ITAUKEI LANDS TRUST BOARD
(iTaukei Lands, Our Heritage, Our Future)

TENDER SPECIFICATIONS

CYBERSECURITY RISK ASSESSMENT & REMEDIATION SERVICES

1.0 General Terms & Conditions

The following general terms and conditions will apply:

1.1 Submission of Tenders

a. Tenders must be received no later than **4:00pm Friday 1st May 2026**.

b. Tenderers must submit two signed copies of the proposal with one copy marked as "Original." The original version will prevail if there are any inconsistencies between the original and the copy.

c. All Tenders submissions are to be in sealed envelopes, clearly marked: "**Tender for Cybersecurity Risk Assessment & Remediation Services**" and to be placed in the Tender Box located at first floor, TLTB Building, 431 Victoria Parade, Suva.

d. Submissions can also be emailed to tendersecretariat@tltb.com.fj

e. All Tenders to be submitted prior to the tender closing time.

f. The Tender response must be in the English language.

g. Should the Tenderer become aware of any discrepancy, error or omission in the Tender document submitted, and the Tenderer wishes to lodge a correction or provide additional information that material must be in writing and lodged prior to the Tender closing time.

1.2 Format of Tender Response

Each Tenderer must provide a formal letter of transmittal that must:

a. Be signed by an authorized representative of the organization and must state that the signing official is authorized to legally bind the organization.

b. Include the names, titles, office addresses and office telephone numbers of the persons authorized by the organization to conduct negotiations on the Proposal, including their expected roles in negotiations and in performance of any resulting

Agreement; and

c. Provide a contact name, address, facsimile number, and email address which TLTB will use in serving notices to the Tenderer.

d. Submit a clause-by-clause response indicating compliance with the requirements as documented in section 5.

1.3 Late Tenders

Any Tender lodged after the closing time will be deemed to be late and will not be considered.

1.4 Amendment of RFT

TLTB may, at its discretion, vary, add to, or amend the terms of this RFT, including: the nature and/or scope of the services required under this RFT; and any other subject matter to which this RFT relates.

1.5 Termination of RFT

TLTB may, in their sole and absolute discretion, suspend, terminate, or abandon this RFT at any time prior to the execution of a formal written agreement acceptable to TLTB, by an authorized officer of TLTB and by the Successful Tenderer/s, by giving written notice of such a decision to each of the registered Tenderers.

1.6 Tenderers to Inform Themselves

a. Each Tenderer should:

   i. Examine this RFT, and documents referred to in the RFT and any other information made available by TLTB to Tenderers.

   ii. Obtain any further information about the facts, risks, and other circumstances relevant to its Tender by making all lawful inquiries; and

   iii. Satisfy itself that its Tender, and all information on which its Tender is based, is true, accurate, and complete.

b. By submitting their Tenders, Tenderers will be deemed to have:

   i. examined the RFT and any other information made available in writing by TLTB to Tenderers for the purpose of tendering.

   ii. examined all information relevant to the risks, contingencies, and other circumstances influencing their Tender and which is obtainable by the making of reasonable inquiries; and

   iii. satisfied themselves as to the correctness and sufficiency of their Tenders and that their prices cover the cost of complying with the RFT requirements and of all matters and things necessary for the due and proper performance and completion of the work described in the RFT.

1.7 Tenderer's Risk

The Tenderer's participation in any stage of the Tender process is at the tenderer's sole risk, cost and expense, in particular, all costs incurred by or on behalf of the

Tenderers in relation to this RFT, including preparing and lodging the Tender and providing TLTB with any further information are wholly the responsibility of the Tenderer.

TLTB accepts no responsibility, liability, or obligation whatsoever for costs incurred by or on behalf of any Tenderer in connection with any Tender or any participation in the Tender process.

1.8 Clarification and Variation of Tenders

TLTB may, at their absolute discretion, seek clarification or request further information from Tenderers after the closing date for the submission of Tenders.

Each Tenderer must nominate a person to provide additional information or answer specific questions that may arise during the selection process as required by TLTB.

