FIJI REVENUE AND CUSTOMS SERVICE

TERMS OF REFERENCE

Procurement of Co-Managed Security Operations Centre (SOC) Service

24x7x365 Monitoring, Detection and Response with a Provider-Hosted SIEM

Fiji Revenue and Customs Service/ ICT Division

Issued: 10th July 2026

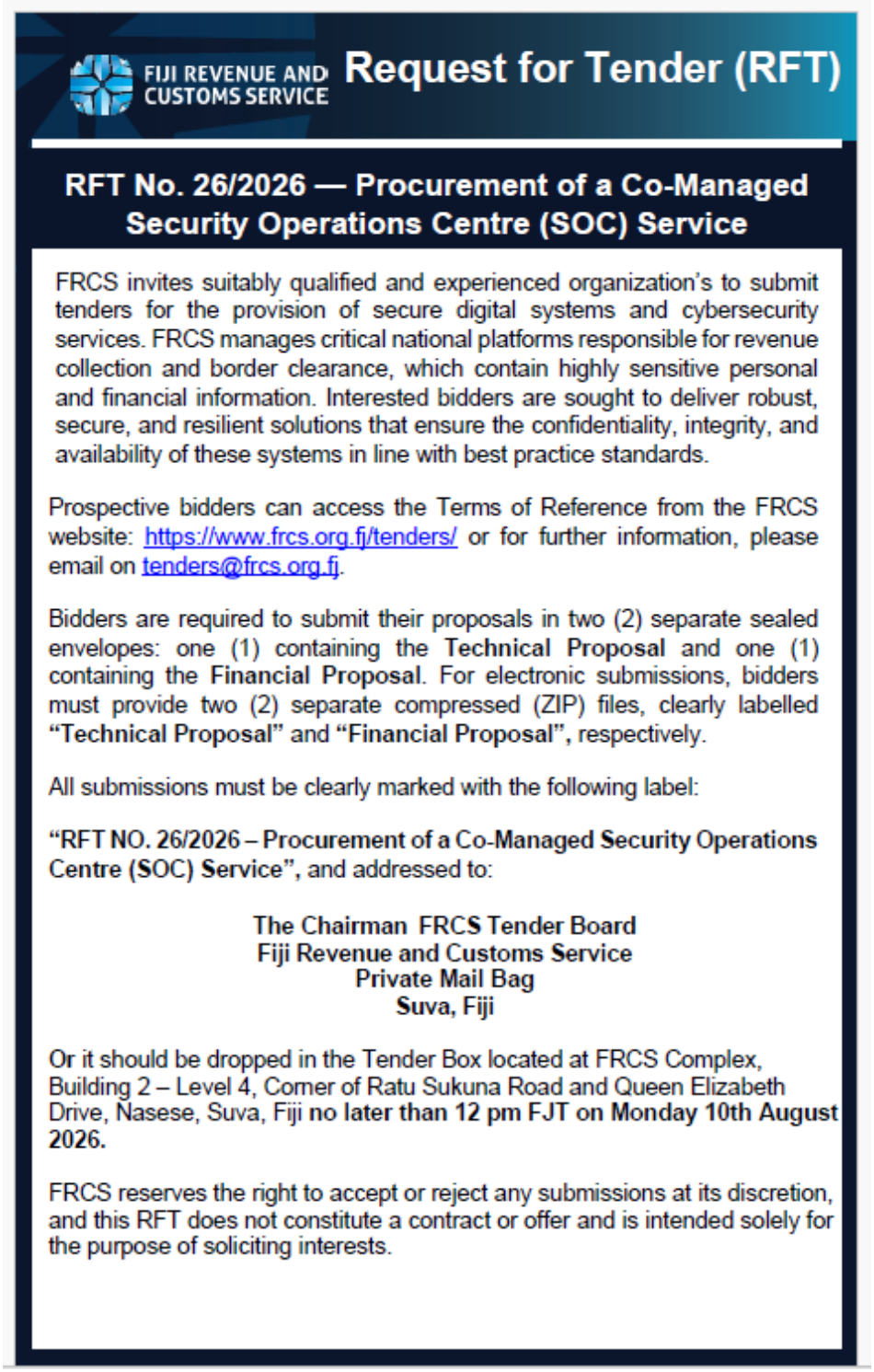
Closing Date: 10th August 2026

Reference No.: RFT 26/2026

Contents

Advertisement

The following is the advertisement for Fiji Revenue and Customs Service as it originally appeared in the local media and should be used as the basis to submit your responses:



FIJI REVENUE AND CUSTOMS SERVICE

Request for Tender (RFT)

RFT No. 26/2026 — Procurement of a Co-Managed Security Operations Centre (SOC) Service

FRCS invites suitably qualified and experienced organization's to submit tenders for the provision of secure digital systems and cybersecurity services. FRCS manages critical national platforms responsible for revenue collection and border clearance, which contain highly sensitive personal and financial information. Interested bidders are sought to deliver robust, secure, and resilient solutions that ensure the confidentiality, integrity, and availability of these systems in line with best practice standards.

Prospective bidders can access the Terms of Reference from the FRCS website: https://www.frcs.org.fj/tenders/ or for further information, please email on tenders@frcs.org.fj.

Bidders are required to submit their proposals in two (2) separate sealed envelopes: one (1) containing the **Technical Proposal** and one (1) containing the **Financial Proposal**. For electronic submissions, bidders must provide two (2) separate compressed (ZIP) files, clearly labelled **"Technical Proposal"** and **"Financial Proposal"**, respectively.

All submissions must be clearly marked with the following label:

"RFT NO. 26/2026 – Procurement of a Co-Managed Security Operations Centre (SOC) Service", and addressed to:

The Chairman FRCS Tender Board
Fiji Revenue and Customs Service
Private Mail Bag
Suva, Fiji

Or it should be dropped in the Tender Box located at FRCS Complex, Building 2 – Level 4, Corner of Ratu Sukuna Road and Queen Elizabeth Drive, Nasese, Suva, Fiji **no later than 12 pm FJT on Monday 10th August 2026.**

FRCS reserves the right to accept or reject any submissions at its discretion, and this RFT does not constitute a contract or offer and is intended solely for the purpose of soliciting interests.

