

GOVERNMENT OF SAINT LUCIA

Ministry of the Public Service, Transport, Information and Utilities Regulation

REQUEST FOR EXPRESSIONS OF INTEREST

CONSULTING SERVICES

FOR

Consultancy to Establish and Operationalise the GOSL Cyber Incident Response Team (CIRT) and Develop the National CIRT Institutional and Operational Framework

Project Name	Caribbean Digital Transformation Project (CARDTP)
Loan/Credit/Grant No.	IDA Credit #6682-LC
Assignment Title	Consultancy to Establish and Operationalise the GOSL Cyber Incident Response Team (CIRT) and Develop the National CIRT Institutional and Operational Framework
REOI Reference No.:	LC-DPS-575690-CS-QCBS
Country	Saint Lucia
Date:	November 18, 2026

The Government of Saint Lucia has received financing from the International Development Association (IDA) (the "Bank") in the form of a Credit (hereinafter called "Credit") toward the cost of the Caribbean Digital Transformation Project. The Ministry of the Public Service, Transport, Information and Utilities Regulation an implementing agency of the Client, intends to apply a portion of the proceeds toward the procurement of consulting services for the establishment and operationalisation of a Government Cybersecurity Incident Response Team (Government CIRT), and the development of the National CIRT Institutional and Operational Framework.

The Government intends to engage a suitably qualified consulting firm to implement the assignment through a Design-Build-Operate-Transfer (DBOT) model over a twelve (12) month implementation period.

The Consultant shall establish and demonstrate Initial Operational Capability by the end of Month 3 and complete the technical and operational transfer of the functioning Government CIRT to designated Government personnel by the end of Month 12. In parallel, the Consultant shall develop the proposed National CIRT Institutional and Operational Framework to guide the future establishment and coordination of a national cybersecurity incident response capability.

The assignment comprises two parallel workstreams:

Workstream A – Government CIRT Establishment and Operationalisation

The Consultant shall design, build, operate and transfer a functioning Government Cybersecurity Incident Response Team (Government CIRT), including responsibility for:

- Assessment of existing cybersecurity capabilities and operational requirements;
- Design of the Government CIRT operating model, governance arrangements, service catalogue and technical architecture;
- Procurement, supply, delivery, installation, configuration, integration, testing and commissioning of the hardware, software, licenses and supporting technologies required for the Government CIRT;
- Establishment and operation of cybersecurity incident reporting, incident registration and case management, incident classification, incident response coordination, cybersecurity advisory and awareness services;
- Delivery of capacity building, mentoring, supervised operations and knowledge transfer activities;
- Progressive transition to Government-led operations and transfer of assets, operational capability, documentation, licenses, support arrangements and institutional knowledge.

Workstream B – National CIRT Institutional and Operational Framework

The Consultant shall develop a proposed National Cybersecurity Incident Response Team (National CIRT) institutional and operational framework, including governance arrangements,

stakeholder coordination mechanisms, implementation roadmap and supporting institutional instruments.

The Government of Saint Lucia now invites eligible consulting firms to indicate their interest in providing the Services. Interested firms should provide information demonstrating that they possess the qualifications and relevant experience required to implement a complex cybersecurity Design-Build-Operate-Transfer assignment.

Shortlisting criteria shall include:

1. Demonstrated experience in the establishment, operationalisation, management and transfer of Computer Security Incident Response Teams (CSIRTs), Cybersecurity Incident Response Teams (CIRTs), Security Operations Centres (SOCs) or comparable cybersecurity incident management capabilities.
2. Demonstrated experience in the design, procurement, supply, deployment, integration, testing and commissioning of cybersecurity technologies, platforms and secure technical environments.
3. Demonstrated experience providing managed cybersecurity services, incident response services, security operations or cybersecurity operational support functions.
4. Demonstrated experience undertaking Design-Build-Operate-Transfer (DBOT), Build-Operate-Transfer (BOT) or comparable end-to-end implementation assignments involving operational technology transfer and institutional capacity development.
5. Demonstrated experience in cybersecurity governance, institutional development, cybersecurity operating models, incident response frameworks and operational procedures.
6. Demonstrated experience in capacity building, mentoring, operational readiness, competency transfer and transition to client-led operations.
7. Demonstrated experience managing hardware, software, licensing, warranty, maintenance, supplier and subcontractor arrangements as part of integrated cybersecurity implementation assignments.
8. Experience supporting governments, public sector organisations, regional institutions or other multi-stakeholder operating environments.
9. Experience in developing national cybersecurity frameworks, national incident response arrangements, cybersecurity governance mechanisms or institutional coordination frameworks will be an advantage.

The attention of interested Consultants is drawn to the World Bank's Procurement Regulations for IPF Borrowers. A Consultant will be selected using the Quality and Cost-Based Selection (QCBS) method.

Consultants may associate with other firms in the form of a joint venture or a subconsultancy to enhance their qualifications.

For shortlisting purposes, the qualifications and relevant experience of all members of a joint venture will be considered collectively. However, the qualifications and experience of proposed subconsultants will not be taken into account in determining whether a consulting firm meets the shortlisting criteria.

Consultants submitting Expressions of Interest as a joint venture shall clearly identify the proposed members and the lead firm. Where subconsultants are proposed, their intended roles should also be indicated.Key Experts will not be evaluated at the shortlisting stage and shall not be required to submit curriculum vitae with the Expression of Interest.

Further information can be obtained at the address below during office hours

Attention: Mrs. Sheralin Monrose-Gustave
Project Manager
Caribbean Digital Transformation Project (CARDTP)
Division of Public Sector Modernization
Ministry of the Public Service, Transport, Information and Utilities Regulations
William Peter Boulevard, Castries, St. Lucia
Tel: (758) 468-4977 / 468-1407
Email: sheralin.monrose@govt.lc, copied to cardtpslu@gmail.com

Expressions of Interest must be submitted electronically via email to **cardtpslu@gmail.com**, with a copy to **sheralin.monrose@govt.lc**, no later than **11:59 PM, Eastern Caribbean Time on January 8, 2027**.

The detailed Terms of Reference (TOR) for the assignment can be found below.



GOVERNMENT OF SAINT LUCIA

Ministry of the Public Service, Transport, Information and Utilities Regulation

TERMS OF REFERENCE

FOR

Consultancy to Establish and Operationalise the GOSL Cyber Incident Response Team (CIRT) and Develop the National CIRT Institutional and Operational Framework

1.0 Background and Purpose

The Government of Saint Lucia (GOSL), through the Caribbean Digital Transformation Project (CARDTP), is implementing initiatives to strengthen digital government, enhance cybersecurity, improve institutional resilience and promote the secure delivery of public services. As Government institutions increasingly depend on interconnected information and communication technology (ICT) systems, there is a growing need for coordinated mechanisms to prevent, identify, report, assess and respond to cybersecurity incidents that may compromise Government information, infrastructure and essential services.

The Government recognizes that effective cybersecurity incident response requires clearly defined institutional responsibilities, trained personnel, operational procedures, secure incident reporting and information-sharing mechanisms, appropriate technologies, and sustainable arrangements for coordinating and managing cybersecurity incidents.

Two complementary planning instruments provide the foundation for this assignment:

- **The CIRT Establishment Plan**, which identifies Information Security Incident Management and Knowledge Transfer, including cybersecurity awareness and training, as priority services for initial CIRT establishment and provides recommendations concerning its organization, operations and development.
- **The National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030)**, which identifies national priorities for cybersecurity governance, critical information infrastructure protection, incident response, cybersecurity awareness, workforce development, and national, regional and international cooperation.

Together, these instruments recognize the need to strengthen Government's immediate cybersecurity incident response capability while progressively developing the institutional and coordination arrangements necessary to support a broader national response capability. The Consultant shall build upon these instruments and relevant supporting deliverables made available by Government, avoiding duplication of completed work.

Against this background, the Government intends to engage a suitably qualified consulting firm under a **twelve (12)-month Design–Build–Operate–Transfer (DBOT) model** to stand up a functional **Government Cybersecurity Incident Response Team (Government CIRT)**.

A single firm shall be responsible for all four DBOT phases. Its responsibilities shall include the design, procurement, supply, installation, configuration, integration, testing and commissioning of the hardware and software required for the Government CIRT; operation and support of the agreed services during the contract; and transfer of the functioning capability to designated Government personnel.

The Government CIRT shall initially support Government ministries, departments and agencies through coordinated incident reporting, assessment, triage, response coordination, cybersecurity advisories, awareness activities and related operational services. The Consultant shall establish and demonstrate Initial Operational Capability within the first three (3) months, using the supplied technologies, approved existing Government resources and appropriate

Consultant-provided interim arrangements where necessary. Additional agreed capabilities shall be developed progressively within the twelve-month assignment.

Government shall provide the agreed physical premises, base utilities and internet connectivity, designated counterpart personnel, and the legal and administrative authority required for operations. The Consultant shall identify and validate the requirements for these inputs during inception. Government-provided facilities shall not remove the Consultant's responsibility to supply and integrate the CIRT-specific hardware and software included in the contract.

In parallel, the Consultant shall assist Government in developing the **institutional, governance and operational coordination framework for a National Cybersecurity Incident Response Team (National CIRT)**. This work shall include recommendations on the national mandate, institutional arrangements, stakeholder responsibilities, information sharing, incident coordination and a phased implementation roadmap consistent with the National Cybersecurity Strategy.

The Government CIRT shall constitute the principal operational DBOT deliverable. The National CIRT framework shall provide the institutional and strategic foundation for Government's consideration and subsequent implementation. Formal institutional designation, adoption of legal instruments, Cabinet approval and legislative action shall remain Government responsibilities. Establishment of the Government CIRT shall not, by itself, constitute establishment of a nationwide National CIRT.

Bidders shall include in their technical proposals a proposed technical architecture identifying the main hardware and software components, their functionalities, integration arrangements and dependencies on Government-provided resources. Solutions shall be cost-effective, secure, scalable, interoperable and sustainable. Both open-source and proprietary solutions may be proposed, with particular attention to Government's ability to operate and maintain the solution after the Bank-financed project ends.

Financial proposals shall include all acquisition, licensing, implementation, operation, maintenance, support, training and transfer costs required throughout the DBOT period, together with estimated recurrent costs following transfer to Government.

The consultancy shall use a hybrid delivery model supported by targeted in-country missions, practical operational mentoring and direct participation by designated Government personnel. This delivery model shall not diminish the Consultant's accountability for technology delivery, operational performance or successful transfer.

The Consultant shall demonstrate the agreed operational capabilities and ensure appropriate arrangements for asset ownership, software licensing, documentation, Government administrative access, knowledge transfer, warranty coverage and continuity of operations following transfer.

By the conclusion of the twelve-month assignment, Government expects to have a functioning Government CIRT under Government operational control, trained personnel capable of performing the agreed core functions, the supplied technology and associated rights transferred

as required by the contract, and a completed institutional and implementation framework to guide future National CIRT development.

2.0 Objectives and Required Results

2.1 Overall Objective

The overall objective is to strengthen the Government of Saint Lucia's cybersecurity incident response capability by engaging a single consulting firm to design, build, operate and transfer a functioning Government Cybersecurity Incident Response Team (Government CIRT) within twelve (12) months.

The assignment shall include the procurement, supply, installation, configuration, integration, testing and commissioning of the required hardware and software; delivery and support of the agreed operational services; development of Government personnel competencies; and transfer of the functioning capability, assets, applicable licence rights, documentation and operational control to Government.

In parallel, the Consultant shall develop a proposed institutional, governance and operational coordination framework and phased implementation roadmap for the future National Cybersecurity Incident Response Team (National CIRT). Formal adoption of that framework and establishment of the National CIRT shall remain Government responsibilities.

The assignment shall build upon the CIRT Establishment Plan, the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030), and relevant supporting deliverables made available by Government, avoiding duplication of completed work.

2.2 Specific Objectives

Objective 1 — Design Build Operate and Transfer the Government CIRT

To establish a sustainable Government CIRT capable of delivering the agreed cybersecurity incident management and related services to Government ministries, departments and agencies.

The Consultant shall:

1. Develop and submit for Government approval the proposed operational mandate, service catalogue, organizational arrangements, technical architecture, staffing requirements and operating procedures. Formal institutional authority and Government staff appointments shall remain Government responsibilities.
2. Finalize the detailed technical specifications and procure, supply, deliver, install, configure, integrate, test and commission all hardware, software, licences and supporting services included in the agreed Government CIRT scope, consistent with the accepted technical proposal and awarded contract price.
3. Conduct a joint baseline SIM3 maturity assessment with designated Government personnel during the Design phase. Develop realistic, measurable targets for selected capabilities, with supporting evidence requirements, responsibilities and implementation milestones, for Government approval.

4. Establish and demonstrate Initial Operational Capability by the end of Month 3, prioritizing Information Security Incident Management and Knowledge Transfer, including cybersecurity awareness, training and advisory services. Any necessary interim technologies and services shall be provided within the Consultant's agreed contractual scope and price.
5. Operate, maintain and support the Government CIRT's agreed services from Initial Operational Capability through final transfer. The Consultant shall remain accountable for operational performance, technology availability and the performance of its suppliers and subcontractors.
6. Progressively implement and strengthen the additional capabilities specified in the agreed scope, including incident analysis, response coordination, situational awareness, vulnerability coordination and security event management. Implementation priorities shall not reduce mandatory contractual requirements.
7. Deliver practical cybersecurity awareness, stakeholder engagement, role-based training, supervised incident handling, operational mentoring and exercises to develop the competencies of designated Government personnel.
8. Establish and test emergency escalation and on-call arrangements for high-severity and critical incidents, consistent with the prescribed service levels. Continuous staffed twenty-four-hour security operations shall not be required unless expressly included in the agreed scope.
9. Facilitate an independent SIM3 assessment at least two months before contract completion and address identified deficiencies within the Consultant's contractual responsibilities before final handover.
10. Progressively transfer routine operational leadership to designated Government personnel during Months 9–12 and demonstrate their ability to perform the agreed core functions.
11. Complete the transfer of the functioning Government CIRT by Month 12, including physical assets, applicable software usage rights, support entitlements, administrative access, technical documentation, operational records, procedures and institutional knowledge.
12. Provide the verified Asset Register, executed Title Transfer Document, applicable licence and support assignments, Warranty and Latent Defects Schedule, and sustainability information required for continued Government operation.

Objective 2 — Develop the National CIRT Institutional and Operational Framework

To provide Government with a comprehensive, consultation-informed proposed framework for the future establishment and development of a sustainable National CIRT.

The Consultant shall:

1. Assess existing national cybersecurity institutional arrangements, policies, mandates, stakeholder responsibilities and coordination mechanisms.

2. Develop recommendations concerning the National CIRT's mandate, institutional positioning, governance, accountability, organizational structure and relationship with the Government CIRT.
3. Define proposed arrangements for national incident reporting, information sharing, incident classification, escalation and response coordination across Government and priority critical sectors.
4. Facilitate consultations with relevant Government entities, critical infrastructure stakeholders and designated national, regional and international partners.
5. Prepare draft governance instruments, institutional procedures, stakeholder coordination protocols and supporting documentation for Government consideration and legal review, where required.
6. Develop a phased implementation roadmap identifying service priorities, institutional dependencies, staffing, technology, indicative establishment and recurrent costs, sustainability requirements and implementation stages.
7. Submit a substantive draft framework by Month 6 and a final proposed framework by Month 8, incorporating consolidated Government and stakeholder feedback.
8. Provide technical and institutional advice to support Government consideration of the proposed framework. Formal designation, policy adoption, legal enactment, funding approval and staff appointments shall remain Government responsibilities.

2.3 Required Results

The consultancy shall achieve the following results within the twelve-month implementation period:

1. **Approved Technical Design and Build Baseline:** Within thirty (30) calendar days, the Consultant submits the Technical Architecture and Build Specifications, including the components to be supplied, licensing and support arrangements, implementation schedule, Government interface requirements and technical acceptance procedures, for Government approval.
2. **Government CIRT Initial Operational Capability:** By the end of Month 3, secure incident reporting channels, incident registration and case management, initial triage and classification, escalation and response coordination, cybersecurity advisory dissemination and initial awareness activities are functioning and demonstrated through an agreed operational exercise.
3. **Delivered and Commissioned Technology:** The complete contracted hardware and software solution is supplied, installed, securely configured, integrated, tested and commissioned within the approved Build Schedule. Interim arrangements shall not substitute for completion of the agreed Build obligations unless expressly authorised through contractual change control.
4. **Demonstrated Operational Services:** From Initial Operational Capability through final transfer, the Consultant delivers and supports the agreed services, supported by operational records, service-level reporting, exercises, maintenance and corrective actions.

5. **Demonstrated Personnel Competence:** Designated Government personnel receive structured training, practical mentoring and supervised operational experience and demonstrate competence in their assigned core CIRT functions.
6. **Government-Led Operations:** During Months 9–12, Government personnel progressively assume primary responsibility for routine operations, with the Consultant retaining its contractual delivery and support obligations until final acceptance.
7. **Verified Maturity Progress:** A joint SIM3 baseline and agreed targets guide implementation. An independent assessment is completed at least two months before contract completion, with documented findings, corrective actions and evidence of resolution of deficiencies within the Consultant's responsibility.
8. **Verified Transfer Readiness:** By Month 11, the Government-led operational readiness assessment is completed, the Asset Register is verified, draft transfer documents are prepared, and outstanding corrective actions have assigned responsibilities and completion dates.
9. **Completed Government CIRT Transfer:** By Month 12, the agreed core services function under Government operational control. Required assets, licence rights, support entitlements, administrative access, documentation, records and responsibilities are transferred, supported by executed handover documents and the Warranty and Latent Defects Schedule.
10. **Completed National CIRT Framework:** A substantive draft is submitted by Month 6 and a final proposed institutional and operational framework by Month 8, including governance arrangements, coordination mechanisms, supporting draft instruments, resource requirements and a phased implementation roadmap. Acceptance of this consultancy output shall not depend on subsequent Government adoption or legislative enactment.
11. **Sustainable Operational Arrangements:** Government receives a practical sustainability plan addressing staffing, recurrent expenditure, licensing, maintenance, supplier support, technology lifecycle management, professional development and operational continuity. The Consultant shall establish the arrangements within its contractual responsibility and clearly identify decisions and funding commitments requiring Government action.

The detailed activities are set out in Section 4. Deliverables, deadlines, verification requirements, acceptance criteria and payment arrangements are consolidated in Section 7. Government-provided premises, personnel, legal authority and other agreed inputs shall be distinguished consistently from the Consultant's full DBOT delivery obligations.

3.0 Implementation Model and Core Principles

The assignment shall be implemented through a twelve (12)-month Design–Build–Operate–Transfer (DBOT) model, with a single Consultant accountable for the complete design, technology supply, implementation, operation and transfer of the Government CIRT.

The Consultant shall concurrently develop the proposed National CIRT institutional and operational framework. The two workstreams shall be coordinated while retaining their distinct operational and institutional deliverables.

3.1 Design–Build–Operate–Transfer Approach

The Consultant shall deliver a functioning Government CIRT, including all hardware, software, licences, integration, operational services, training and transfer activities specified in the agreed contractual scope.

The assignment shall not be considered complete solely through the submission of reports, preparation of specifications, delivery of training or installation of technologies. Completion shall require demonstrated operational capability, competent Government personnel, and verified technical and operational transfer.

Consultant Accountability for Third Parties

Unless otherwise stated, the Consultant shall remain fully responsible for the performance of all subcontractors, suppliers, licensors, service providers and other third parties engaged under this assignment. Government review, approval, participation, acceptance of interim deliverables, or provision of facilities and resources shall not transfer responsibility for delivery of the contracted solution or services from the Consultant to Government.

The Consultant shall implement the following overlapping phases:

Phase 1 — Design — Months 1–2

The Consultant shall assess existing Government cybersecurity capabilities, institutional arrangements, personnel, infrastructure and operational requirements, building upon the CIRT Establishment Plan, National Cybersecurity Strategy and relevant supporting deliverables.

Within thirty (30) calendar days, the Consultant shall submit the Technical Architecture and Build Specifications, including the solution components, quantities, licensing and support arrangements, implementation schedule, Government interface requirements and technical acceptance procedures.

The Consultant and designated Government personnel shall jointly assess baseline maturity using SIM3. During the Design phase, the Consultant shall propose measurable maturity targets for selected capabilities, together with evidence requirements, responsibilities and implementation milestones, for Government approval.

The Consultant shall also initiate preparation of operational procedures, stakeholder engagement, training plans and the proposed National CIRT framework. Required Government decisions concerning staffing, legal authority, premises and access shall be identified and tracked from inception.

Phase 2 — Build — Commencing in Month 1 with Initial Operational Capability by Month 3

The Consultant shall procure, supply, deliver, install, securely configure, integrate, test and commission the hardware, software, licences and supporting components included in the contract.

The Consultant shall establish secure reporting channels, incident registration and case management, classification and triage, escalation and response coordination, initial advisory services, and the supporting operational procedures.

By the end of Month 3, the Consultant shall demonstrate Initial Operational Capability through a Government-witnessed operational exercise. Where necessary, approved Consultant-provided interim technologies shall support this milestone within the agreed contract price.

The complete contracted solution shall be delivered and commissioned according to the approved Build Schedule, allowing sufficient time for operational validation, Government personnel training and final transfer within the twelve-month period. Interim operation shall not replace outstanding Build obligations.

Phase 3 — Operate — Months 3–12

From Initial Operational Capability until final transfer, the Consultant shall operate, maintain and support the agreed Government CIRT services, working alongside designated Government personnel.

Activities shall include incident management, response coordination, cybersecurity advisories, awareness, operational mentoring, exercises, performance monitoring, technology maintenance and implementation of the additional capabilities included in the agreed scope.

Services shall be delivered during standard Government business hours, supported by the prescribed emergency escalation and on-call arrangements for high-severity and critical incidents.

Government personnel shall progressively undertake operational duties. This participation shall not relieve the Consultant of its contractual service and performance obligations before final acceptance.

Phase 4 — Transfer — Months 9–12

The Consultant shall progressively transfer routine operational leadership to designated Government personnel through supervised operations, practical mentoring, competency assessments and readiness exercises.

An independent SIM3 assessment shall be completed at least two months before contract completion, comparing demonstrated maturity against the joint baseline and agreed targets. The Consultant shall facilitate access to evidence and address deficiencies within its contractual responsibility before final handover.

By Month 11, the Consultant shall complete the Government-led operational readiness assessment, verify the Asset Register, prepare draft title and licence transfer documents, and identify corrective actions required for final acceptance.

By Month 12, the Consultant shall complete the technical and operational handover, including physical assets, applicable software rights, support entitlements, administrative access, configurations, documentation, incident records, procedures and institutional knowledge.

Final transfer shall include the executed Title Transfer Document, applicable licence and support assignments, Warranty and Latent Defects Schedule, final competency records, sustainability plan and formal handover record.

Government shall verify that the agreed core services function under its operational control and that designated personnel can perform the required functions. Submission of a final report or expiry of the contract period alone shall not constitute completion.

The four phases shall overlap where necessary. The Consultant shall not defer institutional development, staff training, stakeholder engagement or initial operations until completion of technology procurement. Government shall remain responsible for the agreed premises, counterpart staffing, legal authority and required access and approvals.

3.2 Parallel Workstreams

The assignment shall comprise two complementary workstreams implemented concurrently.

Workstream A — Government CIRT Establishment and Operationalization

This workstream shall encompass the design, establishment, operation, progressive strengthening and transfer of the Government CIRT under the DBOT model.

The Government CIRT shall initially serve Government ministries, departments and agencies. Its initial service priorities shall be Information Security Incident Management and Knowledge Transfer, including cybersecurity awareness, training and advisory services.

Additional capabilities, including situational awareness, vulnerability coordination and information security event management, shall be developed progressively in accordance with the approved implementation plan, operational requirements and available resources.

Workstream B — National CIRT Institutional and Operational Framework

This workstream shall support the development of the institutional, governance and coordination arrangements necessary for the future establishment and operation of a National CIRT.

The Consultant shall assess relevant institutional arrangements, facilitate stakeholder consultations, recommend governance and operational coordination mechanisms, develop supporting instruments and prepare a phased implementation roadmap consistent with the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030).

The Consultant shall examine how the Government CIRT may support or form part of the future national incident response arrangements, without presupposing the final institutional model.

The Consultant shall coordinate the two workstreams to ensure consistency between the Government CIRT's operational arrangements and the proposed national framework, while maintaining their distinct objectives and expected results.

3.3 Hybrid Delivery Model

The consultancy may be delivered through a predominantly remote operating model, supplemented by targeted in-country missions and direct engagement with designated Government personnel.

The Consultant shall propose a delivery arrangement appropriate to the assignment, identifying the responsibilities of remote and onsite personnel, the anticipated timing and purpose of in-country missions, and the arrangements for maintaining effective operational support throughout the DBOT period.

Remote delivery shall not diminish the Consultant's responsibility for achieving the agreed operational milestones, maintaining appropriate service availability, delivering practical training and mentoring, or completing the transfer of capabilities to Government personnel.

All remote access, communication, information exchange and operational support arrangements shall comply with Government-approved security, confidentiality, access control and data protection requirements.

3.4 Government Ownership and Sustainability

The Government shall retain ownership and control of Government CIRT operational information, incident records, approved configurations, documentation, procedures and other contractual outputs, subject to the applicable contractual provisions and third-party intellectual property rights.

The Consultant shall ensure that the Government has the necessary access, documentation, licenses or other agreed rights to continue operating the approved solutions following completion of the assignment.

The Consultant shall avoid unnecessary dependence on proprietary technologies, individual consultants or arrangements that cannot reasonably be sustained by the Government.

All proposed technologies, operating arrangements and staffing requirements shall take account of the Government's institutional capacity, available resources and long-term operational sustainability.

3.5 Technology Procurement and Interim Operational Arrangements

The Consultant shall be responsible for the procurement, supply, delivery, installation, configuration, integration, and commissioning of all hardware, software, and associated infrastructure required to establish the permanent Government CIRT environment. This responsibility constitutes the Build phase of the DBOT model and shall remain with the Consultant, at its risk and within the awarded contract price, subject to Government approval of the technical baseline and any contractual changes requiring prior authorisation.

The Consultant shall prepare and submit for Government approval a Build Plan identifying all technology components to be procured, the proposed supply chain and vendor arrangements, a delivery and installation schedule, cost estimates, licensing and warranty arrangements, and the criteria for Government CIRT technical acceptance.

The Consultant shall ensure that all procured solutions are vendor-neutral where practicable, comply with applicable Government security and interoperability requirements, and are transferable to the Government at the end of the Operate phase without residual financial or licensing encumbrances requiring further Consultant involvement.

