:

- Operational continuity and service availability;
- Regulatory compliance and secure information handling;
- Internal administration and business support functions;
- External stakeholder engagement and digital service delivery;
- Strategic modernisation and digitisation initiatives.

VISMA currently operates with approximately fifty (50) users and is no longer a single-location organisation. In addition to its headquarters in the British Virgin Islands, VISMA now also operates an office in London and may in future maintain additional international office representation, remote access arrangements, or expanded digital service requirements.

Accordingly, VISMA requires an IT Services Provider that can support a multi-site operating environment and provide coordinated service delivery across locations, including support for network connectivity, user support, endpoint management, system standardisation, and consistent cybersecurity controls.

VISMA is seeking an experienced IT Services Provider to deliver a comprehensive managed service that includes, at a minimum:

- IT infrastructure and operations support;
- Help desk and end-user support;
- Cybersecurity services;
- Strategic IT advisory and governance support;
- Service Level Agreement (SLA) management;
- Support for digitisation and business process improvement initiatives.

VISMA's intention is to appoint a provider that can support the organisation in a structured and measurable manner, with clearly defined service boundaries, governance, reporting, service levels, and a proactive continuous improvement approach.

3.1 CURRENT STATE / AS-IS ENVIRONMENT

The purpose of this section is to provide Proponents with a high-level understanding of VISMA's current operating environment and to improve the quality, comparability, and accuracy of proposals submitted.

VISMA currently operates across more than one office location, including:

- Headquarters in the British Virgin Islands;
- A small office presence in London;
- Remote working or future international support requirements, where applicable.

The environment currently comprises approximately fifty (50) staff users and associated endpoint devices. The successful Proponent will be expected to support a multi-site environment and provide consistent service delivery across all locations.

During the transition and onboarding phase, the successful Proponent shall validate and document VISMA's current IT environment in detail. Proponents should anticipate that the environment may include, but not necessarily be limited to, the following:

- User devices such as laptops, desktops, and approved mobile devices;
- Productivity, collaboration, and communication platforms;
- Network infrastructure and internet connectivity;
- Cloud and/or on-premises systems;
- File storage, email, and user identity management services;
- Backup and recovery arrangements;
- Firewalls, security controls, endpoint protection, and access controls;
- Third-party vendor and technology dependencies.

Proponents are required to clearly state any assumptions they have made regarding VISMA's current state environment and pricing model.

4.0 TERMS OF REFERENCE

The selected Proponent shall provide comprehensive Information Technology (IT) Services to VISMA. The services shall be delivered through a structured service delivery model that is measurable, proactive, secure, and scalable.

The Proponent shall clearly describe how each service area will be delivered, what tools and platforms will be used, what deliverables will be produced, what assumptions apply, and what activities are considered out of scope.

The required services include, but are not limited to, the following:

I. SERVICE DELIVERY MODEL

The Proponent shall provide a clearly defined service delivery model which demonstrates how services will be delivered to VISMA across all locations and supported users.

The service delivery model shall include:

- Description of the operating model for managed services;
- Explanation of how remote and on-site support will be delivered;
- Hours of support and arrangements for after-hours support for critical issues;
- Support channels, including portal, email, phone, and remote support tools;
- Escalation model for incidents, service requests, security events, and critical outages;
- Proposed service management tools and platforms;
- Governance and reporting arrangements;
- Approach to supporting VISMA's BVI and London offices and any future remote or international support requirements.

The Proponent shall identify any geographic limitations, dependency on third parties, or assumptions affecting service delivery.

II. IT INFRASTRUCTURE AND OPERATIONS

The Proponent shall provide support, management, maintenance, monitoring, and administration of VISMA's IT infrastructure and operational environment.

The service shall include, at a minimum:

- Network support and administration, including firewalls, switches, wireless access points, VPN connectivity, and internet connectivity;
- Support for server infrastructure, whether on-premises, cloud-hosted, or hybrid;
- Endpoint management for desktops, laptops, and other approved end-user devices;
- User administration and access support;
- Monitoring and performance oversight of infrastructure and critical systems;
- Preventative maintenance and system health checks;
- Patch and update management for relevant operating systems, devices, servers, and infrastructure;
- Backup support, backup monitoring, and support for recovery processes;
- Disaster recovery and business continuity support;
- Telecommunications and VoIP coordination where applicable;
- Management of third-party vendor escalations related to infrastructure and services where required.