Tenderers whose Tenders have been shortlisted may be required to engage in formal discussions with TLTB or make presentations to TLTB on their Tenders. In such an event TLTB will make the necessary arrangements with Tenderers.

1.9 Selection of Preferred Tender

Neither the lowest priced Tenders, nor any Tenders, will necessarily be selected by TLTB as the Preferred Tender/s. TLTB IT Steering Committee may decide not to accept any Tender or reject all Tenders at any time. TLTB reserves the right to cancel this RFT and pursue an alternative course of action at any time.

A Tenderer will not be deemed to have been selected as one of the Preferred Tenderer/s unless and until notice in writing for and on behalf of TLTB of such selection is:

- Handed to the Tenderer; or
- Is sent by prepaid post to or is left at the address stated in the Tender for service of notices; or
- Sent by facsimile to the number provided by the Tenderer, followed by an original by post.

Selection of Preferred Tenderer/s shall not be treated as acceptance of the Tender and no binding relationship will exist between the Preferred Tenderer/s and TLTB until a written agreement acceptable by TLTB is executed by an authorized officer of TLTB and the Successful Tenderer/s.

1.10 Conduct of Tenderers

The conduct of Tenderers or any of their consortium members, may affect the outcome of their Tender responses, including non-consideration of the Tender.

Tenderers warrant TLTB that they (and their consortium members) have not and will not engage in any of the following activities in relation to this RFT Process:

- Lobbying of or discussions with any politician or political groups during this RFT process.
- Attempts to contact or discuss the RFT process with officers, any member,

staff, or contractor currently working in TLTB or any agent of this Department; Exception to members stated in Proposal for tender.

- Provision of gifts or future promise of gifts of any sort to the previously mentioned personnel.

- Accepting or providing secret commissions.

- Submitting an inflated Tender to the advantage of another Tenderer; Entering any improper commercial arrangement with any other party.

- Seeking to influence any decisions of TLTB by an improper means; or otherwise acting in bad faith, fraudulently or improperly.

1.11 Unlawful Inducements and Collusive Tendering

Tenderer and its officers, employees, agents, and advisers must not:

- Offer unlawful inducements in connection with the Tender process; or

- Engage in any collusive tendering, anti-competitive conduct or any other similar conduct with any other Tenderer or any other person in relation to the preparation or lodgment of Tenders.

1.12 Contact with Tenderers

During the Tender process, neither TLTB nor their representatives are required to answer questions or otherwise discuss the contents of this RFT with potential Tenderers or their representatives, except in accordance with this RFT. Tenderers must not attempt to make any contact of that nature. Any unauthorized contact may disqualify the Tenderer from further consideration.

1.13 Costs

Tenderers must provide a detailed and itemized cost breakdown for all proposed services and deliverables. Lump-sum pricing without sufficient breakdown will not be considered compliant.

At a minimum, pricing must be broken down by:

- Each major phase or workstream (e.g. assessment, vulnerability assessment, policy development, incident response planning, roadmap development)
- Individual deliverables where feasible
- Professional services effort (e.g. estimated days or hours)
- Any optional, phased, or deferred components

The cost breakdown must clearly distinguish between one-time professional service costs and any recurring or ongoing costs (if applicable).

All pricing must be quoted in Fiji Dollars (FJD), be VAT inclusive, and represent the full cost of delivery for the proposed scope.

Prices must remain valid for a minimum period of ninety (90) days from the tender closing date.

Where estimates are provided, vendors must clearly state the assumptions used. TLTB reserves the right to seek clarification or reject proposals that present pricing as a single aggregated total without adequate detail.

TLTB expects that a meaningful portion of the engagement effort will be dedicated to practical implementation activities, including security control hardening, policy operationalization, and incident response readiness. Proposals that focus predominantly on assessment deliverables, reports, or high-level recommendations with limited implementation support and limited measurable uplift may be scored lower during evaluation and may be considered non-responsive to TLTB's objectives.

