Anti-Corruption Commission

REQUEST FOR PROPOSALS

Reference Number: (IUL)123-P/123/2026/62

Request for Proposals: Provision of Managed Cybersecurity Services (LOT 1 – LOT 4)

Anti-Corruption Commission

CONTENTS

1. BACKGROUND AND OBJECTIVES

1.1 Introduction

The Anti-Corruption Commission (hereinafter referred to as the **"Client"** or **"ACC"**) seeks to procure managed cybersecurity services and platforms to strengthen the security, integrity and resilience of its information systems and data.

ACC processes highly sensitive case information, complaints, investigation data, financial and personal records. Protecting this data from cyber threats, insider risks and data leakage is critical to the effective discharge of the Commission's mandate and for maintaining public trust.

To achieve this, ACC intends to engage a qualified service provider to supply, implement and support the following cybersecurity solutions under **four (4) lots**:

- **LOT 1** – Managed XDR (MXDR) with ITDR & MDR Services
- **LOT 2** – SIEM / Monitoring & Observability Stack with L3 Support Services
- **LOT 3** – Privileged Access Management (PAM) & Database Activity Monitoring (DAM) Platform
- **LOT 4** – Edge security platform providing DNS, WAF, Bot Detection and DDoS Protection

1.2 Primary Objectives

The main objectives of this RFP are to:

a) Implement a robust **MXDR/XDR and MDR** capability for endpoints and identities, with at least **90 days** data retention on the XDR platform.
b) Establish a **central SIEM / monitoring and observability stack** for infrastructure, applications and security telemetry, with L3 support and long-term retention.
c) Deploy an integrated **PAM & DAM** platform to secure privileged access and database activity.
d) Supply and implement a managed **edge security platform** providing DNS, WAF, Bot Detection and DDoS protection for critical web applications.
e) Ensure the solutions are effectively integrated, monitored and supported by a qualified team with **certified incident responders**, SIEM/DevOps engineers and PAM/DAM specialists.
f) Ensure that all licences, subscriptions, maintenance and managed services procured under this RFP cover a continuous period of **three (3) years** from go-live, and that Bidders submit pricing **only for the full three-year period**.
g) Give preference, during evaluation, to Bidders who operate a **local Security Operations Center (SOC)** within the Maldives staffed with qualified **Incident Response (IR) engineers**, as an added advantage.

2. INSTRUCTIONS TO BIDDERS

2.1 General Information

2.1.1 Project

a) Provision of managed cybersecurity services and platforms for the Anti-Corruption Commission, covering LOT 1–4 as defined in Section 3.

2.1.2 Proposal

a) Prospective Bidders are invited to submit proposals for this Contract. The Proposal submitted by the Bidder will form the basis for contract negotiations and, ultimately, the signed Contract with the selected Bidder.

b) Bidders shall familiarise themselves with local conditions and take them into account when preparing their proposals.

c) ACC is not bound to accept any proposal and reserves the right to annul the selection process at any time prior to contract award, without thereby incurring any liability to any Bidder.

d) Each Bidder may submit only one proposal, either as a single entity or as a member of one (1) joint venture (JV). No company shall participate in more than one bid (whether individually or as part of a JV). Where a proposal contains alternative technical solutions, such alternatives shall be clearly indicated.

e) Bidders are required to submit proposals for all four (4) LOTs (LOT 1, LOT 2, LOT 3 and LOT 4). Partial bids that do not cover all LOTs will be rejected as non-responsive. Evaluation of eligibility, technical and financial scores will be based on the combined proposal covering all LOTs.

2.1.3 Eligibility of Bidders

a) This bidding process is open only to Bidders registered in accordance with the requirements stated in this RFP and the Bid Data Sheet.

b) The Bidder (whether a single entity or a joint venture) shall consist only of companies that are registered in the Maldives and classified as Small and Medium Enterprises (SMEs) in accordance with applicable Maldivian laws and regulations. Evidence of SME status (e.g., SME registration/certification) shall be submitted for each company forming the Bidder.

c) **Outsourcing** or **subcontracting** of any part of the services under this RFP is not permitted. All services must be delivered using the Bidder's own internal resources.

d) All personnel assigned to the Contract must be full-time employees of the Bidder (single entity or JV member). Independent contractors, freelancers, or third-party staff are not permitted.

e) These restrictions ensure compliance with **ACC's data security** and **NDA** requirements.

f) ACC may request evidence to verify full-time employment of proposed staff (salary slips, payroll records, employment contracts). Failure to comply may result in rejection or termination.

2.1.4 Fraud and Corruption

a) Bidders must maintain the highest ethical standards during the procurement and execution of the Contract.

b) ACC will reject a proposal or terminate a contract if the Bidder is found to have engaged in corrupt, fraudulent, collusive, coercive, or obstructive practices.

2.1.5 Joint Ventures (JV)

a) Bids may be submitted by a single SME company or a JV composed only of SMEs registered in the Maldives. No foreign or non-SME entities may participate.

b) All JV members shall be jointly and severally liable.

c) One member shall be appointed as Lead Partner, authorised to represent and bind all JV members.

d) Bids must include either a signed JV agreement or a signed letter of intent identifying members, Lead Partner, roles, responsibilities, and joint/several liability.

e) Personnel may be employed by any JV member, provided they are full-time employees and no work is outsourced outside the JV.

f) Eligibility, technical, financial and experience requirements apply to the JV collectively unless stated otherwise.