1. Background and Context

The Fiji Revenue & Customs Service (FRCS) administers national taxation and customs and operates the digital platforms through which the bulk of national revenue is collected and through which border-clearance workflows are processed. These systems hold highly sensitive personal and financial information, including passports, national identity documents, birth certificates and taxpayer records. The confidentiality, integrity and availability of these systems is therefore a matter of national revenue assurance, regulatory obligation and public trust.

FRCS has undertaken a comprehensive information security review as part of its ISO/IEC 27001:2022 uplift programme. The review comprised three connected assessments whose findings collectively justify the establishment of a Security Operations Centre (SOC) capability:

- **ISO/IEC 27001:2022 ISMS Gap Analysis —** all 93 Annex A controls were assessed through structured interviews across every division. SOC is one of the new controls identified as an enhancement to our security incident management process.

Critically, the ISMS gap analysis expressly names “a SOC” as the solution for a broad set of Annex A controls spanning threat intelligence, the full incident-management lifecycle, logging, monitoring, network security, vulnerability tracking, malware detection, web filtering and security event reporting. This Terms of Reference (TOR) translates those findings into a procurement specification.

Table 1 — ISMS compliance by control domain

Annex A Domain	Implication for SOC scope
A.5 — Organizational Controls	Threat intelligence and incident-management controls largely absent; SOC is the named solution.
A.6 — People Controls	Security event reporting and awareness require a central SOC reporting point and threat input.
A.7 — Physical Controls	Physical-security monitoring can be correlated with digital events by the SOC.
A.8 — Technological Controls	Logging , vulnerability management and network monitoring are at the heart of SOC operations.
Overall ISMS maturity	Continuous detection and response capability required to bring controls within tolerance.

2. Purpose and Objectives

The purpose of this TOR is to specify the requirements for the procurement of a co-managed Security Operations Centre (SOC) service that will provide FRCS with continuous, 24x7x365 security monitoring, threat detection, incident response and threat intelligence across its revenue-bearing platforms and supporting infrastructure, and that will directly remediate the control gaps identified in the ISMS gap analysis and IT risk register.

2.1 Objectives

1. Establish a continuous (24x7x365) capability to detect, triage, investigate and respond to information security events and incidents across FRCS systems.

2. Remediate the ISO/IEC 27001:2022 Annex A control gaps for which the gap analysis identifies a SOC as the solution (see Section 5).
3. Protect the revenue systems (TPOS/NTIS, ASYCUDA World, TaxCore/VMS) and the sensitive taxpayer data they hold from unauthorised access, exfiltration and disruption.
4. Provide a structured threat-intelligence function and a managed incident-management lifecycle, including forensic readiness and evidence preservation.
5. Operate as a co-managed service that augments and progressively upskills the FRCS Information Management Office (IMO) and System Engineering teams, addressing the technical skills capability risk.
6. Provide assurance to the Board, the IT Governance Committee and external auditors through measurable service levels, KPIs and regular reporting.

3. Scope of Services

3.1 Delivery Model

FRCS is procuring a **co-managed (hybrid) SOC service operating 24x7x365, with the Service Provider supplying and hosting the SIEM / security-monitoring platform.** Under this model, the Service Provider operates the SIEM and provides Level 1 and Level 2 monitoring, detection, triage and analysis around the clock, while FRCS retains accountability for in-environment containment actions, change approval and asset ownership. Roles and responsibilities are defined in the responsibility matrix in Section 7.

3.2 Systems In Scope

The following FRCS platforms and environments are within the scope of monitoring. The three revenue-bearing platforms are the highest priority for onboarding.

System / Environment	Function
TPOS / NTIS	Taxpayer Online Service / National Tax Information System
ASYCUDA World	Customs declaration and border-clearance platform
TaxCore (VMS)	VAT Monitoring System
Perimeter & WAF	External internet perimeter and FRCS Web Application Firewall
Identity & cloud	Active Directory, AWS-hosted workloads, cloud-migrated services
Endpoint & email	Endpoint protection (EDR), email gateway
Network & infrastructure	Core network devices, servers, on-prem and DR (Lautoka) sites

3.3 Out of Scope

- Remediation of application-code defects within TPOS, ASYCUDA World or TaxCore (these remain with the respective solution providers, e.g. Invenio); the SOC provides detection, advisory and validation support only.
- Physical security guarding and facilities management (though physical-access log integration is in scope for correlation).

- Procurement of Privileged Access Management (PAM), Data Loss Prevention (DLP) and endpoint tooling, which are procured separately; the SOC must, however, integrate with and monitor these once deployed.
- General IT service-desk and non-security operational support.

4. Functional Service Requirements

The Service Provider shall deliver the following functional services. Each requirement is mandatory unless explicitly marked as desirable. Bidders shall describe, for each, how the requirement is met, the supporting tooling, and the division of responsibility under the co-managed model.

4.1 SIEM Platform and Log Management

- Provide, host, operate and maintain an enterprise-grade SIEM platform (including underlying infrastructure, licensing, storage and tuning) for the full duration of the contract, at no additional capital cost to FRCS.
- Ingest, normalise, parse, enrich and correlate logs and telemetry from all in-scope sources (Annex A), including the three revenue platforms, WAF, firewalls, Active Directory, AWS/cloud workloads, EDR, email gateway, network devices, servers and databases.
- Provide log retention of a minimum of 12 months online/searchable and a minimum of 24 months in archive (or longer where required by Fiji law or FRCS records-retention policy), with tamper-evident storage.
- Maintain accurate, synchronised time across all log sources to support correlation and forensic timelines (supports A.8.17 Clock Synchronisation).
- Provide FRCS with read access to dashboards, searches and reports through a secure portal, with role-based access for nominated FRCS staff.