1.14 Non-Delivery of Service(s)

TLTB reserves the right to hold full or partial payment until such time that the product has been delivered to the quality and expectation of TLTB.

TLTB has the right to withhold (as penalties) a percentage of the payment for vendor non-performance. Non-performance may be classed as:

- Failure to deliver on time.
- Failure to respond to queries within a reasonable amount of time.
- Introduction of unauthorized "new" clauses

1.15 Validity of Submissions

All proposals and prices shall remain valid for a period of 90 days from the closing date of the submission of the proposal. However, the responding organization is encouraged to state a longer period of validity for the proposal.

1.16 Currency

All currency in the proposal shall be quoted in Fiji Dollars and VAT inclusive and include all duties and taxes. Pricing must incorporate all Professional Services costs associated with TLTB receiving a fully configured and operational solution and must include Delivery, Installation, Configuration, Commissioning, Testing, Project Management, Documentation and Training costs.

1.17 Mergers Acquisition or Sale of Tenderer

Where such information is publicly accessible, the Tenderer must indicate whether any mergers, acquisitions or sales are planned presently or during the year following the submission of the Tender.

2.0 Project Objective & Strategic Context

TLTB seeks proposals from suitably qualified and experienced cybersecurity service providers to deliver a comprehensive Cybersecurity Risk Assessment and Targeted Remediation Engagement.

This engagement is designed to provide TLTB with both deep diagnostic insight and immediate, tangible security improvements. It is structured around two complementary work streams:

- Assessment & Analysis – establishing a clear, evidence-based picture of TLTB's current cybersecurity risk exposure across systems, data and applications; and

- Remediation Activities – delivering measurable security uplift within the engagement period, including policy development, technical hardening and incident response capability.

This engagement is intended to establish foundational governance, documentation, and practical security controls that position TLTB for ISO/IEC 27001:2022 readiness. It is not an ISO/IEC 27001 certification audit or full certification implementation project. "Readiness" in this context means that TLTB has the core ISMS building blocks in place (policies, risk management structure, governance, and operational procedures) and a realistic roadmap for continued implementation beyond the engagement period.

At least 30–40% of the total engagement effort must be allocated to practical remediation activities, implementation support, and technical hardening measures rather than assessment-only activities.

TLTB is seeking a pragmatic, risk-based engagement focused on establishing strong foundations, delivering visible security uplift, and enabling sustainable improvement. The preferred vendor will demonstrate prioritization and cost awareness within the 16-week period rather than attempting to implement everything at once. Proposals will be scored higher where they demonstrate measurable outcomes, capability transfer, and realistic delivery within scope, time, and budget constraints.

The Request for Tender document contains statements derived from information that is believed to be relevant on the date but does not provide all the information that may be necessary or desirable to enable an intending contracting party to determine whether to enter a contract or arrange an agreement with TLTB. Neither TLTB nor any of its employees, agents, contractors, or advisers give any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

The outcomes of this engagement directly support the following strategic objectives:

1. Establish a clear understanding of TLTB's current cybersecurity risk exposure across systems, data, and applications.

2. Define, assess against, and establish an evidence-based pathway toward NIST Cybersecurity Framework (CSF) 2.0 Tier 3 (Repeatable). This engagement is not expected to achieve full Tier 3 maturity across the organization within this tender period, but will confirm current maturity, define what Tier 3 means for TLTB's context, and produce a prioritized, cost-conscious plan to reach Tier 3 over time.

3. Align IT policies and procedures to an Information Security Management System (ISMS) consistent with ISO/IEC 27001:2022 principles, positioning TLTB for ISO 27001 certification.

4. Build and document incident management capabilities, including detection, response, and recovery.

5. Deliver quick-win technical hardening improvements within the engagement period to reduce residual risk immediately.

6. Produce a prioritized, cost-effective, and actionable three-year Cybersecurity Strategy that reflects identified risks, desired maturity outcomes and a clear path toward ISO 27001 readiness.