2.2 Bid Information Documents

2.2.1 Contents of Bidding Documents

a) The Bidding Documents comprise:
- Section 1: Background and Objective
- Section 2: Instructions to Bidders
- Section 3: Terms of Reference (ToR)
- Section 4: Bid Evaluation Methodology
- Section 5: Standard Proposal Forms & Compliance Sheets

b) Bidders are expected to examine all instructions, forms, terms and other information in the Bidding Documents. Failure to furnish all required information may result in rejection of the bid.

2.2.2 Bid Registration

a) The registration procedure is specified in Section 2.7 – Bid Data Sheet.

b) Only registered Bidders will receive clarifications or amendments issued by ACC.

2.2.3 Clarification of Bidding Documents

a) Bidders may request clarification of any part of the Bidding Documents within the timeframe specified in the Bid Data Sheet.

b) All requests for clarification and ACC responses will be communicated in writing to all registered Bidders. Bidders seeking clarification are required to submit their queries via email to: **procurement@acc.gov.mv** and Bidders are required to clearly state the reference number in the subject line of the email.

2.2.4 Amendment of Bidding Documents

a) ACC may amend the Bidding Documents at any time prior to the deadline for submission of bids.

b) Any addenda issued will form an integral part of the Bidding Documents and will be communicated in writing to all registered Bidders.

c) ACC may extend the bid submission deadline, if necessary, to allow Bidders a reasonable time to incorporate amendments.

2.2.5 Confidentiality of Bid Information

a) All documents and information supplied by ACC to Bidders in connection with this RFP are to be treated as confidential.

2.2.1 Contents of Bidding Documents

a) The Bidding Documents comprise:

- Section 1: Background and Objective
- Section 2: Instructions to Bidders
- Section 3: Terms of Reference (ToR)
- Section 4: Bid Evaluation Methodology
- Section 5: Standard Proposal Forms & Compliance Sheets

b) Bidders are expected to examine all instructions, forms, terms and other information in the Bidding Documents. Failure to furnish all required information may result in rejection of the bid.

b) The Bidder shall not disclose such information to third parties or use it for purposes other than preparation of the proposal, without ACC's prior written consent.

2.2.6 Security and Guarantee

a) Advance Payment:

If the total value of the submitted bid exceeds MVR 250,000 (Two Hundred and Fifty Thousand Maldivian Rufiyaa), and the party contracted to perform the work, service (excluding consultancy), or supply materials requests an advance payment within a maximum of 45 (forty-five) days from the date of the award, an amount not exceeding 15% (fifteen percent) of the total value may be released as an advance.

Deductions shall be made from the invoices submitted, at a rate not less than the proportion of the advance payment granted, until the total amount provided as an advance is fully recovered.

The advance payment shall only be released to the contracted party performing the work, service (excluding consultancy), or supplying materials upon the submission of an advance payment guarantee equal to the value of the advance payment. This advance payment guarantee must be issued by a bank or financial institution registered under the relevant laws of the Maldives, or by a bank or financial institution that has a corresponding banking arrangement with such an entity.

b) **Bid Security:**

Bidders are required to submit a Bid Security of MVR 40,000.00 (Forty Thousand Maldivian Rufiyaa) for this Proposal.

The duration of the bid security must be at least **06 months** from the date of bid submission.

The bid security must be a document issued by a bank or financial institution registered under the relevant laws of the Maldives, or by a bank or financial institution that has a corresponding banking arrangement with such an entity. Cheque will not be accepted as bid security.

c) Performance Guarantee:

If the total price submitted by the winning bidder exceeds MVR 500,000 (Five Hundred Thousand Maldivian Rufiyaa), a performance guarantee set at 4% (four percent) of the total submitted price must be provided on the day the agreement is

signed and the work is handed over. The performance guarantee must be a document issued by a bank or financial institution registered under the relevant laws of the Maldives, or by a bank or financial institution that has a corresponding banking arrangement with such an entity. Cheque will not be accepted as a performance guarantee.

The duration of the performance guarantee must not be shorter than the entire period of the project, starting from the date the agreement is signed. Failure to submit the performance guarantee shall be treated as a refusal to accept the contract.

If this Commission decides to terminate the contract for any reason, or if the contractor abandons the work for any reason, the Commission reserves the right to forfeit the funds specified in the performance guarantee as state revenue.

2.3 Preparation of Bids

2.3.1 Language

a) The proposal shall be written in **English or Dhivehi**. Documents in any other language shall be accompanied by an English translation.

2.3.2 Documents Comprising the Bid

a) Bidders shall submit bid documents using the forms and formats provided in Section 5.

b) Proposals should preferably be typewritten or computer generated. Hand-written alterations, corrections or overwriting may result in rejection.

c) Bids shall include all documents listed in the Submission Checklist (Section 5.9).

2.3.3 Bid Price

a) The bid price shall be quoted in the Bid Submission Form (Section 5.1) and must match the total price stated in the Financial Proposal (Section 5.4).

b) Prices shall be firm and not subject to escalation during the bid validity or Contract period, except where explicitly allowed under the Contract.