The Consultant shall hold all relevant vendor contracts, warranties, and licences in its name during the Build and Operate phases. On Transfer, all contracts, licences, warranties, and support arrangements shall be novated or formally assigned to the Government in accordance with the Transfer requirements under Section 4.9.

The Government shall not procure permanent Government CIRT infrastructure separately unless the Consultant fails to deliver agreed components within the approved schedule and the Government exercises its step-in rights under the contract. Any Government-initiated variation to the approved technology scope shall be subject to the applicable change-control provisions.

Where, pending commencement of the Build phase, interim technologies are required to establish Initial Operational Capability within Month 3, the Consultant shall deploy approved interim solutions at its own cost. Interim arrangements shall be secure, provide for continuity of Government CIRT operations, and shall be managed by the Consultant until the permanent environment is commissioned and accepted.

3.6 Operational Service Availability

The Government CIRT shall initially operate during standard Government business hours, supported by documented emergency escalation and on-call arrangements for high-severity and critical cybersecurity incidents occurring outside normal business hours, including weekends and public holidays.

The Consultant shall establish and test the applicable incident reporting, notification, escalation, response coordination and emergency contact arrangements.

Continuous staffed twenty-four-hour security operations shall not be a mandatory requirement of this consultancy. Automated monitoring and alerting capabilities may be implemented where supported by approved technologies and operational resources.

The minimum incident acknowledgement, triage and escalation service levels shall be those specified in Section 4.6.13. The detailed operational procedures, escalation arrangements and verification mechanisms shall be established through the approved Government CIRT operating model and shall not reduce the prescribed minimum service levels except through an approved contractual amendment.

3.7 Capacity Building and Progressive Government Leadership

The Consultant shall adopt a practical, competency-based approach to capacity development, combining structured training with hands-on operational activities, supervised incident handling, simulations, exercises and progressive transfer of responsibility.

Designated Government personnel shall participate in the establishment and operation of the Government CIRT from the early stages of the assignment.

During Months 9–12, Government personnel shall progressively assume primary responsibility for routine operations, with the Consultant providing mentoring, supervision and technical support.

The Consultant shall assess and document personnel readiness and address identified competency gaps before final transfer.

3.8 Implementation Coordination, Risk Management and Change Control

The Consultant shall maintain an integrated implementation approach covering both workstreams, including dependencies, risks, institutional decisions, staffing availability, technical procurement, stakeholder engagement and operational milestones.

The Consultant shall promptly identify and communicate matters that may affect implementation and recommend appropriate mitigation measures.

Delays or dependencies arising from Government-controlled procurement, approvals or other external processes shall be documented and managed in accordance with the contract. Such dependencies shall not automatically constitute Consultant non-performance, nor shall they result in automatic acceptance of incomplete services or deliverables.

Any material changes to the agreed scope, implementation arrangements, milestones or contractual obligations shall be subject to the applicable contract provisions and required approvals.

3.9 Optional Post-DBOT Support

The Consultant may be requested to provide separately priced options for six (6) and twelve (12) months of post-DBOT technical assistance, mentoring, specialized incident response support or other agreed transitional services.

Any such support shall be optional and subject to separate Government approval, funding availability and the applicable contractual arrangements.

Optional post-DBOT support shall not substitute for the mandatory establishment, operationalization and transfer of the Government CIRT within the twelve-month DBOT period.

4.0 Scope of Services

The Consultant shall undertake the full design, build, operation and transfer of the Government Cybersecurity Incident Response Team (Government CIRT), including procurement and supply of the required hardware, software and licences; installation, configuration, integration, testing and commissioning; operational service delivery and maintenance; capacity building; and final technical and operational handover.

Concurrently, the Consultant shall develop the proposed institutional and operational coordination framework for the future National Cybersecurity Incident Response Team (National CIRT).

The activities shall be implemented through two complementary workstreams under the twelve (12)-month Design–Build–Operate–Transfer (DBOT) model.

The Consultant shall ensure that technical design, technology procurement and implementation, institutional development, interim operational arrangements, cybersecurity awareness, stakeholder engagement and capacity building proceed concurrently where appropriate.

Government-provided inputs and decisions shall be distinguished from the Consultant's delivery obligations.

4.1 Inception and Baseline Assessment

During the initial stage of the assignment, the Consultant shall undertake a focused inception and baseline assessment to establish the institutional, technical and operational conditions necessary for implementing both workstreams.

The assessment shall build upon, rather than duplicate, the findings and recommendations of the existing CIRT Establishment Plan, the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030), and relevant supporting deliverables made available by Government.

The Consultant shall undertake the following activities:

4.1.1 Review of Existing Documentation and Institutional Arrangements

1. Review the CIRT Establishment Plan, National Cybersecurity Strategy and Action Plan, and other relevant Government cybersecurity policies, strategies, assessments and technical documentation.
2. Assess existing cybersecurity governance, institutional responsibilities, operational coordination arrangements and relevant Government ICT security functions.
3. Identify existing capabilities, initiatives and resources that may support Government CIRT establishment and development of the National CIRT framework.
4. Identify significant institutional, technical and operational gaps, dependencies and risks requiring attention during implementation.
5. Map relevant existing recommendations to the proposed implementation activities and explain any departures requiring Government consideration.

4.1.2 Government CIRT Operational Baseline

1. Assess existing Government cybersecurity incident reporting, detection, analysis, escalation, response coordination and recovery support arrangements.
2. Review available Government ICT infrastructure, cybersecurity technologies, communication facilities, secure access arrangements and other resources relevant to establishing the Government CIRT.
3. Confirm the proposed Government CIRT constituency, priority operational services and requirements for achieving Initial Operational Capability by Month 3.
4. Assess existing incident management procedures, reporting channels, information-sharing practices and arrangements for handling sensitive cybersecurity information.
5. Identify existing Government resources that may be reused and any Consultant-provided interim technologies necessary for early operations. Interim arrangements shall be included in the agreed contractual scope and price and shall not replace the Consultant's obligation to deliver the complete contracted solution.
6. Assess the availability, assigned roles and existing competencies of designated Government personnel.
7. Jointly with designated Government personnel, assess baseline maturity using SIM3, recording the methodology, model version, parameter-level findings, supporting evidence and identified gaps.

8. Propose realistic, measurable maturity targets for selected capabilities, with evidence requirements, assigned responsibilities, Government dependencies and implementation milestones, for Government approval during the Design phase.
9. Distinguish deficiencies within the Consultant's delivery responsibilities from matters requiring Government staffing decisions, legal authority, institutional approval or other Government action.

The SIM3 baseline and agreed targets shall guide implementation and provide the reference for the independent assessment required before contract completion. They shall complement, and shall not reduce, the mandatory operational and technical requirements of the assignment.

4.1.3 National CIRT Institutional Baseline

1. Review existing national cybersecurity governance and coordination arrangements relevant to the proposed National CIRT.
2. Identify key institutional stakeholders, including Government entities, relevant regulators, designated critical infrastructure operators and other priority organisations.
3. Assess existing arrangements for incident reporting, information sharing, cross-sector coordination and engagement with regional and international cybersecurity partners.
4. Identify institutional, policy, legal and operational matters requiring consideration in developing the proposed National CIRT framework.
5. Identify how Government CIRT operational arrangements may support future national incident response coordination, subject to Government decisions concerning the national institutional model.
6. Distinguish proposed arrangements that may be implemented under existing authority from those requiring formal designation, additional legal instruments, policy approval or funding commitments.

4.1.4 Inception Planning and Implementation Arrangements

Based on the baseline assessment, the Consultant shall prepare an integrated implementation approach covering both workstreams and all four DBOT phases.

The approach shall address:

1. The methodology, sequencing and coordination of Design, Build, Operate and Transfer activities.
2. The initial Government CIRT service priorities and the implementation pathway for demonstrating Initial Operational Capability by Month 3.
3. Preparation and submission of the Technical Architecture and Build Specifications within thirty (30) calendar days, consistent with Section 4.2.3.
4. The Consultant's procurement, supply, installation, configuration, integration, testing and commissioning arrangements, including supplier responsibilities, delivery milestones and technical acceptance procedures.

5. Assessment of the proposed Government-provided hosting location, including physical security, power, cooling, connectivity and site access, with identified gaps and responsibilities.
6. Arrangements for achieving operational milestones without dependence on National Data Centre reconstruction or a separate Government procurement of the CIRT-specific technologies included in the contract.
7. The methodology and timetable for developing, consulting on and finalising the proposed National CIRT institutional and operational framework.
8. Stakeholder mapping, consultation and engagement arrangements.
9. The hybrid delivery model, including remote activities, necessary in-country missions, expert deployment and responsibilities.
10. Counterpart staffing, role-based training, supervised operations, competency assessment, mentoring and knowledge-transfer arrangements.
11. The SIM3 baseline assessment, proposed maturity targets, evidence collection and arrangements for facilitating an independent assessment at least two months before contract completion.
12. Government readiness requirements concerning designated personnel, premises, lawful operational authority, information sharing, data handling and authorised system access.
13. An implementation risk and dependency register identifying owners, required decisions, deadlines, mitigation measures and escalation procedures.
14. Operational service delivery, performance monitoring, quality assurance, reporting and coordination arrangements.
15. Progressive Government-led operations during Months 9–12, the Month 11 readiness assessment and final technical and operational transfer by Month 12.
16. Change-control arrangements for proposed adjustments to scope, technology, price, milestones or acceptance requirements.

The Consultant shall distinguish its procurement, supplier management and delivery obligations from Government-provided inputs and decisions.

Inception activities shall proceed concurrently with technical design, implementation preparation, institutional development, training and arrangements for initial operations. They shall not delay commencement of activities necessary to meet the mandatory milestones.

The inception outputs shall include the joint SIM3 baseline, the implementation schedule and responsibility and dependency register. Proposed SIM3 targets shall be submitted for approval during the Design phase. Relevant outputs shall be incorporated into the deliverables specified in Section 7.

4.2 Technical Architecture and Build Implementation

The Consultant shall design and deliver a secure, scalable, interoperable and sustainable technical environment for the Government Cybersecurity Incident Response Team (Government CIRT). Its responsibilities shall include procurement, supply, delivery, installation, configuration, integration, testing and commissioning of all hardware, software, licences and supporting services included in the agreed contractual scope.

The Consultant shall operate, maintain and support the supplied solution during the DBOT period and complete its technical and operational transfer to Government.

Within thirty (30) calendar days of contract commencement, the Consultant shall submit the Technical Architecture and Build Specifications for Government approval. This document shall elaborate the solution included in the accepted technical proposal and establish the detailed Build baseline within the awarded contract price.

Government shall provide the agreed premises, base utilities and connectivity, counterpart personnel, access and required authorisations. The Consultant shall identify and validate these interfaces during inception. Implementation shall not depend on separate Government procurement of the contracted CIRT technologies or completion of National Data Centre reconstruction.

4.2.1 Technical Environment Assessment

The Consultant shall assess the existing Government technical environment to confirm the requirements for establishing and operating the Government CIRT.

The assessment shall build upon available technical documentation, cybersecurity assessments, the CIRT Establishment Plan and the inception findings. It shall cover:

1. Existing Government network and security infrastructure.
2. Available hosting, computing, storage and connectivity resources.
3. Existing cybersecurity technologies and monitoring capabilities.
4. Identity management, authentication and privileged access arrangements.
5. Incident reporting and management mechanisms.
6. Logging, audit and information management capabilities.
7. Backup, recovery and operational continuity arrangements.
8. Integration requirements and opportunities for reuse of existing resources.
9. Suitability of the proposed hosting location, including physical security, power, cooling and access.
10. Potential future interfaces with the National Data Centre.
11. Technical and operational constraints affecting implementation.

The assessment shall confirm information necessary for design, technology delivery and operational establishment. It shall not duplicate completed assessments or constitute a new comprehensive Government-wide cybersecurity assessment unless expressly included in the contract.

The Consultant shall record critical information gaps, proposed assumptions, mitigation measures and Government decisions required to maintain the implementation schedule.

4.2.2 Government CIRT Technical Architecture

The Consultant shall prepare an architecture appropriate to the Government CIRT's agreed mandate, service catalogue, operating model and contractual requirements.

The architecture shall address:

1. Secure incident reporting channels.
2. Incident registration, classification, triage and case management.
3. Protection, storage, retrieval and retention of incident information.
4. Secure communication and collaboration.
5. Authentication, access control and privileged administration.
6. Logging, auditing and operational monitoring.
7. Cybersecurity advisory and information-sharing capabilities.
8. Backup, recovery and operational continuity.
9. Network connectivity and secure integration.
10. Hosting, infrastructure and system administration.
11. Interoperability with relevant Government technologies.
12. Scalability and potential future integration with additional capabilities.

The architecture shall distinguish:

- Mandatory components and services included in the contract.
- Existing Government resources approved for reuse.
- Government-provided infrastructure interfaces.
- Optional enhancements or future capabilities outside the mandatory scope.

Mandatory requirements shall not be deferred or reclassified as optional during design without an approved contractual variation.

The architecture shall support standard Government business-hour operations and the prescribed emergency on-call arrangements. It shall not assume a continuously staffed twenty-four-hour Security Operations Centre.

The Consultant shall explain major design decisions, dependencies, security implications, lifecycle costs and sustainability considerations.

4.2.3 Technical Architecture and Build Specifications

Within thirty (30) calendar days of contract commencement, the Consultant shall submit for Government approval a Technical Architecture and Build Specifications document. This document shall constitute the detailed Build Plan and govern the Consultant's procurement, supply, installation, integration, testing and commissioning activities under Sections 3.5 and 4.5.

The document shall include:

1. Detailed technical architecture and system design.
2. Functional and non-functional requirements consistent with the contractual scope.
3. An itemised bill of materials identifying hardware, software, quantities, licences and supporting services to be supplied.

4. Hosting, connectivity, site readiness and infrastructure requirements, distinguishing Consultant obligations from Government-provided inputs.
5. Security, interoperability, integration, data protection, access control, logging and audit requirements.
6. Backup, recovery and operational continuity arrangements.
7. Installation, configuration, commissioning and testing procedures.
8. Measurable acceptance criteria and test protocols for Government verification under Section 4.5.7.
9. Supplier and subcontractor arrangements, delivery milestones and implementation sequencing consistent with Section 4.5.1.
10. Licensing, warranty, maintenance and support arrangements, including Government rights and entitlements after transfer.
11. A breakdown of acquisition, implementation, licensing and support costs included in the contract price, together with projected post-transfer recurrent costs.
12. A compliance matrix demonstrating how the components and integrated solution meet the contractual requirements.
13. Technical risks, dependencies and mitigation measures.
14. Any interim arrangements necessary for Month 3 Initial Operational Capability and their transition to the complete contracted solution.

Government shall provide written approval or consolidated comments within ten (10) working days of submission. The Consultant shall incorporate agreed comments and resubmit within five (5) working days. Procurement and supply of the proposed solution components shall proceed following written approval.

The Consultant shall schedule submissions, reviews and procurement to achieve the mandatory milestones. Proposed changes to scope, price or completion dates shall follow the applicable contractual change-control procedures.

4.2.4 Technology Selection and Procurement Safeguards

The Consultant shall use objective, performance-based requirements and justify its technology choices against the agreed scope.

The Consultant shall:

1. Define requirements in terms of functionality, performance, security and interoperability.
2. Consider recognised standards and accepted cybersecurity practices.
3. Avoid unjustified restrictions on interoperability or future supplier choice.
4. Evaluate open-source and proprietary options on functionality, security, supportability and lifecycle cost.
5. Disclose supplier affiliations, commercial interests and potential conflicts of interest.
6. Identify licensing restrictions and arrangements that could create unnecessary vendor dependency.
7. Explain compatibility requirements affecting product selection.

8. Maintain records supporting the compliance of selected components.
9. Comply with procurement and subcontracting requirements applicable to the contract.
10. Obtain approval for substitutions affecting the approved technical baseline.

The Consultant shall select and manage suppliers within its agreed contractual scope and approved Build Plan. It shall not exercise Government approval powers or enter into additional commitments on Government's behalf.

4.2.5 Security Privacy and Information Protection Requirements

The Consultant shall incorporate, implement and test appropriate security controls in the supplied solution, including:

1. Role-based access control and least-privilege administration.
2. Strong authentication and protection of privileged accounts.
3. Secure configuration and system hardening.
4. Encryption of sensitive information in transit and at rest, as appropriate.
5. Protection of incident records and supporting evidence.
6. Audit logging and accountability for administrative actions.
7. Secure remote access.
8. Backup, recovery, retention and secure disposal.
9. Vulnerability management and security updates.
10. Secure integration and appropriate segregation of environments.
11. Protection of confidential Government information.
12. Secure migration and termination of temporary services.
13. Security testing and documented remediation.

External hosting or third-party processing of Government information shall require prior Government approval. The Consultant shall disclose proposed processing locations, third-party access and relevant dependencies.

Controls shall reflect the sensitivity of the information and Government-approved requirements. Identified security deficiencies within the Consultant's scope shall be corrected before the relevant acceptance milestone.

4.2.6 Interoperability and Integration Planning

The Consultant shall prepare and implement an integration approach covering:

1. Systems and infrastructure requiring integration.
2. Technical interfaces and information exchange requirements.
3. Compatibility with existing Government security and ICT arrangements.
4. Dependencies on existing third-party systems and providers.
5. Authentication, communication and data protection requirements.
6. Configuration, integration testing and commissioning activities.
7. Responsibilities of the Consultant, its suppliers and subcontractors, Government personnel and providers of existing Government systems.

8. Implementation sequencing and testing milestones.
9. Risks arising from incompatible systems, unavailable information or delayed access.
10. Measures supporting future interoperability and expansion.

4.2.7 Technology Lifecycle and Sustainability Assessment

The Consultant shall assess and document:

1. Acquisition and implementation costs included in the contract.
2. Licence and subscription terms, expiry dates and renewal requirements.
3. Maintenance and technical support costs.
4. Hosting, connectivity and infrastructure operating costs.
5. Security updates, component replacement and technology refresh.
6. Backup, recovery and storage requirements.
7. Required system administration competencies.
8. Supplier dependencies and support availability.
9. Scalability and future capacity needs.
10. Risks of obsolescence, discontinued products or unsupported software.

The lifecycle assessment shall use clearly stated assumptions and a planning horizon agreed with Government. It shall distinguish costs included in the DBOT contract, mandatory post-transfer recurrent expenditure and optional enhancements.

The Consultant shall identify significant recurring obligations before Government approves the technical baseline and recommend sustainable alternatives where appropriate. Government shall not be committed to additional expenditure without the required approval.

4.2.8 Technology Procurement and Supplier Management

The Consultant shall procure and manage all hardware, software, licences and supporting services within its agreed scope.

Its responsibilities shall include:

1. Confirming specifications, quantities and supplier arrangements.
2. Managing purchasing, delivery, installation and commissioning.
3. Verifying compliance with technical, security and interoperability requirements.
4. Coordinating suppliers and subcontractors.
5. Resolving delivery, compatibility, installation and integration deficiencies.
6. Maintaining a component-level delivery and compliance tracker.
7. Providing evidence of valid licences, warranties and support entitlements.
8. Securing Government ownership or usage rights and continuity of support.
9. Arranging replacement or correction of defective or non-compliant components.
10. Obtaining approval for changes affecting the technical baseline or contractual requirements.

All costs required for the mandatory DBOT scope shall be included in the agreed contract price.

Government shall approve the technical baseline, authorise contractual changes and verify acceptance. These functions shall not transfer procurement or supplier-management responsibility to Government.

4.2.9 Interim Technology Transition Planning

Where interim technologies are used, the Consultant shall prepare and implement a transition plan covering:

1. Interim systems and services to be replaced or retained.
2. Delivery and commissioning of the contracted solution.
3. Migration of incident records, configurations and other Government information.
4. Compatibility and integration requirements.
5. Data protection, security testing and validation.
6. Backup, recovery and rollback procedures.
7. Continuity of core services during migration.
8. Government personnel participation and knowledge transfer.
9. Termination of temporary licences, hosting and supplier access.
10. Secure decommissioning and disposal where applicable.

Necessary interim arrangements and migration activities shall be included in the contract price. The Consultant shall preserve service continuity and Government access throughout the transition.

Continued interim operation shall not substitute for completion of the agreed solution unless expressly authorised through contractual change control.

4.2.10 Technical Documentation and Knowledge Transfer

The Consultant shall prepare and maintain:

1. Approved architecture and interface diagrams.
2. Build specifications, component schedules and the Asset Register.
3. Installation, configuration and integration records.
4. Security configuration and access control documentation.
5. Technical operating and administration procedures.
6. Backup, recovery and continuity procedures.
7. Testing, commissioning and acceptance records.
8. Licensing, warranty, subscription and support information.
9. Defect, risk and dependency registers.
10. Maintenance, update and lifecycle guidance.
11. Transfer requirements and evidence of Government ownership, usage rights and support entitlements.

Documentation shall reflect the actual environment supplied and transferred. It shall be delivered in accessible, editable formats where applicable, subject to disclosed third-party intellectual property restrictions.

Designated Government personnel shall participate in design reviews, installation, testing, administration and practical knowledge-transfer activities. Administrative credentials shall be transferred through secure, Government-approved procedures.

These requirements shall be coordinated with Section 4.5 and the final handover obligations under Section 4.9.

4.3 Institutional Establishment and Governance

The Consultant shall develop and support the implementation of appropriate institutional, governance and operational coordination arrangements for the Government Cybersecurity Incident Response Team (Government CIRT), while concurrently developing a draft comprehensive institutional and governance framework to guide the future establishment of the National Cybersecurity Incident Response Team (National CIRT).

The assignment shall distinguish between:

a. **Government CIRT:** The operational cybersecurity incident response capability to be established, operated and transferred to designated Government personnel within the twelve-month Design–Build–Operate–Transfer (DBOT) period; and

b. **National CIRT:** The proposed national-level institutional and coordination framework to be developed through stakeholder consultation, technical assessment and policy recommendations for subsequent Government consideration and implementation.

The Consultant shall build upon the existing CIRT Establishment Plan, the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030), and relevant Government policies, institutional arrangements and implementation decisions.

The Consultant shall avoid duplicating completed strategic assessments and shall focus on producing practical, implementation-ready institutional arrangements and governance instruments.

The Consultant shall assess institutional requirements, develop recommendations, prepare draft instruments and support implementation of Government-approved arrangements within its contractual scope. Government shall remain responsible for formally establishing the Government CIRT, conferring its mandate and authority, designating personnel, and adopting the legal or administrative instruments required for lawful operations, incident reporting, information sharing and data handling. The Consultant shall identify and track these prerequisites early enough to support Month 3 Initial Operational Capability. Preparation of the proposed National CIRT framework shall not constitute its formal adoption or the establishment of a nationwide National CIRT.

4.3.1 Government CIRT Institutional Establishment

The Consultant shall develop and support the implementation of the institutional arrangements necessary for the effective establishment and operation of the Government CIRT.

These activities shall include:

1. Reviewing and confirming the proposed Government CIRT mandate, institutional placement, scope of responsibility and operational constituency.
2. Defining the respective institutional, management and operational responsibilities of the Ministry responsible for the Public Service, Government Information Technology Services (GITS), designated Government CIRT personnel and participating Government institutions.
3. Developing an appropriate organizational structure, reporting relationships, staffing roles and operational responsibilities.
4. Preparing a Government CIRT charter or equivalent establishment instrument defining its purpose, mandate, authority, service scope and accountability arrangements.
5. Establishing a practical governance and decision-making structure for Government CIRT operations, including arrangements for operational supervision, management reporting and institutional escalation.
6. Defining the Government CIRT's initial service catalogue, distinguishing mandatory core services from additional capabilities to be introduced progressively.
7. Establishing institutional arrangements for incident reporting, information sharing, coordination and escalation among participating Government ministries, departments and agencies.
8. Identifying relevant legal, policy, administrative and institutional requirements affecting Government CIRT operations.
9. Developing arrangements for the protection, confidentiality, authorized disclosure and management of cybersecurity incident information.
10. Supporting the designation and orientation of Government CIRT personnel and institutional ICT focal points.
11. Identifying institutional and operational decisions requiring Government consideration and providing the necessary technical advice and supporting documentation.

The proposed arrangements shall be proportionate to the Government CIRT's initial mandate, staffing, operational capabilities and available resources.

The Consultant shall support the Government in putting into effect those arrangements that fall within the approved scope and authority of the participating institutions.

4.3.2 Government CIRT Governance and Operational Authority

The Consultant shall establish clear governance and operational authority arrangements to support the consistent, accountable and secure delivery of Government CIRT services.

These arrangements shall define:

1. Responsibility for receiving, assessing, prioritising and coordinating responses to reported cybersecurity incidents.
2. The respective roles of Government CIRT personnel, affected Government institutions, ICT administrators, senior management and other relevant authorities.
3. Authority for operational decisions, including incident escalation, requests for technical assistance and recommendations for containment or recovery actions.
4. Procedures for obtaining approval before undertaking actions that may affect Government systems, services, data or institutional operations.
5. Arrangements for escalating significant cybersecurity incidents to appropriate Government decision-makers.
6. Responsibility for issuing cybersecurity advisories, operational notifications and other authorised communications.
7. Requirements for maintaining incident records, decision logs, operational reports and supporting evidence.
8. Confidentiality, information-sharing and access control arrangements.
9. Accountability and reporting arrangements for Government CIRT operational performance.
10. Coordination with other Government security, ICT, business continuity and emergency management functions, where applicable.

The Consultant shall ensure that operational procedures and governance arrangements are mutually consistent and clearly distinguish the Government CIRT's coordination and advisory responsibilities from the authority retained by individual Government institutions and other competent authorities.

The Government CIRT shall not be assumed to possess statutory, regulatory, law enforcement or other powers that have not been lawfully conferred upon it.

4.3.3 National CIRT Institutional and Governance Framework

The Consultant shall develop a draft comprehensive proposed institutional and governance framework for the future establishment and operationalization of the National CIRT.

The framework shall be consistent with the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030) and shall reflect Saint Lucia's institutional, legal, technical and financial context.

The Consultant shall:

1. Assess relevant existing institutional mandates, responsibilities and cybersecurity coordination arrangements.
2. Identify and evaluate feasible institutional placement and governance options for the proposed National CIRT.

3. Recommend an appropriate institutional model, including its mandate, organizational structure, accountability and reporting arrangements.
4. Define the proposed national constituency, scope of services and relationships with Government institutions, critical infrastructure operators and other relevant stakeholders.
5. Identify the proposed roles and responsibilities of the National CIRT in national cybersecurity incident coordination, information sharing, advisories and cooperation.
6. Recommend arrangements for coordination between the operational Government CIRT and the proposed National CIRT.
7. Determine whether and how the Government CIRT could serve as an operational foundation for subsequent National CIRT development.
8. Identify the institutional, legal, regulatory and administrative requirements necessary to support the proposed National CIRT mandate.
9. Recommend appropriate governance, oversight and accountability mechanisms.
10. Identify the resources, personnel competencies, technical capabilities and operating arrangements required for phased implementation.