The Proponent shall describe the proposed monitoring model, patching frequency, maintenance windows, alerting approach, and how infrastructure issues will be prioritised and resolved.

III. HELP DESK AND END-USER SUPPORT

The Proponent shall provide Help Desk and End-User Support services for VISMA users, including Tier 1, Tier 2, and Tier 3 support as appropriate.

The Help Desk service shall include:

- Support for desktops, laptops, standard peripherals, approved software, and core business systems;
- Assistance with password resets, login issues, file access, email support, software troubleshooting, and connectivity issues;
- Incident logging, triage, prioritisation, assignment, escalation, and resolution;
- Service request handling for standard user requests such as software installation, access changes, device setup, and approved configuration requests;
- On-site and remote support, as required;
- Communication with end users throughout the support lifecycle;
- Ticket ownership through to closure;
- Escalation to technical specialists or third-party vendors where appropriate;
- Maintenance of knowledge articles and user support documentation;
- Trend analysis and reporting of recurring issues and root causes.

The Proponent shall clearly describe user support channels, staffing model, support hours, ticket ownership process, and escalation arrangements.

IV. IT SERVICE MANAGEMENT (ITSM), INCIDENT MANAGEMENT, SERVICE REQUEST MANAGEMENT, AND CHANGE MANAGEMENT

The Proponent shall provide or integrate with an IT Service Management (ITSM) platform capable of supporting the structured delivery and management of IT services.

The ITSM platform shall, at a minimum, support:

- Ticket submission via portal, email, and/or telephone;
- Categorisation and prioritisation of tickets;
- Distinction between incidents, service requests, problems, and changes;
- Workflow-based assignment and escalation;
- SLA tracking and reporting;
- Full audit trail and case history;
- Knowledge base or documentation repository functionality;
- Dashboarding and reporting capability;
- Access for authorised VISMA personnel to review tickets, statuses, service history, and reports.

The Proponent shall define and document its incident management process, including:

- Logging and classification of incidents;
- Initial response and triage;
- Investigation and remediation;
- Escalation procedures;
- Communication and status updates;
- Closure and confirmation process;
- Root cause review for significant or recurring incidents.

The Proponent shall define and document its service request process, including request categories, approvals, fulfilment standards, and expected turnaround times.

The Proponent shall define and document its change management process, including:

- Standard changes;
- Normal changes;
- Emergency changes;
- Approval requirements;
- Risk and impact assessment;
- Communication protocols;
- Documentation updates post-implementation.

VISMA expects the selected Proponent to operate formal service management controls and to ensure that all support activity is properly logged, managed, and reported.

V. CYBERSECURITY SERVICES

The Proponent shall provide a robust and clearly defined cybersecurity service model appropriate to VISMA's size, risk profile, public-sector obligations, and multi-site operating environment.

The cybersecurity services shall include, at a minimum:

- Security monitoring and event management;
- Security incident identification, response, escalation, and reporting;

- Vulnerability management, including scanning, assessment, prioritisation, and remediation tracking;
- Endpoint protection and endpoint security management;
- Firewall administration and security configuration oversight;
- User access control administration and privileged access support;
- Identity security support, including multifactor authentication and conditional access recommendations where applicable;
- Security hardening recommendations and support for secure configuration;
- Support for data protection and cyber risk reduction measures;
- Cybersecurity awareness training for users;
- Cybersecurity awareness testing and validation, including phishing simulations or equivalent exercises;
- Regular reporting on cybersecurity posture, trends, risks, and recommendations.

The Proponent shall specifically describe:

- Whether security monitoring is provided during business hours, extended hours, or 24x7;
- The escalation path for security incidents;
- The process for managing critical or high-risk cybersecurity events;
- Vulnerability scanning approach and frequency;
- Expected remediation timelines by severity;
- Awareness training delivery model and frequency;
- Testing methodology for awareness validation;
- Security reporting deliverables.