2.3.1 Language	a) The proposal shall be written in **English or Dhivehi**. Documents in any other language shall be accompanied by an English translation. c) Prices shall include all applicable taxes and fees and represent the complete financial obligation of ACC. d) All prices shall be quoted in **Maldivian Rufiyaa (MVR).** e) All licences, subscriptions, maintenance and managed services offered under this RFP shall be valid for a continuous period of three (3) years from go-live. Bidders shall submit only the total price for the full three (3) year period for the LOTs. ACC does not require separate 1-year or 2-year pricing.
2.3.4 Bid Validity Period	a) Bids shall remain valid for a minimum period of **six (6) months** after the deadline for bid submission as stated in the Bid Data Sheet.

2.4 Submission of Bids

2.4.1 Submission	a) The method, address, and deadlines for submission (including any phased/electronic and hardcopy submissions) are specified in the Bid Data Sheet (Section 2.7).
2.4.2 Late Bids	a) Any bid received by ACC after the deadline for submission prescribed in the Bid Data Sheet will be rejected and returned unopened.

2.5 Bid Evaluation

2.5.1 Clarification of Bids	a) During evaluation, ACC may request clarification from Bidders. b) Requests and responses shall be in writing, and no change in the bid price or substantial change in the technical content shall be permitted.
2.5.2 Preliminary Examination of Bids	a) ACC will examine the bids to determine whether they are complete, properly signed, and substantially responsive. b) ACC may correct purely arithmetical errors. If the Bidder does not accept the correction, its bid will be rejected.

c) ACC may waive minor nonconformities, provided such waiver does not prejudice or affect the ranking of any Bidder.

d) Bids that do not provide a complete proposal and pricing for all four (4) LOTs (LOT 1, LOT 2, LOT 3 and LOT 4) shall be rejected and will not proceed to Technical Evaluation.

2.5.3 Evaluation and Comparison of Bids

a) ACC shall evaluate and compare substantially responsive bids in accordance with Section 4 – Bid Evaluation Methodology.

b) ACC is not required to accept the lowest-priced bid and may consider overall value and quality.

2.5.4 Contacting ACC

a) Bidders shall not contact ACC on matters relating to their bid during the evaluation process, except in response to ACC requests for clarification.

b) Any attempt by a Bidder to influence ACC's decision may result in rejection of the bid.

2.5.5 Rejection of Bids

a) ACC reserves the right to accept or reject any or all bids, and to annul the bidding process, without thereby incurring any liability to the affected Bidder(s).

2.6 Award of Contract

2.6.1 Award Criteria

a) Subject to the stated evaluation methodology, ACC will award the Contract to the Bidder whose bid has been determined to be substantially responsive and achieves the highest combined Technical and Financial score, based on the combined proposal covering all LOTs.

2.6.2 Notification of Award

a) Prior to expiry of the bid validity period, ACC shall notify the successful Bidder in writing that its bid has been accepted, subject to contract negotiations (if any).

b) ACC shall promptly notify other Bidders of the outcome.

2.6.3 Negotiations and Award

a) Negotiations may cover the Terms of Reference, timelines, methodology and special conditions.

b) Where negotiations fail to result in an acceptable agreement, ACC may terminate the negotiations and invite the next ranked Bidder.

2.6.1 Award Criteria	a) Subject to the stated evaluation methodology, ACC will award the Contract to the Bidder whose bid has been determined to be substantially responsive and achieves the highest combined Technical and Financial score, based on the combined proposal covering all LOTs.
2.6.4 Signing of Contract	a) ACC shall send the final Contract to the successful Bidder after notification of award. b) The Contract shall be signed within the period specified by ACC.

2.7 Bid Data Sheet

Ref	Item	Description
2.7.1	Publication Date	30th June 2026
2.7.2	Registration Deadline	09 July 2026 & Time:15:00 hrs and for registration, please use the link below. Link: https://forms.office.com/r/hRfihW4smV
2.7.3	Clarification Deadline	Date: 12 July 2026 & Time: 15:00 hrs. Email address for queries: procurement@acc.gov.mv and Bidders are required to state the **reference number** in the subject line of the email.
2.7.5	Bid Submission	Date: 14 July 2026 & Time: 10:00 hrs Bid submission at Anti-Corruption Commission, 7th floor, M.Finifaru,Majeedhee Magu, Male' City,Maldives.

3. TERMS OF REFERENCE (TOR)

3.1 Introduction

ACC invites proposals from eligible local service providers to supply, implement and support integrated cybersecurity solutions and managed services under four LOTs.

3.2 Objectives

The selected service provider shall:

a) Provide robust protection against malware, ransomware, identity-based attacks and data exfiltration.

b) Enable centralised logging, monitoring, detection and response with long-term retention.

c) Implement strong privileged access and database activity controls.

d) Provide skilled and certified incident responders, SIEM/DevOps engineers and PAM/DAM engineers to support ACC throughout the Contract.

e) Provide licences, subscriptions and support services valid for three (3) years from go-live, priced as a single 3-year total per LOT.

f) Where available, leverage a local Security Operations Center (SOC) within the Maldives staffed with Incident Response engineers to improve response times and collaboration, which will be considered an added advantage in evaluation.

3.3 Scope of Work (By LOT)

Bidders are required to bid for all four (4) LOTs. Partial bids for selected LOTs only are not permitted.