The Consultant shall clearly distinguish between arrangements that may be implemented administratively under existing Government authority and those requiring additional policy decisions, formal designation, legislation or other approvals.

The Government CIRT shall not automatically be designated or treated as the National CIRT by virtue of its establishment under this consultancy.

4.3.4 National Cybersecurity Coordination and Stakeholder Engagement

The Consultant shall develop proposed national cybersecurity coordination arrangements through structured engagement with relevant public and private sector stakeholders.

The Consultant shall identify and consult, as appropriate, with:

1. Relevant Government ministries, departments and agencies.
2. Institutions responsible for national security, public safety and emergency management.
3. Relevant regulatory and oversight authorities.
4. Telecommunications and digital infrastructure stakeholders.
5. Operators of critical information infrastructure and essential services.
6. Representatives of other priority sectors identified through the National Cybersecurity Strategy and stakeholder assessment.
7. Appropriate regional and international cybersecurity cooperation partners.

The Consultant shall:

a. Prepare a stakeholder mapping and consultation plan identifying the relevant institutions, proposed engagement methods and expected consultation outcomes.

b. Assess existing cybersecurity incident reporting, coordination and information-sharing arrangements among relevant stakeholders.

c. Identify institutional gaps, overlapping responsibilities, coordination challenges and opportunities for strengthening cooperation.

d. Develop proposed arrangements for national cybersecurity incident notification, escalation, information sharing and coordination.

e. Recommend appropriate mechanisms for engagement with critical infrastructure operators and essential service providers.

f. Identify confidentiality, information protection and information-sharing requirements applicable to the proposed coordination arrangements.

g. Facilitate technical consultations and validation sessions to review the proposed institutional and coordination framework.

h. Document stakeholder feedback, significant areas of agreement, unresolved institutional matters and recommendations requiring Government consideration.

The Consultant shall ensure that proposed arrangements respect the statutory mandates and responsibilities of participating institutions.

Formal designation of critical infrastructure, mandatory reporting obligations and other regulatory requirements shall remain subject to the relevant Government and competent authority processes.

4.3.5 Governance Instruments and Institutional Documentation

The Consultant shall prepare practical draft instruments and supporting documentation necessary to facilitate Government consideration and subsequent implementation of the proposed National CIRT arrangements.

These shall include, as appropriate:

1. A proposed National CIRT charter or equivalent institutional establishment instrument.
2. A proposed mandate, functions and organisational structure.
3. Draft terms of reference for the proposed national cybersecurity coordination or governance body, where applicable.
4. Proposed membership, reporting, decision-making and secretariat arrangements for relevant coordination mechanisms.
5. Draft institutional coordination protocols identifying responsibilities and escalation pathways.

6. Proposed incident reporting and information-sharing protocols for participating stakeholders.
7. Draft confidentiality and information-sharing templates, as appropriate.
8. Proposed arrangements for coordination with critical infrastructure operators and other relevant institutions.
9. Institutional options and recommendations addressing legal, policy and administrative requirements.
10. A proposed phased institutional establishment and operational development approach.

The Consultant shall ensure that the instruments are mutually consistent, practical and sufficiently developed to support Government review and subsequent implementation.

The Consultant shall identify any instruments that require legal review, formal institutional endorsement, Cabinet consideration or other Government approval before they may take effect.

The preparation of draft instruments shall not constitute their formal adoption or legal enactment.

4.3.6 Government Decision-Support and Approval Documentation

The Consultant shall provide technical and institutional support to facilitate Government consideration of the proposed National CIRT framework.

This shall include:

1. Identifying the principal policy, institutional, financial and administrative decisions required to advance the establishment of the National CIRT.
2. Preparing a concise assessment of recommended institutional options and the rationale for the preferred approach.
3. Documenting the proposed mandate, governance structure, implementation requirements, resource implications and expected benefits.
4. Identifying relevant legal and regulatory matters requiring further review or action.
5. Preparing draft technical and institutional material suitable for incorporation into Cabinet submissions, ministerial briefs or other Government decision-making documents, where required.
6. Supporting technical presentations and consultations with designated Government representatives.
7. Revising the proposed framework and supporting documentation to address consolidated Government comments.

The Consultant shall be responsible for preparing the agreed technical and institutional documentation but shall not be responsible for obtaining Cabinet approval, securing legislative amendments or making decisions reserved for the Government.

4.3.7 Phased National CIRT Implementation Roadmap

The Consultant shall draft a practical, phased roadmap to guide the future establishment and operational development of the National CIRT.

The roadmap shall identify:

1. Recommended institutional establishment and governance actions.
2. Required policy, legal, regulatory and administrative measures.
3. Proposed staffing structure, competencies and recruitment or capacity-building requirements.
4. Initial and progressively expanded National CIRT services.
5. Technical infrastructure, systems and operational support requirements.
6. Stakeholder coordination and information-sharing arrangements.
7. Indicative establishment and recurrent operating costs.
8. Proposed implementation phases, priorities and indicative timeframes.
9. Institutional responsibilities and critical dependencies.
10. Key risks, mitigation measures and proposed indicators for monitoring implementation progress.

The roadmap shall distinguish between actions that may be undertaken during the present consultancy and subsequent actions requiring additional Government decisions, resources or implementation arrangements.

The roadmap shall be realistic, financially informed and aligned with the priorities of the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030).

4.3.8 Validation and Institutional Knowledge Transfer

The Consultant shall facilitate appropriate Government review and stakeholder validation of the proposed institutional and governance arrangements.

The Consultant shall:

1. Present the proposed Government CIRT governance arrangements to designated Government counterparts.
2. Support the practical implementation and understanding of approved Government CIRT institutional procedures.
3. Facilitate review of the proposed National CIRT framework with relevant Government authorities and identified stakeholders.
4. Document and address consolidated technical and institutional comments.
5. Explain the proposed governance instruments, coordination arrangements and implementation dependencies to designated Government personnel.
6. Transfer the final draft instruments, consultation records, institutional assessments and supporting documentation to the Government.
7. Provide recommendations on the next steps required to advance the National CIRT framework through the appropriate Government processes.

The Consultant shall complete the institutional and governance activities within the agreed twelve-month implementation period and in accordance with the deadlines established in Section 7.

Formal adoption of the proposed National CIRT institutional framework shall remain subject to the relevant Government approval processes and shall not be a prerequisite for acceptance of satisfactorily completed consultancy outputs.

4.4 Establishment of Initial Operational Capability

The Consultant shall establish and demonstrate Government CIRT Initial Operational Capability (IOC) by the end of Month 3.

The Consultant shall implement the initial operating arrangements and technology capabilities necessary to deliver the agreed core services. These shall include secure incident reporting channels, incident registration and case management, initial classification and triage, escalation and response coordination, cybersecurity advisory dissemination, and initial awareness and training activities.

IOC shall be established using technologies supplied under the contract, approved existing Government resources and, where necessary, secure Consultant-provided interim solutions. All interim tools, licences, hosting, configuration, integration and support necessary to achieve and maintain IOC shall be included in the agreed contract price.

Achievement of IOC shall not depend on a separate Government procurement of CIRT-specific hardware or software or completion of the National Data Centre reconstruction. Government shall provide the agreed premises, base utilities and connectivity, counterpart personnel, access and lawful operational authorisations.

The Consultant shall demonstrate IOC through a Government-witnessed operational exercise supported by technical evidence, operational records, test results and a corrective action register. Documentation or installation of technology alone shall not satisfy this milestone.

Where interim solutions are used, the Consultant shall maintain secure Government access, protect incident information and preserve service continuity. It shall implement an orderly transition to the complete contracted solution without loss of records or essential functionality.

Acceptance of IOC shall not constitute acceptance of the complete Build phase or relieve the Consultant of its remaining technology delivery, operational service, training and transfer obligations.

4.4.1 Minimum Operational Services

The Consultant shall establish, configure, document and demonstrate the following minimum operational services by Month 3:

a. Cybersecurity Incident Reporting and Intake

Establish secure and accessible channels through which participating Government institutions and authorised personnel may report suspected or confirmed cybersecurity incidents.

These arrangements shall include:

1. Designated incident reporting channels and contact information.
2. Procedures for receiving and acknowledging incident reports.
3. Mechanisms for capturing essential incident information.
4. Defined arrangements for identifying and escalating urgent incidents.
5. Appropriate safeguards for the confidentiality and integrity of incident reports.
6. Guidance for participating Government institutions on the reporting process.

b. Incident Registration and Case Management

Establish an operational mechanism for recording, tracking and managing reported cybersecurity incidents.

The mechanism shall support:

1. Assignment of unique incident identifiers.
2. Recording of incident details, affected institutions and relevant technical information.
3. Classification and prioritisation of incidents.
4. Assignment of incident handling responsibilities.
5. Recording of response actions, communications and decisions.
6. Tracking of incident status and outstanding actions.
7. Maintenance of an auditable incident history.
8. Preparation of basic operational reports.

The Consultant may utilise an approved interim case management solution, provided that it meets the Government's security, confidentiality, access control and information management requirements.

c. Incident Triage, Classification and Prioritisation

Establish documented procedures for the initial assessment and prioritisation of cybersecurity incidents.

These shall include:

1. A practical incident classification and severity framework.
2. Criteria for determining incident urgency, potential impact and required escalation.
3. Procedures for assessing reported incidents and identifying additional information requirements.

4. Defined responsibilities for incident triage and initial technical assessment.
5. Arrangements for prioritising critical and high-severity incidents.
6. Procedures for reassessing incident severity as additional information becomes available.

The classification and severity framework shall be proportionate to the Government CIRT's mandate and operational resources.

d. Incident Escalation and Response Coordination

Establish procedures and communication arrangements for coordinating responses to cybersecurity incidents affecting participating Government institutions.

These shall include:

1. Identification of appropriate technical, operational and management contacts.
2. Documented incident escalation pathways.
3. Procedures for communicating incident assessments and recommended response actions.
4. Arrangements for coordinating with affected Government ICT teams and other designated authorities.
5. Mechanisms for recording incident response decisions and actions.
6. Procedures for escalating significant incidents to the appropriate Government decision-makers.
7. Arrangements for coordinating specialist technical assistance where required.

The Government CIRT shall operate within its approved mandate and shall not undertake containment, system isolation or other actions affecting Government systems without the required authorisation.

e. Cybersecurity Advisories and Knowledge Sharing

Establish an initial capability for receiving, assessing and communicating relevant cybersecurity information to participating Government institutions.

This shall include:

1. Identifying appropriate and reliable cybersecurity advisory and vulnerability information sources.
2. Establishing procedures for reviewing and assessing the relevance of received information.
3. Preparing and disseminating relevant cybersecurity advisories and alerts.
4. Providing practical recommendations for preventive or corrective action.
5. Maintaining records of advisories issued and institutions notified.

6. Establishing an initial knowledge repository containing relevant incident handling guidance and cybersecurity information.

This capability shall be proportionate to the Government CIRT's initial service mandate and shall not require the establishment of a fully developed threat intelligence platform by Month 3.

f. Initial Cybersecurity Awareness and Incident Reporting Orientation

Provide initial orientation and awareness activities to designated Government stakeholders.

These activities shall include:

1. Introducing the Government CIRT's mandate and initial services.
2. Communicating the approved incident reporting channels.
3. Explaining the types of cybersecurity incidents that should be reported.
4. Providing guidance on incident notification and escalation responsibilities.
5. Promoting timely reporting and cooperation with the Government CIRT.
6. Providing initial awareness materials for use by participating Government institutions.

These activities shall complement the broader cybersecurity awareness programme established under Section 4.7.

4.4.2 Interim Technical Environment

The Consultant shall identify, establish and support an appropriate interim technical environment necessary to achieve IOC.

The interim environment may utilise approved existing Government resources, securely configured open-source solutions, temporary hosted services or other appropriate technologies, subject to Government authorisation.

The Consultant shall:

1. Assess the suitability and availability of existing Government infrastructure and technical resources.
2. Identify the minimum technology requirements necessary to support the initial core services.
3. Recommend appropriate interim technologies and hosting arrangements.
4. Document the security, operational, licensing and financial implications of the proposed arrangements.
5. Obtain the required Government approval before implementing interim solutions.
6. Configure appropriate access controls, authentication arrangements, logging and data protection safeguards.
7. Establish suitable backup, recovery and operational continuity arrangements.

8. Document the interim system architecture, configurations and administrative procedures.
9. Identify any technical limitations and corresponding risk mitigation measures.
10. Prepare a practical transition approach for migrating to permanent Government-approved technologies.

The interim environment shall be sufficiently secure and reliable to support actual incident management activities.

The Consultant shall ensure that interim technology arrangements do not create unnecessary vendor dependency or impede subsequent migration to the permanent Government CIRT environment.

Where temporary services, software or infrastructure are proposed, the Consultant shall identify their expected duration, associated costs, data ownership arrangements and procedures for secure termination or transition.

4.4.3 Initial Operational Procedures and Governance

The Consultant shall prepare and implement the minimum operational procedures required to support IOC.

These shall include:

1. Incident reporting and acknowledgement procedures.
2. Incident registration and case management procedures.
3. Incident classification and prioritisation procedures.
4. Initial incident triage and assessment procedures.
5. Incident escalation and response coordination procedures.
6. Procedures for handling sensitive incident information.
7. Initial cybersecurity advisory preparation and dissemination procedures.
8. Operational reporting and record management procedures.
9. Emergency contact and notification arrangements.
10. Procedures for managing access to interim operational systems.

The procedures shall identify the respective responsibilities of the Consultant, designated Government CIRT personnel, participating Government institutions and other relevant authorities.

The Consultant shall ensure that the procedures are consistent with the institutional and governance arrangements developed under Section 4.3.

4.4.4 Government Personnel Participation and Initial Capacity Building

The Consultant shall ensure that designated Government personnel participate directly in establishing, testing and operating the initial Government CIRT capability.

The Consultant shall:

1. Provide initial orientation on the Government CIRT's mandate, services and operational arrangements.
2. Train designated personnel in the use of the interim incident reporting and case management mechanisms.
3. Provide practical instruction in incident registration, classification, triage and escalation.
4. Demonstrate the preparation of cybersecurity advisories and operational reports.
5. Conduct supervised incident handling exercises.
6. Assign progressively increasing operational responsibilities to designated Government personnel.
7. Record initial competency observations and identify areas requiring further development.
8. Establish a structured mentoring arrangement for the subsequent operational phase.

Government personnel shall not be limited to observing Consultant activities. They shall participate directly in practical exercises and operational processes under appropriate supervision.

The training and mentoring activities shall be integrated with the broader capacity-building programme established under Section 4.8.

4.4.5 Initial Operating Hours and Emergency Escalation

The Government CIRT shall initially operate during standard Government business hours, supported by appropriate emergency notification and escalation arrangements for critical and high-severity cybersecurity incidents outside normal working hours.

The Consultant shall:

1. Define the initial operating hours and contact arrangements.
2. Establish procedures for reporting and escalating urgent incidents outside normal operating hours.
3. Identify the respective responsibilities of designated Government personnel and Consultant specialists.
4. Establish an emergency contact and escalation roster.
5. Implement and test the minimum incident acknowledgement, triage and escalation targets specified in Section 4.6.13, including the emergency on-call arrangements for Critical and High incidents.
6. Test the emergency notification and escalation arrangements.
7. Document the procedures for maintaining and updating contact information.

The arrangements shall provide for access to appropriate incident response coordination and specialist advice in accordance with the approved operating model.

The IOC requirement shall not be interpreted as requiring a continuously staffed twenty-four-hour Security Operations Centre.

4.4.6 Initial Operational Capability Demonstration and Testing

Before the end of Month 3, the Consultant shall conduct a formal operational demonstration and exercise to verify that the Government CIRT can perform its agreed minimum core services.

The demonstration shall include an end-to-end simulated cybersecurity incident, or another Government-approved test scenario, covering:

1. Submission of an incident report through the approved reporting channel.
2. Acknowledgement and registration of the incident.
3. Initial assessment, classification and severity determination.
4. Assignment of incident handling responsibilities.
5. Escalation to the appropriate Government personnel or institutional contacts.
6. Preparation and communication of appropriate response recommendations.
7. Recording of operational actions, decisions and communications.
8. Updating of the incident record and status.
9. Preparation of an incident summary or operational report.
10. Demonstration of the relevant Government personnel's participation in the process.

The Consultant shall also demonstrate:

a. The operational availability of the interim reporting and case management mechanisms.

b. The application of appropriate information security and access control measures.

c. The availability and use of the initial operational procedures.

d. The functioning of the emergency contact and escalation arrangements.

e. The capability to prepare and disseminate an initial cybersecurity advisory.

f. The availability of basic operational reporting information.

g. The readiness of designated Government personnel to participate in supervised Government CIRT operations.

The Government shall be afforded the opportunity to observe the demonstration, examine the supporting records and verify the functionality of the agreed services.

Any deficiencies identified during the demonstration shall be documented and addressed in accordance with the agreed acceptance procedures.

4.4.7 Initial Operational Capability Documentation and Acceptance

Following the operational demonstration, the Consultant shall submit an Initial Operational Capability Report containing:

1. A description of the established Government CIRT operational capability.
2. The approved initial service catalogue.
3. Details of the interim technical environment and implemented security arrangements.
4. The operational procedures and governance arrangements in effect.
5. Evidence of the incident reporting and case management functionality.
6. Results of the operational demonstration and incident response exercise.
7. Details of Government personnel participation and initial competency observations.
8. Evidence of tested emergency notification and escalation arrangements.
9. Initial cybersecurity advisory and awareness outputs.
10. Identified operational limitations, outstanding risks and proposed corrective actions.
11. The implementation plan for strengthening operations and transitioning to permanent infrastructure.
12. Recommendations for the subsequent Consultant-supported operational phase.

The Month 3 IOC milestone shall be considered achieved only when the Government has verified that the agreed minimum operational services are functioning and the required operational demonstration has been satisfactorily completed.

The submission of reports, plans, procedures or training records alone shall not constitute satisfactory achievement of IOC.

Acceptance shall be undertaken in accordance with the deliverable and acceptance arrangements established in Section 7.

4.4.8 Transition from Initial Operational Capability

Following acceptance of IOC, the Consultant shall maintain and progressively strengthen the Government CIRT's operational services throughout the remaining DBOT period.

The Consultant shall:

1. Continue providing the agreed operational support and mentoring.
2. Address identified IOC limitations and implement approved corrective actions.
3. Strengthen operational procedures based on experience and performance assessments.
4. Support the deployment and integration of permanent Government-approved technologies as they become available.

5. Transition relevant incident records, configurations, procedures and operational knowledge to the permanent environment.
6. Expand approved services progressively in accordance with Government priorities and available resources.
7. Increase Government personnel responsibility for routine operational activities.
8. Prepare the Government CIRT for Government-led operations during Months 9–12 through progressive transfer of operational responsibilities, structured mentoring, practical competency assessments and supervised incident response activities.

The Consultant shall ensure that the transition from Initial Operational Capability to Government-led operations is supported by continuous operational service delivery, progressive capacity development and appropriate technical and institutional arrangements. The transition shall culminate in the formal operational readiness assessment by Month 11 and completion of the agreed Government CIRT handover by Month 12, in accordance with Sections 4.8, 4.9 and 7.

4.5 Technology Supply Deployment and Integration

The Consultant shall be directly responsible for procuring, supplying, delivering, installing, securely configuring, integrating, testing and commissioning the complete Government CIRT technology environment included in the agreed contractual scope.

These activities constitute the Build phase of the DBOT model.Government review, approval or participation shall not transfer these responsibilities to Government.

The Consultant shall deliver the solution in accordance with the approved Technical Architecture and Build Specifications, awarded contract price and implementation schedule. Necessary interim arrangements shall support Month 3 Initial Operational Capability without replacing the obligation to complete the contracted solution.

4.5.1 Deployment Planning and Build Schedule

The Consultant shall prepare and maintain a deployment schedule consistent with the Technical Architecture and Build Specifications required under Section 4.2.3.

The schedule shall identify:

1. Technology components, quantities and delivery milestones.
2. Supplier and subcontractor responsibilities.
3. Government-provided premises, utilities, connectivity, access and other interfaces.
4. Installation, configuration and integration activities.
5. Security hardening and testing.
6. Commissioning and Government acceptance tests.
7. Interim technology arrangements and migration activities.
8. Government personnel participation and practical training.
9. Licensing, warranty and support commencement dates.

10. Risks, dependencies, mitigation measures and escalation points.
11. Completion dates allowing sufficient operational validation before final transfer.

Government approval of the schedule shall not reduce the Consultant's contractual responsibilities. Changes affecting scope, price, milestones or acceptance requirements shall follow the applicable change-control procedures.

4.5.2 Warranty and Defect Liability

The Consultant shall provide a minimum twelve (12)-month warranty from final acceptance and operational transfer under D10 for defects attributable to its design, supplied components, installation, configuration or integration.

The Consultant shall also correct defects arising during the Build and Operate phases at no additional cost to Government. Defects attributable to its suppliers or subcontractors shall remain the Consultant's responsibility.

Manufacturer and third-party warranties shall supplement, and shall not replace, the Consultant's contractual obligations. The Consultant shall secure the Government ownership, beneficiary status or enforceable rights necessary to use these warranties.

Before final acceptance, the Consultant shall submit a Warranty and Latent Defects Schedule specifying:

1. Components and integrated functions covered.
2. Warranty commencement and expiry dates.
3. Coverage, exclusions and applicable conditions.
4. Defect notification and escalation procedures.
5. Response, workaround and rectification periods.
6. Responsible parties and support contacts.
7. Manufacturer and third-party warranty entitlements.
8. Contractual obligations concerning defects discovered after handover.

Warranty response and rectification requirements shall be specified in the procurement and contract documents and reflected in the approved support arrangements.

Final acceptance shall not extinguish warranty or latent-defect obligations that survive completion under the contract. Warranty rectification shall not be conditional on purchasing optional post-DBOT support.

4.5.3 Secure Configuration and System Hardening

The Consultant shall securely configure and harden all supplied components before operational use.

Activities shall include:

1. Removing or disabling unnecessary services and default accounts.
2. Changing default credentials and securing privileged access.

3. Implementing role-based access and strong authentication.
4. Applying supported security updates.
5. Configuring network segmentation, access restrictions and secure communications.
6. Implementing encryption appropriate to the information handled.
7. Establishing audit logging and monitoring.
8. Configuring backup, recovery and retention controls.
9. Assessing and correcting configuration vulnerabilities.
10. Documenting the approved configuration baseline.

Any unresolved security risks shall be reported to Government with proposed treatment. Exceptions shall require documented Government approval and shall not silently waive contractual security requirements.

4.5.4 Integration with Government Infrastructure

The Consultant shall implement the agreed interfaces between its supplied solution and relevant Government systems.

It shall:

1. Confirm interface requirements and authorised access.
2. Coordinate with GITS, designated Government personnel and providers of existing systems.
3. Configure secure authentication, connectivity and information exchange.
4. Test compatibility, data flows, logging and access controls.
5. Verify that integration does not introduce unacceptable disruption or security exposure.
6. Document configurations, dependencies and administration responsibilities.
7. Resolve integration deficiencies within its contractual scope.

Government shall facilitate agreed access and coordination with existing service providers.

Initial deployment shall not depend on completion of National Data Centre reconstruction. Any later relocation or additional integration shall be governed by the agreed scope and contractual change-control arrangements.

4.5.5 Transition from Interim Systems

Where interim technologies are used, the Consultant shall implement the transition plan required under Section 4.2.9.

The transition shall include:

1. Verification that the contracted solution is ready for migration.
2. Secure migration of incident records, configurations and other Government information.
3. Backup and tested rollback arrangements.
4. Validation of migrated information and functionality.
5. Preservation of incident reporting and essential operational services.

6. Government personnel participation and practical knowledge transfer.
7. Transfer of administrative access and applicable usage rights.
8. Secure termination or decommissioning of superseded services.

Interim systems shall not be withdrawn until the replacement capability has been verified and Government has authorised the transition.

Continued interim operation shall not constitute completion of outstanding Build obligations unless expressly authorised through an approved contractual variation.

4.5.6 Technical Testing and Commissioning

The Consultant shall prepare and execute a documented test and commissioning plan covering individual components and the integrated solution.

Testing shall address:

1. Compliance with the approved specifications.
2. Functional performance of agreed CIRT services.
3. Incident reporting, registration, triage, escalation and case management.
4. Authentication, authorisation and privileged administration.
5. Security configuration, logging and auditability.
6. Interfaces and information exchange.
7. Backup, restoration and operational recovery.
8. Service continuity and relevant failure scenarios.
9. Licensing validity and support availability.
10. Government administration and operation of the solution.

The Consultant shall provide test scripts, expected results, actual results, evidence, identified defects and corrective actions. It shall facilitate Government-witnessed tests and practical participation by designated personnel.

Commissioning shall require satisfactory demonstration of the agreed capabilities. Equipment delivery or installation alone shall not constitute commissioning or acceptance.

4.5.7 Technical Acceptance and Defect Management

Government shall verify the supplied solution against the approved specifications, acceptance criteria and test procedures.

The Consultant shall maintain a defect register identifying severity, operational impact, responsibility, proposed remedy, target completion date and verification status.

The Consultant shall rectify non-compliance, defects and integration failures attributable to its design, supplied components, installation, configuration, suppliers or subcontractors at no additional cost to Government.

Government-controlled constraints affecting premises, access, existing systems or required approvals shall be separately evidenced and managed under the contract. They shall not be used to exclude responsibility for the Consultant's own delivery obligations.

Any acceptance subject to outstanding minor items shall be expressly documented in accordance with the contract, including the items, deadlines and applicable remedies. Government shall not be required to accept a solution that fails mandatory operational or security requirements.

Technical acceptance of a component or subsystem shall not constitute final acceptance of the DBOT assignment. Final acceptance shall remain subject to Section 7.6 and D10.

4.5.8 Government Technical Capacity Building

The Consultant shall involve designated Government personnel in design reviews, installation, configuration, integration, testing, commissioning and administration.

Practical instruction shall cover:

1. System administration and privileged access management.
2. Secure configuration and routine maintenance.
3. Software updates and vulnerability remediation.
4. Logging, monitoring and troubleshooting.
5. Backup, restoration and continuity procedures.
6. Incident management platform administration.
7. Licence, subscription, warranty and supplier support management.
8. Configuration changes and technical documentation.
9. Escalation of technical problems.
10. Secure migration and component replacement.