Monthly cybersecurity reporting shall include, at a minimum:

- Summary of security alerts and notable events;
- Open and resolved security incidents;
- Vulnerability status and remediation progress;
- Endpoint protection and security compliance status;
- Security awareness training activities completed;
- Results of awareness testing exercises;
- Key risks, observations, and recommendations.

General statements of cybersecurity capability will not be sufficient. Proponents must provide clear operational detail regarding how cybersecurity services will be delivered.

VI. STRATEGIC IT ADVISORY SERVICES

The Proponent shall provide strategic advisory support to VISMA in relation to the planning, improvement, governance, and modernisation of its technology environment.

This shall include:

- IT strategy and roadmap recommendations;
- Technology modernisation planning;
- Infrastructure and application lifecycle advice;
- Advice on security improvements and resilience;

- Budget forecasting support in relation to IT requirements;
- Advice on standardisation, optimisation, and digital service delivery;
- Support for governance frameworks and decision-making processes;
- Recommendations for future improvements based on service trends, risks, and business needs.

The Proponent shall ensure that strategic advisory support is embedded within the overall service model and supported by scheduled review meetings and documented recommendations.

VII. SERVICE LEVEL AGREEMENT (SLA) MANAGEMENT

The Proponent shall propose a Service Level Agreement (SLA) framework covering all major service areas included within the engagement.

The proposed SLA framework shall, at a minimum, include:

- Service coverage hours;
- Incident priority / severity definitions;
- Response time targets;
- Resolution or restoration time targets;
- Escalation procedures;
- Communication protocols for major incidents;
- Security incident response expectations;
- Scheduled maintenance and exclusions;
- Service level measurement and reporting methodology.

Proponents shall clearly distinguish between response time and resolution time and shall set out how service performance will be monitored and reported.

VISMA expects the selected Proponent to support performance review and continuous improvement through routine reporting and governance meetings.

VIII. CONTINUOUS IMPROVEMENT / INNOVATION HOURS

VISMA requires the selected Proponent to adopt a proactive service model rather than a purely reactive break-fix approach.

Accordingly, the Proponent shall include within its proposal a defined allocation of continuous improvement capacity or “innovation hours” to support ongoing enhancement of the environment.

These hours may be used for activities such as:

- System and configuration improvements;
- Security hardening and control enhancement;
- Documentation updates and support knowledge improvements;
- Small-scale automation or productivity enhancements;
- Service optimisation initiatives;
- Improvements arising from monthly or quarterly review meetings;
- User experience improvements and support process enhancements.

The Proponent shall clearly state:

- The number of innovation hours included per month or quarter;

- What activities are covered;
- How such hours will be prioritised and approved;
- How outputs will be reported to VISMA;
- Whether unused hours roll forward, expire, or are otherwise treated.

IX. DIGITISATION AND BUSINESS PROCESS DEVELOPMENT SUPPORT

The Proponent shall provide support services required to enable VISMA's digitisation initiatives and digital transformation objectives.

These services may include, but are not limited to:

- Assessment and documentation of existing manual or semi-automated business processes;
- Business process mapping, analysis, and re-engineering;
- Identification of digitisation opportunities;
- Development of improved technology-enabled workflows;
- Support for digitisation of records, forms, and operational activities;
- Development or documentation of Standard Operating Procedures (SOPs);
- User acceptance testing support;
- Change management and user adoption support;
- Support for governance, roles, approvals, and process controls.

These services are intended to ensure that technology services and system improvements are aligned to VISMA's operational and long-term business requirements.

Where these services are proposed outside the base managed services fee, the Proponent shall clearly identify this in the proposal.

X. TRANSITION, ONBOARDING, AND SERVICE COMMENCEMENT

The Proponent shall provide a structured transition and onboarding plan that supports the commencement of services and the orderly takeover of responsibility for the VISMA environment.