3.3.1 LOT 1 – Managed XDR (MXDR) with ITDR & MDR Services

3.3.1.1 Brief Description	Supply, implement and support an enterprise-grade MXDR/XDR platform and Managed Detection and Response (MDR) service with Identity Threat Detection and Response (ITDR) for a minimum of 150 endpoints (servers and workstations), with at least 90 days online/searchable data retention.All MXDR/XDR licences, subscriptions and MDR services under LOT 1 shall be valid for, and

	priced for, a continuous period of three (3) years from go-live. Vendors shall submit only a single three-year total price for LOT 1.
3.3.1.2 Platform Technical Requirements – LOT 1	(Full detail in Compliance Sheet – LOT 1. Summary:) a) Licences/subscriptions for at least 150 endpoints. b) Platform recognised as a Leader in a major analyst report (e.g. Gartner MQ for EPP/EDR/XDR) for at least 3 consecutive years. c) AI-driven prevention, detection and response against malware, ransomware, fileless and zero-day threats. d) Cloud-based management console with potential on-prem/sovereign option. e) ITDR capabilities (credential theft, privilege abuse, lateral movement, anomalous identity behaviour). f) 24x7 MDR services via SOC. g) Remote incident containment (isolation, process termination, approved scripts). h) Minimum 90 days online/searchable retention for telemetry and alerts. i) Unified console for policy, triage, hunting and reporting. j) API integration with SIEM (LOT 2), PAM/DAM (LOT 3) and ticketing/messaging tools.
3.3.1.3 Implementation & Service Requirements – LOT 1	a) Minimum three (3) Incident Response Engineers available locally in Maldives. b) At least **two (2)** successful deployments of **300 endpoints** or more for an enterprise-grade MXDR/XDR platform. c) Proof that Bidder is an authorised incident response / managed services partner for the proposed platform. d) MDR runbook with severity definitions, SLAs, escalation paths, communication channels and reporting templates. e) Administrator training, knowledge transfer sessions and full documentation.

f) All incident responders, SOC analysts and engineers assigned to LOT 1 shall be full-time employees of the Bidder (single entity or JV member). Outsourcing or use of third-party personnel is not permitted, in line with ACC's strict data security and NDA requirements.

g) Bidders that operate a local SOC within the Maldives staffed with IR engineers and propose to use this SOC for ACC services will be viewed favourably and may be awarded additional marks under the Technical Evaluation.

3.3.2 LOT 2 – SIEM / Monitoring & Observability Stack & L3 Support Services

3.3.2.1 Brief Description

Design, implement and support a SIEM / monitoring and observability stack based on a scalable search-and-analytics platform, providing observability, case management, alerting, threat hunting and ML-based analytics, with L3 support and multi-year data retention.All SIEM/monitoring stack licences, subscriptions and L3 support services under LOT 2 shall be valid for, and priced for, a continuous period of three (3) years from go-live. Vendors shall submit only a single three-year total price for LOT 2.

3.3.2.2 Platform Technical Requirements – LOT 2

The proposed SIEM / monitoring stack shall, at a minimum, meet the following requirements (detailed in the Compliance Sheet – LOT 2):

a) Search & Analytics Core

i. Ingest, index and visualise logs and metrics from servers, network devices, security platforms and applications.

ii. Provide interactive dashboards, search and analytics for security and operational use cases.

b) Observability – Logs, Metrics, APM & Uptime

i. Provide integrated observability capabilities covering logs, metrics and traces.

ii. Provide Application Performance Monitoring (APM) features, including distributed tracing, error rate monitoring, latency, throughput and service dependency/service map views.

iii. Provide uptime / availability monitoring, including endpoint and URL checks, synthetic probes and alerting on unavailability or degraded performance.

iv. Provide infrastructure metrics monitoring (CPU, memory, disk, network, etc.) and correlation with logs and APM data.

v. Provide unified dashboards and alerting across logs, metrics, APM and uptime (similar to the capabilities available in leading observability platforms such as Elastic Observability – APM, Uptime, Metrics, Logs, etc., or equivalent).

c) Alerting, Case Management & Threat Hunting

i. Rule-based and behavioural alerting with correlation rules and notifications.

ii. Case management for investigations, with linkage to underlying events/logs.

iii. Threat hunting with flexible queries and dashboards.

iv. ML/advanced analytics for anomaly and outlier detection.

d) Integration, Security & Data Retention

i. Secure integration with LOT 1 (MXDR) and LOT 3 (PAM/DAM) for central visibility and correlation.

ii. Role-based access control (RBAC), audit logging and integration with identity providers (SSO/LDAP/MFA).

iii. The stack must support hot, warm and archive data tiers, with policy-based movement of data between tiers.

iv. The solution must provide an effective data retention period of at least three (3) years across these tiers (hot + warm + archive).

v. The archive tier shall support storage of data in encrypted object storage (e.g. S3-compatible or equivalent), using encryption-at-rest and key management compliant with ACC's security policies.

vi. The solution must support automatic deletion / purge of data once the configured archive retention period expires, to enforce data lifecycle and privacy requirements.

e) Hardware & Deployment Architecture

i. The SIEM/search & analytics cluster shall be deployed on a minimum of two (2) physical nodes to provide high availability.

ii. Each node shall have at least 256 GB RAM and 64 CPU cores, and provide 10 TB usable SSD storage (after RAID) for SIEM data, with additional SSD disks configured as hot spares.

iii. Storage shall be on enterprise-grade SSDs with appropriate RAID, with redundant power supplies and network interfaces.

iv. The SIEM / monitoring stack shall be deployed on bare-metal servers (no shared multi-tenant environment) within ACC's designated environment or as agreed with ACC.

v. Core SIEM / observability components (e.g. data ingestion, indexing, API, UI) shall be deployed as containers, managed via a container orchestration platform (e.g. Kubernetes or equivalent) to support horizontal scalability, rolling upgrades and high availability.

vi. The architecture shall support future scale-out by adding additional nodes and/or container instances with minimal downtime.