Competence shall be demonstrated through practical tasks and assessments coordinated with Section 4.8. Attendance alone shall not demonstrate readiness for transfer.

4.5.9 Technical Documentation and Handover

The Consultant shall maintain and hand over documentation reflecting the actual solution supplied, including:

1. Final architecture and interface diagrams.
2. Component schedules and the verified Asset Register.
3. Installation, configuration and integration records.
4. Security baselines and administration procedures.
5. Testing, commissioning and acceptance evidence.
6. Backup, recovery and continuity procedures.
7. Operating and maintenance instructions.
8. Licence terms, subscriptions and renewal dates.
9. Warranty and technical support arrangements.

10. Known limitations, residual risks and outstanding actions.
11. Required title, licence and support transfer documents.
12. Secure transfer of administrative accounts and credentials.

Documents shall be provided in accessible and editable formats where applicable, subject to disclosed third-party intellectual property restrictions.

Technical handover shall be coordinated with the operational transfer requirements under Section 4.9.

4.5.10 Management of Deployment Dependencies

The Consultant shall identify and manage dependencies affecting technology delivery, installation, integration, commissioning and transfer.

Dependencies shall distinguish:

1. Consultant-controlled procurement, supplier and subcontractor delivery, configuration, integration and defect rectification.
2. Government-controlled premises, base utilities, connectivity, site and system access, counterpart personnel and required approvals.

The Consultant shall promptly notify Government in writing of material constraints, their cause, affected activities, likely milestone impacts and proposed mitigation measures.

It shall continue unaffected activities, maintain approved interim services where necessary, and propose revised sequencing to minimise disruption.

Delays or deficiencies involving the Consultant's suppliers or subcontractors shall remain its responsibility, subject to the applicable contract provisions.

Any relief for a proven Government-caused delay shall be assessed through the contractual procedures. No extension, additional payment, scope reduction or acceptance shall arise automatically.

The Consultant shall complete the contracted solution and transfer obligations unless expressly varied through the required approvals. Interim capability alone shall not discharge the complete Build obligation.

4.6 Operational Services and Incident Response

The Consultant shall establish, operate, progressively strengthen and transfer the agreed operational services of the Government Cybersecurity Incident Response Team (Government CIRT) in accordance with the approved mandate, service catalogue, operational procedures and Design–Build–Operate–Transfer (DBOT) implementation plan.

From Initial Operational Capability until final acceptance, the Consultant shall lead, deliver, maintain and support the agreed Government CIRT operational services, working alongside

designated Government personnel. It shall provide the personnel, technical expertise, tools and specialist support necessary to meet its contractual obligations. Progressive Government participation shall not relieve the Consultant of responsibility for service delivery and performance before final acceptance.

The Government CIRT shall initially provide core cybersecurity incident management and knowledge transfer services to participating Government ministries, departments and agencies.

Additional cybersecurity services may be introduced progressively, subject to Government priorities, available resources, technical readiness and the approved implementation plan.

The Consultant shall ensure that the operational model is appropriate to the Government CIRT's staffing, institutional mandate, technical environment and sustainability requirements.

4.6.1 Operational Service Catalogue

The Consultant shall develop, implement and maintain an approved Government CIRT operational service catalogue.

The service catalogue shall identify:

1. The Government CIRT's operational constituency and participating institutions.
2. The purpose and scope of each service.
3. The mandatory core services to be provided.
4. The responsibilities of Government CIRT personnel and participating institutions.
5. Service availability and operating arrangements.
6. Incident reporting and communication channels.
7. Service response and escalation arrangements.
8. Operational dependencies and limitations.
9. Performance indicators and reporting requirements.
10. Additional services recommended for progressive implementation.

The initial service catalogue shall include, at a minimum:

a. Cybersecurity incident reporting and intake.
b. Incident registration, classification and case management.
c. Initial incident analysis, triage and prioritisation.
d. Cybersecurity incident escalation and response coordination.
e. Cybersecurity advisories, alerts and relevant knowledge sharing.
f. Cybersecurity awareness and incident reporting guidance.
g. Operational reporting and incident management performance monitoring.

The Consultant shall ensure that these core services are established by the Month 3 IOC milestone and maintained and progressively strengthened throughout the remaining DBOT period.

The introduction of additional services shall not compromise the availability, effectiveness or sustainability of the mandatory core services.

4.6.2 Cybersecurity Incident Reporting and Case Management

The Consultant shall operate and progressively transfer a structured incident reporting and case management process.

The process shall provide for:

1. Receipt and acknowledgement of suspected or confirmed cybersecurity incidents.
2. Registration of incident reports using unique case identifiers.
3. Recording of relevant technical, operational and institutional information.
4. Initial assessment of the nature, severity and potential impact of reported incidents.
5. Assignment of incident handling responsibilities.
6. Tracking of incident status, response actions and outstanding matters.
7. Recording of communications, decisions and escalation activities.
8. Maintenance of appropriate supporting evidence and operational records.
9. Preparation of incident summaries and management reports.
10. Documented case closure and post-incident review, where appropriate.

The Consultant shall establish procedures to ensure the confidentiality, integrity, availability and appropriate retention of incident information.

Access to incident records shall be restricted according to approved roles and responsibilities.

The Government shall retain ownership and control of Government CIRT operational records and information, subject to the applicable contractual provisions and Government information management requirements.

4.6.3 Incident Classification, Severity and Prioritization

The Consultant shall develop and implement a standardized incident classification and severity framework appropriate to the Government CIRT's mandate and operating environment.

The framework shall provide for the classification of incidents according to their nature, potential impact, urgency and required response.

At a minimum, the framework shall distinguish between:

1. **Critical incidents:** Incidents involving actual or imminent severe disruption to essential Government services, significant compromise of sensitive Government information, or other consequences requiring immediate senior-level attention and coordinated response.
2. **High-severity incidents:** Significant cybersecurity incidents requiring urgent technical assessment, escalation and coordinated action to prevent or limit serious operational or security consequences.
3. **Medium-severity incidents:** Incidents requiring structured investigation and response coordination but not ordinarily warranting emergency escalation.
4. **Low-severity incidents:** Lower-impact incidents, suspected events or requests that can be managed through routine operational procedures.

The Consultant shall define clear criteria for each severity level, including examples relevant to the Government operating environment.

The framework shall establish procedures for:

a. Initial severity assessment.
b. Incident prioritization.
c. Reclassification where additional information becomes available.
d. Escalation according to severity and potential impact.
e. Notification of designated Government authorities.
f. Documentation of severity decisions and changes.

The classification framework shall be approved by the Government and incorporated into the Government CIRT's operational procedures.

4.6.4 Incident Response and Coordination Procedures

The Consultant shall develop, implement and maintain operational procedures and incident response playbooks to support the consistent handling of cybersecurity incidents.

The procedures shall address, as appropriate:

1. Incident identification and initial assessment.
2. Incident triage and technical analysis.
3. Collection and preservation of relevant incident information.
4. Identification of affected systems, services and institutions.
5. Assessment of potential operational and security impacts.
6. Recommendations for containment and mitigation.
7. Coordination of incident response actions with affected Government institutions.
8. Referral to specialist technical resources or competent authorities.
9. Recovery coordination and follow-up actions.
10. Incident documentation, reporting and closure.
11. Post-incident review and lessons learned.

12. The Consultant shall develop practical response playbooks for priority incident categories relevant to the Government environment, which may include:
    a. Phishing and credential compromise.
    b. Malware and ransomware incidents.
    c. Unauthorised access or suspected system compromise.
    d. Data breaches or suspected information exposure.
    e. Denial-of-service and service disruption incidents.
    f. Exploitation of significant security vulnerabilities.
    g. Other priority scenarios identified through the inception assessment and Government consultations.

The playbooks shall define the Government CIRT's coordination responsibilities, relevant technical actions, escalation pathways and required authorisations.

The Government CIRT shall not independently undertake disruptive containment, system isolation, forensic acquisition or other consequential actions affecting Government systems without the appropriate authorization.

4.6.5 Operational Support and Specialist Incident Response

During the operational phase, the Consultant shall undertake incident handling, technical analysis and response coordination within the agreed service scope, while training and mentoring designated Government personnel. During the progressive transition to Government-led operations, the Consultant shall continue to provide the operational capacity, supervision and specialist support necessary to maintain the agreed services and service levels. Actions affecting Government systems shall remain subject to the required Government authorisations.

This shall include:

1. Supporting the assessment and prioritization of reported incidents.
2. Providing technical guidance on incident investigation and response coordination.
3. Advising on containment, mitigation and recovery options.
4. Supporting analysis of available technical information and incident indicators.
5. Assisting with the interpretation of relevant threat and vulnerability information.
6. Supporting communication and coordination with affected Government institutions.
7. Advising on the referral of incidents requiring specialized expertise.
8. Supporting post-incident reviews and corrective action recommendations.
9. Mentoring Government CIRT personnel through practical incident handling activities.
10. Documenting technical lessons and incorporating them into operational procedures and training.

The Consultant shall provide access to appropriate specialist expertise for incidents that fall within the agreed contractual support arrangements.

Where an incident requires capabilities outside the Government CIRT's approved mandate or the Consultant's contractual scope, the Consultant shall advise on appropriate referral or escalation arrangements.

The Consultant shall not be responsible for guaranteeing the prevention of cybersecurity incidents or the successful recovery of every affected system. Its responsibilities shall be assessed against the agreed services, response obligations, professional standards and contractual performance requirements.

4.6.6 Operational Hours and Emergency Response Arrangements

The Government CIRT shall operate during standard Government business hours, supported by an emergency notification and on-call escalation mechanism for critical and high-severity cybersecurity incidents outside normal operating hours, including weekends and public holidays.

The Consultant shall establish and implement the necessary operating arrangements, including:

1. Approved service operating hours.
2. Designated incident reporting and emergency contact channels.
3. A documented on-call and escalation roster.
4. Procedures for receiving and escalating urgent incident notifications outside normal working hours.
5. Responsibilities of Consultant specialists and designated Government personnel.
6. Severity-based acknowledgement, notification and escalation targets.
7. Arrangements for access to specialist incident response advice.
8. Procedures for maintaining and testing emergency contact arrangements.
9. Contingency arrangements where designated personnel are unavailable.
10. Recording and reporting of emergency incident notifications and response activities.

The minimum service levels specified in Section 4.6.13 shall apply. During inception, the Consultant shall propose the detailed procedures, staffing, on-call roster, measurement arrangements and any additional performance targets for Government approval. These arrangements shall not reduce the prescribed minimum service levels except through an approved contractual amendment.

The targets shall distinguish between incident acknowledgement, initial assessment, escalation and subsequent response coordination.

The Consultant shall identify the staffing, communication and technical arrangements necessary to meet the approved targets.

The Consultant shall test the emergency notification and escalation mechanism during the implementation period and shall progressively transfer responsibility for maintaining and operating the mechanism to designated Government personnel.

The operational requirements shall not be interpreted as requiring a continuously staffed twenty-four-hour Security Operations Centre.

Where automated monitoring or alerting is implemented using approved technologies, the Consultant shall define the applicable alert review, notification and escalation arrangements.

4.6.7 Cybersecurity Threat Intelligence and Vulnerability Coordination

The Consultant shall establish an initial, proportionate capability for receiving, evaluating and disseminating cybersecurity threat and vulnerability information relevant to Government institutions.

The activities shall include:

1. Identifying reliable national, regional and international sources of cybersecurity threat and vulnerability information.
2. Establishing procedures for receiving and reviewing relevant alerts and advisories.
3. Assessing the potential relevance and impact of identified threats and vulnerabilities on participating Government institutions.
4. Preparing and communicating appropriate cybersecurity alerts, advisories and recommended mitigation actions.
5. Coordinating with designated Government ICT personnel to obtain information on potential exposure or required action.
6. Tracking significant vulnerability notifications and related coordination activities, where appropriate.
7. Maintaining records of advisories issued and relevant follow-up actions.
8. Supporting knowledge sharing and awareness of emerging cybersecurity risks.

The Consultant may recommend additional capabilities such as enhanced threat intelligence analysis, vulnerability coordination or security event management for progressive implementation.

Such capabilities shall be introduced only where justified by the Government CIRT's operational requirements, available infrastructure, staffing and resources.

The initial scope shall not require the Government CIRT to provide continuous enterprise-wide vulnerability scanning, comprehensive security monitoring or advanced threat hunting across all Government institutions unless these services are separately approved and appropriately resourced.

4.6.8 Operational Reporting and Performance Monitoring

The Consultant shall establish and maintain an operational performance monitoring framework for the Government CIRT.

The framework shall include measurable indicators appropriate to the approved service catalogue.

These may include:

1. Number of cybersecurity incidents reported and registered.
2. Incidents classified by severity and category.
3. Timeliness of incident acknowledgement.
4. Timeliness of initial assessment and escalation.
5. Compliance with approved incident handling procedures.
6. Completeness and accuracy of incident records.
7. Number and status of incidents under active coordination.
8. Number of cybersecurity advisories issued.
9. Performance of emergency notification and escalation arrangements.
10. Results of incident response exercises and operational tests.
11. Progress in Government personnel participation and competency development.
12. Identified operational weaknesses and corrective actions.

The Consultant shall establish baseline measurements where feasible and propose appropriate performance targets for Government approval.

Operational performance shall be reviewed regularly with designated Government counterparts.

The Consultant shall prepare monthly operational performance summaries, highlighting service activity, significant incidents, emerging risks, operational constraints and recommended corrective actions.

Incident reporting and performance monitoring shall respect applicable confidentiality and information security requirements.

4.6.9 Operational Exercises and Continuous Improvement

The Consultant shall design and conduct practical operational exercises to strengthen the Government CIRT's incident handling capability and assess its operational readiness.

The exercise programme shall include:

1. The Month 3 Initial Operational Capability demonstration required under Section 4.4.
2. Subsequent incident handling exercises covering priority cybersecurity scenarios.
3. Testing of emergency notification and escalation arrangements.

4. Exercises involving designated Government CIRT personnel and relevant institutional ICT representatives.
5. At least one Government-led operational exercise during the transfer phase.
6. A multi-agency coordination exercise, involving relevant stakeholders where feasible and approved by the Government.
7. Structured after-action reviews and documented corrective actions.

The Consultant shall ensure that exercises assess practical operational performance rather than merely familiarity with documented procedures.

Exercise findings shall inform revisions to incident response playbooks, operational arrangements, training activities and performance improvement measures.

The Consultant shall maintain an action register identifying significant operational deficiencies, corrective measures, responsible parties and target completion dates.

4.6.10 Progressive Transfer of Operational Responsibility

The Consultant shall implement a structured and verifiable transfer of operational responsibilities to designated Government CIRT personnel.

The transfer shall proceed progressively throughout the consultancy and shall be aligned with the capacity-building requirements under Section 4.8 and the operational sustainability and transfer requirements under Section 4.9.

The operational transition shall follow the general progression below:

Months 1–3: Establishment and Initial Operations

The Consultant shall lead the establishment of the operational capability while providing initial training and supervised practical participation for designated Government personnel.

Months 3–9 — Consultant-Led Operations and Mentoring

The Consultant shall lead and deliver the agreed operational services, maintain the supporting technology and provide specialist incident response support. Government personnel shall progressively undertake incident handling, case management, reporting, advisory preparation and response coordination under structured supervision and mentoring.

Months 9–12: Government-Led Operations

Designated Government personnel shall assume primary responsibility for routine Government CIRT operations, with the Consultant providing mentoring, quality assurance, specialist advice and corrective support as necessary.

During this phase, the Consultant shall assess the Government CIRT's ability to:

1. Receive and register incident reports.
2. Conduct initial incident assessment and severity classification.
3. Manage and update incident cases.
4. Apply the approved escalation and coordination procedures.
5. Prepare and issue authorized cybersecurity advisories.
6. Maintain operational records and performance reports.
7. Operate emergency notification and escalation arrangements.
8. Coordinate with participating Government institutions.
9. Apply relevant information security and confidentiality procedures.
10. Identify incidents requiring additional specialist assistance.

The Consultant shall progressively reduce direct involvement in routine activities as Government personnel demonstrate the required competencies.

The Consultant shall document the transfer of operational responsibilities, outstanding capacity gaps and corrective actions.

The final Government-led operational readiness assessment shall be completed in Month 11, with formal transfer of the agreed operational capability completed by Month 12.

4.6.11 Operational Service Continuity and Quality Assurance

The Consultant shall establish practical arrangements to maintain continuity and quality of the agreed Government CIRT services throughout the operational and transfer phases.

These arrangements shall include:

1. Procedures for maintaining incident reporting and case management services.
2. Backup and recovery arrangements for operational records and supporting systems.
3. Maintenance of current operational contact and escalation information.
4. Documented arrangements for managing operational disruptions.
5. Procedures for identifying and addressing service performance deficiencies.
6. Appropriate supervision and quality assurance of incident handling activities.
7. Regular review and updating of operational procedures.
8. Management of operational risks and critical dependencies.
9. Arrangements for continuity during the transition from interim to permanent technologies.
10. Preparation for continued Government CIRT operations following the Consultant's withdrawal.

The Consultant shall ensure that operational improvements and service changes are appropriately documented and communicated to designated Government personnel.

The Government CIRT shall remain capable of delivering the agreed core services throughout the transition, subject to documented and approved arrangements for managing material dependencies and service disruptions.

4.6.12 Operational Documentation and Knowledge Transfer

The Consultant shall maintain and transfer the documentation necessary for the Government to continue operating the agreed Government CIRT services.

This shall include:

1. The approved operational service catalogue.
2. Incident classification and severity criteria.
3. Incident reporting, case management and escalation procedures.
4. Incident response playbooks.
5. Emergency notification and on-call arrangements.
6. Cybersecurity advisory and information-sharing procedures.
7. Operational reporting templates and performance indicators.
8. Relevant technical operating instructions.
9. Incident handling exercise materials and results.
10. Operational lessons learned and corrective action records.
11. Guidance on specialist support and referral arrangements.
12. Documentation of outstanding operational risks and recommended future improvements.

The Consultant shall ensure that documentation is current, accessible to authorised Government personnel and consistent with the operational capability being transferred.

The completion of the operational services workstream shall be subject to the Government's verification of operational performance, personnel readiness and satisfactory transfer in accordance with Sections 4.9 and 7.

4.6.13 Minimum Service Levels and Incident Response Targets

The Consultant shall establish, implement, monitor and progressively transfer defined service levels for the Government CIRT's incident management and response coordination functions.

The following minimum service levels shall apply to cybersecurity incidents reported through the approved Government CIRT reporting channels, subject to the agreed severity classification criteria and operating arrangements.

Severity	Initial Acknowledgement	Initial Triage and Escalation	Coverage
Critical (P1)	Within 30 minutes	Within 1 hour	24/7 emergency on-call

High (P2)	Within 1 hour	Within 2 hours	24/7 emergency on-call
Medium (P3)	Within 4 business hours	Within 1 business day	Government business hours
Low (P4)	Within 1 business day	Within 2 business days	Government business hours

For the purposes of these service levels:

1. **Initial acknowledgement** means confirmation that an incident report has been received, recorded and assigned for assessment. Automated acknowledgements alone shall not satisfy the acknowledgement requirement for Critical (P1) and High (P2) incidents.
2. **Initial triage and escalation** means an initial assessment of the incident, assignment of an appropriate severity classification, identification of the responsible personnel and notification or escalation to the relevant Government institution or authority, as required.
3. **Critical (P1)** incidents are those involving actual or imminent severe disruption of essential Government services, widespread compromise, or other circumstances requiring immediate coordinated response.
4. **High (P2)** incidents are those involving significant actual or potential compromise of Government systems, information or services requiring urgent coordination.
5. **Medium (P3)** incidents are those involving a material but contained cybersecurity impact requiring timely assessment and coordinated action.
6. **Low (P4)** incidents are those involving limited impact or routine cybersecurity matters that do not require urgent intervention.

The approved incident classification framework shall establish the detailed criteria for each severity level.

Service-level measurement shall commence when an incident is received through an approved reporting channel. Where an incident is initially reported at a lower severity but subsequently reclassified as Critical or High, the applicable emergency escalation arrangements shall take effect immediately upon reclassification.

The Consultant shall establish procedures for:

1. Recording incident receipt, acknowledgement, triage and escalation timestamps.
2. Maintaining an emergency contact and on-call roster.
3. Ensuring that an appropriate on-call resource is available to respond to Critical and High incidents outside Government business hours.
4. Escalating incidents where designated personnel are unavailable or fail to respond within the prescribed period.
5. Recording service-level performance and exceptions.

6. Investigating missed service targets and implementing corrective actions.
7. Reviewing service-level performance with designated Government representatives.
8. Training and mentoring Government personnel in the application and monitoring of the approved service levels.

The prescribed targets relate to acknowledgement, initial assessment and response coordination. They shall not be interpreted as guaranteed incident containment, recovery or resolution times, which may depend on the nature of the incident and the actions of affected Government institutions, technology suppliers or other competent authorities.

The Consultant shall demonstrate the emergency on-call arrangements as part of the Month 3 Initial Operational Capability assessment and maintain the agreed service levels throughout the applicable operational phase.

During Months 9–12, the Consultant shall progressively transfer responsibility for managing and monitoring these service levels to designated Government personnel.

The Month 11 operational readiness assessment shall include verification of Government personnel's ability to apply the approved incident classification framework, meet the applicable acknowledgement and escalation targets, and manage emergency on-call procedures.

These arrangements shall not require the establishment of a continuously staffed twenty-four-hour Security Operations Centre.

Progressive reduction of the Consultant’s direct involvement in routine activities shall be based on demonstrated Government personnel competence and an agreed transfer schedule. It shall not reduce service availability, specialist support or the Consultant’s contractual accountability before final acceptance.

4.7 Cybersecurity Awareness and Stakeholder Engagement

The Consultant shall develop and implement a structured cybersecurity awareness and stakeholder engagement programme to support the establishment, operationalization and sustainability of the Government Cybersecurity Incident Response Team (Government CIRT), while facilitating the consultations and coordination arrangements necessary for the development of the proposed National Cybersecurity Incident Response Team (National CIRT) framework.

The programme shall be aligned with the CIRT Establishment Plan and the National Cybersecurity Strategy and Action Plan for Saint Lucia (2026–2030).

The Consultant shall ensure that awareness activities, stakeholder engagement and incident reporting guidance are integrated into the Government CIRT's operational development and are not treated solely as communication or publicity activities.

The Consultant shall undertake the following activities.

4.7.1 Cybersecurity Awareness Needs Assessment and Planning

1. Assess existing Government cybersecurity awareness initiatives, available materials, communication channels and relevant training activities.
2. Identify priority cybersecurity risks, awareness gaps and behavioural practices affecting Government personnel and institutions.
3. Identify target audiences, including Government ICT personnel, institutional cybersecurity focal points, managers and general public officers.
4. Develop a practical cybersecurity awareness and engagement plan identifying priority topics, target audiences, delivery methods, implementation schedules and measures for evaluating effectiveness.
5. Coordinate the proposed activities with existing Government cybersecurity initiatives to minimise duplication and promote consistent messaging.
6. Ensure that awareness activities support the Government CIRT's operational priorities, particularly incident recognition, reporting, escalation and preventive practices.

4.7.2 Government Cybersecurity Awareness Programme

The Consultant shall design and implement an initial cybersecurity awareness programme for Government ministries, departments and agencies.

The programme shall address relevant cybersecurity risks and good practices, including:

1. Recognition and reporting of suspected cybersecurity incidents.
2. Phishing, social engineering and other common cyber threats.
3. Password security, multifactor authentication and protection of user credentials.
4. Safe handling of Government information and sensitive data.
5. Secure use of email, internet services, mobile devices and remote access technologies.
6. Malware, ransomware and other threats affecting Government systems.
7. Appropriate actions to take when a cybersecurity incident is suspected.
8. Responsibilities of Government personnel in supporting incident prevention, reporting and response.
9. Relevant emerging threats and protective measures identified through Government CIRT operations.

The Consultant shall use appropriate delivery methods, including virtual awareness sessions, targeted briefings, presentations, practical demonstrations and reusable digital materials.

The programme shall be designed to reach relevant Government audiences without imposing unnecessary travel or logistical costs.

4.7.3 Incident Reporting Awareness and Institutional Engagement

The Consultant shall establish and implement targeted engagement activities to familiarise participating Government institutions with the Government CIRT's services and operating arrangements.

These activities shall include:

1. Communicating the Government CIRT's initial mandate, service catalogue and scope of assistance.
2. Explaining the approved cybersecurity incident reporting channels and reporting procedures.
3. Providing guidance on incident classification, urgency, escalation and information required when submitting an incident report.
4. Clarifying the respective responsibilities of the Government CIRT, institutional ICT personnel and other authorised Government officials.
5. Identifying and engaging designated institutional focal points responsible for cybersecurity incident reporting and coordination.
6. Providing practical guidance on the protection of sensitive incident information and secure communication with the Government CIRT.
7. Establishing mechanisms for obtaining stakeholder feedback and addressing operational difficulties with reporting and coordination arrangements.

Initial incident reporting guidance and engagement with designated Government focal points shall commence in time to support the Month 3 Initial Operational Capability.

4.7.4 Cybersecurity Advisories and Awareness Materials

The Consultant shall develop and maintain appropriate awareness and communication materials to support Government CIRT operations.

These shall include, as applicable:

1. Cybersecurity awareness presentations and guidance materials.
2. Incident reporting instructions and reference guides.
3. Cybersecurity alerts, advisories and preventive guidance.
4. Templates for communicating relevant cybersecurity threats and recommended protective actions.
5. Briefing materials for Government management and institutional focal points.

6. Frequently asked questions and other practical resources supporting Government CIRT services.

Materials shall be appropriate for the intended audiences, technically accurate, accessible and suitable for continued use and updating by Government personnel following completion of the consultancy.

The Consultant shall establish appropriate procedures for reviewing and approving cybersecurity advisories and official communications before dissemination.

4.7.5 National CIRT Stakeholder Consultation and Engagement

In support of the National CIRT institutional framework workstream, the Consultant shall undertake targeted engagement with relevant national stakeholders.

Stakeholders may include Government institutions, competent national authorities, regulators, designated critical infrastructure operators, relevant private sector representatives, and regional or international cybersecurity cooperation partners, as agreed with the Government.