The transition approach shall include, at a minimum:

- Discovery and environment validation;
- Collection and review of existing documentation;
- Asset and service inventory validation;
- Stakeholder identification and communication planning;
- Establishment of support tools, monitoring, and access arrangements;
- Setup of the ITSM platform and workflows;
- Handover from incumbent resources or third-party providers, where applicable;
- Identification of risks, issues, and immediate remediation priorities;
- Service commencement readiness review;
- Transition to steady-state operational support.

Proponents shall provide a high-level mobilisation and onboarding plan as part of their Technical Proposal, including expected activities during the first thirty (30), sixty (60), and ninety (90) days.

5.0 PROPOSAL SPECIFICATIONS

A. General Requirements

- Language: English
- Currency: United States Dollars (USD)
- Proposal Format: PDF submitted electronically by email
- Technical and Commercial Proposals shall be submitted as separate documents
- Proposals shall remain valid for a period of not less than ninety (90) days from the submission deadline

B. Technical Proposal

The Technical Proposal must demonstrate the Proponent's understanding of VISMA's environment, scope, and service expectations.

The Technical Proposal shall include, at a minimum:

- Understanding of VISMA's operating environment and requirements;
- Proposed service delivery model;
- Detailed methodology for each service area;
- ITSM platform and support processes;
- Cybersecurity operating model;
- Governance, reporting, and communication approach;
- Transition and onboarding plan;
- Proposed SLA framework;
- Continuous improvement / innovation hours model;
- Staffing model and proposed team;
- Relevant experience and case studies;
- Assumptions, exclusions, and dependencies.

The proposal shall clearly distinguish between services included within the recurring managed service and services that would be separately scoped or billed.

C. Commercial Proposal

The Commercial Proposal shall provide a transparent and complete pricing structure.

It shall include, at a minimum:

- Fixed recurring charges for core managed services;
- Basis of pricing assumptions (users, locations, devices, service volumes, etc.);
- Transition or implementation fees, if any;
- Rate card for additional services and project-based work;
- Pricing for optional service enhancements;
- Reimbursable expenses, where applicable;
- Any third-party licence, hosting, or pass-through charges.

D. Clarifications and Amendments

All requests for clarification must be submitted in writing to:

Email: tenders@bvimaritime.vg

VISMA reserves the right to issue addenda, clarifications, or amendments to this RFP at any time prior to the submission deadline.

6.0 INTENT TO RESPOND

Proponents are encouraged to submit a non-binding Intent to Respond by email, identifying the Proponent's primary contact and confirming the intention to submit a proposal.

Email: tenders@bvimaritime.vg

7.0 SUBMISSION DEADLINE OF TENDER PACKAGES

Proposals must be submitted electronically no later than:

17th May 2026 at 4:00 p.m.

Submissions shall be sent to: tenders@bvimaritime.vg

Late submissions may be rejected.

8.0 SELECTION

The selection process will follow a structured and transparent evaluation methodology in accordance with the Virgin Islands Public Procurement Act, 2021 and VISMA's applicable procurement procedures.

VISMA intends to appoint the Proponent that offers the best overall value, taking into account technical capability, service quality, cybersecurity maturity, transition readiness, governance approach, and pricing.

9.0 EVALUATION COMMITTEE

An internal Evaluation Committee comprising representatives of VISMA and, where appropriate, subject-matter advisors, shall assess the proposals received.

10.0 EVALUATION CRITERIA

The Evaluation Committee will assess proposals using a weighted scoring methodology.

Proponents must achieve a minimum score of seventy percent (70%) of the total points allocated under the Technical Evaluation in order to be considered for Financial Evaluation.