3.3.2.3 Implementation & Service Requirements – LOT 2

a) The Bidder shall assign at least **one (1) dedicated SIEM / monitoring engineer** with hands-on experience deploying and operating the proposed search/analytics-based monitoring stack.

b) The Bidder shall assign at least **one (1) DevOps engineer** with demonstrable experience in container orchestration (e.g. Kubernetes or equivalent), CI/CD and operating data analytics / search clusters.<br)

c) The Bidder shall assign at least **one (1) cybersecurity engineers / analysts** with proven experience in threat hunting, security monitoring and incident investigation using SIEM or equivalent tools.

d) The Bidder shall provide L3 support services for the monitoring stack with defined SLAs for incident response and performance tuning.

e) The Bidder shall provide documentation, runbooks and basic user training for ACC IT/security staff.

f) All engineers and support staff providing SIEM / monitoring and L3 support services shall be full-time employees of the Bidder (single entity or JV member). Outsourcing or use of third-party personnel is not permitted, in line with ACC's strict data security and NDA requirements.

3.3.3 LOT 3 – Privileged Access Management & Database Activity Monitoring (PAM & DAM)

3.3.3.1 Brief Description

Supply, implement and support an integrated PAM & DAM platform to manage privileged access, secure credentials, monitor privileged sessions and perform real-time database activity monitoring.All PAM & DAM licences, subscriptions and support services under LOT 3 shall be valid for, and priced for, a continuous period of three (3) years from go-live. Vendors shall submit only a single three-year total price for LOT 3.

3.3.3.2 Platform Technical Requirements – LOT 3

(Full detail in Compliance Sheet – LOT 3. Summary:)

a) PAM & DAM platform and licences appropriate for ACC.

b) Centralised secure credential vault with rotation and approval workflows.

c) Agentless, outbound-only connectivity (no inbound firewall rules, VPNs or endpoint agents).

d) Built-in masking and tokenisation of sensitive data; no third-party masking tools.

e) Single unified platform for PAM, DAM, authorisation and audit.

f) Just-in-Time (JIT) access and time-bound approvals.

g) Secure vendor and break-glass access with full auditing.

h) Least-privilege policies for users and workloads.

i) Real-time DAM across hybrid/multi-cloud with policy-based responses.

j) Tamper-evident audit logs and export.

k) Session recording and keystroke logging.

l) Integration with SSO/MFA and SIEM.

m) SOC 2 Type II (or equivalent) for underlying platform.

3.3.3.3 Implementation & Service Requirements – LOT 3

a) At least **one (1) engineer** with hands-on deployment experience in the proposed PAM & DAM solution.

b) Bidder is an authorised partner for the proposed PAM & DAM platform.

c) Team includes at least one (1) engineer with relevant security certifications **(e.g. CISA, eCPPT, vendor PAM certs).**

d) Configuration of initial policies, roles, connectors and integrations.

e) Training and handover documentation (as-built diagrams, runbooks).

f) All PAM & DAM engineers, consultants and other technical staff assigned to LOT 3 shall be full-time employees of the Bidder (single entity or JV member). Outsourcing or use of third-party personnel is not permitted, in line with ACC's strict data security and NDA requirements.

g) The Bidder shall have successfully implemented and supported a PAM and/or DAM solution for at least one (1) government ministry/agency or state-owned enterprise based in the Maldives. The Bidder shall provide a reference letter or completion certificate (in English or Dhivehi) including the client name, brief description of scope, duration and a contact person (name, designation, email/phone) for verification.

3.3.4 LOT 4 – Edge security platform providing DNS, WAF, Bot Detection and DDoS Protection

3.3.4.1 Brief Description

Supply, implement and support an integrated edge security platform providing DNS, web application firewall (WAF), bot detection/management and DDoS protection to secure and accelerate ACC's critical web applications and public-facing services. All edge security platform licences, subscriptions and support services under

LOT 4 shall be valid for, and priced for, a continuous period of three (3) years from go-live. Vendors shall submit only a single three-year total price for LOT 4.