The Consultant shall:

1. Identify and map relevant stakeholder groups, their existing cybersecurity responsibilities and their potential roles in national incident response coordination.
2. Assess stakeholder needs, existing incident reporting practices, information-sharing arrangements and institutional coordination challenges.
3. Facilitate consultations concerning the proposed National CIRT mandate, institutional arrangements, service priorities and stakeholder relationships.
4. Examine practical mechanisms for cooperation between the Government CIRT and relevant national stakeholders.
5. Consult on proposed national incident reporting, information-sharing, escalation and coordination protocols.
6. Identify potential requirements for formal cooperation arrangements, information-sharing agreements or other institutional instruments.
7. Document stakeholder feedback, significant areas of agreement, unresolved issues and matters requiring Government decisions.
8. Incorporate relevant consultation findings into the proposed National CIRT institutional and operational framework.

The Consultant shall coordinate these activities with the institutional development requirements under Section 4.3 to avoid duplicating consultations or imposing unnecessary demands on stakeholders.

4.7.6 Regional and International Cybersecurity Cooperation

The Consultant shall assess and recommend appropriate arrangements for engagement with relevant regional and international cybersecurity organisations, CIRT networks and cooperation mechanisms.

The Consultant shall:

1. Identify relevant regional and international cybersecurity cooperation mechanisms appropriate to Saint Lucia's institutional context and operational requirements.
2. Assess potential opportunities for information sharing, technical assistance, capacity development, incident coordination and participation in cybersecurity exercises.
3. Recommend suitable engagement and cooperation arrangements for the Government CIRT and the proposed National CIRT.
4. Identify relevant participation requirements, information-handling considerations, resource implications and institutional dependencies.
5. Support introductory technical engagement with agreed organisations where authorized by the Government.

The Consultant shall not enter into formal cooperation agreements or commit the Government to institutional or financial obligations without the necessary authorisation.

4.7.7 Monitoring and Evaluation of Awareness and Engagement Activities

The Consultant shall establish practical mechanisms for assessing the reach, relevance and effectiveness of the cybersecurity awareness and stakeholder engagement programme.

These shall include:

1. Maintaining records of awareness sessions, stakeholder consultations and related activities.
2. Tracking participation by target audience and institution.
3. Obtaining participant feedback and assessing understanding of priority cybersecurity messages.
4. Evaluating awareness of Government CIRT reporting channels and procedures.
5. Identifying recurring questions, awareness gaps and opportunities for improvement.
6. Assessing the effectiveness of engagement with institutional focal points and other relevant stakeholders.
7. Providing recommendations for sustaining and strengthening awareness and stakeholder engagement activities beyond the consultancy period.

The Consultant shall use the findings to refine awareness materials, engagement methods and related operational guidance.

4.7.8 Transfer and Sustainability of Awareness and Engagement Functions

The Consultant shall ensure that designated Government personnel are progressively equipped to plan, coordinate and deliver routine cybersecurity awareness and stakeholder engagement activities.

This shall include:

1. Providing practical mentoring in the preparation and delivery of awareness sessions.
2. Transferring approved communication templates, training materials, presentations and related resources.
3. Establishing procedures for maintaining stakeholder contact information and distributing approved advisories.
4. Providing guidance on the periodic review and updating of awareness materials.
5. Supporting Government personnel in conducting awareness and stakeholder engagement activities during the latter stages of the DBOT period.
6. Recommending sustainable arrangements for continued cybersecurity awareness, stakeholder engagement and advisory dissemination following the consultancy.

The corresponding awareness and stakeholder engagement deliverables, verification requirements and acceptance criteria are specified in Section 7.

4.8 Training, Mentoring and Capacity Building

The Consultant shall design and implement a comprehensive, role-based training, mentoring and capacity-building programme to develop the technical, operational, managerial and institutional competencies required for the effective operation and long-term sustainability of the Government Cybersecurity Incident Response Team (Government CIRT).

The programme shall be integrated into the twelve-month Design–Build–Operate–Transfer (DBOT) implementation model and shall progressively prepare designated Government personnel to assume responsibility for the Government CIRT's agreed core services.

The Consultant shall adopt a practical, competency-based approach that combines structured training, supervised operational experience, technical demonstrations, incident response exercises, mentoring and progressive transfer of responsibilities.

The programme shall address the needs of designated Government CIRT personnel, relevant Government Information Technology Services (GITS) staff, participating Government ICT focal points and other authorised personnel whose responsibilities are directly related to Government CIRT operations.

Training activities shall be aligned with the Government CIRT's approved mandate, operational service catalogue, technical environment and institutional arrangements.

The completion of training sessions or attendance requirements alone shall not constitute satisfactory achievement of the capacity-building and transfer obligations.

4.8.1 Training Needs and Competency Assessment

The Consultant shall conduct an initial assessment of the knowledge, skills and competencies of designated Government personnel who will participate in establishing and operating the Government CIRT.

The assessment shall identify:

1. Existing cybersecurity knowledge and technical experience.
2. Experience in incident reporting, analysis and response.
3. Familiarity with incident classification, prioritisation and escalation.
4. Knowledge of incident case management and operational documentation.
5. Experience with relevant cybersecurity technologies and system administration.
6. Understanding of cybersecurity governance, confidentiality and information-sharing requirements.
7. Experience in preparing technical reports and cybersecurity advisories.
8. Operational coordination and communication capabilities.
9. Management and supervisory competencies relevant to Government CIRT operations.
10. Individual and institutional capacity gaps requiring targeted development.

The Consultant shall prepare a Training Needs and Competency Assessment identifying the competencies required for the designated Government CIRT roles and the proposed measures for addressing identified gaps.

The assessment shall inform the training programme, mentoring arrangements, operational assignments and subsequent competency verification activities.

4.8.2 Role-Based Competency Framework

The Consultant shall develop a practical competency framework defining the knowledge, skills and operational abilities required for the Government CIRT's agreed functions.

The framework shall distinguish competencies appropriate to the following roles, as applicable:

1. Government CIRT management and operational supervision.
2. Cybersecurity incident intake and case management.
3. Incident triage, analysis and response coordination.
4. Cybersecurity advisory preparation and knowledge sharing.
5. Technical system administration and security configuration.
6. Operational reporting and performance monitoring.
7. Emergency incident escalation and coordination.
8. Government institutional ICT focal points.

For each relevant role, the framework shall identify:

a. Required knowledge and practical skills.
b. Expected operational responsibilities.
c. Applicable tools, procedures and technical competencies.
d. Proposed training and mentoring activities.
e. Methods for assessing practical competence.
f. Minimum proficiency expectations for independent or supervised performance.
g. Any continuing professional development requirements.

The competency framework shall be proportionate to the Government CIRT's approved staffing structure and shall not assume that each function requires a separate full-time position.

Where individual personnel are expected to perform multiple functions, the framework shall identify the corresponding competency requirements.

4.8.3 Training and Capacity-Building Plan

The Consultant shall prepare a detailed Training and Capacity-Building Plan based on the initial assessment and approved competency framework.

The plan shall specify:

1. Training objectives and expected learning outcomes.
2. Target participants and role-specific requirements.
3. Training topics and practical activities.
4. Proposed delivery methods.
5. Training materials and technical resources.
6. Indicative training schedules.
7. Mentoring and supervised operational assignments.
8. Practical exercises and competency assessments.
9. Requirements for refresher or corrective training.
10. Arrangements for recording attendance, participation and performance.
11. Responsibilities of the Consultant and designated Government counterparts.
12. Measures for sustaining institutional knowledge after the consultancy.

The plan shall be integrated with the DBOT implementation schedule and updated as necessary to address operational developments, staffing changes and identified competency gaps.

Training shall commence sufficiently early to support the Month 3 Initial Operational Capability milestone and continue throughout the operational and transfer phases.

4.8.4 Technical and Operational Training

The Consultant shall deliver structured technical and operational training covering the competencies required for the Government CIRT's agreed core services.

Training shall address, as appropriate:

a. Government CIRT Mandate and Operational Arrangements

1. Government CIRT objectives, mandate and service scope.
2. Institutional governance and reporting arrangements.
3. Roles and responsibilities of Government CIRT personnel.
4. Coordination with participating Government institutions.
5. Operational authority, confidentiality and information-sharing requirements.

b. Cybersecurity Incident Management

1. Cybersecurity incident identification and reporting.
2. Incident intake and acknowledgement.
3. Incident registration and case management.
4. Incident classification and severity assessment.
5. Incident prioritisation and escalation.
6. Initial technical assessment and analysis.
7. Incident response coordination.
8. Incident documentation and reporting.
9. Case closure and post-incident review.
10. Application of approved incident response playbooks.

c. Cybersecurity Threat and Vulnerability Information

1. Identification of reliable cybersecurity information sources.
2. Interpretation of relevant threat and vulnerability advisories.
3. Assessment of potential implications for Government systems.
4. Preparation of cybersecurity alerts and recommendations.
5. Coordination with Government ICT personnel on relevant mitigation activities.
6. Appropriate documentation and dissemination of cybersecurity information.

d. Government CIRT Technology Administration

1. Government CIRT technical architecture.
2. Operation and administration of approved case management tools.
3. Secure configuration and access control.
4. Relevant logging and audit requirements.
5. Backup and recovery procedures.
6. Routine system administration and maintenance.
7. Technical troubleshooting and escalation.
8. Relevant integration and information protection requirements.

e. Operational Reporting and Communication

1. Preparation of incident summaries and technical reports.
2. Communication with affected Government institutions.
3. Preparation of cybersecurity advisories.
4. Management reporting and operational performance indicators.
5. Documentation of decisions, actions and lessons learned.
6. Communication and escalation during significant cybersecurity incidents.

Training shall use the actual Government CIRT operational procedures and approved technologies wherever practicable.

The Consultant shall ensure that training materials reflect the systems, responsibilities and service arrangements that Government personnel will be required to maintain.

4.8.5 Practical Mentoring and Supervised Operations

The Consultant shall provide continuous practical mentoring throughout the operational phases of the consultancy.

Mentoring shall be integrated into actual Government CIRT activities and approved simulation exercises.

The Consultant shall:

1. Demonstrate relevant operational procedures and technical tasks.
2. Guide Government personnel through incident reporting and case management activities.
3. Provide supervised experience in incident classification, triage and escalation.
4. Support Government personnel in preparing operational reports and cybersecurity advisories.
5. Provide practical instruction in the use and administration of relevant technologies.
6. Guide personnel in applying incident response playbooks.
7. Review operational decisions and provide constructive technical feedback.
8. Identify recurring competency gaps and provide targeted coaching.
9. Progressively assign greater responsibility to Government personnel.
10. Record mentoring activities and observed improvements in operational performance.

The mentoring arrangements shall promote learning through direct participation and shall not be limited to classroom instruction or Consultant demonstrations.

Where actual cybersecurity incidents are unsuitable for training purposes because of confidentiality, operational risk or other constraints, the Consultant shall use realistic simulated scenarios.

4.8.6 Incident Response Exercises and Practical Assessments

The Consultant shall design and conduct practical exercises to assess and strengthen Government personnel's ability to perform the agreed Government CIRT functions.

The exercise programme shall include:

1. Initial exercises supporting the Month 3 Initial Operational Capability demonstration.
2. Incident reporting and case management exercises.
3. Incident classification and escalation scenarios.
4. Technical incident analysis and response coordination exercises.
5. Cybersecurity advisory preparation activities.
6. Emergency notification and escalation tests.
7. Exercises involving relevant Government ICT focal points.
8. A Government-led operational exercise during the final transfer phase.

Exercises shall incorporate realistic scenarios relevant to the Government operating environment.

The Consultant shall establish appropriate assessment criteria covering:

- Correct application of operational procedures.
- Accuracy of incident classification and prioritisation.
- Timeliness and appropriateness of escalation.
- Quality of incident documentation.
- Effectiveness of operational communication and coordination.
- Appropriate use of Government CIRT technologies.
- Compliance with security and confidentiality requirements.
- Ability to make or recommend appropriate operational decisions.
- Identification of matters requiring specialist assistance.
- Ability to complete assigned tasks with the expected level of independence.

The Consultant shall document exercise results, individual or role-based competency observations and recommended corrective measures.

4.8.7 Progressive Capacity Development and Transfer

The Consultant shall align capacity-building activities with the progressive DBOT transfer arrangements.

Months 1–3: Foundational Training and Initial Operational Capability

During the initial phase, the Consultant shall:

1. Conduct the training needs and competency assessment.

2. Develop the role-based competency framework.
3. Deliver foundational Government CIRT training.
4. Provide initial instruction in approved operational procedures and interim technologies.
5. Conduct supervised incident management exercises.
6. Ensure Government personnel participate in the Month 3 operational demonstration.

Months 3–9: Applied Training and Consultant-Led Operations

During this phase, the Consultant shall:

1. Provide advanced role-specific training as required.
2. Deliver practical mentoring through Government CIRT operations.
3. Assign progressively greater operational responsibilities to Government personnel.
4. Conduct incident response exercises and technical assessments.
5. Train Government personnel to operate, administer and maintain the hardware and software supplied under the contract, coordinating training with deployment, integration and commissioning milestones.
6. Review competency development and address identified gaps.
7. Prepare personnel for Government-led operations.

Months 9–12: Government-Led Operations and Competency Verification

During the final phase, the Consultant shall:

1. Support Government personnel in assuming primary responsibility for routine operations.
2. Observe and assess their performance during operational activities.
3. Provide targeted corrective training where necessary.
4. Conduct practical competency verification.
5. Support the Government-led operational readiness assessment in Month 11.
6. Address outstanding capacity gaps within the Consultant's responsibilities.
7. Complete the transfer of relevant training materials, procedures and technical knowledge.
8. Provide recommendations for continued professional development following handover.

The Consultant shall ensure that the capacity-building programme supports the Government CIRT's ability to continue delivering its agreed core services following completion of the consultancy.

4.8.8 Competency Verification and Readiness Assessment

The Consultant shall establish a structured process for verifying that designated Government personnel have acquired the competencies necessary to perform their assigned Government CIRT functions.

Competency verification shall include, as appropriate:

1. Observation of operational tasks.
2. Practical technical assessments.
3. Incident response exercises.
4. Review of incident management records prepared by Government personnel.
5. Assessment of operational reporting and advisory preparation.
6. Verification of relevant technical administration tasks.
7. Evaluation of incident escalation and coordination performance.
8. Assessment of compliance with approved procedures.
9. Review of performance during Government-led operations.
10. Documentation of remaining competency gaps.

The Consultant shall maintain a competency matrix indicating the assessed readiness of designated personnel or operational roles.

The matrix shall distinguish between tasks that personnel can perform independently, tasks requiring limited specialist support and tasks for which further capacity development is necessary.

The Consultant shall use the results to prepare targeted corrective training and mentoring activities.

The competency verification findings shall form part of the Month 11 Government-led Operational Readiness Assessment required under Section 4.9.

Training attendance, participation certificates or completion of theoretical assessments alone shall not be sufficient evidence of operational readiness.

4.8.9 Training Materials and Institutional Knowledge Transfer

The Consultant shall prepare and transfer the training and knowledge resources necessary for the Government to maintain and further develop the Government CIRT's capabilities.

These shall include, as applicable:

1. Training presentations and participant materials.
2. Practical exercises and scenario materials.
3. Incident handling guides and job aids.
4. System administration and technical operating guides.
5. Incident response playbooks and operational reference materials.

6. Competency assessment instruments.
7. Training attendance and participation records.
8. Mentoring and practical assessment records.
9. Training evaluation findings.
10. Recommendations for refresher training and continuing professional development.

The Consultant shall provide editable versions of materials developed specifically for the assignment, subject to the applicable contractual intellectual property and licensing provisions.

The Consultant shall identify any third-party training resources that are subject to separate licensing or usage restrictions.

The knowledge-transfer approach shall support the Government's ability to orient new personnel, maintain operational consistency and reduce dependence on external consultants.

4.8.10 Management and Institutional Capacity Building

In addition to technical training, the Consultant shall provide targeted capacity building for designated Government managers, supervisors and institutional focal points.

This shall address:

1. Government CIRT governance and management responsibilities.
2. Oversight of operational service delivery.
3. Interpretation of cybersecurity incident and performance reports.
4. Escalation and management decision-making.
5. Institutional coordination and information-sharing responsibilities.
6. Operational risk management.
7. Resource planning and staffing requirements.
8. Technology maintenance and recurrent expenditure considerations.
9. Business continuity and operational sustainability.
10. Planning for the progressive development of Government CIRT services.

The Consultant shall also provide appropriate orientation to designated Government representatives concerning the proposed National CIRT institutional framework, including its recommended governance arrangements, stakeholder coordination mechanisms, implementation dependencies and phased development roadmap.

Such orientation shall support Government understanding and future decision-making but shall not constitute a requirement to establish or operate the National CIRT during the consultancy.

4.8.11 Training Delivery and Participation Arrangements

The Consultant shall deliver the training and capacity-building programme through a combination of remote and targeted in-country activities, consistent with the approved hybrid implementation model.

The delivery approach shall be selected according to the nature of the activity, required practical participation, technical environment and operational objectives.

The Consultant shall:

1. Coordinate training schedules with designated Government counterparts.
2. Provide sufficient advance notice of planned activities.
3. Identify any required technical facilities, systems or participant prerequisites.
4. Ensure that training is accessible and appropriate to the designated participants.
5. Provide opportunities for practical application and clarification.
6. Maintain attendance and participation records.
7. Evaluate the effectiveness of training activities.
8. Adjust training methods where necessary to address identified learning needs.
9. Coordinate technical training with system deployment and integration activities.
10. Minimise unnecessary disruption to Government operational responsibilities.

Where feasible, practical training shall be delivered using the Government CIRT's approved operational environment.

Remote training and mentoring arrangements shall comply with applicable Government security, confidentiality and access requirements.

4.8.12 Training Performance Reporting and Acceptance

The Consultant shall report regularly on implementation of the capacity-building programme.

Reporting shall include:

1. Training activities completed.
2. Participants and roles covered.
3. Training topics and learning objectives.
4. Practical exercises conducted.
5. Mentoring activities undertaken.
6. Competencies assessed and verified.
7. Identified knowledge and skills gaps.
8. Corrective training measures.
9. Progress towards Government-led operations.
10. Outstanding capacity-building requirements.

The Consultant shall prepare a final Training, Mentoring and Competency Transfer Report as part of the Month 12 handover documentation.

The report shall summarise the training delivered, practical mentoring undertaken, competencies demonstrated, outstanding limitations and recommendations for continuing professional development.

Acceptance of the capacity-building obligations shall be based on the agreed training outputs, documented practical assessments and demonstrated readiness of designated Government personnel to perform their assigned core functions.

The Consultant shall remain responsible for delivering the agreed training, mentoring and competency assessment activities.

Where readiness is materially affected by Government-controlled staffing changes, prolonged unavailability of designated personnel or other documented dependencies, the Consultant shall promptly identify the impact, implement feasible mitigation measures and report any outstanding requirements in accordance with the contract.

The capacity-building activities shall be coordinated with the operational service requirements under Section 4.6 and the sustainability and final transfer requirements under Section 4.9.

4.9 Operational Performance, Sustainability and Transfer

The Consultant shall establish and implement comprehensive arrangements for monitoring Government CIRT operational performance, ensuring service continuity, strengthening institutional sustainability and progressively transferring operational responsibility to designated Government personnel.

The Consultant shall adopt a structured, evidence-based approach to operational transition consistent with the twelve (12)-month Design–Build–Operate–Transfer (DBOT) implementation model.

The Government CIRT shall remain operational throughout the applicable DBOT phases, with the Consultant providing the agreed technical assistance, operational support, mentoring and quality assurance while Government personnel progressively assume responsibility for the agreed core services.

The transfer process shall commence during the operational phase and shall not be deferred until the final month of the consultancy.

The Consultant shall ensure that the Government CIRT is capable of continuing its agreed core operations under Government control following completion of the assignment, using the complete contracted technology solution, including all required hardware, software, licences and supporting components, duly installed, configured, integrated, tested, commissioned and technically accepted at the Government-approved location. Interim arrangements shall not substitute for completion of the contracted technology solution or satisfy the final transfer

and acceptance requirements unless expressly authorised through an approved contractual variation.

4.9.1 Operational Performance Management Framework

The Consultant shall develop and implement an operational performance management framework appropriate to the Government CIRT's approved mandate, service catalogue and operating model.

The framework shall include:

1. Defined operational performance indicators and measurement methods.
2. Monitoring and measurement of compliance with the minimum incident acknowledgement, initial triage and escalation targets specified in Section 4.6.13, including the emergency on-call requirements for Critical (P1) and High (P2) incidents.
3. Incident registration, case management and closure indicators.
4. Measures of incident response coordination and stakeholder engagement.
5. Cybersecurity advisory preparation and dissemination indicators.
6. Training, mentoring and personnel competency indicators.
7. Operational availability and continuity indicators.
8. Emergency notification and escalation performance measures.
9. Quality assurance and service improvement arrangements.
10. Management reporting and performance review procedures.

The Consultant shall establish an operational performance baseline following Initial Operational Capability and progressively refine the framework as Government CIRT services mature.

Performance targets shall be proportionate to the agreed service catalogue, operating hours, available personnel and approved technical capabilities.

The framework shall distinguish between activities under the Government CIRT's direct control and outcomes dependent on the actions of affected Government institutions, external service providers or other authorities.

The Consultant shall monitor compliance with the minimum service-level targets established under Section 4.6.13, document any instances of non-compliance, identify the reasons for missed targets and implement appropriate corrective measures. Service-level performance shall be included in periodic operational reports and assessed as part of the Month 11 operational readiness assessment.

4.9.2 Operational Monitoring and Reporting

The Consultant shall monitor and document the performance of the Government CIRT throughout the operational phase.

The Consultant shall:

1. Maintain appropriate records of cybersecurity incidents received and managed.
2. Monitor compliance with approved incident management and escalation procedures.
3. Track operational performance against agreed indicators and service targets.
4. Record cybersecurity advisories, stakeholder notifications and relevant knowledge-sharing activities.
5. Monitor the availability and effectiveness of incident reporting and case management mechanisms.
6. Document operational issues, service limitations and corrective actions.
7. Track Government personnel participation and progressive assumption of operational responsibilities.
8. Review the effectiveness of emergency notification and escalation arrangements.
9. Identify emerging operational risks and capacity constraints.
10. Prepare periodic operational performance reports for Government review.

Operational performance reporting shall be incorporated into the Consultant's monthly progress reports and the relevant deliverables specified in Section 7.

Reports shall provide sufficient evidence to enable the Government to assess actual operational capability and progress towards Government-led operations.

Where no actual cybersecurity incidents occur during a reporting period, the Consultant shall use approved exercises, simulations and operational tests to provide evidence of continued readiness.

4.9.3 Operational Quality Assurance and Continuous Improvement

The Consultant shall establish and maintain practical quality assurance and continuous improvement arrangements for the Government CIRT.

These arrangements shall include:

1. Periodic reviews of incident management procedures and operational workflows.
2. Quality checks of incident records, classification decisions and escalation actions.
3. Reviews of response coordination effectiveness.
4. Assessment of cybersecurity advisory processes and information-sharing practices.
5. Evaluation of operational exercises and simulations.
6. Identification of recurring operational weaknesses and procedural gaps.
7. Documentation of lessons learned from actual incidents and exercises.
8. Development and implementation of corrective action plans.
9. Periodic updates to operational procedures, templates and playbooks.

10. Verification that corrective actions have achieved their intended results.

The Consultant shall maintain a documented operational improvement register identifying corrective actions, responsible parties, target dates and implementation status.

Material operational deficiencies shall be promptly communicated to the designated Government representatives.

4.9.4 Operational Continuity and Resilience

The Consultant shall establish and maintain appropriate operational continuity arrangements to ensure that the Government CIRT can continue delivering its agreed core services during technical disruptions, personnel unavailability or other operational difficulties.

The arrangements shall address:

1. Continuity of cybersecurity incident reporting and intake.
2. Availability of alternative incident communication channels.
3. Backup and recovery of incident management information.
4. Protection and recovery of operational records and supporting evidence.
5. Emergency contact and escalation arrangements.
6. Alternative arrangements for critical operational personnel.
7. Recovery of essential technical systems and configurations.
8. Management of dependencies on external hosting, connectivity, software and support providers.
9. Continuity during technology migration or infrastructure replacement.
10. Periodic testing and updating of operational continuity procedures.

The Consultant shall conduct appropriate practical tests of the agreed continuity arrangements and document the results.

The arrangements shall be proportionate to the Government CIRT's approved operating model and shall not be interpreted as requiring a continuously staffed twenty-four-hour Security Operations Centre.

4.9.5 Government CIRT Sustainability Plan

The Consultant shall prepare and implement, within its contractual responsibilities, a practical Government CIRT Sustainability Plan enabling continued delivery of the agreed core services after transfer.

The Plan shall distinguish arrangements that the Consultant must deliver from decisions, appointments and funding commitments requiring Government action.

The Plan shall address:

1. **Staffing and organisational arrangements:** Agreed roles, responsibilities, competency requirements, succession arrangements and remaining staffing gaps. Government shall retain responsibility for staff appointments and deployment.
2. **Recurrent operating budget:** A costed annual operating budget distinguishing mandatory expenditure from optional enhancements. The Consultant shall provide supporting information and engage the relevant Government entities to facilitate budget planning. Approval and allocation of Government funding shall remain Government responsibilities.
3. **Licence and service continuity:** Valid Government usage rights, licence terms, subscription expiry dates, renewal procedures, supplier contacts and projected costs. Licences and support entitlements shall be registered directly to Government or lawfully transferred before final acceptance.
4. **Technical support:** Documented arrangements covering the supplied solution, including a mandatory twelve (12)-month technical support period commencing on the effective date of final transfer and final acceptance. The scope, service levels, exclusions and costs of this support shall be expressly identified in the contract price. Technical support shall be distinct from warranty obligations, which shall relate to the correction of defects, and from any optional additional post-DBOT services that may be procured separately by Government.
5. **Operational continuity and recovery:** Tested backup, restoration, continuity and emergency escalation procedures that designated Government personnel can execute.
6. **Capability development:** A phased roadmap for continued professional development, technology maintenance and future service enhancement, with indicative costs and responsibilities.

The Plan shall be submitted in draft by Month 10 and finalised before transfer. The Consultant shall complete arrangements within its contractual control and record outstanding Government decisions with named owners, required actions and target dates.

The existence of an unresolved Government decision shall not automatically excuse an incomplete Consultant obligation or constitute acceptance of the assignment.

The Sustainability Plan shall identify any activities, resources, funding approvals, staffing actions or procurement actions required by the Government to maintain operations after transfer. Such items shall be clearly distinguished from the Consultant's contractual obligations.

4.9.6 Progressive Transfer of Operational Responsibilities

The Consultant shall implement a structured transfer programme through which designated Government personnel progressively assume responsibility for Government CIRT operations.

The programme shall commence during the Consultant-supported operational phase and intensify during Months 9–12.