Technical Evaluation – 112 Points (70%)

No.	Description	Maximum Score
1	Firm's Relevant Experience	20
1a	Experience providing managed IT services to public-sector, statutory, regulated, or similarly governed organisations	8
1b	Experience in cybersecurity, and multi-site environments	6
1c	Completion of at least three comparable assignments	6
2	Technical Approach and Methodology	35

No.	Description	Maximum Score
2a	Understanding of VISMA's operating environment and requirements	8
2b	Proposed service delivery model, ITSM processes, and support methodology	8
2c	Cybersecurity operating model and risk management approach	8
2d	Governance, reporting, and continuous improvement approach	6
2e	Transition and onboarding plan	5
3	Staffing and Key Personnel	15
3a	Qualifications and certifications of key personnel	8
3b	Adequacy of staffing model and resource availability	7
4	Service Levels and Commercial Transparency within Technical Proposal	10
4a	Quality and realism of proposed SLA framework	5
4b	Clarity of assumptions, exclusions, and service boundaries	5

Financial Evaluation – 48 Points (30%)

No.	Description	Maximum Score
5	Commercial Proposal	20
5a	Cost competitiveness	8
5b	Pricing transparency and completeness	6
5c	Overall value for money	6

VISMA reserves the right to invite shortlisted Proponents to clarification meetings, interviews, demonstrations, or presentations as part of the evaluation process.

11.0 TENDER CLARIFICATION

VISMA reserves the right to request written clarifications from any Proponent and to seek additional supporting information where necessary.

VISMA may also invite shortlisted Proponents to present or demonstrate their proposed service model, tools, governance approach, or cybersecurity capability.

12.0 NOTIFICATION AND CONTRACT AWARD

The successful Proponent will be notified in writing and may be invited to enter into contract negotiations with VISMA.

VISMA reserves the right to negotiate aspects of the final scope, pricing, service levels, schedules, and implementation approach with the preferred Proponent prior to contract award.

All unsuccessful Proponents will be informed accordingly.

13.0 RIGHT TO REJECT OR CANCEL

VISMA reserves the right to reject any or all proposals, waive minor informalities, cancel this RFP, revise the RFP, or reissue a new solicitation without incurring liability to any Proponent.

14.0 ADDITIONAL REQUIREMENTS

Proponents must demonstrate:

- Legal standing and authority to conduct business in the relevant jurisdiction(s);
- Financial capacity and stability;
- Technical capability and access to suitably qualified personnel;
- The ability to deliver the services described in this RFP;
- Appropriate insurance coverage;
- Willingness to comply with confidentiality, data protection, and conflict of interest requirements.

VISMA may request documentary evidence of the above at any stage of the procurement process.

APPENDICES

The following Appendices form an integral part of this Request for Proposal (RFP). Proponents are required to complete and submit all mandatory forms and supporting documents.

Failure to submit required forms may result in disqualification.

APPENDIX A: TECHNICAL PROPOSAL FORMS

Form 1A: Technical Proposal Submission Letter

To	Virgin Islands Shipping & Maritime Authority
RFP Title	The Provision of Information Technology (IT) Services
RFP Reference No.	VISMA/IT-01/2026
Name of Firm	
Registered Address / Contact Details	

Declaration

- We, the undersigned, hereby submit our Technical Proposal in response to the Request for Proposal for the provision of Information Technology (IT) Services for VISMA.
- We confirm that the information contained in this proposal is true and accurate.
- We have reviewed and understood the requirements of the RFP and agree to abide by its terms, conditions and instructions.
- Our proposal shall remain valid for the period stated in the RFP.

VISMA Representative	**Proponent Representative**
Name:	**Name:**
Title:	**Title:**
Signature:	**Signature:**
Date:	**Date:**

Form 2A: Methodology, Workplan, and Deliverables

Please complete the table below and provide sufficient detail under each heading.

Section	Bidder Response
Understanding of VISMA and the Assignment	
Proposed IT / Managed Services Methodology	
Approach to Service Delivery Model	
Approach to IT Infrastructure and Operations	

Section	Bidder Response
Approach to Help Desk and End-User Support	
Approach to ITSM and Change Management	
Approach to Cybersecurity Services	
Approach to Strategic IT Advisory Services	
Approach to Continuous Improvement / Innovation Hours	
Approach to Digitisation and Business Process Support	
Transition and Onboarding Plan	
Proposed SLA Framework	
Proposed Workplan and Sequencing of Activities	
Key Deliverables	
Quality Assurance Process	
Assumptions, Exclusions, and Dependencies	

Form 3A: Proposed Team – CV Summary Table

Name	Proposed Position	Qualifications	Years of Experience	Relevant Experience Summary	Availability / Level of Effort

Form 4A: Team Composition and Task Assignments

A. Core Professional Team

Name	Position / Role	Key Responsibilities	Relevant Expertise	Estimated Input

B. Support Team

Name	Position / Role	Support Function	Relevant Expertise	Estimated Input

Form 5A: Professional Qualification Certificates

Please list all professional qualifications and certifications relevant to the proposed team and attach copies as an appendix.