3.3.4.2 Platform Technical Requirements – LOT 4

(Full detail in Compliance Sheet – LOT 4. Summary)

a) Edge security platform and licences appropriate for ACC, providing integrated DNS, WAF, bot detection/management, CDN/caching and DDoS protection for internet-facing services.

b) Anycast, highly-available authoritative DNS with low-latency resolution, support for standard record types (A/AAAA/CNAME/TXT, etc.) and management via web console and API.

c) WAF with built-in protection against OWASP Top 10 and common web exploits, including virtual patching, geolocation controls, IP reputation filtering and custom rule sets.

d) Always-on L3–L7 DDoS detection and mitigation for web applications, with automatic attack detection and rate-based protection to maintain availability during volumetric and application-layer attacks.

e) Bot detection and management capabilities to distinguish between legitimate automation and malicious bots, including support for challenge/response, JavaScript and behavioural challenges.

f) TLS termination with support for modern cipher suites and protocols, automated certificate lifecycle management and support for both platform-managed certificates and customer-provided certificates.

g) Fine-grained security policies (per hostname, path, API, application) with support for rate limiting, IP lists, geofencing, header-based rules and API protection.

h) Centralised logging with export of DNS, WAF, bot and DDoS events to ACC's SIEM/SOC via API, syslog or supported log streaming mechanisms.

i) Role-Based Access Control (RBAC) for authentication.

j) High-availability, globally distributed cloud architecture with no dependency on inbound VPNs or on-premises appliances for core protection functions.

k) Detailed analytics and reporting for traffic, performance, security events and policy effectiveness, with configurable dashboards for ACC operations and management teams.

3.3.4.3 Implementation & Service Requirements – LOT 4

a) At least one (1) engineer with hands-on deployment experience in the edge security platforms (DNS, WAF, DDoS, bot management) assigned to the project.

b) Project team to include at least one (1) engineer holding relevant security/network certifications (e.g. web security certs, network/security professional certs).

c) Design and configuration of initial DNS, WAF, DDoS and bot management policies, including migration of existing DNS zones if required, definition of security rules and performance/caching policies for all in-scope applications.

d) Development and execution of a cutover and rollback plan to transition ACC's applications to the new edge security platform with minimal downtime and validated rollback procedures.

e) Integration with ACC's SIEM/SOC tooling for centralised log ingestion and alerting.

f) Comprehensive testing, including functional, performance and security validation (e.g. test attacks, failover tests) prior to go-live, with documented test results.

g) Training and handover for ACC technical and operations staff, including as-built diagrams, configuration documentation, runbooks and incident response playbooks related to the edge security platform.

h) All engineers, consultants and other technical staff assigned to LOT 4 shall be full-time employees of the Bidder (single entity or JV member). Outsourcing or use of third-party personnel is not permitted, in line with ACC's strict data security and NDA requirements.

i) The Bidder shall have successfully implemented and supported an edge security and/or WAF/DNS protection solution for at least two (2) government ministry/agency or state-owned enterprise based in the Maldives, and shall provide a reference letter or completion certificate (in English) including client name, brief scope, duration and contact person for verification.

3.4 Deliverables and Tasks

Key deliverables include:

a) Detailed solution designs and architecture documents for all LOTs.

b) Configured and operational MXDR, SIEM/observability, PAM/DAM and Edge Security platforms.

c) Integration with ACC's existing systems and infrastructure.

d) Runbooks and procedures for operations and incident handling.

e) Training of ACC staff and knowledge transfer.

f) Periodic reports on security incidents, system performance and service levels.

3.5 Engagement Period

a) Implementation and go-live for the awarded LOT(s) shall be completed within three (3) months from the date of Contract signing.

b) All licenses, subscriptions, maintenance and managed services (including MDR, SIEM L3 support, PAM & DAM and Edge Security platform) shall be valid and provided for a continuous period of three (3) years from the go-live date of each LOT.

c) Bidders shall therefore quote only the total three-year price for the LOTs.

3.6 Data Security, Confidentiality & Staffing Requirements

a) Due to the highly sensitive nature of ACC data (including complaints, investigations, case files and related information), the successful Bidder shall comply with all data security policies, procedures and controls prescribed by ACC.

b) The successful Bidder shall sign a Non-Disclosure Agreement (NDA) with ACC prior to accessing any ACC systems or data.

c) All personnel of the Bidder (single entity or JV) who will have access to ACC systems or data shall be full-time employees of one of the JV member companies and shall be bound by the Bidder's internal confidentiality obligations and codes of conduct.

d) Outsourcing, subcontracting or off-loading of any part of the services to external entities or individuals is strictly prohibited. No external contractors, consultants or third-party resources may be assigned to work on ACC systems or data under this Contract.

e) These measures are required to ensure that the selected firm operates within a controlled and auditable environment that meets ACC's strict data security requirements and NDA obligations, and to minimize the risk of unauthorized disclosure or misuse of ACC information.

f) ACC may, at its discretion, request salary slips / payroll evidence and employment documentation to verify that the personnel proposed and deployed under this Contract are full-time employees of the Bidder (single entity or JV member), in line with the no-outsourcing requirement and ACC's strict data security and NDA obligations.

4. BID EVALUATION METHODOLOGY

4.1 Overview

Proposals will be evaluated in **two stages**:

a) **Technical Evaluation** – maximum **70 marks**
b) **Financial (Price) Evaluation** – maximum **30 marks**

Only Bidders achieving at least **60 marks out of 70** (85% of technical marks) in the Technical Evaluation will proceed to Financial Evaluation.

The Technical and Financial evaluation is conducted on the **combined proposal across LOT 1, LOT 2, LOT 3 and LOT 4**.