The Consultant shall:

1. Define the operational responsibilities to be transferred to Government personnel.
2. Establish a responsibility and competency matrix identifying the required roles and capabilities.
3. Agree a phased transfer schedule with designated Government representatives.
4. Provide practical mentoring and supervised operational experience.
5. Assign progressively greater responsibility for incident intake, registration, classification and triage.
6. Support Government personnel in undertaking incident escalation and response coordination.
7. Transfer responsibility for preparing cybersecurity advisories and operational reports.
8. Develop Government personnel capability to administer and maintain the agreed operational systems.
9. Support Government personnel in managing operational performance, risks and corrective actions.
10. Assess the effectiveness of the progressive transfer and address identified competency gaps.
11. Document the responsibilities transferred and any outstanding operational dependencies.
12. Prepare Government personnel to lead routine operations and coordinate emergency escalation arrangements.

The Consultant shall ensure that Government personnel actively perform the relevant operational functions rather than merely observe Consultant activities.

The transfer process shall be coordinated with the competency-based training and mentoring requirements specified in Section 4.8.

4.9.7 Government-Led Operations During Months 9–12

During Months 9–12, the Consultant shall support the transition to Government-led operations.

Under this arrangement, designated Government personnel shall progressively assume primary responsibility for the routine delivery and management of the agreed core Government CIRT services.

The Consultant shall continue to provide supervision, mentoring, technical assistance, quality assurance and agreed specialist support.

The Government-led operational phase shall include:

1. Government personnel receiving and managing cybersecurity incident reports.
2. Government personnel undertaking incident classification, triage and prioritisation.

3. Government personnel coordinating incident escalation and response activities.
4. Government personnel preparing cybersecurity advisories and operational communications.
5. Government personnel maintaining incident records and operational reports.
6. Government personnel applying approved procedures and incident response playbooks.
7. Government personnel administering agreed technical systems and operational access arrangements.
8. Government personnel coordinating emergency notification and escalation procedures.
9. Government personnel participating in operational performance reviews and corrective action management.
10. The Consultant assessing and documenting the Government's increasing operational independence.

The Consultant shall identify and address material competency, procedural or technical deficiencies that may affect the Government's ability to sustain operations following handover.

Government-led operations shall be demonstrated through actual operational activities where available and supplemented by approved practical exercises and simulations.

4.9.8 Operational Readiness Assessment

The Consultant shall prepare and facilitate a formal Government-led operational readiness assessment no later than Month 11.

The assessment shall verify the Government CIRT's ability to perform the agreed core operational functions under Government leadership.

The assessment shall include:

1. Review of the approved Government CIRT mandate and operational service catalogue.
2. Verification of functioning incident reporting and case management arrangements.
3. Practical assessment of incident classification, triage and escalation.
4. Demonstration of incident response coordination and operational decision-making.
5. Assessment of cybersecurity advisory and stakeholder communication capabilities.
6. Verification of emergency notification and escalation procedures.
7. Assessment of Government personnel competencies and operational responsibilities.
8. Verification of technical administration, access control and information protection arrangements.
9. Review and testing of backup, recovery and operational continuity procedures.
10. Assessment of operational documentation, procedures and playbooks.

11. Review of operational performance indicators and outstanding corrective actions.
12. Identification of residual risks and outstanding requirements affecting final transfer.

The assessment shall include a witnessed practical exercise in which designated Government personnel perform the agreed incident management and coordination functions under Government leadership.

The Consultant shall prepare an Operational Readiness Assessment Report documenting the methodology, results, demonstrated competencies, identified deficiencies, corrective actions and recommendations concerning final transfer readiness.

The Government shall review and verify the assessment results in accordance with Section 7.

The Consultant shall address deficiencies attributable to its contractual responsibilities before final handover.

4.9.9 Technical Operational and Institutional Handover

The Consultant shall complete a documented handover transferring the functioning Government CIRT capability to Government operational control. The handover shall include ownership of supplied physical assets, applicable software usage rights, operational records, documentation, administrative access and the responsibilities specified in the contract.

Government's institutional mandate and legal authority shall derive from the relevant Government instruments and shall not be created by the Consultant's transfer documents.

The Handover Package shall include:

1. Verified Asset Register: A complete register reconciled against the supplied and installed solution, identifying hardware, equipment, software, quantities, serial numbers or other identifiers, locations, ownership or licensing status, warranty details and support coverage.
2. Title Transfer Document: An executed instrument confirming Government ownership of supplied physical assets in accordance with the contract, without liens or undisclosed encumbrances.
3. Licences and support entitlements: Evidence of direct Government registration or executed assignments, novations and required third-party consents. The documentation shall identify usage rights, restrictions, expiry dates, renewal requirements and costs.
4. Warranty and Latent Defects Schedule: Coverage, commencement and expiry dates, notification procedures, response and rectification requirements, responsible parties and continuing obligations, consistent with Section 4.5.2 and the contract. Supplier warranties shall not replace the Consultant's contractual obligations.
5. Operational documentation: The Government-approved mandate and service catalogue, procedures, playbooks, escalation arrangements, advisory templates and governance documentation.

6. Technical documentation: Final architecture, configurations, integration records, security baselines, installation and commissioning records, acceptance tests, and backup and recovery procedures.
7. Administrative access: Secure transfer of privileged accounts, credentials and management access. Consultant access shall be revoked at transfer except where expressly authorised by Government for surviving contractual obligations or approved support, subject to defined security controls.
8. Incident and operational records: Secure transfer of Government-owned records, logs and relevant information in accessible formats, including export formats where supported, together with the tools and rights necessary for continued use.
9. Training and competency records: Training materials, mentoring records, assessment results, the final competency matrix and evidence of Government personnel readiness.
10. SIM3 assessment records: The joint baseline, agreed targets, independent assessment report, corrective action evidence and any residual findings requiring Government disposition.
11. Sustainability arrangements: The final Sustainability Plan, support arrangements and disclosure of recurrent expenditure and renewal obligations.
12. Residual risks and outstanding actions: Assigned responsibilities, deadlines and approved contractual treatment. Recording an outstanding matter shall not itself waive the relevant obligation.
13. Formal handover record: A signed record identifying the assets, rights, responsibilities and documents transferred, the effective transfer date, authorised signatories and any expressly approved outstanding matters.

The Handover Package and required transfer instruments shall be completed by Month 12. Government shall verify their completeness before issuing final acceptance under Section 7.6.

4.9.10 Technology Completion and Transfer Dependencies

The Consultant shall coordinate transfer with the completion, testing and acceptance of the technology solution supplied under the DBOT contract.

Procurement, supplier and subcontractor delivery, installation, configuration, integration, commissioning and defect rectification within the agreed scope shall remain the Consultant's responsibility. These activities shall not be treated as separate Government procurement dependencies.

Government-controlled dependencies shall be limited to agreed inputs and decisions, including premises, base utilities and connectivity, site and system access, counterpart personnel and required legal or administrative approvals.

Where a dependency materially affects implementation, the Consultant shall:

1. Notify Government promptly in writing, identifying its cause, contractual responsibility and likely effect on milestones.
2. Record affected activities, required decisions, responsible parties and proposed resolution dates.
3. Implement reasonable mitigation measures and continue unaffected activities.
4. Maintain approved interim services where necessary to preserve operational continuity.
5. Update implementation sequencing and submit any proposed contractual adjustment for consideration.
6. Identify residual risks and outstanding actions affecting transfer readiness.

Any relief for a proven Government-caused delay shall be assessed under the contract. No extension, additional payment, scope reduction or acceptance shall arise automatically.

Interim operation shall not replace completion of the contracted solution unless expressly authorised through an approved contractual variation. National Data Centre reconstruction shall not be a prerequisite for handover at the agreed Government-approved location.

Final transfer shall remain subject to the technical, operational, personnel readiness and documentation requirements of Sections 4.9 and 7.

4.9.11 Final Operational Transfer and Completion

The Consultant shall complete the agreed operational transfer of the Government CIRT by the end of Month 12.

Final transfer shall be based on verified operational capability, demonstrated Government personnel competence, satisfactory completion of the applicable technical and institutional handover requirements, and establishment of sustainable arrangements for continued core service delivery.

The Consultant shall prepare a Final Completion and Handover Report documenting:

1. The status of the Government CIRT's agreed operational capabilities.
2. The operational responsibilities transferred to Government personnel.
3. The results of the Month 11 operational readiness assessment.
4. The status of identified corrective actions.
5. The training, mentoring and competency development completed.
6. The technical systems, configurations, documentation and access arrangements transferred.
7. The completion, commissioning and technical acceptance status of the complete contracted Government CIRT technology solution, including confirmation of the resolution or formally approved contractual treatment of any outstanding integration requirements.The operational continuity and sustainability arrangements established.
8. The residual risks, dependencies and recommended follow-up actions.

9. The status of the National CIRT framework deliverables and their transfer to the Government.
10. Confirmation of the completion of the applicable contractual obligations.
11. A formal record of the final Government CIRT handover.

The Consultant shall demonstrate that designated Government personnel can independently perform the agreed routine core CIRT functions and apply the approved emergency notification and escalation procedures.

The Final Completion and Handover Report shall also confirm completion and acceptance of the contracted technology solution; reconciliation of the Asset Register; execution of title and applicable licence and support transfer documents; acceptance of the Warranty and Latent Defects Schedule; and the status of findings from the independent SIM3 assessment completed at least two months before contract completion. Consultant-controlled deficiencies shall be rectified before final acceptance, except for matters expressly treated otherwise under the applicable contractual procedures.

The Government shall verify completion of the applicable requirements before issuing written final acceptance in accordance with Section 7.6.

Submission of the Final Completion and Handover Report alone shall not constitute satisfactory completion of the consultancy.

Any optional post-DBOT support shall be separately priced and subject to Government discretion, funding availability and applicable contractual arrangements.

Such support shall not substitute for the mandatory establishment, operationalisation and transfer of the Government CIRT within the twelve-month implementation period.

4.9.11.a Transfer Acceptance Criteria

The Government CIRT shall be considered ready for final transfer and acceptance only where the Government has verified that:

1. The Operational Readiness Assessment has been completed.
2. Agreed operational capabilities have been demonstrated.
3. Designated Government personnel have demonstrated the required competencies.
4. Government-led operations have been conducted in accordance with Section 4.9.7.
5. The Handover Package has been submitted and verified.
6. All required operational documentation has been transferred.
7. Applicable licences, support arrangements and asset ownership transfers have been completed.
8. Outstanding Consultant-controlled deficiencies have been corrected or otherwise resolved through approved contractual procedures.
9. Sustainability arrangements have been established.

10. Any remaining risks have been documented and assigned.

5.0 Institutional Arrangements and Responsibilities

The consultancy shall be implemented under the oversight of the Ministry responsible for the Public Service, with technical and operational coordination provided through Government Information Technology Services (GITS) and project implementation support from the Caribbean Digital Transformation Project (CARDTP) Project Implementation Unit (PIU).

The institutional arrangements shall facilitate effective coordination, timely decision-making, access to relevant Government personnel and information, and the progressive transfer of Government CIRT responsibilities during the twelve (12)-month Design–Build–Operate–Transfer (DBOT) period.

The Consultant shall work closely with the designated Government counterparts throughout the assignment, ensuring that institutional development, technical implementation, operational activities and capacity building are appropriately coordinated.

5.1 Ministry Responsible for the Public Service

The Ministry responsible for the Public Service shall provide strategic and institutional oversight of the assignment.

Its responsibilities shall include:

1. Providing overall institutional direction and oversight of the consultancy.
2. Facilitating coordination among relevant Government ministries, departments and agencies.
3. Supporting the designation and participation of appropriate Government personnel in the establishment and operation of the Government CIRT.
4. Reviewing and considering institutional and governance recommendations arising from the assignment.
5. Facilitating the consideration of matters requiring senior Government decisions, policy direction or formal approval.
6. Supporting the development of sustainable institutional arrangements for continued Government CIRT operations.
7. Participating in the review and acceptance of relevant consultancy outputs in accordance with the applicable contractual arrangements.
8. Securing the formal Government instruments and approvals necessary to establish the Government CIRT, define its mandate, functions, constituency and authority, and enable lawful incident reporting, information sharing and data handling before operational service commencement.

9. Ensuring the timely designation and availability of counterpart personnel for training, supervised operations and transfer.
10. Coordinating confirmation of suitable Government-provided premises, base utilities and connectivity, with technical input from GITS.
11. Coordinating Government consideration of staffing, recurrent funding and institutional decisions necessary to sustain operations following transfer.

The Ministry shall retain responsibility for institutional decisions and Government approvals falling within its authority.

5.2 Government Information Technology Services (GITS)

GITS shall serve as the principal technical and operational counterpart for the establishment and operationalization of the Government CIRT.

Its responsibilities shall include:

1. Coordinating technical engagement between the Consultant and relevant Government ICT personnel.
2. Facilitating access to available technical information, existing cybersecurity tools and relevant Government ICT infrastructure, subject to applicable approvals and security requirements.
3. Supporting the identification and participation of designated Government CIRT personnel and institutional ICT focal points.
4. Participating in the review of the proposed Government CIRT architecture, service catalogue, operating procedures and technical requirements.
5. Coordinating Government-provided technical inputs, site and system access, existing infrastructure interfaces and counterpart participation during the Consultant's technology deployment, integration, testing and commissioning. Procurement and supply of the CIRT-specific technologies included in the contract shall remain the Consultant's responsibility.
6. Supporting the establishment of incident reporting, escalation and operational coordination arrangements across participating Government institutions.
7. Participating in operational exercises, performance reviews, competency assessments and readiness verification.
8. Supporting the progressive assumption of Government CIRT operational responsibilities by designated Government personnel.
9. Reviewing technical and operational outputs and providing recommendations concerning their acceptance.
10. Supporting the implementation of sustainable technical and operational arrangements following completion of the consultancy.

11. Participating in the assessment of the proposed hosting location and confirming technical requirements for Government-provided power, cooling, connectivity, physical security and access.
12. Participating in the joint SIM3 baseline assessment, review of proposed maturity targets and provision of Government-held evidence for the independent assessment.
13. Verifying the technical completeness of the Asset Register, configurations, administrative access, licence rights, warranty information and support arrangements proposed for handover.

GITS shall coordinate with the Ministry responsible for the Public Service and other relevant Government institutions on matters requiring institutional direction, approval or escalation.

5.3 Consultant Responsibilities

The Consultant shall be responsible for the complete Design–Build–Operate–Transfer delivery of the Government CIRT and development of the proposed National CIRT institutional and operational framework within the agreed scope, contract price and twelve-month implementation period.

The Consultant's responsibilities shall include:

1. Planning, coordinating and implementing both workstreams and all four DBOT phases.
2. Preparing the Technical Architecture and Build Specifications within thirty (30) calendar days of commencement.
3. Procuring, supplying, delivering, installing, configuring, integrating, testing and commissioning all hardware, software, licences and supporting services included in the contract.
4. Establishing and demonstrating Initial Operational Capability by the end of Month 3, including any necessary Consultant-provided interim arrangements within the agreed contract price.
5. Delivering, operating, maintaining and supporting the agreed Government CIRT services from Initial Operational Capability until final acceptance, including the prescribed emergency escalation and on-call arrangements.
6. Conducting the joint SIM3 baseline assessment with designated Government personnel and preparing measurable maturity targets for Government approval.
7. Facilitating the independent SIM3 assessment at least two months before contract completion, providing evidence and addressing deficiencies within its contractual responsibilities.
8. Developing and implementing operational procedures, incident response playbooks, reporting mechanisms and service-performance monitoring.

9. Delivering cybersecurity awareness, technical training, mentoring, exercises and practical competency assessments.
10. Supporting progressive Government-led operations during Months 9–12 while retaining its contractual service obligations until final acceptance.
11. Completing the Month 11 operational readiness assessment and addressing identified deficiencies within its responsibility.
12. Developing the proposed National CIRT framework, draft supporting instruments and phased implementation roadmap through the required consultations.
13. Identifying and promptly reporting Government decisions, inputs, authorisations and dependencies required to achieve the milestones.
14. Maintaining implementation schedules, progress reports, risk and dependency registers, operational records and quality assurance arrangements.
15. Complying with applicable security, confidentiality, information-handling and access requirements.
16. Completing the technical and operational transfer by Month 12, including assets, applicable licence rights, support entitlements, administrative access, documentation, operational records and institutional knowledge.
17. Providing the verified Asset Register, executed Title Transfer Document, applicable licence and support assignments, Warranty and Latent Defects Schedule, and final Sustainability Plan.
18. Completing all deliverables and continuing warranty, support and defect-rectification obligations in accordance with the contract.

Government approval, participation or progressive assumption of operational duties shall not transfer the Consultant's delivery responsibilities to Government.

The Consultant shall manage procurement within its own contractual scope but shall not exercise Government approval powers, confer statutory authority, appoint Government personnel or commit Government to additional expenditure without the required authorisation.

5.4 Designated Government CIRT Personnel

Government shall designate a CIRT lead and appropriate operational and technical counterpart personnel before contract commencement or confirm a time-bound designation and mobilisation arrangement during inception that supports Month 3 Initial Operational Capability. Government shall ensure their availability for training, supervised operations, practical assessments and progressive transfer throughout the assignment.

Where necessary, Government may separately engage individual consultants under applicable project and procurement arrangements to provide counterpart capacity. Any subsequent appointment or absorption into the public service shall remain subject to Government decisions and applicable procedures.

Their participation shall include, as appropriate:

1. Supporting the establishment of operational procedures, incident reporting arrangements and the Government CIRT service catalogue.
2. Participating in technical training, mentoring, practical exercises and competency assessments.
3. Undertaking supervised incident registration, triage, classification, escalation, case management and response coordination.
4. Supporting cybersecurity advisory preparation, operational reporting and communication with participating Government institutions.
5. Participating in the operation and administration of approved Government CIRT technologies.
6. Progressively assuming responsibility for routine Government CIRT operations during the implementation period.
7. Leading agreed operational activities and exercises during the Government-led transition phase.
8. Participating in operational readiness verification and formal handover activities.
9. Supporting the maintenance of operational records, procedures and technical documentation.
10. Continuing the delivery of the agreed Government CIRT services following completion of the DBOT period.

During inception, Government and the Consultant shall confirm named personnel, assigned roles, participation schedules, time commitments and arrangements for replacement or succession. Staffing gaps and their effects on training, operational readiness and transfer shall be recorded and escalated promptly.

The Consultant shall structure its implementation and mentoring programme to support meaningful counterpart participation while maintaining its contractual delivery obligations. Government personnel participation shall not substitute for the Consultant staffing and expertise required to deliver the agreed DBOT scope.

5.5 National CIRT Stakeholder Coordination

The Ministry responsible for the Public Service, with support from GITS and other relevant Government institutions, shall facilitate appropriate stakeholder engagement for the development of the proposed National CIRT framework.

The Consultant shall undertake the required institutional assessments, technical consultations and preparation of recommendations in accordance with Sections 4.3 and 4.7.

Relevant stakeholders may include Government ministries and agencies, national security and other competent authorities, regulators, designated critical infrastructure operators and appropriate regional or international cybersecurity partners.

Stakeholder participation shall be coordinated through the designated Government counterparts, taking account of institutional mandates, confidentiality requirements and the nature of the matters under consideration.

The Consultant shall document significant consultation findings, institutional dependencies and matters requiring Government consideration.

The proposed National CIRT framework shall remain subject to the applicable Government review, policy development and approval processes.

5.6 Coordination Reporting and Review Arrangements

The Consultant shall maintain effective coordination and communication with the Ministry responsible for the Public Service, GITS and the CARDTP PIU throughout the assignment.

The arrangements shall include:

1. An inception meeting to confirm the implementation approach, designated counterparts, responsibilities, Government inputs, reporting arrangements and escalation procedures.
2. Regular technical and operational meetings to review design, technology procurement and delivery, installation, integration, commissioning and service performance.
3. Monthly progress reports covering both workstreams, milestones, supplier delivery, operational services, training, expenditure-related commitments within the contract, risks, dependencies, corrective actions and planned activities.
4. Prompt written notification of significant incidents, implementation constraints and matters requiring Government decisions.
5. Review meetings for technical designs, operational procedures, institutional recommendations and other deliverables.
6. Coordination of stakeholder consultations, training, exercises and in-country missions.
7. Periodic assessment of Government personnel competencies and readiness to assume operational responsibilities.
8. Formal review of the Month 3 Initial Operational Capability, technology commissioning milestones, the independent SIM3 assessment, the Month 11 operational readiness assessment and the Month 12 final transfer.

The Ministry shall coordinate institutional decisions, GITS shall lead technical and operational review, and the CARDTP PIU shall coordinate contractual and administrative processes. Formal acceptance shall follow Section 5.8 and Section 7.

Independent SIM3 Assessment

Government shall approve the selection and appointment of an independent SIM3 evaluator in accordance with the applicable procurement and contractual procedures. The evaluator shall

not have participated in designing, supplying or operating the solution being assessed and shall submit its findings directly to Government.

The assessment shall be completed by the end of Month 10, at least two months before contract completion. It shall compare the Government CIRT's demonstrated maturity with the joint baseline and agreed targets.

The Consultant shall provide the evaluator with authorised access to relevant systems, documentation, operational evidence and personnel. It shall not direct, alter or approve the evaluator's findings.

Following the assessment, the Consultant shall prepare and implement a corrective action plan for deficiencies within its contractual responsibility. Government shall verify their resolution before final acceptance, in accordance with the contract.

The arrangements for the appointment, contracting and payment of the independent SIM3 evaluator shall be agreed and documented before contract award, ensuring that the evaluator remains independent of the Consultant and reports directly to Government. The independent SIM3 assessment shall complement, and shall not replace, technical acceptance testing or the Month 11 operational readiness assessment.

Meetings may be conducted virtually unless onsite participation is necessary. The Consultant shall maintain records of decisions, agreed actions, responsible parties, deadlines and outstanding matters.

5.7 Government Inputs and Dependencies

Government shall provide or facilitate the agreed inputs and decisions necessary for implementation. Their scope, responsible entities and required dates shall be confirmed during inception and maintained in the responsibility and dependency register.

Government inputs shall include:

1. Relevant strategies, policies, technical documentation, existing assessments and NRD deliverables, subject to applicable confidentiality and access controls.
2. Designated institutional counterparts and Government CIRT personnel with sufficient availability for training, operations and transfer.
3. Suitable premises, base utilities and connectivity, with agreed physical security and site access arrangements.
4. Authorised access to relevant Government systems, existing infrastructure, operational information and technical personnel.
5. The formal establishment instrument and other legal or administrative authorisations required for lawful Government CIRT operations.
6. Coordination with participating ministries, departments, agencies and providers of existing Government systems.

7. Timely review of designs, procedures, institutional recommendations and other deliverables.
8. Government decisions concerning institutional arrangements, staffing, recurrent funding and sustainability.
9. Participation in consultations, training, exercises, assessments and handover verification.
10. Arrangements for the independent SIM3 assessment in accordance with the procurement and contract documents.

Procurement and supply of the CIRT-specific hardware, software, licences and services included in the contract shall remain the Consultant's responsibility. Supplier and subcontractor delivery risks within that scope shall not be treated as Government procurement dependencies.

The Consultant shall identify required Government inputs sufficiently early, promptly notify Government of constraints, explain milestone impacts and implement reasonable mitigation measures while continuing unaffected activities.

Any relief for a proven Government-caused delay shall be assessed through the applicable contractual procedures. No extension, additional payment, reduction of scope or acceptance of incomplete deliverables shall arise automatically.

5.8 Review and Acceptance of Consultancy Outputs

The Consultant shall submit all contractual deliverables through the arrangements established for the assignment.

Technical and operational outputs shall be reviewed by designated Government representatives, including GITS where appropriate, while institutional and governance outputs shall be reviewed by the relevant Ministry and other designated authorities.

The CARDTP PIU shall coordinate the applicable contractual review and administrative processes.

Acceptance of deliverables shall be based on the requirements, verification evidence and acceptance criteria specified in Section 7 and the applicable contract provisions.

Participation in technical meetings, review of draft documents or provision of comments shall not, by itself, constitute formal acceptance of a deliverable.

The Government shall retain responsibility for formal contractual acceptance and associated payment authorisation in accordance with the applicable contractual arrangements.

6.0 Duration, Location and Contractual Conditions

6.1 Duration of the Assignment

The consultancy shall be implemented over a period of twelve (12) calendar months from the commencement date specified in the contract.

The Consultant shall complete all mandatory Design–Build–Operate–Transfer (DBOT) activities within this period, including the establishment, operationalisation and transfer of the Government Cybersecurity Incident Response Team (Government CIRT), and the development of the proposed institutional and operational coordination framework for the National Cybersecurity Incident Response Team (National CIRT).

The implementation schedule shall provide for the following mandatory milestones:

1. **Within thirty (30) calendar days:** Submission of the Technical Architecture and Build Specifications, including the detailed solution design, itemised hardware and software requirements, licensing and support arrangements, procurement and delivery schedule, installation and commissioning milestones, Government-provided inputs, and technical acceptance procedures. Procurement, supply and implementation of the contracted solution shall remain the Consultant's responsibility.
2. **By the end of Month 3:** Establishment and successful demonstration of the Government CIRT Initial Operational Capability.
3. **Months 3–9:** Consultant-supported operations, progressive service development and practical mentoring of designated Government personnel.
4. **Months 9–12:** Government-led operations, supported by Consultant supervision, mentoring and specialist technical assistance.
5. **By the end of Month 11:** Completion of the formal operational readiness and competency assessment.
6. **By the end of Month 12:** Completion of the mandatory Government CIRT operational transfer and all agreed National CIRT institutional framework outputs.

The Consultant shall propose a detailed implementation schedule demonstrating how both workstreams will be completed within the contractual period.

The detailed deliverables, submission deadlines, acceptance requirements and payment milestones are specified in Section 7.

6.2 Location and Hybrid Delivery Arrangements

The assignment shall be undertaken in Saint Lucia through a hybrid delivery model comprising predominantly remote technical and advisory services, supported by targeted in-country missions and direct engagement with designated Government personnel.

The Consultant shall propose an appropriate combination of remote and onsite activities, taking account of the nature of the services, operational requirements, technical dependencies, stakeholder engagement and knowledge transfer obligations.

The Consultant's technical proposal shall identify:

1. The proposed location and deployment arrangements of key personnel.
2. The activities to be performed remotely and those requiring physical presence in Saint Lucia.
3. The number, indicative timing, duration and purpose of proposed in-country missions.
4. The arrangements for secure remote access, communication and operational support.
5. The approach for conducting practical training, mentoring, technical exercises and readiness assessments.
6. The arrangements for ensuring timely specialist assistance and continuity of Government CIRT operations.
7. The measures proposed to maintain effective coordination with Government counterparts throughout the assignment.