4.2 24x7x365 Security Monitoring and Detection

- Provide continuous, around-the-clock monitoring of all in-scope sources by qualified SOC analysts, with no gaps in coverage including Fiji public holidays.
- Operate a tiered analyst model (L1 triage, L2 investigation, L3 advanced analysis / incident response) with defined escalation paths to FRCS.
- Detect, validate and prioritise security events; suppress false positives through continuous tuning; and alert FRCS within the agreed service levels (Section 6).
- Continuously monitor network traffic and network services for suspicious activity, attempted compromise and lateral movement (supports A.8.20, A.8.21).

4.3 Detection Engineering and Use-Case Development

- Develop, document and maintain a detection use-case library aligned to a recognised framework (e.g. MITRE ATT&CK), covering at minimum: unauthorised access and broken-access-control exploitation, account takeover and credential abuse, mass enumeration of taxpayer records, insecure file-upload abuse, web-application attacks, malware, data exfiltration and privilege escalation.
- Prioritise detection content for the specific risks identified in the FRCS penetration test (e.g. enumeration of predictable reference numbers, directory traversal, absence of rate limiting).
- Review and update detection content at least quarterly and after every major incident or change.

4.4 Threat Intelligence (A.5.7)

- Establish and operate a threat-intelligence function that collects, analyses and applies strategic, operational and tactical threat intelligence relevant to revenue authorities, government and the Pacific region.
- Integrate threat-intelligence feeds (commercial, open-source and sector/government sources) into the SIEM for automated indicator matching.
- Support FRCS engagement with relevant authorities and CERTs, including AusCERT (Pacific region), and consume their advisories (supports A.5.5 Contact with Authorities).
- Provide regular threat advisories and an annual threat-landscape assessment tailored to FRCS.

4.5 Incident Management and Response Lifecycle (A.5.24 – A.5.27)

The Service Provider shall facilitate the full information-security incident-management lifecycle, which the gap analysis identifies as a primary SOC responsibility:

- Planning and preparation — assist FRCS to develop and maintain an incident-response plan, playbooks and an incident classification/severity scheme (A.5.24).
- Assessment and decision — assess and categorise security events, determine whether they constitute incidents, and prioritise them (A.5.25).
- Response — respond to confirmed incidents in accordance with documented playbooks and timelines, providing analysis, containment guidance and remediation recommendations; for co-managed actions, direct and validate FRCS containment (A.5.26).
- Learning — conduct post-incident reviews / root-cause analysis and feed lessons learned back into detection content and playbooks (A.5.27).

- Provide a defined major-incident escalation and crisis-communications procedure, including out-of-hours contact with nominated FRCS executives.

4.6 Threat Hunting

- Conduct proactive, hypothesis-driven threat hunting across in-scope systems at a defined cadence (at minimum monthly), targeting indicators of compromise and adversary techniques not covered by existing detections.
- Document hunt findings and convert successful hunts into permanent detection content.

4.7 Vulnerability Management Support (A.8.8)

- Identify, evaluate, track and report technical vulnerabilities across monitored assets, and correlate vulnerability data with active threats to support risk-based prioritisation.
- Integrate with FRCS vulnerability-scanning outputs and the penetration-test remediation programme; monitor for exploitation attempts against known unpremeditated findings (e.g. ASYCUDA end-of-life components) and provide compensating-control recommendations.
- Support independent re-testing by alerting on, and validating, attempted exploitation of items pending remediation.

4.8 Digital Forensics and Evidence Collection (A.5.28)

- Provide, during incident response, the proper identification, collection, acquisition and preservation of evidence in a forensically sound manner, maintaining chain of custody suitable for disciplinary, regulatory or legal proceedings.
- Provide forensic-investigation support (remote and, where required, on-site within Fiji) for major incidents, with a defined response time.

4.9 Malware and Endpoint Detection (A.8.7)

- Monitor and analyse endpoint detection and response (EDR) and anti-malware telemetry to detect, analyse and respond to malware threats in real time, and integrate alerts into the SIEM.

4.10 Network and Web-Filtering Monitoring (A.8.20, A.8.21, A.8.23)

- Continuously monitor network security controls and the security of network services, and detect attempts to compromise them.
- Monitor web-filtering and proxy logs to detect access to malicious destinations and analyse web traffic for threats.

4.11 Reporting, Dashboards and Advisories (A.6.8)

- Serve as a central, accessible mechanism for FRCS personnel to report observed or suspected security events, and triage such reports.

- Provide real-time dashboards, scheduled operational reports, monthly service reports and quarterly executive/Board-level reports (see Section 10).

4.12 Capability Building and Knowledge Transfer

- As a co-managed service, progressively transfer knowledge and skills to the FRCS IMO and System Engineering teams through joint working, documented runbooks, shadowing and structured training, addressing the FRCS technical-skills capability risk.
- Provide input of real-world threat and incident examples into the FRCS security-awareness programme (supports A.6.3).

4.13 Physical-Digital Correlation (Desirable) (A.7.4)

- Where feasible, integrate physical-security telemetry (access-control logs, surveillance events) to correlate physical and digital events and detect unauthorised physical access that may precede a digital breach.

5. ISO/IEC 27001:2022 Control Mapping

The table below maps the SOC service directly to the Annex A controls for which the FRCS gap analysis identifies a SOC as the solution. This mapping shall be used to confirm that the proposed service closes the identified gaps and shall form the basis of acceptance testing.