Name of Team Member	Qualification / Certification	Issuing Institution / Body	Year Obtained	Copy Attached (Yes/No)

Form 6A: Proposed Project Plan / Time Schedule

Task No.	Activity / Deliverable	Proposed Timing	Milestone / Output	Responsible Team Member
1				
2				
3				
4				
5				

Form 7A: Confidentiality Agreement

Parties	This Confidentiality Agreement is made between the Virgin Islands Shipping & Maritime Authority (VISMA) and the Proponent.
Purpose	The Proponent may receive confidential information in connection with this RFP and agrees to keep such information confidential.
Confidential Information	Includes all non-public documents, data, reports, policies, financial or operational information, and any derived materials shared in connection with this RFP.
Exclusions	Information shall not be considered confidential if it becomes public through no fault of the Proponent, was lawfully known beforehand, is independently developed, or must be disclosed by law.
Proponent Obligations	The Proponent shall use the information only for purposes of this RFP, keep it strictly confidential, not disclose it without written consent, and restrict access to authorised personnel only.
Return / Destruction	Upon request or completion of the RFP process, all confidential information shall be returned or destroyed, with written confirmation to VISMA.
Ownership	All confidential information remains the property of VISMA.
Remedies	VISMA may seek appropriate legal or equitable remedies in the event of a breach.
Term	This Agreement shall remain in effect for five (5) years or as long as the information remains confidential, whichever is longer.
Governing Law	This Agreement shall be governed by the laws of the Virgin Islands.

Signatures

VISMA Representative	**Proponent Representative**
Name:	**Name:**
Title:	**Title:**
Signature:	**Signature:**
Date:	**Date:**

Form 8A: No Conflict of Interest Declaration

Name of Firm	
Authorised Signatory	

Title	
Date	

Declaration

We hereby declare that no actual, potential or perceived conflict of interest exists, or is likely to arise, in connection with this proposal and the services to be provided under this RFP. We further undertake to disclose promptly to VISMA any circumstance that may give rise to an actual or potential conflict of interest during the procurement process or contract period.

Authorised Signature	
Date	

Form 9A: Form of Contract Acknowledgement

Name of Firm	
Authorised Signatory	
Title	
Date	

Acknowledgement

We acknowledge that, if selected, a standard VISMA consultancy/services contract will be issued to the successful proponent. We understand that the contract will set out the agreed scope of services, deliverables, pricing, payment terms, confidentiality obligations, intellectual property provisions, termination rights, and other contractual requirements.

Authorised Signature	
Date	

Form 10A: Proponents Declaration Form

Please tick the appropriate response and provide details where necessary.

Question	Yes	No	Details (if Yes)
Has the firm ever been convicted of any criminal offence?	☐	☐	
Has any director, partner or principal had a professional licence suspended or revoked?	☐	☐	
Has the firm ever been subject to bankruptcy, insolvency, receivership or winding-up proceedings?	☐	☐	

Question	Yes	No	Details (if Yes)
Are there any pending civil, regulatory or criminal matters involving the firm or its principals?	☐	☐	
Has the firm ever been terminated for default under a public or private contract?	☐	☐	

Name of Firm	
Authorised Signatory	
Title	
Signature	
Date	

APPENDIX B: COMMERCIAL PROPOSAL FORMS

Form 1B: Commercial Proposal Submission Letter

To	Virgin Islands Shipping & Maritime Authority
RFP Title	The Provision of Information Technology (IT) Services
RFP Reference No.	VISMA/IT-01/2026
Name of Firm	
Registered Address	
Contact Person	
Email Address	
Total Proposed Price (USD)	

Declaration

- We, the undersigned, hereby submit our Commercial Proposal in response to the Request for Proposal for the provision of Information Technology (IT) Services for VISMA.
- The proposed price includes all professional fees, reimbursable expenses, taxes and other costs necessary to deliver the services, except where otherwise clearly identified.
- We agree to abide by all conditions, requirements and instructions contained in the RFP.
- We acknowledge that VISMA is not bound to accept any proposal received.