In-country missions shall be scheduled to support critical implementation activities, including, as appropriate, inception and technical assessment, stakeholder consultations, infrastructure deployment and integration, practical training, operational exercises and final readiness verification.

The Consultant shall be responsible for proposing sufficient onsite inputs to achieve the required results. The Government shall not be obligated to accept a delivery model that relies excessively on remote engagement where physical participation is necessary for effective implementation.

6.3 Personnel Deployment and Availability

The Consultant shall deploy appropriately qualified personnel with the technical, operational and institutional expertise necessary to implement both workstreams.

The proposed staffing arrangements shall provide for effective coordination, continuity of technical support and timely completion of contractual activities.

The Consultant shall:

1. Identify the responsibilities and anticipated level of effort of each proposed key expert.

2. Demonstrate that the proposed personnel inputs are adequate for the design, establishment, operation and transfer of the Government CIRT.
3. Provide sufficient specialist expertise to support the National CIRT institutional and governance framework.
4. Ensure the availability of appropriate technical personnel during critical operational activities, exercises, deployment activities and incident response situations.
5. Maintain continuity of key personnel and obtain the necessary contractual approvals for any proposed personnel substitutions.
6. Provide suitable coordination arrangements where experts are working from different locations or time zones.
7. Ensure that designated Government counterparts have reliable access to the relevant Consultant personnel during agreed working periods.

The Consultant shall remain responsible for the quality, timeliness and completeness of all services, irrespective of the location from which personnel perform their duties.

6.4 Operational Support and Service Availability

Following establishment of the Initial Operational Capability, the Consultant shall provide operational support to the Government CIRT throughout the remaining DBOT period.

The Government CIRT shall initially provide routine services during standard Government business hours, supported by an agreed emergency on-call arrangement for high-severity and critical cybersecurity incidents occurring outside normal business hours, including weekends and public holidays.

The Consultant shall propose operational support arrangements addressing:

1. Routine technical and operational support during agreed service hours.
2. Availability of qualified personnel for incident assessment, technical advice and response coordination.
3. Procedures for receiving and acknowledging emergency notifications.
4. Escalation arrangements and specialist support for high-severity and critical incidents.
5. Communication channels, designated contacts and arrangements for coordinating with Government personnel.
6. Appropriate acknowledgement, escalation and support response targets.
7. Continuity arrangements in the event of key personnel unavailability or disruption to remote communication facilities.
8. Documentation and reporting of operational support activities.

The proposed service arrangements and response targets shall be reviewed and approved by the Government and incorporated into the applicable operational procedures and contractual requirements.

The consultancy shall not require the establishment of a continuously staffed twenty-four-hour Security Operations Centre.

The Consultant shall nevertheless ensure that the agreed emergency on-call arrangements are functional, documented and tested.

6.5 Security, Confidentiality and Remote Access

The Consultant shall comply with applicable Government cybersecurity policies, confidentiality obligations, information-handling requirements and contractual security provisions.

All remote access to Government systems, operational environments and cybersecurity incident information shall be subject to prior Government authorisation and appropriate security controls.

The Consultant shall:

1. Use Government-approved remote access and communication arrangements.
2. Implement appropriate authentication, access control, encryption and audit logging measures.
3. Restrict access to sensitive Government information to authorised personnel with a legitimate operational requirement.
4. Protect incident records, technical information, system configurations and other confidential Government data against unauthorised disclosure, alteration or loss.
5. Obtain Government approval before using external hosting, third-party processing services or technologies that may store or transmit sensitive Government information.
6. Comply with applicable requirements concerning data retention, backup, recovery and secure disposal.
7. Promptly report any suspected or confirmed security incident affecting information or systems accessed or managed under the consultancy.
8. Ensure that Consultant personnel and approved subcontractors are subject to appropriate confidentiality and security obligations.
9. Return or securely dispose of Government information and revoke Consultant access at the conclusion of the assignment, in accordance with Government instructions and contractual requirements.

The Government shall retain ownership and control of its operational information, incident records and other relevant data, subject to the applicable contractual provisions.

6.6 Technology Supply and Implementation Dependencies

The Consultant shall be responsible for procuring, supplying, delivering, installing, configuring, integrating, testing, commissioning, operating and transferring all hardware, software, licences and supporting services included in the agreed DBOT scope.

All costs necessary to deliver the mandatory scope during the twelve-month DBOT period shall be included in the agreed contract price. Warranty and mandatory post-transfer support obligations shall be provided as specified in Sections 4.5.2 and 4.9.5. Optional additional services shall be separately identified and priced.

Government shall not undertake a separate procurement of the CIRT-specific hardware, software or services included in the Consultant's contractual scope.

Government review, approval or acceptance of individual components shall not relieve the Consultant of its remaining contractual obligations.

Government shall provide the agreed premises, base utilities and connectivity, designated counterpart personnel, authorised access to relevant systems and information, and the legal and administrative authorisations required for lawful operations. The Consultant shall identify and validate these requirements during inception and maintain an agreed responsibility and dependency register.

Implementation shall not depend on completion of the National Data Centre reconstruction. The Consultant shall establish and operate the agreed capability at the Government-approved location and provide any necessary interim technology arrangements within the agreed contract price.

The Consultant shall promptly notify Government in writing of any material dependency, identify its cause and effect on milestones, propose mitigation measures and continue unaffected activities.

Delays involving the Consultant's procurement, suppliers or subcontractors shall remain its responsibility, subject to the applicable contract provisions. Any relief for a proven Government-caused delay shall be assessed through the contractual procedures. No extension, additional payment, scope reduction or acceptance of incomplete deliverables shall arise automatically.

The Consultant shall maintain approved interim services where necessary to preserve operational continuity. Interim operation shall not substitute for completion of the contracted solution unless expressly authorised through an approved contractual variation.

Final acceptance shall remain subject to the operational, technical, personnel readiness, asset transfer, licensing, warranty and documentation requirements specified in Section 7.6.

6.7 Government Participation and Access to Resources

The successful implementation of the DBOT model require the active participation of designated Government personnel throughout the consultancy.

The Government shall facilitate reasonable access to relevant personnel, available documentation, approved technical resources and participating institutions, subject to applicable administrative, operational and security requirements.

The Consultant shall identify its requirements for Government participation, information and approvals sufficiently in advance to support implementation planning.

The Consultant shall maintain a record of significant outstanding Government inputs and shall promptly communicate matters that may affect achievement of the agreed milestones.

The Consultant shall not defer practical training, operational mentoring or knowledge transfer until the final stages of the assignment.

6.8 Reporting and Contract Administration

The Consultant shall maintain regular communication with the designated Government counterparts and provide progress information throughout the assignment.

The Consultant shall submit monthly progress reports addressing:

1. Activities undertaken under both workstreams.
2. Progress against the approved implementation schedule and contractual milestones.
3. Government CIRT operational activities and service performance.
4. Training, mentoring and competency development activities.
5. Progress on National CIRT institutional framework development and stakeholder consultations.
6. Technology procurement, supplier and subcontractor delivery, installation, configuration, integration, testing and commissioning against the approved Build Schedule, including outstanding defects and corrective actions.
7. Significant implementation risks, external dependencies and corrective actions.
8. Planned activities and decisions required during the subsequent reporting period.
9. Progress against the agreed SIM3 maturity targets, preparation for the independent assessment and resolution of assessment findings.
10. Readiness for asset, licence, support and operational transfer, including the Asset Register, transfer documents, warranty arrangements and Sustainability Plan.

The Consultant shall promptly report significant implementation issues and matters requiring Government decisions without waiting for the next monthly report.

Formal submission, review, acceptance and payment arrangements shall be governed by Section 7 and the applicable contract.

6.9 Optional Post-DBOT Support

The Consultant may be required to include separately priced options for an additional six (6) months and twelve (12) months of post-DBOT technical support.

Such options may include specialist incident response assistance, technical mentoring, system administration support, operational advisory services and other agreed transitional assistance.

The optional services shall:

1. Be clearly distinguished from the mandatory twelve-month DBOT scope.
2. Identify the proposed services, personnel inputs, service availability and associated costs.
3. Be subject to Government discretion, funding availability and applicable procurement and contractual requirements.
4. Not be assumed to form part of the mandatory contract unless expressly provided for in the procurement and contractual arrangements.
5. Not substitute for the requirement to establish and transfer the agreed Government CIRT capability by Month 12.

The Government shall have no obligation to procure optional post-DBOT support.

Optional post-DBOT services shall be additional to the mandatory warranty, defect-rectification and post-transfer technical support obligations specified in Sections 4.5.2 and 4.9.5. Services already included in those obligations shall not be reclassified or charged again as optional support. Government's decision not to purchase optional services shall not affect its ability to operate the transferred core capability or enforce surviving contractual obligations.

6.10 Completion of the Assignment

Final acceptance of the twelve-month DBOT implementation shall require Government verification that:

1. The complete contracted hardware and software solution has been supplied, installed, securely configured, integrated, tested and commissioned.
2. The agreed core Government CIRT services are functioning under Government operational control.
3. Designated Government personnel have demonstrated the competencies required for their assigned functions.
4. The independent SIM3 assessment and Month 11 operational readiness assessment have been completed, with Consultant-controlled deficiencies resolved or otherwise expressly addressed under the contract.
5. Required assets, applicable software rights, support entitlements, administrative access, configurations, documentation and operational records have been transferred.

6. The verified Asset Register, executed Title Transfer Document, applicable licence and support assignments, Warranty and Latent Defects Schedule, Sustainability Plan and formal handover record have been accepted.
7. The final proposed National CIRT institutional and operational framework and phased implementation roadmap have been completed and accepted as consultancy outputs.
8. Outstanding matters have been addressed through the applicable contractual procedures. Recording an outstanding matter shall not itself waive the relevant obligation.

Final acceptance shall be issued in accordance with Section 7. Submission of reports, equipment delivery, interim operation or expiry of the twelve-month period alone shall not constitute completion.

Warranty, latent-defect, mandatory post-transfer support and other obligations that survive final acceptance shall remain enforceable for their applicable contractual periods. Government shall not be required to purchase optional support to receive services already included in the contract.

7.0 Deliverables, Implementation Milestones, Acceptance Criteria and Payment Schedule

7.1 General Requirements

The Consultant shall complete the mandatory Design–Build–Operate–Transfer implementation within twelve (12) months from the contract commencement date, in accordance with the scope specified in Section 4.

The Consultant shall submit ten (10) principal deliverables covering the design, technology procurement and supply, installation, integration, commissioning, operation, capacity building and transfer of the Government CIRT, together with development of the proposed National CIRT institutional and operational framework.

The deliverables shall reflect two complementary workstreams:

- Workstream A — Government CIRT Establishment and Operationalization: Full design, build, operation, progressive strengthening and transfer of a functioning Government CIRT, including the contracted hardware, software, licences and supporting services.
- Workstream B — National CIRT Institutional and Operational Framework: Development of the proposed institutional, governance, stakeholder coordination and phased implementation framework for the future National CIRT. Formal adoption and institutional designation shall remain Government responsibilities.

The Consultant shall achieve the following mandatory milestones:

1. Within thirty (30) calendar days: Submission of the Inception Report, joint Consultant–Government SIM3 baseline assessment, and Technical Architecture and Build Specifications.
2. By Month 2: Submission of proposed measurable SIM3 maturity targets for selected capabilities, with evidence requirements and assigned responsibilities, for Government approval.
3. By Month 3: Establishment and witnessed demonstration of Government CIRT Initial Operational Capability.
4. By Month 6: Submission of the draft National CIRT institutional and operational framework.
5. By Month 8: Submission of the final proposed National CIRT framework.
6. By the approved Build Schedule milestone, and no later than Month 9: Commissioning and technical acceptance of the complete contracted technology solution.
7. During Months 9–12: Progressive Government-led operations, with the Consultant retaining its contractual service obligations until final acceptance.
8. By Month 10: Completion of the independent SIM3 assessment, at least two months before contract completion. The Consultant shall submit its corrective action plan within ten (10) working days of receiving the findings.
9. By Month 11: Completion of the Government-led operational readiness assessment, verification of the Asset Register and preparation of draft transfer documents.
10. By Month 12: Completion of the technical and operational transfer, required corrective actions and final acceptance requirements.

The milestones shall be incorporated into the deliverables and acceptance criteria under Section 7.2. They shall not create separate payment entitlements beyond the agreed payment schedule.

All deliverables shall be submitted in English, in electronic and editable formats where applicable, together with the technical records, operational evidence, assessment results and other supporting documentation required for Government verification.

Submission of reports, equipment delivery, installation, training attendance or expiry of the implementation period alone shall not constitute satisfactory completion of an operational milestone or the assignment.

Warranty, latent-defect, mandatory post-transfer support and other obligations that survive final acceptance shall continue for their applicable contractual periods.

7.2 Deliverables Implementation Milestones and Acceptance Criteria

The Consultant shall submit the following ten (10) principal deliverables. Each deliverable shall include the supporting evidence necessary for Government verification. Acceptance shall depend on demonstrated compliance with the specified requirements and shall not be based solely on submission of a report.

No.	Deliverable	Minimum Requirements and Outputs	Submission Deadline	Acceptance Criteria
D1	**Inception Report and Detailed Implementation Plan**	Integrated twelve-month DBOT plan covering both workstreams; methodology and schedule; expert deployment and in-country missions; stakeholder engagement plan; joint Consultant–Government SIM3 baseline and evidence register; initial training needs assessment; Month 3 IOC pathway; Government readiness requirements; responsibility and dependency register; reporting and quality assurance arrangements.	**Within 30 calendar days**	Government acceptance of a realistic implementation plan that assigns responsibilities, addresses dependencies and demonstrates how the mandatory milestones will be achieved. The SIM3 baseline shall document the assessment scope, model version, findings and supporting evidence.
D2	**Technical Architecture and Build Specifications**	Detailed architecture; functional and non-functional requirements; itemised hardware, software and licence schedules; supplier arrangements; Government interfaces; procurement, delivery, installation, integration and commissioning schedule; security and recovery requirements; acceptance tests; warranty and support arrangements; interim transition plan; cost breakdown within the contract price; projected recurrent costs.	**Within 30 calendar days**	Government approval of a complete, implementable technical baseline consistent with the accepted proposal and contract price. Technology procurement and delivery shall be assigned to the Consultant. Acceptance shall not constitute equipment acceptance or completion of Build.

D3	**Government CIRT Institutional and Operational Establishment Framework**	Proposed charter and mandate; governance and organisational arrangements; staffing roles; initial service catalogue; reporting, classification, escalation and coordination procedures; information-handling arrangements; draft instruments for Government consideration; Month 3 readiness requirements; proposed SIM3 targets for selected capabilities, evidence requirements, responsibilities and milestones.	**Month 2**	Government acceptance of practical institutional and operational proposals and approval of measurable SIM3 targets. Matters requiring formal Government authorisation shall be identified with responsible entities and required dates. Consultant preparation of draft instruments shall not constitute legal establishment.
D4	**Government CIRT Initial Operational Capability**	Functioning reporting channels, incident registration and case management, classification, triage, escalation, response coordination, initial advisories and awareness; functioning Consultant-supplied or Consultant-provided interim technology; valid licences; tested emergency notifications; Government personnel participation; witnessed end-to-end exercise and corrective action register.	**Month 3**	Government verification that the minimum services and supporting technologies function in practice. Documentation or equipment installation alone shall not satisfy IOC. Acceptance shall not discharge remaining Build obligations.
D5	**Operational Procedures and Initial Capacity-Building Outputs**	Implemented operational procedures and response playbooks; classification and escalation arrangements;	**Month 4**	Government verification that procedures are being applied, designated personnel participate

		performance indicators; role-based training materials; training and mentoring records; updated competency assessments; quality assurance arrangements; awareness and advisory materials; operational improvement register.		in supervised operations, and training and operational materials support continued service delivery.
D6	**Intermediate Government CIRT Operational Performance and Draft National CIRT Framework**	Operational performance evidence; incident records or approved simulations; exercises; service indicators; training and competency progress; technology delivery and integration status against the Build Schedule; progress against SIM3 targets; corrective actions; substantive draft National CIRT framework addressing mandate, governance, coordination, information sharing, legal considerations, resources and phased implementation.	**Month 6**	Government acceptance of demonstrated continuing operations and a substantive draft National CIRT framework suitable for consultation. Build progress, outstanding components and risks shall be evidenced against the approved schedule.
D7	**Government CIRT Sustainability Assessment and Final National CIRT Framework**	Updated operational and sustainability assessment; staffing and recurrent cost requirements; continuity and support proposals; readiness for Government-led operations; final proposed National CIRT framework incorporating	**Month 8**	Government acceptance of a comprehensive, consultation-informed National CIRT framework and practical Government CIRT sustainability assessment. Formal Cabinet approval, legislative enactment or National CIRT

		consultation findings, governance instruments, coordination protocols, legal and policy requirements, indicative costs and phased implementation roadmap.		designation shall not be prerequisites for acceptance of the proposed framework.
D8	**Government-Led Operations and Transfer Preparation**	Evidence of progressive Government-led operations; service records; competency matrix; exercises; updated documentation; draft handover inventory and Sustainability Plan; evidence that the complete contracted technology solution was commissioned and technically accepted by Month 9; independent SIM3 assessment report submitted directly to Government by Month 10; Consultant corrective action plan.	**Month 10**	Government verification of functioning contracted technologies and progressive Government leadership. The independent assessment shall be received, with corrective actions, responsibilities and deadlines recorded. Consultant self-assessment shall not substitute for independent evaluation.
D9	**Government-Led Operational Readiness Assessment and Asset Transfer Preparation**	Government-led practical readiness assessment; incident response exercise; verification of reporting, triage, escalation, coordination, emergency arrangements, administration and recovery; competency assessment; updated SIM3 corrective-action evidence; verified Asset Register; draft Title Transfer Document and applicable licence and	**Month 11**	Government verification of operational readiness and personnel competence. The Asset Register shall reconcile with the supplied solution. Draft transfer documents shall identify ownership, usage rights, required consents and outstanding actions, with responsibilities and deadlines for

		support transfer documents; final transfer recommendations.		completion before D10 acceptance.
D10	**Final Government CIRT Transfer and Consultancy Completion**	Verified functioning core services under Government control; completed contracted technology solution; operational and technical documentation; administrative access and records; final competency evidence; verified Asset Register; executed Title Transfer Document and applicable licence and support assignments; Warranty and Latent Defects Schedule; mandatory support arrangements; final Sustainability Plan; independent SIM3 findings and corrective-action closure evidence; residual risk register; final completion report and signed handover record.	**Month 12**	Government verification that the contracted solution and services function under its operational control, personnel can perform the agreed functions, and required transfer documents, rights, warranties and support arrangements are complete. Consultant-controlled deficiencies shall be resolved or expressly addressed under the contract. Final acceptance shall not extinguish surviving warranty, latent-defect or support obligations. A final report alone shall not constitute completion.

The detailed requirements in Section 4 remain applicable. Consolidation in this table shall not reduce the Consultant's contractual scope or continuing service obligations.

The independent SIM3 assessment shall be completed by Month 10. The Consultant shall submit its corrective action plan within ten (10) working days of receiving the findings. The assessment report shall be issued independently to Government; the Consultant shall facilitate the assessment and address findings within its responsibility.

7.2.1 Implementation and Submission Requirements

The Consultant shall manage design, technology procurement, implementation, operations, capacity building and transfer concurrently where necessary to achieve the mandatory milestones within twelve (12) months.

Deliverables D1 and D2 shall be submitted within the first thirty (30) calendar days. The Consultant shall allocate sufficient resources to undertake inception, the joint SIM3 baseline assessment and detailed technical design concurrently.

Initial Operational Capability shall be established and demonstrated by Month 3 using the supplied technologies, approved existing Government resources and any necessary Consultant-provided interim arrangements. Interim deployment shall not reduce the Consultant's obligation to deliver the complete contracted solution.

The complete contracted technology environment shall be commissioned and technically accepted by the milestone specified in the approved Build Schedule, which shall be no later than Month 9. The schedule shall allow sufficient operational evidence for the Month 10 independent SIM3 assessment and sufficient time for corrective action, competency verification and final transfer.

Where no actual cybersecurity incidents have occurred, the Consultant shall demonstrate operational capability through realistic exercises, simulations, technical demonstrations and other Government-approved verification activities.

The Consultant shall maintain the agreed operational services and continue training, mentoring and knowledge transfer throughout the operational and transfer phases, irrespective of individual deliverable submission dates.

Government approval of designs, schedules or individual deliverables shall not reduce the Consultant's remaining obligations or automatically authorise additional expenditure.

The detailed requirements of Section 4 shall remain applicable notwithstanding their consolidation in the deliverables table.

7.3 Payment Schedule

Payments shall be linked to satisfactory completion and written Government acceptance of the corresponding deliverables.

The payment schedule shall comprise ten (10) milestones:

Payment	Deliverable	Submission Deadline	Payment
P1	D1 — Inception Report and Detailed Implementation Plan	Within 30 calendar days	10%
P2	D2 — Technical Architecture and Build Specifications	Within 30 calendar days	15%
P3	D3 — Government CIRT Institutional and Operational Establishment Framework	Month 2	10%

P4	D4 — Government CIRT Initial Operational Capability	Month 3	10%
P5	D5 — Operational Procedures and Initial Capacity-Building Outputs	Month 4	5%
P6	D6 — Intermediate Government CIRT Operational Performance and Draft National CIRT Framework	Month 6	10%
P7	D7 — Government CIRT Sustainability Assessment and Final National CIRT Framework	Month 8	10%
P8	D8 — Government-Led Operations and Transfer Preparation	Month 10	5%
P9	D9 — Government-Led Operational Readiness Assessment and Asset Transfer Preparation	Month 11	5%
P10	D10 — Final Government CIRT Transfer and Consultancy Completion	Month 12	20%
	Total		**100%**

The submission deadlines do not constitute automatic payment dates. Payments shall follow acceptance, submission of the required invoice and compliance with the applicable contract provisions.

7.3.1 Payment and Acceptance Conditions

1. **Basis of payment:** Each payment shall require satisfactory completion and written acceptance of the corresponding deliverable.
2. **Supporting evidence:** The Consultant shall submit the technical documentation, operational records, test results, assessment findings, competency evidence and other materials required for verification.
3. **Incomplete deliverables:** Deficiencies within the Consultant's responsibility shall be corrected before acceptance and payment, except where the contract expressly permits another documented treatment.
4. **Design milestone:** Acceptance of D2 shall cover the Technical Architecture and Build Specifications only. It shall not constitute acceptance of equipment delivery, commissioning or completion of the Build phase.
5. **Technology completion:** Payment for D8 shall require verification that the complete contracted technology solution was commissioned and technically accepted by Month 9, together with receipt of the independent SIM3 assessment and the required corrective action plan.
6. **Continuing services:** Acceptance of an individual deliverable shall not relieve the Consultant of its continuing operational service, maintenance, training, support or transfer obligations.
7. **Routine reporting:** Monthly progress reports and routine coordination shall form part of the contract price and shall not attract separate payment.
8. **Final payment:** The final twenty per cent (20%) shall require satisfactory completion of D10 and the final acceptance requirements under Section 7.6.

9. **Surviving obligations:** Final acceptance and payment shall not extinguish warranty, latent-defect, mandatory post-transfer support or other obligations that survive completion under the contract.
10. **Additional payments:** Any advance or equipment-specific payment arrangement shall be expressly provided in the contract, including applicable security, ownership, verification and recovery requirements. No additional payment entitlement is created by this subsection.

All payments shall remain subject to the contract's invoicing, approval, taxation and payment provisions.

7.4 Deliverable Review and Acceptance Procedures

The Consultant shall submit each deliverable to the designated Government representative through the agreed contractual submission arrangements.

Government shall coordinate review through the Ministry responsible for the Public Service, GITS, the CARDTP PIU and other designated stakeholders, as appropriate.

Technical and operational review shall assess demonstrated compliance with the contractual requirements. Institutional review shall assess the quality, completeness and practical applicability of proposed frameworks and instruments.

Only the authorised Government representative may issue formal contractual acceptance. Attendance at meetings, comments on drafts or participation in testing shall not, by themselves, constitute acceptance.

7.4.1 Review Process

The review and acceptance process shall comprise:

1. **Submission:** The Consultant submits the completed deliverable and required supporting evidence.
2. **Review:** Government examines compliance with the agreed scope, outputs and acceptance criteria.
3. **Verification:** Government witnesses tests, examines operational records, checks supplied components or assesses personnel competence where required.
4. **Consolidated comments:** Government identifies deficiencies, corrections or clarifications.
5. **Correction and resubmission:** The Consultant addresses matters within its responsibility and resubmits the deliverable.
6. **Written acceptance:** The authorised Government representative confirms satisfactory acceptance.

The review and correction periods specified in Section 4.2.3 shall apply to the Technical Architecture and Build Specifications. Periods for other deliverables shall be established in the contract and reflected in the implementation schedule.

Acceptance shall not arise solely because a review period has elapsed, unless expressly provided in the contract.

7.4.2 Operational Deliverable Verification

Acceptance of operational, technology, readiness and transfer deliverables shall be based on demonstrated results.

Verification shall include, as applicable:

1. Observation of incident reporting, registration and case management.
2. Demonstration of classification, triage, escalation and response coordination.
3. Review of procedures, playbooks and operational decision records.
4. Examination of service-level performance and appropriately protected incident records.
5. Practical exercises and simulations.
6. Testing of emergency notification and on-call arrangements.
7. Assessment of Government personnel competencies.
8. Physical and documentary verification of supplied components against the approved specifications and Asset Register.
9. Verification of valid licences, Government usage rights, warranty coverage and support entitlements.
10. Review of installation, integration, security, commissioning and recovery test results.
11. Review of the independent SIM3 findings and corrective-action evidence.
12. Verification of Government administrative access and operational control.
13. Review of executed title and applicable licence and support transfer documents.
14. Verification of the Warranty and Latent Defects Schedule and continuity arrangements.

The Consultant shall correct deficiencies within its contractual responsibility. Verification shall protect confidential Government information and sensitive incident records.

Component acceptance, IOC acceptance and final DBOT acceptance shall remain distinct milestones.

7.4.3 Acceptance of the National CIRT Framework

Acceptance shall be based on the completeness, technical quality, institutional relevance and practical applicability of the proposed National CIRT framework.

Government shall assess whether it:

1. Addresses the agreed mandate, governance and institutional requirements.
2. Reflects relevant stakeholder consultations.
3. Defines proposed incident reporting, coordination and information-sharing arrangements.