Control	Control & current maturity	How the SOC service addresses it
A.5.7	Threat intelligence	Threat-intelligence function: collection, analysis and application of intelligence (4.4).
A.5.24	Incident management planning	Facilitates incident-management planning, playbooks and classification (4.5).
A.5.25	Assessment & decision on events	Assesses, categorizes and prioritizes security events 24x7 (4.5).
A.5.26	Response to incidents	Structured response per playbooks with containment direction and validation (4.5).
A.5.27	Learning from incidents	Post-incident review and feedback into detections and playbooks (4.5).
A.5.28	Collection of evidence	Forensically sound evidence collection and chain of custody (4.8).
A.6.3	Security awareness	SOC supplies real-world threat and incident examples (4.12).
A.6.8	Security event reporting	SOC as central event-reporting and triage point (4.11).
A.7.4	Physical security monitoring	Correlates physical-access and surveillance telemetry (4.13, desirable).
A.8.7	Protection against malware	EDR + SIEM real-time malware detection and response (4.9).
A.8.8	Technical vulnerabilities	Identify, evaluate, track and prioritise vulnerabilities (4.7).
A.8.15	Logging	Centralised log collection, retention and analysis — core SIEM (4.1).
A.8.16	Monitoring activities	Continuous 24x7 monitoring and correlation (4.2).
A.8.20	Networks security	Continuous network-traffic monitoring and response (4.10).
A.8.21	Security of network services	Detects attempts to compromise network services (4.10).
A.8.23	Web filtering	Monitors web-filtering logs and analyses web traffic (4.10).

Note: The SOC also provides supporting assurance for related controls including A.5.5 (Contact with Authorities), A.8.17 (Clock Synchronisation) and A.8.12 (Data Leakage Prevention, once DLP is deployed).

6. Service Levels (SLA)

The Service Provider shall meet or exceed the following service levels. Bidders may propose tighter levels. Service credits shall apply for sustained failure to meet committed levels, on terms to be agreed in the contract.

6.1 Incident Severity and Response Targets

Severity	Definition (examples)	Acknowledge & notify FRCS	Begin investigation
Critical	Active compromise or confirmed exfiltration of taxpayer data; outage of a revenue platform; mass enumeration in progress	15 minutes (24x7)	30 minutes
High	Credible attack on a crown-jewel system; broken-access-control exploitation attempt; privileged-account abuse	30 minutes	1 hour
Medium	Targeted scanning, repeated failed authentication, malware contained by endpoint controls	2 hours	4 hours
Low / Info	Policy deviations, low-confidence anomalies, informational alerts	Next business day	Best effort

6.2 Availability and Operational SLAs

Metric	Target
SIEM platform / monitoring availability	99.9% monthly (excluding agreed maintenance windows)
Continuity of 24x7 monitoring coverage	100% — no monitoring gaps
Log-source ingestion / health monitoring	Loss of a critical log source detected and FRCS notified within 30 minutes
Mean time to detect (MTTD) — known techniques	Continuous improvement target reported monthly
Monthly service report delivery	Within 5 business days of month-end
Major-incident forensic support (remote)	Commence within 2 hours of FRCS request

7. Co-Managed Operating Model and Responsibilities

The service operates as a co-managed partnership. The matrix below sets out the primary division of responsibility. (R = Responsible / leads; S = Supports; A = Accountable / final authority.)

Activity	Service Provider	FRCS (IMO / SE)
SIEM hosting, operation, tuning, licensing	**R / A**	S
Log-source onboarding & integration	**R**	S (access, approvals)
24x7 monitoring, triage, L1/L2 analysis	**R / A**	S
Detection-content development & tuning	**R**	S (context)
Threat intelligence	**R / A**	S
Incident declaration & severity assignment	**R**	A (confirms)
In-environment containment actions	S (directs/validates)	**R / A**
Change approval in FRCS systems	S	**R / A**
Asset ownership & business decisions	S	**R / A**
Forensics & evidence preservation	**R**	S
Application-code remediation (TPOS etc.)	S (advisory)	A (via solution providers)
Knowledge transfer & upskilling	**R**	S (participates)

8. Technical and Integration Requirements

- The Service Provider shall integrate with the in-scope log sources listed in Annex A using secure, encrypted transport, with minimal performance impact on production revenue systems.
- Onboarding of log sources shall be planned with FRCS to avoid disruption; the three revenue platforms shall be prioritized.
- The solution shall support both on-premises (Nasese; Lautoka DR) and cloud (AWS) environments and hybrid architectures.
- All collector/agent components deployed within the FRCS environment shall be hardened, supported, patched and inventoried.
- The Service Provider shall support API-based integration for automated enrichment and, where appropriate, orchestrated response (SOAR) subject to FRCS approval of any automated action.

9. Data Protection, Sovereignty and Confidentiality

Because in-scope systems hold highly sensitive taxpayer personal data, the following requirements are mandatory and material to evaluation:

- **Data sovereignty —** the bidder shall declare where SIEM data (logs and any extracted content) will be stored and processed. Any storage or processing outside Fiji shall be explicitly disclosed and shall comply with FRCS data-handling requirements, applicable Fiji law and any tax-secrecy/confidentiality obligations. FRCS reserves the right to require in-country or specified-jurisdiction data residency.
- **Confidentiality & secrecy —** the Service Provider and all personnel shall sign FRCS non-disclosure and tax-secrecy undertakings before access is granted; taxpayer information observed during monitoring shall not be disclosed, copied or used for any purpose other than the service.

- **Personnel vetting —** all SOC personnel with access to FRCS data shall be background-screened to a standard acceptable to FRCS (supports A.6.1 Screening).
- **Encryption & access —** data in transit and at rest shall be encrypted; access to FRCS data shall be role-based, least-privilege, logged and auditable.
- **Provider security posture —** the Service Provider should itself hold ISO/IEC 27001 certification (or equivalent) and shall permit FRCS to audit its handling of FRCS data.
- **Data return & destruction —** on exit, the Service Provider shall return and/or securely destroy all FRCS data and provide certification of destruction.