The selection of the successful vendor will be based on, but not limited to, the following five criteria:

1. Company credibility – market presence and experience with similar projects
2. Ability to meet the documented requirements
3. Technical Methodology and Approach
4. Relevant Experience, Qualifications and Capability
5. Total Cost and Deliverables

3.0 Project Timelines

TLTB expects this project to be completed within 16 weeks from the date the tender is awarded. Tenderers must provide a proposed project schedule with key milestones and deliverables as part of their proposal.

The following high-level phasing is expected:

- Phase 1 (Weeks 1–4): Discovery, stakeholder engagement and Threat Landscape Analysis.
- Phase 2 (Weeks 5–9): Vulnerability Assessment and Security Control Assessment.
- Phase 3 (Weeks 10–11): Risk Register Development and ISMS Policy Alignment Review
- Phase 4 (Weeks 12–13): Incident Response Plan Development
- Phase 5 (Weeks 10–14): Quick-Win Technical Hardening Activities (running concurrently)
- Phase 6 (Weeks 14–16): Three-Year Cybersecurity Strategy consolidation and final reporting

Vendors may propose an alternate phasing approach and timelines, provided it is well-justified.

4.0 Scope of Works

4.1 In-Scope Domains

The Cyber Risk Assessment shall encompass the following three primary domains:

a. Systems
   - All on-premises servers, network devices, and infrastructure components (firewalls, switches, routers, wireless access points).
   - Cloud-hosted infrastructure and platform services.
   - Identity and Access Management (IAM) systems and directory services.
   - Endpoint devices, including workstations, laptops, and servers.
   - Backup and disaster recovery systems.

b. Data
   - Classification and mapping of data assets, including personal information, financial data, intellectual property, and operationally critical data.
   - Data storage locations, including on-premises repositories, cloud storage, and third-party data processors.
   - Data flows and integration points between internal systems and external parties.
   - Data retention, archival, and disposal practices.

c. Applications
   - Business-critical and line-of-business applications (commercial off-the-shelf and custom-developed).
   - Web-facing and externally accessible applications and portals.
   - Third-party and Software-as-a-Service (SaaS) applications with access to TLTB data.
   - Application authentication and authorization controls.

- Software development and patch management practices.

4.2 Out of Scope

- Offensive security exercises
- Red Team or adversary simulation activities
- Code-level security review
- Major Infrastructure remediation

4.3 Assumptions and Client Responsibilities

a. TLTB will provide an initial asset inventory (or best available list), network diagrams, and system owners.
b. TLTB will provide a dedicated point-of-contact and schedule stakeholder interviews.
c. The vendor must specify what access is needed (VPN, accounts, whitelisting) and how they will minimize disruption.
d. TLTB will provide timely review of draft deliverables to enable finalization within the project timeline.

4.4 Remediation Activities

In addition to assessment activities, the following remediation activities are explicitly in-scope and must be delivered as part of this engagement:

a. Quick-Win Technical Hardening: The vendor must implement a defined set of practical security improvements during the engagement period. These activities must result in measurable reduction in risk exposure and may include configuration hardening, MFA rollout support, patch remediation guidance, privileged access improvements, or monitoring enhancements. The vendor must provide before-and-after evidence demonstrating security posture improvement.

   Quick-win technical hardening must be limited to configuration improvements, control strengthening, and targeted uplift activities that can be completed within the engagement period. Major architectural redesign, platform replacement, or large-scale infrastructure upgrades are out of scope. Quick-win activities must be agreed with TLTB during the early phase of the project and prioritized based on risk reduction, feasibility, and minimal business disruption.

b. ISMS-Aligned Information Security Policy Suite: Vendor to draft a minimum of 8 core information security policies aligned to ISO/IEC 27001:2022 Annex A, ready for TLTB adoption. Policies must include at minimum: Information Security Policy, Acceptable Use Policy, Access Control Policy, Incident Management Policy, Data Classification Policy, Change Management Policy, Business Continuity & Disaster Recovery Policy, and Supplier/Third-Party Security Policy.