4. Identifies legal, policy and administrative requirements.
5. Provides practical draft governance instruments and decision-support documentation.
6. Includes organisational, staffing, technology and indicative resource requirements.
7. Provides a realistic, phased implementation roadmap.
8. Explains the relationship between the Government CIRT and proposed national arrangements.

The Consultant shall address consolidated review comments within its contractual scope.

Formal Cabinet approval, legislative enactment, funding allocation or institutional designation of the National CIRT shall remain Government responsibilities and shall not be prerequisites for acceptance of satisfactorily completed proposed framework deliverables.

7.5 Management of Implementation Dependencies

The Consultant shall maintain a responsibility and dependency register identifying required inputs, owners, deadlines, implementation impacts, mitigation measures and escalation actions.

Government-controlled dependencies shall include agreed premises, base utilities and connectivity, site and system access, designated personnel, legal authority, institutional approvals and stakeholder participation.

Technology procurement, supplier and subcontractor delivery, installation, configuration, integration, commissioning and defect rectification within the Consultant's scope shall remain its responsibility.

The Consultant shall promptly notify Government in writing of material constraints, identify their cause and contractual responsibility, explain milestone impacts and propose mitigation measures. It shall continue unaffected activities and maintain approved interim services where necessary.

Any relief for a proven Government-caused delay shall be assessed under the contract. No extension, additional payment, scope reduction or acceptance of incomplete deliverables shall arise automatically.

Changes to scope, deadlines, price or acceptance requirements shall follow the applicable contractual procedures and required approvals. Recording an outstanding dependency shall not itself waive an obligation.

7.6 Completion and Final Acceptance

Final acceptance of the twelve-month DBOT implementation shall require Government verification that:

1. **Operational establishment:** The Government CIRT is functioning within its lawful mandate and approved service catalogue.
2. **Initial Operational Capability:** The Month 3 IOC requirements were achieved and demonstrated, with identified deficiencies appropriately addressed.

3. **Complete technology solution:** All contracted hardware, software and supporting components have been supplied, installed, securely configured, integrated, tested and commissioned. Interim operation alone shall not satisfy the complete Build obligation unless expressly authorised through an approved contractual variation.
4. **Operational performance:** The agreed incident reporting, case management, triage, escalation, response coordination, advisory and emergency arrangements are functioning.
5. **Government personnel competence:** Designated personnel have received practical training and mentoring and demonstrated the competencies required for their assigned functions.
6. **Government-led operations:** Government personnel can perform routine core functions and apply the approved emergency escalation procedures.
7. **Independent SIM3 assessment:** The assessment has been completed against the joint baseline and agreed targets. Consultant-controlled deficiencies have been rectified or otherwise expressly addressed under the contract. Remaining Government dependencies and residual findings have documented responsibilities and disposition.
8. **Operational readiness:** The Month 11 readiness assessment and required corrective actions have been completed.
9. **Asset and rights transfer:** Government has received the verified Asset Register, executed Title Transfer Document, applicable licence and support assignments, administrative access and required usage rights.
10. **Documentation and records:** Technical configurations, operational records, procedures, playbooks, training resources and other agreed information assets have been transferred securely.
11. **Warranty and sustainability:** The Warranty and Latent Defects Schedule, mandatory support arrangements, final Sustainability Plan, recovery procedures and recurrent cost information have been accepted.
12. **National CIRT framework:** The final proposed framework and phased implementation roadmap have been completed and accepted as consultancy outputs.
13. **Contractual completion:** Other obligations due before final acceptance have been fulfilled, except for matters expressly treated otherwise under approved contractual procedures.

Final acceptance shall not extinguish warranty, latent-defect, mandatory post-transfer support or other obligations that survive completion.

7.6.1 Government Inputs and Completion Dependencies

Government shall provide the agreed facilities, base utilities and connectivity, access to existing infrastructure, designated personnel and required authorisations.

The Consultant shall remain responsible for all technology procurement, supply, implementation, operation and transfer activities within its scope, including supplier and subcontractor performance.

Where a documented Government action or omission materially affects performance, the Consultant shall promptly notify Government, explain the impact, implement reasonable mitigation measures, continue unaffected activities and submit any proposed adjustment through contractual change control.

Schedule and cost consequences shall be determined under the contract. There shall be no automatic extension, additional payment or waiver of incomplete obligations.

Outstanding activities shall have documented responsibility, completion requirements and approved contractual treatment. Government shall not be required to accept an incomplete solution merely because the implementation period has expired.

Any step-in or other remedy shall be exercised only as provided in the signed contract.

7.6.2 Final Acceptance and Handover

The Consultant shall submit a Final Completion and Handover Report supported by the complete Handover Package required under Section 4.9.9.

The report shall document:

1. Completion of contractual deliverables and milestones.
2. The functioning services and operational responsibilities transferred.
3. Commissioning and technical acceptance of the complete contracted solution.
4. Results of the independent SIM3 and operational readiness assessments.
5. Corrective-action closure evidence and approved treatment of outstanding matters.
6. Training, mentoring and demonstrated personnel competencies.
7. The verified Asset Register and executed title and applicable licence and support transfer documents.
8. Administrative access, configurations, records and documentation transferred.
9. The Warranty and Latent Defects Schedule and mandatory post-transfer support arrangements.
10. The final Sustainability Plan, continuity arrangements and recurrent obligations.
11. Completion and acceptance of the National CIRT framework.
12. Residual risks, assigned responsibilities and required follow-up.
13. A signed formal handover record.

The authorised Government representative shall issue written final acceptance following satisfactory verification of Section 7.6 and the applicable contractual requirements.

Submission of the report, signing of an inventory or expiry of the twelve-month implementation period alone shall not constitute final acceptance.

7.6.3 Optional Post-DBOT Support

The Consultant may propose separately priced options for six (6) and twelve (12) months of additional post-DBOT technical or operational assistance.

Any such services shall be subject to Government discretion, funding availability and the applicable procurement and contractual arrangements.

Optional services shall be clearly additional to mandatory warranty, defect-rectification and post-transfer support obligations. Services already included in the contract shall not be reclassified or charged again as optional support.

Government shall have no obligation to purchase optional services. Its decision not to do so shall not affect surviving contractual obligations or its ability to operate the transferred routine core capability.

Optional services shall not substitute for completion of the mandatory DBOT scope within the twelve-month implementation period.

8.0 QUALIFICATIONS OF THE CONSULTING FIRM AND KEY PERSONNEL

8.1 Qualifications and Experience of the Consulting Firm

The assignment shall be undertaken by a qualified consulting firm, or a joint venture of consulting firms, with demonstrated experience in establishing, operating and transferring cybersecurity incident response capabilities, preferably within Government or comparable public sector environments.

The Consulting Firm shall demonstrate the technical, operational, institutional and capacity-building expertise necessary to implement the proposed twelve-month Design–Build–Operate–Transfer (DBOT) model.

The Consulting Firm shall possess:

1. Demonstrated experience in the design, establishment, operationalisation or strengthening of Computer Security Incident Response Teams (CSIRTs), Cybersecurity Incident Response Teams (CIRTs), or comparable cybersecurity incident management functions.
2. Experience in providing operational cybersecurity incident response services, including incident triage, technical analysis, escalation, response coordination and incident case management.
3. Experience in the development and implementation of cybersecurity governance frameworks, operational procedures, incident response playbooks and institutional coordination arrangements.
4. Demonstrated expertise in cybersecurity technical architecture, security infrastructure planning, systems integration and the preparation of technical specifications for cybersecurity technologies.
5. Demonstrated experience in procuring, supplying, installing, securely configuring, integrating, testing and commissioning cybersecurity infrastructure and systems,

including management of suppliers, subcontractors, licensing, warranties and technical support.

6. Demonstrated experience in cybersecurity training, mentoring, practical exercises and institutional capacity building.
7. Experience in transferring operational cybersecurity responsibilities and technical knowledge to client personnel.
8. Experience in developing cybersecurity institutional frameworks, strategies, policies or national-level incident coordination arrangements.
9. Experience working with Government institutions, public sector organisations or other environments involving multiple institutional stakeholders.
10. The organisational capacity to provide the required technical expertise and operational support throughout the twelve-month consultancy.
11. Demonstrated experience in operating and maintaining cybersecurity incident response capabilities and transferring functioning systems, assets, applicable software rights, documentation and operational responsibilities to client personnel.
12. Demonstrated capability to apply SIM3 through baseline assessment, maturity improvement planning, evidence collection and implementation of corrective actions.

Experience in Small Island Developing States, Caribbean countries or other environments with comparable institutional and resource constraints shall be considered advantageous.

Experience with internationally recognized incident response frameworks, standards and good practices shall also be advantageous.

The Consulting Firm shall demonstrate that its experience extends beyond the preparation of cybersecurity strategies or assessments and includes practical implementation and operational support.

8.2 Relevant Assignment Experience

The Consulting Firm shall provide details of relevant assignments undertaken within the preceding ten (10) years, including, where available:

1. The name and location of the client.
2. The assignment objectives and scope.
3. The nature of the cybersecurity incident response capabilities established or supported.
4. The Consultant's specific responsibilities.
5. The duration and implementation approach.
6. The operational services and technical capabilities delivered.
7. The training, mentoring or knowledge-transfer activities undertaken.
8. The principal outcomes achieved.
9. Client references or other appropriate evidence of satisfactory performance.
10. Hardware, software and integrated technology solutions supplied and commissioned.

11. Responsibility for procurement, suppliers, subcontractors, licensing, warranty and support.
12. Operational services delivered and performance achieved.
13. Asset, licence and operational transfer arrangements completed.
14. SIM3 assessment or maturity improvement activities, where applicable.

Particular consideration shall be given to assignments demonstrating the successful establishment or strengthening of operational incident response capabilities and the transfer of responsibilities to client personnel.

The Consulting Firm may demonstrate the required experience through its own qualifications or those of eligible joint venture members, subject to the applicable procurement requirements.

8.3 Key Personnel

The Consultant shall provide a suitably qualified multidisciplinary team capable of delivering both workstreams of the assignment.

The following four (4) key expert positions are considered essential.

8.3.1 Key Expert 1 — Team Leader / CIRT Establishment Specialist

The Team Leader shall have overall responsibility for technical leadership, assignment coordination, implementation quality, stakeholder engagement and delivery of the agreed DBOT outcomes.

Minimum qualifications:

- A postgraduate degree in Cybersecurity, Information Security, Computer Science, Information Technology, Information Systems, Engineering or a closely related discipline.
- At least ten (10) years of relevant professional experience in cybersecurity, information security or related ICT security functions.
- At least five (5) years of demonstrated experience in cybersecurity incident response capability development, CIRT/CSIRT establishment, operational management or comparable assignments.
- Experience leading multidisciplinary cybersecurity projects or institutional implementation assignments.
- Demonstrated knowledge of cybersecurity governance, incident response operations, institutional coordination and capacity development.

Specific responsibilities shall include:

1. Overall coordination and technical management of the consultancy.
2. Preparation and oversight of the DBOT implementation plan.
3. Coordination of Government CIRT institutional establishment activities.
4. Oversight of operational service development and transfer.
5. Coordination of the National CIRT institutional framework workstream.
6. Stakeholder engagement and management reporting.
7. Oversight of risks, dependencies and implementation milestones.
8. Quality assurance of technical and institutional deliverables.
9. Coordination of expert inputs and Government consultations.
10. Verification of readiness for final operational transfer.
11. Overall accountability for coordinated delivery of all four DBOT phases, including technology supply, commissioning, operational services and transfer.
12. Oversight of supplier performance, Build milestones, warranty and support arrangements, and final handover requirements.
13. Coordination of the joint SIM3 baseline, maturity improvement activities and corrective actions arising from the independent assessment.

Experience in Government cybersecurity institutional development and national cybersecurity coordination arrangements shall be an advantage.

8.3.2 Key Expert 2 — Cybersecurity Architecture and Infrastructure Specialist

The Cybersecurity Architecture and Infrastructure Specialist shall lead the technical design and delivery of the Government CIRT environment, including technical management of procurement, supply, installation, secure configuration, integration, testing, commissioning and technical transfer.

Minimum qualifications:

- A university degree in Computer Science, Information Technology, Cybersecurity, Computer Engineering, Network Engineering or a related discipline.
- At least eight (8) years of relevant professional experience in cybersecurity architecture, information security infrastructure or secure ICT systems.
- Demonstrated experience designing or implementing cybersecurity technologies and secure technical environments.
- Experience preparing technical specifications, system architecture documentation and integration requirements.
- Experience with secure system configuration, access control, logging, backup, recovery and technical acceptance testing.

Specific responsibilities shall include:

1. Assessing the existing technical environment and proposed hosting location.

2. Preparing the Technical Architecture and Build Specifications within thirty (30) calendar days.
3. Defining component requirements, quantities, licences, interfaces and acceptance tests.
4. Providing technical leadership for the Consultant's procurement and supplier-management activities.
5. Verifying supplied components against the approved requirements.
6. Directing secure configuration, installation and integration.
7. Planning and conducting commissioning, security and recovery tests.
8. Managing migration from interim technologies to the complete contracted solution.
9. Resolving technical defects and integration deficiencies.
10. Preparing the Asset Register, configuration records, technical documentation and licence and support information.
11. Delivering practical technical knowledge transfer to Government personnel.
12. Verifying technical readiness for final handover.

The Specialist shall demonstrate practical experience delivering integrated cybersecurity solutions, including supplier coordination, acceptance testing and technical handover. Experience limited to preparing specifications or advising on procurement shall not, by itself, demonstrate the required implementation capability**.**

8.3.3 Key Expert 3 — CIRT Operations and Incident Response Specialist

The CIRT Operations and Incident Response Specialist shall lead the establishment, operation and progressive strengthening of the agreed Government CIRT services from Initial Operational Capability until final acceptance. The Specialist shall coordinate incident handling, service-level performance, emergency escalation, operational mentoring and progressive transfer to Government personnel.

Minimum qualifications:

- A university degree in Cybersecurity, Information Security, Computer Science, Information Technology or a related discipline.
- At least eight (8) years of relevant professional experience in cybersecurity operations, incident response, digital security investigations or comparable functions.
- Demonstrated practical experience in cybersecurity incident triage, classification, analysis, escalation and response coordination.
- Experience developing incident response procedures, operational playbooks and case management arrangements.
- Experience supporting or managing operational cybersecurity incident response services.
- Experience conducting incident response exercises and assessing operational readiness.

Specific responsibilities shall include:

1. Establishment of Government CIRT incident reporting and management processes.
2. Development of operational procedures and incident response playbooks.
3. Implementation of incident classification and severity arrangements.
4. Establishment of incident escalation and emergency notification procedures.
5. Operational leadership and delivery of incident assessment, triage, escalation and response coordination within the agreed scope, including the prescribed emergency on-call arrangements.
6. Development of cybersecurity advisory and knowledge-sharing processes.
7. Support for the Month 3 Initial Operational Capability demonstration.
8. Operational performance monitoring and quality assurance.
9. Mentoring Government personnel during actual and simulated incident handling.
10. Support for Government-led operations and the Month 11 readiness assessment.

Experience in public sector incident response operations, multi-agency coordination and the establishment of CIRT/CSIRT services shall be advantageous.

8.3.4 Key Expert 4 — Cybersecurity Training and Capacity Building Specialist

The Cybersecurity Training and Capacity Building Specialist shall lead the design and delivery of the competency-based training, mentoring and knowledge-transfer programme.

Minimum qualifications:

- A university degree in Cybersecurity, Information Security, Information Technology, Computer Science, Education, Training and Development or a related discipline.
- At least seven (7) years of relevant professional experience in cybersecurity training, technical capacity building, organisational development or related functions.
- Demonstrated experience developing and delivering role-based cybersecurity training programmes.
- Experience designing practical exercises, competency assessments and technical learning materials.
- Experience supporting institutional knowledge transfer and operational capacity development.
- Familiarity with cybersecurity incident response processes and relevant technical competencies.

Specific responsibilities shall include:

1. Conducting the initial training needs and competency assessment.
2. Developing the role-based competency framework.
3. Preparing the Training and Capacity-Building Plan.
4. Designing and delivering technical and operational training.
5. Coordinating practical mentoring and supervised learning activities.
6. Developing training materials, exercises and assessment instruments.
7. Monitoring competency development.

8. Identifying and addressing training gaps.
9. Supporting Government-led operational readiness assessments.
10. Preparing final training and knowledge-transfer documentation.

Experience delivering cybersecurity capacity-building programmes for Government institutions or operational cybersecurity teams shall be advantageous.

8.4 Additional Specialist Expertise

The Consultant shall provide additional specialist expertise as necessary to deliver the full contractual scope of both workstreams and all four DBOT phases.

Such expertise shall cover, as required:

1. Cybersecurity governance and institutional development.
2. Cybersecurity law, policy and regulatory analysis.
3. National cybersecurity coordination and critical information infrastructure protection.
4. Cybersecurity threat intelligence and vulnerability management.
5. Digital forensics and specialist incident response.
6. Secure systems integration, testing and technical commissioning.
7. Technology supply-chain management and coordination of suppliers and subcontractors.
8. Software licensing, warranty administration, technical support arrangements and asset transfer.
9. SIM3 baseline assessment, maturity improvement planning, evidence collection and corrective actions.
10. Business continuity and operational resilience.
11. Stakeholder consultation and institutional change management.

The Consultant may propose suitably qualified non-key experts, specialist subcontractors or other technical resources to provide these inputs, subject to the applicable procurement and contractual requirements. Necessary inputs shall be identified in the staffing and deployment plan and included in the agreed contract price.

The proposed arrangements shall demonstrate sufficient expertise to complete the National CIRT institutional framework, including draft governance instruments, legal and policy analysis, stakeholder consultations, resource requirements and the phased implementation roadmap. Formal adoption of instruments and institutional decisions shall remain Government responsibilities.

Independent SIM3 Evaluation

The independent SIM3 evaluator shall be separate from the Consultant's implementation team and appointed in accordance with Section 5.6 and the applicable procurement and contract documents.

The evaluator shall not have participated in designing, supplying or operating the solution being assessed and shall report directly to Government. The Consultant's SIM3 specialists shall support implementation and provide assessment evidence but shall not substitute for, direct or approve the independent evaluation.

The Consultant shall provide authorised access to relevant documentation, systems and personnel and shall address assessment findings within its contractual responsibilities before final acceptance.

8.5 Staffing and Level of Effort

The Consultant shall propose a staffing and deployment plan demonstrating sufficient capacity to deliver both workstreams and all four DBOT phases within the twelve-month implementation period.

The plan shall identify the inputs, responsibilities, deployment periods, availability and reporting relationships of key experts, non-key experts and specialist resources. It shall distinguish Consultant personnel from designated Government counterparts and identify activities requiring onsite participation.

The proposed level of effort shall account for:

1. Concurrent inception, joint SIM3 baseline assessment and preparation of the Technical Architecture and Build Specifications within the first thirty (30) calendar days.
2. Technology procurement, supplier and subcontractor management, delivery, installation, secure configuration and integration.
3. Establishment and demonstration of Initial Operational Capability by Month 3.
4. Consultant-led operational services, technology maintenance, service-performance monitoring and the prescribed emergency on-call coverage.
5. Commissioning and technical acceptance of the complete contracted technology solution by the approved Build Schedule milestone and no later than Month 9.
6. Cybersecurity awareness, role-based training, practical mentoring, exercises and competency assessment.
7. Stakeholder consultations and preparation of the draft and final proposed National CIRT framework.
8. Progressive Government-led operations during Months 9–12, while maintaining the Consultant's contractual service obligations.
9. Facilitation of the independent SIM3 assessment by Month 10 and implementation of corrective actions within the Consultant's responsibility.
10. The Month 11 operational readiness assessment and preparation of asset, licence and support transfer documents.
11. Final technical and operational handover by Month 12.
12. Necessary in-country missions, installation activities, practical training and Government-witnessed verification.
13. Resources and arrangements for warranty, defect rectification and mandatory post-transfer support during their applicable contractual periods.

The Team Leader and relevant experts shall remain sufficiently engaged to ensure implementation continuity, quality assurance, timely decisions and achievement of the mandatory milestones.

The Consultant shall demonstrate adequate operational coverage, specialist availability and backup arrangements to maintain services during leave, personnel changes, concurrent incidents and transfer activities. These arrangements shall support standard Government business-hour services and the prescribed emergency on-call obligations without assuming a continuously staffed twenty-four-hour Security Operations Centre.

Not all experts are required to be deployed full-time or remain physically present in Saint Lucia throughout the assignment. However, remote delivery shall not diminish the Consultant's responsibility for physical implementation, operational performance, practical knowledge transfer or verified handover.

The staffing plan shall not depend on Government personnel performing obligations assigned to the Consultant. Government counterparts shall participate in training, supervised operations and progressive transfer, while the Consultant retains responsibility for its agreed delivery and service obligations until final acceptance.

All personnel inputs, travel, onsite deployment and specialist resources necessary for the mandatory scope shall be included in the agreed contract price. The independent SIM3 evaluator's appointment and funding arrangements shall be separately identified in accordance with Section 5.6.

Proposed changes to key personnel, deployment or level of effort shall follow the applicable contractual approval procedures and shall not reduce service availability, mandatory scope or required outcomes.

8.6 Personnel Continuity and Replacement

The Consultant shall maintain continuity of key personnel throughout the assignment.

Any proposed replacement of key personnel shall be subject to the applicable contractual provisions and Government approval.

Replacement personnel shall possess qualifications and experience at least equivalent to those of the personnel being replaced.

The Consultant shall ensure that personnel changes do not adversely affect implementation milestones, operational service continuity or knowledge transfer.

8.7 Language and Communication Requirements

All key personnel shall possess strong written and spoken English communication skills.

The Consultant shall be capable of preparing clear technical reports, operational procedures, training materials, governance instruments and stakeholder consultation documentation in English.

The Consultant shall ensure effective communication with Government technical personnel, senior management and other relevant stakeholders throughout the assignment.

9.0 Completion and Expected Outcomes

9.1 Expected Outcomes

The assignment shall deliver a functioning Government CIRT through a complete twelve-month Design–Build–Operate–Transfer model, together with a proposed institutional and implementation framework for the future National CIRT.

9.1.1 Established and Operational Government CIRT

The Government CIRT shall deliver the agreed core services to participating Government ministries, departments and agencies under the approved mandate, service catalogue and operating arrangements.

Initial Operational Capability shall be demonstrated by Month 3. The capability shall progressively develop through Consultant-led operations and Government personnel participation, culminating in Government operational control by Month 12.

9.1.2 Complete Technology Solution

The Consultant shall have procured, supplied, installed, securely configured, integrated, tested and commissioned the complete hardware, software, licences and supporting components included in the contract.

The solution shall be technically accepted by the approved Build Schedule milestone and no later than Month 9, allowing operational validation and preparation for transfer.

Government shall possess the physical assets, applicable software usage rights, administrative access, documentation and support entitlements necessary for continued operation. Interim arrangements shall not replace completion of the contracted solution unless expressly authorised through contractual change control.

9.1.3 Demonstrated Government Personnel Competence

Designated Government personnel shall demonstrate the technical and operational competencies required for their assigned functions through practical assessments, supervised operations and exercises.

Training attendance or certification alone shall not constitute evidence of readiness. Personnel shall demonstrate the ability to perform routine core functions, administer the agreed technologies and apply emergency escalation procedures.

9.1.4 Verified Operational Performance and Maturity Progress

The Government CIRT shall demonstrate functioning incident reporting, case management, classification, triage, escalation, response coordination, advisory and emergency on-call arrangements.

A joint SIM3 baseline and Government-approved targets shall guide maturity improvement. An independent assessment shall be completed by Month 10, with corrective actions within the Consultant's responsibility addressed before final acceptance or otherwise expressly treated under the contract.

The Month 11 operational readiness assessment shall separately verify practical Government-led capability and transfer readiness.

9.1.5 Sustainable Operational Arrangements

Government shall receive a final Sustainability Plan addressing staffing, recurrent costs, licensing, maintenance, technical support, professional development, continuity and recovery.

The Consultant shall complete arrangements within its contractual responsibility and identify outstanding Government decisions with assigned owners and required actions.

Warranty, defect-rectification and mandatory post-transfer support arrangements shall be documented and enforceable for their applicable contractual periods. Government shall not be required to purchase optional services to receive support already included in the contract.

9.1.6 Cybersecurity Awareness and Institutional Engagement

Participating Government institutions shall understand the Government CIRT's role, approved reporting channels, incident escalation procedures and respective institutional responsibilities.

Government personnel shall receive reusable awareness materials, communication templates, stakeholder contact arrangements and practical knowledge to sustain the agreed awareness and engagement functions.

9.1.7 National CIRT Institutional and Implementation Framework

Government shall receive a comprehensive final proposed framework addressing the National CIRT's mandate, governance, organisational arrangements, coordination mechanisms, information sharing, legal and policy requirements, resources and phased implementation.

The framework shall reflect stakeholder consultations and explain its relationship with the operational Government CIRT.

Acceptance of the proposed framework shall not constitute formal establishment of a nationwide National CIRT. Adoption, legal designation, staffing and funding decisions shall remain Government responsibilities.

9.2 Completion of the DBOT Implementation

Completion shall be determined through the verification and acceptance procedures in Section 7.

Government shall verify that:

1. The complete contracted technology solution and agreed core services are functioning.
2. Designated personnel have demonstrated the required competencies.
3. The independent SIM3 assessment and operational readiness assessment have been completed, with findings addressed in accordance with the contract.
4. The verified Asset Register, executed Title Transfer Document and applicable licence and support transfer documents have been accepted.
5. Administrative access, configurations, operational records, procedures and technical documentation have been transferred securely.
6. The Warranty and Latent Defects Schedule, mandatory support arrangements and final Sustainability Plan have been accepted.
7. The final proposed National CIRT framework and implementation roadmap have been completed and accepted.
8. Other obligations due before final acceptance have been fulfilled or expressly addressed through the applicable contractual procedures.

The Consultant shall submit the Final Completion and Handover Report and complete Handover Package. Final acceptance shall be confirmed in writing by the authorized Government representative.

Submission of reports, equipment delivery, interim operation or expiry of the twelve-month implementation period alone shall not constitute completion.

Warranty, latent-defect, mandatory post-transfer support and other surviving obligations shall continue after final acceptance for their applicable contractual periods.

9.3 Long-Term Contribution

The Government CIRT shall provide a sustainable operational foundation for coordinated cybersecurity incident management across Government and improved resilience of digital public services.

The proposed National CIRT framework shall provide a practical basis for Government consideration of broader national coordination, including engagement with critical infrastructure operators and other relevant stakeholders.

Together, these outputs shall support the Government’s digital transformation and cybersecurity objectives while enabling continued capability development under Government ownership and leadership.