10. Governance and Reporting

Report / forum	Frequency	Audience / content
Real-time dashboard	Continuous	FRCS IMO/SE — live alerts, open incidents, system health
Operational sync	Weekly	IMO/SE — open items, tuning, onboarding progress
Service / SLA report	Monthly	CIO/HOI — alerts handled, incidents, SLA attainment, MTTD/MTTR trends, tuning
Threat advisory	As needed + monthly digest	IMO/SE — relevant threats, IOCs, recommended actions
Executive / governance report	Quarterly	IT Governance Committee / Board — risk posture, KPIs, control-gap closure progress
Post-incident report	Per major incident	CIO + stakeholders — timeline, root cause, lessons learned
Annual service review	Annual	CIO — performance, threat-landscape assessment, roadmap

11. Team, Personnel and Certifications

- The Service Provider shall maintain a SOC team sufficient to deliver genuine 24x7x365 coverage with defined L1, L2 and L3 roles and a named service-delivery manager as FRCS's primary point of contact.
- Analysts shall hold relevant, current certifications (e.g. CompTIA Security+/CySA+, GIAC GCIA/GCIH, EC-Council, OSCP for IR/hunting, or vendor SIEM certifications); incident responders and forensic staff shall hold relevant IR/forensic qualifications.
- The Service Provider shall disclose the location(s) of the delivering SOC and confirm capacity to support the Fiji (FJT) time zone and Fiji public holidays.
- Bidders shall provide CVs/profiles of key personnel and shall not substitute key personnel without FRCS approval.

12. Compliance and Legal

- The service shall be designed and operated to support FRCS compliance with ISO/IEC 27001:2022 and to provide auditable evidence for the controls in Section 5.
- The Service Provider shall comply with all applicable Fiji laws and regulations, including data-protection, privacy and revenue/tax-secrecy obligations, and shall support FRCS's identification and maintenance of legal and regulatory requirements (supports A.5.31).
- The engagement shall be governed by a formal contract and Service Level Agreement; this TOR shall be read with, and incorporated into, that contract. FRCS legal and procurement shall review final terms.

13. Performance Management and KPIs

Key Performance Indicator	Target
SLA attainment (acknowledge/notify by severity)	≥ 98% monthly
24x7 monitoring coverage	100% — no gaps
Critical/High true-positive incidents missed by SOC	Zero
False-positive rate	Reduced quarter-on-quarter via tuning
Detection coverage (MITRE ATT&CK techniques relevant to FRCS)	Expanding, reported quarterly
ISMS control-gap closure (Section 5 controls)	All mapped controls evidenced within agreed onboarding period
Knowledge-transfer milestones to FRCS team	Met per agreed plan
Customer satisfaction (FRCS review)	≥ agreed threshold at each quarterly review

14. Contract Term and Commercial Requirements

- Proposed term: an initial period of [2–3] years with options to extend, to allow stable operation and progressive capability transfer. FRCS to confirm.
- Pricing shall be presented as: (i) one-off onboarding/transition cost; (ii) recurring annual managed-service subscription (inclusive of SIEM hosting, licensing and 24x7 staffing); and (iii) clearly itemised optional/usage-based elements (e.g. additional log sources, on-site forensic call-out, additional threat-intel feeds).
- **Indicative internal estimate / budget note:** the FRCS risk register recorded indicative figures of approximately FJD 25,000 (SOC function) and FJD 7,000 (threat-intelligence subscription), plus FJD 12,000 for AusCERT engagement. FRCS notes these were preliminary internal estimates; the realistic cost of a hosted, fully-staffed 24x7 co-managed service is expected to exceed these figures, and the budget should be validated against market responses. Bidders shall price the service as specified rather than to the indicative figure.
- All prices shall be in Fijian Dollars (FJD), state whether inclusive or exclusive of VAT, and remain valid for [90] days.

15. Bidder Eligibility and Mandatory Requirements

- Demonstrable experience operating a 24x7 SOC / managed-detection-and-response service, ideally for government, financial-services or revenue/tax organisations.
- At least [three] verifiable client references of comparable scale and sensitivity.
- Evidence of the Service Provider's own information-security certification (ISO/IEC 27001 or equivalent).
- Financial stability and legal standing to contract with FRCS, with all statutory registrations and tax compliance in order.
- Confirmed ability to meet the data-sovereignty, confidentiality and personnel-vetting requirements in Section 9.

16. Evaluation Criteria

Proposals will be evaluated on a combined technical and commercial basis. Indicative weighting (FRCS to finalise per procurement policy):

Criterion	Weight	Notes
Technical solution & coverage of Section 4–5 requirements	30%	Completeness, SIEM capability, detection coverage
24x7 SOC capability, team & certifications	15%	Genuine coverage, qualifications, key personnel
Relevant experience & references	15%	Comparable government/financial clients
Data sovereignty, security & compliance	15%	Section 9 — pass/fail elements may apply
Transition, co-management & knowledge transfer	10%	Onboarding plan and upskilling of FRCS
Commercial / value for money	15%	Total cost of ownership over the term
Total	**100%**	

17. Deliverables and Milestones

Phase	Deliverable	Indicative timing
Mobilisation	Signed contract/SLA, NDAs, project plan, named team	Week 0–2
Onboarding 1	SIEM live; revenue platforms (TPOS, ASYCUDA, TaxCore) + WAF onboarded; baseline detections	Week 2–6
Onboarding 2	Remaining sources onboarded; incident playbooks; runbooks; FRCS portal access	Week 6–10
Go-live (steady state)	Full 24x7 monitoring; SLA reporting commences; control-mapping evidence pack	Week 10–12
Optimisation	Tuning, threat hunting, first quarterly governance report, KT milestone 1	Quarter 1 ongoing
Ongoing	Continuous service, reporting, advisories, annual review	For contract term

Timings are indicative; bidders shall propose a detailed plan. FRCS's roadmap targets SOC services procurement within the 14–30 day immediate horizon and advanced SIEM/SOC deployment within 90–180 days.

18. Assumptions and Dependencies

- FRCS will provide timely access, accounts, network connectivity and points of contact required for onboarding.
- FRCS will maintain in-scope source systems and forward the necessary logs/telemetry.
- Containment actions inside FRCS systems remain FRCS's responsibility under the co-managed model, executed on SOC guidance.
- Application-code fixes for TPOS, ASYCUDA World and TaxCore are delivered by the respective solution providers; the SOC provides detection and advisory support.
- PAM and DLP tooling are procured separately and will be integrated with the SOC once available.