   Policies are expected to be tailored to TLTB's environment and ready for management review and adoption. Organization-wide embedding, cultural change, and full operationalization of all policies is a longer-term activity and will be addressed through the post-engagement roadmap.

c. Incident Response Plan (IRP): Develop a fit-for-purpose Incident Response Plan (IRP) for TLTB. Full IRP requirements including mandatory components such as RACI matrix, escalation paths, forensic guidance, and recovery objectives are detailed in Section 5.8

5.0 Technical Requirements

The vendor must demonstrate the capability and methodology to address all the following technical work streams. Proposals must describe the specific approach, tools, techniques, and outputs for each area.

5.1 Threat Landscape Analysis

The vendor shall develop an Organization-specific threat profile based on current intelligence and TLTB's operating context. This shall include:

a. Identification of threat actors relevant to TLTB's sector and profile (e.g., ransomware groups, nation-state actors, insider threats, supply chain threats).
b. Analysis of threat vectors most likely to be exploited given TLTB's technology environment.

c. Review of publicly available threat intelligence sources relevant to TLTB's industry.

d. High-level review of security logging and monitoring posture (SIEM, firewall logs, cloud logging, alerting). The findings from this review will detail the Monitoring Capability Assessment in Section 5.6.

e. Assessment of third-party and supply chain risk as it relates to the threat landscape.

f. Documentation of threat scenarios to be used as inputs into the risk register.

5.2 Vulnerability Assessment

a. The vendor shall deploy industry-standard vulnerability scanning tools across in-scope network segments and endpoints.

b. Authenticated scanning of servers, workstations, and network devices to identify missing patches, misconfigurations, and known vulnerabilities.

c. Assessment of web-facing application components for known vulnerability types (e.g., OWASP Top 10 categories), without active exploitation.

d. Review of cloud service configurations against provider security benchmarks.

e. Identification and categorization of vulnerabilities by severity (Critical, High, Medium, Low) using the Common Vulnerability Scoring System (CVSS).

f. Analysis of vulnerability exposure in the context of existing compensating controls.

g. Detailed Vulnerability Assessment Report with remediation priorities and recommended timelines.

h. Vulnerability Remediation Expectations:

The vendor is not expected to remediate all identified vulnerabilities within this engagement. Remediation effort must focus on a defined set of high-risk/high-impact issues agreed with TLTB, and on practical risk reduction actions that can

be completed within the engagement timeframe.

5.3 Security Control Assessment and Maturity Review

a. The vendor shall assess the effectiveness and maturity of TLTB's existing security controls using the NIST Cybersecurity Framework 2.0 as the primary reference framework.

b. Evaluation of TLTB's current security posture across all six NIST CSF 2.0 Functions: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER.

c. Assessment of current Tier level across each Function, with documented justification and evidence.

d. Development of a target state profile at NIST CSF 2.0 Tier 3 (Repeatable), defining what 'Tier 3' looks like for the TLTB's specific context and risk appetite.

e. Gap analysis between current state and Tier 3 target state, with prioritized findings for each Function and applicable Categories and Subcategories.

f. Production of a visual maturity heatmap and detailed written findings for stakeholder reporting.

5.4 Control Assessment Activities

The following activities describe how the control assessment and maturity review in Section 5.3 will be conducted:

a. Structured interviews and workshops with key stakeholders including IT management, security personnel, business process owners, and senior leadership.

b. Review of existing security policies, procedures, standards, and guidelines.

c. Review of security tool configurations and outputs.

d. Assessment of identity and access management practices, including privileged access, multi-factor authentication, and user lifecycle management.

e. Review of backup and recovery procedures and testing practices.

f. Assessment of security awareness training programs and staff capability.

g. Evaluation of third-party and vendor management practices from a security perspective.