4.2 Compliance Evaluation

ACC will first verify that:

a) All required forms and documents listed in the Submission Checklist (Section 5.9) are provided.
b) Bid Submission Form, Bid Declaration Form, Litigation History and Financial Proposal are completed.
c) Legal and registration documents (company registration, SME evidence, GST certificate, etc.) are provided.
d) The bid includes **complete technical and financial proposals for all four LOTs**.

Bidders satisfying these requirements will be considered for Technical Evaluation.

4.3 Technical Evaluation (70 Marks)

4.3.1 Technical Passing Mark

- Maximum Technical Score: **70 marks**
- Minimum passing score: **60 marks** (85% of 70)
- Only Bidders scoring **≥ 60/70** are considered for Financial Evaluation.

The Technical Score is calculated on the **combined proposal across LOT 1, LOT 2, LOT 3 and LOT 4**, and the Bidder must demonstrate adequate compliance and capability for **each LOT**; failure to meet the mandatory requirements of any LOT may result in disqualification.

4.3.2 Technical Evaluation Matrix

Category	**Sub-Criteria**	**Max Marks**
A. Technical Requirements Coverage & Compliance	A1. Functional compliance with LOT requirements (all LOTs)	35
	A2. Solution design, integration & alignment with ToR	5
B. Firm Experience & References	B1. Experience in similar projects (MXDR/MDR, SIEM/observability, PAM/DAM, WAF)	10
	B2. Client references & proof of successful delivery	5
C. Technical Team Qualifications & Experience	C1. Certified incident responders / SOC team and local SOC capability	10
	C2. Other key technical experts (SIEM, DevOps, PAM & DAM) & overall team experience	5
TOTAL TECHNICAL	—	70

4.3.3 Technical Requirements Coverage & Compliance (40 Marks)

a) A1 – Functional Compliance (35 marks):

compliance is assessed as follows:

• **Compliant (5 marks):**
The proposed solution fully meets the stated requirement in terms of functionality, performance, and operational relevance to ACC's cybersecurity needs.

•**Partially Compliant (2 marks):**
The proposed solution meets the requirement to a limited extent or through alternative methods, but does not fully satisfy the functional or operational intent of the requirement.

• **Not Compliant (0 marks):**
The proposed solution does not meet the requirement, or the required functionality/service is unavailable or unsupported.

• Based on the Bidder's completed Technical Requirements Compliance Sheets (Section 5.10) for each LOT and the Technical Proposal.

• Assessment of how comprehensively the proposed solutions meet or exceed all mandatory and relevant requirements. b) A2 – Solution Design, Integration & Alignment (5 marks).

• Assessment of overall architecture; integration between LOT 1–4; data and log flows; incident handling; security controls; retention strategy.

4.3.4 Firm Experience & References (15 Marks)

a) B1 – Experience in Similar Projects (10 marks)

• Evidence of previous projects in MXDR/MDR, SIEM/observability and PAM/DAM (especially in government/regulatory/high-security environments).

b) B2 – Client References (5 marks)

• Strength and relevance of at least three (3) reference letters or completion certificates.

4.3.5 Technical Team Qualifications &

a) C1 – Certified Incident Responders / SOC Team and Local SOC (10 marks)

Experience (15 Marks)	• Number and relevance of certified incident responders and SOC analysts dedicated to this project and MDR service. • The existence of a fully operational local SOC within the Maldives staffed with IR engineers, and its proposed use for ACC services, will be considered an added advantage and may result in higher scores within this sub-criterion. b) C2 – Other Key Technical Experts & Team (5 marks) • Qualifications and experience of SIEM / observability engineers, DevOps engineers, PAM/DAM engineers and Project Manager/Team Lead across the LOTs.

4.4 Financial (Price) Evaluation (30 Marks)

4.4.1 Eligibility for Financial Evaluation

Only Bidders that achieve a minimum Technical score of 60/70 are considered for Financial Evaluation.

4.4.2 Price Scoring

a) Maximum Financial Score: 30 marks.

b) The lowest evaluated price among technically qualified Bidders will receive 30 marks.

c) Other technically qualified Bidders receive a score in proportion to their price

$$\text{Financial Score} = \frac{\text{Lowest Evaluated Price}}{\text{Price of Bid Under Consideration}} \times 30$$

d) The evaluated price shall be based on the grand total three-year cost of ownership for all four (4) LOTs combined (including all licences/subscriptions, implementation, MDR, SIEM/observability L3

support, PAM & DAM support, training, maintenance and all applicable taxes).

e) Bidders shall quote a single three-year total price per LOT and a single three-year grand total price covering LOT 1, LOT 2, LOT 3 and LOT 4. All four LOTs must be priced; bids that omit any LOT will be rejected.

f) Separate 1-year or 2-year prices are not required.

5. STANDARD PROPOSAL FORMS & COMPLIANCE SHEETS

5.1 Bid Submission Form

Standard cover form – Bidder name (single entity or JV), address, contact details, LOTs (1–4), total 3-year price per LOT, grand total, authorized signature, validity, etc.

5.2 Bid Declaration Form

Declaration about correctness of information, acceptance of RFP terms, absence of conflict of interest, etc.

5.3 Litigation History

Table for disclosure of any litigation/arbitration during last 5 years.

5.4 Financial Proposal Form

Instructions to Bidders

Bidders shall provide an itemised cost breakdown per LOT showing:

- One-time implementation / setup costs; and
- A **single three (3) year total price** for all licences/subscriptions and all support/managed services for that LOT.