VISMA Representative	**Proponent Representative**
Name:	**Name:**
Title:	**Title:**
Signature:	**Signature:**
Date:	**Date:**

Form 2B: Summary of Costs

Cost Category	Description	Amount (USD)
Monthly Managed Service Fee		
Transition / Implementation Fee (if applicable)		
Administrative / Support Costs (if applicable)		
Reimbursable Expenses		

Cost Category	Description	Amount (USD)
Other Costs		
Total Commercial Proposal Amount		

Payment Schedule

Milestone / Deliverable	Expected Timing	Amount (USD)
Total		

Form 3B: Detailed Cost Breakdown

Activity No.	Task / Service Line	Team Member / Role	Estimated Hours / Days	Rate (USD)	Amount (USD)
1					
2					
3					
4					
5					
Total					

Consultant Rates

Consultant Name	Proposed Role	Rate Basis (Hourly / Daily / Monthly)	Rate (USD)

Form 4B: Reimbursable and Miscellaneous Expenses

No.	Expense Description	Unit	Quantity	Unit Price (USD)	Total Amount (USD)
1					
2					
3					
4					
5					
Subtotal					
Total Reimbursable Amount					

APPENDIX C: INSURANCE AND COMPLIANCE REQUIREMENTS

Proponents must provide evidence of the following, where applicable:

- Professional Indemnity Insurance;
- Cyber Liability Insurance;
- General Liability Insurance;
- Workers' Compensation Insurance (where applicable);
- Any other insurance relevant to the delivery of the proposed services.

VISMA may request additional compliance information, including evidence of legal registration, tax compliance, and references.

APPENDIX D: CURRENT STATE ENVIRONMENT INFORMATION

VISMA may provide current-state information to support proposal development. Proponents shall review such information and clearly identify any assumptions made.

The successful Proponent shall validate and document the current-state environment during the transition phase.

APPENDIX E: SERVICE CATALOGUE AND SCOPE BOUNDARIES

VISMA may provide or finalise a service catalogue setting out service lines, indicative inclusions, exclusions, dependencies, and expected deliverables.

Proponents shall respond against these requirements and clearly state any deviations, assumptions, or service limitations.

APPENDIX F: SERVICE LEVEL REQUIREMENTS

VISMA may issue baseline service level expectations covering incident priorities, response times, resolution targets, reporting requirements, and major incident communication expectations.

Proponents shall either accept the baseline or clearly propose alternatives with justification.

APPENDIX G: GOVERNANCE, REPORTING, AND CONTINUOUS IMPROVEMENT REQUIREMENTS

VISMA requires a structured governance model that includes:

- Monthly operational service review meetings;
- Quarterly governance and strategic review meetings;
- Service reporting;
- Cybersecurity reporting;
- Continuous improvement / innovation tracking.

Proponents shall describe how these requirements will be met and may include sample reports where available.

APPENDIX H: CYBERSECURITY AND DATA PROTECTION REQUIREMENTS

Proponents shall provide a statement describing how cybersecurity and data protection services will be delivered, including:

- Security monitoring model;
- Incident response arrangements;
- Vulnerability management approach;
- Awareness training and testing model;
- Data protection and confidentiality controls;
- Reporting approach.

APPENDIX I: BUSINESS CONTINUITY AND DISASTER RECOVERY REQUIREMENTS

Proponents shall describe their approach to supporting backup, recovery, resilience, and business continuity planning relevant to the services proposed. This may include:

- Backup monitoring;
- Recovery support;
- Disaster recovery considerations;
- Service continuity measures for critical systems.