19. Proposal Submission

- Submission deadline: **Monday 10th August 2026/12pm, Fiji time**
- Submission method and address: Submission to be dropped in the Tender Box located at FRCS Complex, Building 2 – Level 4, Corner of Ratu Sukuna Road and Queen Elizabeth Drive, Nasese, Suva or emailed to: tenders@frcs.org.fj

  Tender to be in a sealed envelope and clearly market "RFT No. 26/2026- Procurement of a Co-Managed Security Operations Centre (SOC) Service".

  Electronic submission from the local bidders will not be accepted

  Bidders who qualify for electronic submission needs to send the submission in a password protected zipped folder (two envelope bid Technical and Financial)
- Queries / clarifications: tenders@frcs.org.fj
- Proposals shall address each requirement in Sections 4–16 and include the completed pricing schedule and references.

This procurement shall be conducted in accordance with FRCS and Government of Fiji procurement policy. The bracketed placeholders in this document are to be completed by FRCS procurement before issue.

Annex A — Indicative Log-Source Inventory

The following sources shall be onboarded to the SIEM. FRCS will confirm the definitive inventory, volumes (EPS/GB per day) and priority during mobilisation.

Category	Sources
Revenue platforms	TPOS / NTIS, ASYCUDA World, TaxCore (VMS) — application, web and database logs
Perimeter	FRCS Web Application Firewall (WAF), external firewalls, reverse proxies
Identity	Active Directory, authentication/MFA logs, privileged-access logs (PAM when deployed)
Cloud	AWS workloads (CloudTrail, VPC flow, guard/security services), cloud-migrated services
Endpoint & email	EDR/anti-malware, email security gateway
Network & infrastructure	Core switches/routers, VPN, DNS, servers (Windows/Linux), hypervisors, DR site (Lautoka)
Data protection	DLP (when deployed), database activity monitoring
Physical (desirable)	Physical access-control and surveillance event logs

Annex B — FRCS Request for Tender (RFT) Framework

This Annex follows the FRCS standard RFT template structure and consists of three parts: Part B.1 — Invitation to Tender; Part B.2 — General Terms and Conditions (GTC); Part B.3 — Bid Data Sheet (BDS). Schedules A, B, and C (Forms) are provided in Annex C.

B.1 Invitation to Tender (RFT No. 20/2026 — Procurement of a Co-Managed Security Operations Centre (SOC) Service)

1. Fiji Revenue and Customs Service (FRCS) invites qualified and experienced service providers to submit sealed tenders for the provision, enhancement, and ongoing support of secure digital systems and cybersecurity services.
3. Competitive bidding will be conducted under FRCS procurement procedures and guidelines and is open to all eligible companies.
4. Interested bidders can access the tender specifications from the FRCS website at https://www.frcs.org.fj/tenders/ at no cost. All documents are in the English language.
5. It is the bidder's responsibility to ensure that the submission is dropped in the Tender Box located at FRCS Complex, Building 2 — Level 4, Corner of Ratu Sukuna Road and Queen Elizabeth Drive, Nasese, Suva, or via email before the specified closing time stated in Part B.3 (Bid Data Sheet).
6. Local bidders are required to submit valid compliance certificates / letters from FNPF, FRCS, and FNU as part of their bids. Failure to comply with the requirements of the Bidding Documents may invalidate the submission.
7. Bidders seeking further clarification or information on the Tender and/or the process should contact FRCS via email on tenders@frcs.org.fj
8. Bid responses must be hand-delivered or emailed before the deadline stated in Part B.3 (Bid Data Sheet). Late tenders will not be accepted.
9. The highest or any tender may not necessarily be accepted.
10. FRCS reserves the right to accept or reject any Bid, and to annul, in whole or in part, or to suspend the bidding process and reject all Bids at any time and without reason prior to award, without thereby incurring any liability to the affected Tenderer or Tenderers.

B.2 General Terms and Conditions (GTC)

The following 16 General Terms and Conditions (FRCS standard) apply to this Tender.

Clause	Provision
1. Format of Response	Each bidder must provide a formal letter of transmittal that must: a) Be signed by an authorized representative of the organization and 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. c) Provide a contact name, address, landline number and email address which FRCS will use in serving notices to the bidder. d) Two envelopes/zipped folder for email submission, 1 for technical and 2nd for financial.
2. Late Submissions	Submissions received within five (5) minutes of the closing time will be accepted. Five minutes is allowed as variation for any timing difference. Submissions received later than this will not be accepted.
3. Applicants to Inform Themselves	Each applicant should:

	a) Examine this specifications document, any documents referred to within, and any other information made available by FRCS b) Obtain any further information about the facts, risks, and other circumstances relevant to the tender by making all lawful inquiries c) Ensure that the submission and all information on which its proposal is based is true, accurate, and complete. By submitting their proposal, applicants are deemed to have: a) Examined the tender specifications and any other information made available in writing by FRCS to the applicants. b) Examined all information relevant to the risks, contingencies, and other circumstances having an effect on their proposal and which is obtainable by the making of reasonable inquiries.
4. Bidder's Risk	FRCS accepts no responsibility, liability, or obligation whatsoever for costs incurred by or on behalf of any bidder in connection with the EOI/RFT or any participation in the tender process.
5. Selection of Preferred Applicant	• No proposal will necessarily be selected by FRCS as the preferred solution. The FRCS Evaluation Committee may decide not to accept any proposal or to reject all proposals at any time. FRCS reserves the right to cancel this tender and pursue an alternative course of action at any time. • Selection of a Preferred Applicant will not constitute acceptance of the proposal, and no binding relationship will exist between the preferred applicant and FRCS until a written agreement acceptable to FRCS is executed by an authorized officer of FRCS and the successful applicant.
6. Conduct of Applicants	Conduct of Applicants or any of their consortium members may affect the outcome of their tender responses, including non-consideration of the proposal. Applicants warrant that they (and their consortium members) have not and will not engage in: a) Lobbying of, or discussions with, any politician or political groups during this tender process. b) Attempts to contact or discuss the tender process with any officer, member, staff, contractor, or agent of FRCS, except for Evaluation Committee members through the formal clarification channel c) Provision of gifts or future promises of gifts of any sort to the previously mentioned personnel. d) Accepting or providing secret commissions. e) Seeking to influence any decisions of FRCS by improper means or otherwise acting in bad faith, fraudulently or improperly.
7. Currency	All currency in the proposal shall be quoted in Fiji Dollars (FJD) and prices shall be VAT-inclusive.
8. Corporate Information	Each applicant must provide: a) Details of the corporate and ownership structure including identification of any holding/parent companies (Business License and Business Registration). b) Profiles of the company and any parent entity, including the names of all directors and officers. If the company is a subsidiary, the applicant must provide full details of the legal and financial relationship between the subsidiary and parent. c) A full description of current operations including the most recent audited financial statement d) A copy of the company's Certificate of Incorporation. e) Confirmation that the company has the capacity to bid for the Services and that there is no restriction under any relevant law preventing it from bidding. f) Provision of details of any legal proceedings against the company.
9. Qualifications and Capability	Each Applicant must: a) Be FNPF, FRCS, and FNU compliant (valid letters/certificates to be attached). Tax Identification Number (TIN) MUST be quoted in the submission. b) Demonstrate that it will be able to meet its financial obligations under this tender. c) Have a direct partnership with the SAP supplier (Partner Certificate to be included in the proposal) and be an authorized reseller or distributor.