5.5 IT Policy and ISMS Alignment Review

a. Conduct a structured review of the TLTB's IT security policies and governance documentation to assess alignment with an Information Security Management System (ISMS) consistent with ISO/IEC 27001:2022 principles.

b. Review and gap analysis of all existing IT security policies against the ISO/IEC 27001:2022 Annex A control domains and the TLTB's identified risk environment.

c. Identification of policy gaps, outdated policies, and policies requiring update or creation.

d. Assessment of policy governance processes including approval cycles, review cycles, communication, and staff acknowledgement.

e. Review of TLTB's risk management approach and documentation for alignment with ISMS requirements.

f. Recommendations for an ISMS-aligned policy framework, including a suggested policy hierarchy (policy, standard, procedure, guideline) and prioritized policy development roadmap.

5.6 Incident Management Capability Assessment

a. Review of existing incident response policies, plans, and procedures and assessment of security monitoring and detection capabilities.

b. Evaluation of incident classification, escalation, and communication procedures.

c. Review of roles, responsibilities, and accountability structures during a cyber incident.

d. Review of post-incident review processes and lessons-learned practices.

e. Identification of gaps against good-practice frameworks, including NIST CSF 2.0 RESPOND and RECOVER Functions.

f. Recommendations for improving detection and alerting capabilities.

g. Recommendations for incident response plan development or uplift, including tabletop exercise guidance.

h. Recommendations for improving recovery capabilities, including RTO/RPO alignment and backup integrity.

5.7 Risk Register Development

The vendor shall consolidate all findings from the above work streams into a comprehensive, organization-wide Cyber Risk Register.

a. Documentation of each identified risk with a description, affected assets, threat sources, and existing controls.

b. Qualitative risk scoring using a defined likelihood and consequence matrix, producing an inherent risk rating and residual risk rating for each risk.

c. Prioritization of risks to support decision-making and resource allocation.

d. Mapping of each risk to relevant NIST CSF 2.0 Categories and ISO 27001 control domains.

e. Risk treatment options (accept, mitigate, transfer, avoid) with recommended treatment actions for each high and critical risk.

f. The Risk Register shall be provided in a format suitable for ongoing maintenance

by TLTB.

5.8 Incident Response Plan Development

a. The vendor must produce a fully documented Incident Response Plan (IRP) for TLTB. The IRP must include:
   - Purpose, scope and guiding principles.
   - Incident classification criteria (severity levels and triggers).
   - Roles and responsibilities including a RACI matrix.
   - Step-by-step response procedures for common incident types (e.g. ransomware, data breach, account compromise).
   - Escalation and communication procedures, including internal and external notification requirements.
   - Evidence and forensic preservation guidance.
   - Post-incident review and lessons-learned process.
   - Tabletop exercise scenario guidance (minimum one scenario).
   - Recovery objectives aligned to RTO/RPO targets identified during the assessment.

5.9 Three-Year Cybersecurity Requirements

The Three-Year Cybersecurity Strategy (Deliverable No. 7) is a primary outcome of this engagement. Respondents should demonstrate their understanding of what this document must achieve and how their methodology supports its development.

The Strategy must be structured to address the following components:

a. Year 1 – Foundational and Critical Risk Remediation
b. Year 2 – Capability Development and ISMS Alignment
c. Year 3 – Optimization, Assurance and continuous Improvement

Indicative costs for Year 2 and Year 3 activities should be provided as order-of-magnitude ranges rather than fixed quotes and must be accompanied by the key assumptions on which the estimates are based (e.g. headcount, tool licensing, scope inclusions).

6.0 Deliverables

The following deliverables are required from this engagement. All documents shall be provided in Microsoft Word and PDF formats, unless otherwise specified. Draft versions shall be provided for review prior to finalization.