	d) Relevant experience in successfully executing projects or managing service support contracts of a similar scope and monetary value.
10. Mergers, Acquisitions, Sales of Applicant	Where such information is publicly accessible, the Applicant must indicate whether any mergers, acquisitions, or sales are planned presently or during the year following the submission of the proposal.
11. Enquiries	All questions and enquiries regarding this tender are to be made in writing via email or official letter. All questions and enquiries will be responded to in writing via email. Verbal responses will not have any binding on either party.
12. Confidentiality	All Companies shall keep strictly confidential any and all information contained in this RFT and any other information or documents made available to them by or on behalf of FRCS in connection with this RFT. The firms shall not disclose, nor allow any such information to be disclosed. Any effort by a Tenderer to influence FRCS in its decisions on Tender evaluation, comparison, or contract award may result in the rejection of the Tenderer's Bid.
13. Price Bid	The Price(s) should include all non-exempt duties, taxes, and other levies payable by the Tenderer under the contract/purchase order and must be presented as per the Price Schedule (Schedule C) provided in Annex B.
14. Bid Validity Period	The bid shall remain valid for 120 calendar days after the deadline of the receipt of the bids.
15. Notification of Award	FRCS will notify the successful Tenderer in writing prior to the expiration of the period of Bid Validity.
16. Extension of Validity Period	In exceptional circumstances, prior to the expiration of the proposal validity period, FRCS may request bidders to extend the period of validity of their proposals. The request and the responses shall be made in writing and shall be considered integral to the Proposal. If the bidder agrees to extend, it shall be done without any change to the original proposal. The bidder has the right to refuse to extend, in which case the proposal will not be further evaluated.

B.3 Bid Data Sheet (BDS)

BDS No.	Description	Instruction
1	Condition of Tender	Fixed Lump Sum (Base Service Fee)
2	Contract Form	The provisions of the Contract Template are indicative of the terms and conditions the parties may ultimately agree, and will become binding on the parties after the tender has been awarded and upon finalization and execution of the contract. A Memorandum of Understanding ("MOU") and Non-Disclosure Document ("NDD") shall be signed with the successful bidder prior to commencement of works.
3	Mandatory Supplementary Documents	• Company Profile (≤ 15 pages) including Organization Structure • Schedule A — Declaration by Bidder — Conformity (Annex H) • Schedule B — Bidder Information (Annex H) • Schedule C — Declaration by Bidder — Price (Annex H) • Valid FRCS Tax Compliance Certificate • Valid FNPF Compliance Letter (for companies) • Valid FNU Levy Compliance Certificate • Certificate of Tax Registration and Exemption (if any) • Certificate of Incorporation / Business Registration • Audited Financial Statements (last 3 years) • Minimum 3 written Client References with contact details • Minimum 2 written Supplier References • Insurance certificates • Personnel CVs per + Key Personnel
4	Deadline / Submission	Date: Monday 10th August 2026 Time: 12:00 noon FJT Mode: Submission to be dropped in the Tender Box located at FRCS Complex, Building 2 —

		Level 4, Corner of Ratu Sukuna Road and Queen Elizabeth Drive, Nasese, Suva or emailed to : tenders@frcs.org.fj Electronic submission from the local bidders will not be accepted Bidders who qualify for electronic submission needs to send the submission in a password protected zipped folder (two envelope bid Technical and Financial) Tender to be in a sealed envelope and clearly marked: " RFT No. 26/2026 — Procurement of a Co-Managed Security Operations Centre (SOC) Service ".
5	Deliverables	Refer to Section 17 (Deliverables) and Section 3 (Scope of Work) of this TOR for the full deliverables matrix. Bidders shall acknowledge each deliverable in Schedule A.
6	Locations	FRCS Nasese Office
7	Clarifications	Email: tenders@frcs.org.fj All Q&A published to all bidders simultaneously without identifying the questioner. Verbal responses are non-binding.
8	Pre-Bid Conference	Mandatory virtual pre-bid conference 14 days after RFT issue. Attendance to be confirmed by email at least 3 business days in advance.
9	Bid Opening	Two-envelope bid: Technical envelopes and Financial envelopes
10	Evaluation Methodology	Per Section 16.
11	Conflict of Interest	Bidders shall declare any actual, potential, or perceived COI. Material undisclosed COI is grounds for disqualification.
12	Joint Ventures, Consortia, and Sub-Contractors	Permitted with disclosure. Lead bidder bears primary contractual liability with cross-guarantee from JV partners. Sub-contractors > 10% of contract value disclosed at bid; changes during contract require prior written FRCS approval.

Annex C — Schedules (FRCS Standard Forms)

This Annex provides the FRCS standard Schedule forms required as part of the bid submission. Schedules A, B, and C must be completed, signed by the authorized representative, and included in the bid envelope.