No	Deliverable	Description
1	Project Plan	Confirmation of scope, methodology, stakeholder engagement plan, and project schedule.
2	Threat Landscape Report	Organization-specific threat profile and threat scenario documentation.
3	Vulnerability Assessment Report	Findings from technical scanning, categorized by severity with remediation recommendations and prioritized action list.
4	NIST CSF 2.0 Maturity Assessment Report	Current state assessment, Tier 3 target state profile, gap analysis, and maturity heatmap across all six CSF Functions.
5	ISMS Policy Alignment Report	Gap analysis of existing policies against ISO

		27001:2022 Annex A, policy framework recommendations, and development roadmap.
6	Fully Developed ISMS-Aligned Information Security Policy Suite	Core IS policies authored and ready for adoption (minimum 8 policies)
7	Cyber Risk Register	Consolidated risk register with inherent and residual ratings, risk treatment options, and CSF/ISO 27001 mappings.
8	Incident Response Plan	Documented IRP with roles, escalation, comms, tabletop guidance.
9	Quick-Win Technical Hardening Report & Evidence	Patching, hardening actions taken + evidence pack
10	Three-Year Cybersecurity Strategy	Actionable, prioritized roadmap spanning three years with Year 1, Year 2, and Year 3 initiatives, effort estimates, indicative costs, and ownership. Must clearly articulate the path from current state to NIST CSF 2.0 Tier 3. The Strategy must be realistic and cost-conscious, aligned to TLTB's operational capacity, and must clearly distinguish activities achievable using existing internal resources versus items requiring new funding, procurement, or external managed services. Dependencies, prerequisites, and sequencing must be clearly stated.
11	Knowledge Transfer Sessions	Minimum two facilitated sessions for TLTB IT personnel covering key findings, implemented controls, and ongoing security hygiene practices. Session agenda, presentation materials, and attendance record. To be completed prior to final project close-out.

7.0 Methodology and Approach

Respondents must describe their proposed methodology in detail. At minimum, proposals must address:

- Overall engagement methodology and phasing (e.g., discovery, assessment, analysis, reporting).
- Approach to stakeholder engagement, including interviews, workshops, and document review.
- Tools and frameworks to be used for vulnerability scanning and control assessment.
- Approach to NIST CSF 2.0 maturity scoring, including evidence requirements and scoring rationale.
- Approach to delivering the Quick-Win Technical Hardening activities, including change management, testing and rollback procedures.
- Approach to policy authoring, including template standards, customization methodology and review process.
- Approach to Incident Response Plan development, including engagement with TLTB stakeholders.

- Quality assurance processes applied to findings and deliverables.
- Approach to sensitive data handling during the engagement.
- Approach to remote versus on-site engagement, and any implications for cost or timeline.

The vendor must include knowledge transfer sessions for TLTB IT personnel to ensure internal capability is improved and that security improvements implemented during the engagement can be maintained after project completion.

8.0 Other Requirements

Tenderers must provide responses to the following compliance requirements:

No	Requirements	Compliance
1	Provide details of the corporate and ownership structure, including identification of any holding company or parent companies.	
2	Provide a profile of the company and any parent entity. If the company is a subsidiary, the Tenderer must provide full details of the legal and financial relationship between the subsidiary and parent. The names of all directors and officers of the company.	
3	Provide a full description of the current operations of the company. A financial statement for the last 3 years may be requested.	
4	Provide a copy of the company's Certificate of Incorporation.	
5	Provide confirmation that the company has the capacity to bid for the Services and that there is no restriction under any relevant law to prevent it from bidding.	
6	Provide details of any legal proceedings that are in progress against the company.	
7	Confirm the number of years the company has been in business.	
8	Confirm the company holds relevant security certifications/accreditations for the services proposed (e.g., ISO 27001 Lead Auditor/Implementer, CREST equivalence, CISSP/CISM on the team)	
9	The company must demonstrate that it has the experience and skills to successfully deliver the solution to TLTB. Provide details, case studies or client references demonstrating comparable cyber risk assessment engagements, including organizations of similar size and complexity.	
10	The bidder must provide a detailed description of approach for each work stream as outlined in Section 5 – Technical Requirements.	
11	The bidder must provide a project schedule with proposed timelines and milestones and deliverables dates.	
12	Vendor must disclose any commercial relationships that could bias recommendations (e.g., reseller of tools they might recommend). Recommendations must include tool-agnostic alternatives where feasible.	
13	Tenderers are to submit pricing inclusive of all requirements specified in the requirements documented on the previous pages.	