C.1 Schedule A — Declaration by Bidder — Conformity

Tender Reference:	RFT No. 26/2026
Tender Title:	Procurement of a Co-Managed Security Operations Centre (SOC) Service

1. We confirm to have examined the Tender Documents, attended the Pre-Bid Conference (where applicable) and hereby acknowledge any addenda thereof, and offer to supply the services set out in the RFT, the Specifications, the Terms of Reference, and accompanying documents for the price(s) specified in the Price Schedule (Schedule C).

2. We declare that we have read and clearly understood all Sections of this RFT, including the GTC and the TOR, and if required we will sign and return any section of the RFT to form part of the Contract Document.

3. We hereby declare that our firm, its affiliates or subsidiaries or employees, including any JV/Consortium/Association members or subcontractors or suppliers for any part of the contract:

a. have no conflict of interest, are not under procurement prohibition by FRCS, and have not been suspended, debarred, sanctioned, or otherwise identified as ineligible.

b. have not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against them that could impair their operations in the foreseeable future.

c. Undertake not to engage in proscribed practices, including but not limited to corruption, fraud, coercion, collusion, obstruction, or any other unethical practice with FRCS or any other party, and to conduct business in a manner that averts any financial, operational, reputational, or other undue risk to FRCS.

4. We declare that all information and statements made in this Proposal are true and we accept not to deviate, unless the Scope of Work is changed by FRCS.

5. We agree that FRCS has the right to deduct the full Bid Security Sum (if any) in case of any breach of the terms and conditions of the RFT or in the case where we decide to reject the offer by FRCS after the Letter of Award has been issued.

6. We understand that FRCS reserves the right, unless the tenderer stipulates to the contrary in the tender, to accept such portion thereof as FRCS may decide. FRCS is not bound to accept the lowest or any tender.

7. We confirm that our submission shall be valid and remain binding upon us for the period specified in the Bid Data Sheet (90 calendar days).

I, the undersigned, certify that I am duly authorized to sign this Proposal and bind it should FRCS accept this Proposal.

Field	Detail	Common Seal
Authorized Representative - Signature		
Authorized Representative - Name		
Designation		
Company Name		
Date		

C.2 Schedule B - Bidder Information

Field	Bidder Response
Bidder Registered Name	[Complete]

Legal Address - Street Address	[Complete]
Legal Address - Postal Address	[Complete]
Office Number	[Complete]
Website (if any)	[Complete]
Year of Registration	[Complete]
List of Director(s) / Shareholder(s)	[Complete]
Bidder Authorized Representative - Name and Title	[Complete]
Bidder Authorized Representative - Telephone	[Complete]
Bidder Authorized Representative - Email	[Complete]
Countries of Operation	[Complete]
No. of Full-time Employees	[Complete]
No. of Technical Employees	[Complete]
No. of Field / On-site Employees in Asia-Pacific	[Complete]
FRCS Clarification Contact - Name and Title	[Complete]
FRCS Clarification Contact - Telephone	[Complete]
FRCS Clarification Contact - Email	[Complete]

Documents to be Attached with Schedule B

- Company Profile, not exceeding fifteen (15) pages, with Organization Structure, Director(s), specialization, expertise, list of equipment, machinery, and resources.
- Certificate of Incorporation / Business Registration.
- Valid Tax Compliance Certificate issued by FRCS.
- Certificate of Tax Registration and Exemption (if any).
- Valid FNPF Compliance Certificate.
- Valid FNU Levy Compliance Certificate.
- Audited Financial Statements (balance sheets including all related notes, and income statements) for at least the most recent 3 years, prepared by a qualified Accountant professional.
- Minimum 3 written Client References (preferably tax / revenue authority engagements) with contact details.
- Minimum 2 written Supplier References.
- Personnel CVs for all proposed Key Personnel.
- Insurance certificates per Annex I (Professional Indemnity, Public Liability, Cyber Liability, Workers Compensation).
- Methodology Questionnaire response using template B.5.
- Sub-contractor disclosure (where any sub-contractor is > 10% of contract value).
- Anti-Bribery, Sanctions, and Modern-Slavery / Human-Rights Declarations.
- Conflict-of-Interest Declaration.

C.3 Schedule C - Declaration by Bidder - Price

Tender Reference:	RFT No. 26/2026
Tender Title:	Procurement of a Co-Managed Security Operations Centre (SOC) Service

We, the undersigned, submit our Price for the above project in accordance with the Specification prepared by FRCS.

The whole of the works shall be completed and carried out to the entire satisfaction of FRCS for the sum of [Insert amount in words and figures (VIP)].

Our Proposal shall be valid and remain binding upon us for the period of time specified in the Bid Data Sheet. We understand you are not bound to accept any Proposal you receive.

I, the undersigned, certify that I am duly authorized to sign this Proposal and bind it should FRCS accept this Proposal.

Authorized Representative Signature : _____

Authorized Representative Name : _____

Designation : _____

Company Name : _____

Date : _____

[Bidders official stamp/seal]

The Client reserves the right to accept or reject any proposal, and to annul the procurement process at any time prior to contract award, without thereby incurring any liability to the affected proposer(s).

Annex D — Glossary

Term	Meaning
SOC	Security Operations Centre — function delivering monitoring, detection and response
SIEM	Security Information and Event Management — platform for log collection, correlation and alerting
MDR	Managed Detection and Response
EDR	Endpoint Detection and Response
SOAR	Security Orchestration, Automation and Response
WAF	Web Application Firewall
TPOS / NTIS	Taxpayer Online Service / National Tax Information System
ASYCUDA World	Automated System for Customs Data — customs platform
TaxCore / VMS	VAT Monitoring System
IMO / SE	Information Management Office / System Engineering (FRCS teams)
MTTD / MTTR	Mean Time To Detect / Mean Time To Respond
AusCERT	Australian-based Computer Emergency Response Team (Pacific-region engagement)

— End of Terms of Reference —