The Financial Proposal shall clearly indicate:

- The **three-year total price per LOT**, and
- The **grand three-year total price covering LOT 1, LOT 2, LOT 3 and LOT 4**.

Bidders **must** submit pricing for **all four (4) LOTs**. Financial Proposals that do not include a three-year price for any one of the LOTs will be considered **non-responsive**.

Sample Table

LOT	**Description**	**3-Year Total Price (MVR)**
LOT 1	MXDR with ITDR & MDR	_____

LOT 2	SIEM / Monitoring & Observability Stack & L3 Support	_____
LOT 3	PAM & DAM Platform	_____
LOT 4	Edge Security Platform	
Grand Total (LOT 1 + LOT 2 + LOT 3 + LOT 4)	—	_____

5.5 Company / Bidder Information

Basic company profile, registration details, SME evidence, shareholding, contact person information, and for JV: list of all member SMEs and Lead Partner.

5.6 Details of Completed/Ongoing Contracts of Similar Nature

Table for project name, client, description (MXDR/SIEM/Observability/PAM/DAM), scale, value, duration, contact person, etc., plus reference letters.

5.7 CVs of Key Experts

Instructions for providing CVs and copies of certifications for Project Manager, SOC/IR staff, SIEM engineer, DevOps engineer, PAM/DAM engineer(s), threat hunters.

5.8 Technical Proposal Format

Suggested structure:

- Executive Summary
- Proposed Architecture & Integration Across LOTs
- Requirement Compliance Matrix (mapping to Section 5.10)
- SLAs and Service Model (MDR, SIEM/observability L3 support, PAM/DAM support, Edge Security Platform support)
- Implementation Plan & Timeline (3 months to go-live)
- **Staffing Plan** (confirming all staff are full-time employees of a JV member; roles for IR, SIEM, DevOps, PAM/DAM, Edge Security Platform)
- Description of any **local SOC** in Maldives and how it will be used for ACC
- Training & Knowledge Transfer Plan
- Risk Management & Mitigation

5.9 Submission Checklist

Example checklist (Bidders to tick):

- ☐ Bid Submission Form (5.1)
- ☐ Bid Declaration Form (5.2)
- ☐ Litigation History (5.3)
- ☐ Financial Proposal (5.4)
- ☐ Company / Bidder Information (5.5)
- ☐ Details of Similar Contracts (5.6) and reference letters
- ☐ CVs and certifications of Key Experts (5.7)
- ☐ Technical Proposal (5.8)
- ☐ Completed Compliance Sheets for LOT 1, LOT 2, LOT 3 & LOT 4 (5.10)
- ☐ Company Registration Certificate(s) for all JV members
- ☐ SME Registration / Certification for all JV members
- ☐ GST Registration Certificate (if applicable)
- ☐ Tax Clearance / any other required statutory documents
- ☐ Bid Security (2.2.6)

5.10 Technical Requirements Compliance Sheets (with Tick Boxes)

Instruction to Bidders:
For each LOT, complete the corresponding Compliance Sheet.

- Tick **one** option only per requirement (☐ Compliant / ☐ Partially Compliant / ☐ Not Compliant).
- If "Partially Compliant" or "Not Compliant" is selected, provide explanation and reference to your Technical Proposal.

5.10.1 LOT 1 – MXDR with ITDR & MDR Services

Technical Requirements Compliance Sheet

Bidder Name: _____

LOT 1 – Managed XDR (MXDR) with ITDR & MDR Services

Platform Requirements

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Reference
L1.1	Provide an enterprise-grade commercial MXDR/XDR platform licences/subscriptions for a minimum of **150 endpoints** (servers & workstations).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.2	Proposed MXDR/XDR platform recognised as a **Leader** in a major analyst report (e.g. Gartner MQ for EPP/EDR/XDR) for at least **3 consecutive years**.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.3	AI-driven prevention, detection & response for malware, ransomware, fileless attacks & zero-day threats.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.4	Cloud-based management console with option for future on-prem/sovereign deployment.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.5	Support **Identity Threat Detection & Response (ITDR)** (credential theft, privilege abuse, lateral	Y	☐ Compliant ☐ Partially Compliant	

	movement, anomalous identity behaviour).		☐ Not Compliant	
L1.6	Provide **24x7 MDR** services via SOC monitoring alerts from the MXDR/XDR platform.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.7	MDR service supports **remote incident containment** actions (network isolation, process termination, script execution) as approved by ACC.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.8	Provide **minimum 90 days online/searchable telemetry retention** for MXDR/XDR data; optional extended retention may be proposed.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.9	Unified console for policy management, alert triage, threat hunting & reporting.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.10	API-based integration with ticketing systems, SIEM (LOT 2), PAM/DAM (LOT 3) and messaging tools.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Implementation & Service Requirements – LOT 1

Ref	**Requirement**	**Mandatory (Y/N)**	**Bidder Compliance (tick one)**	**Remarks / Proposal Reference**
L1.11	MDR service provides a minimum of **five (5) Incident Response Engineers** available locally in Maldives.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.12	Bidder has at least **two (2) successful deployments** of 3**00 endpoints or larger** for enterprise-grade MXDR/XDR.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.13	Bidder is an **authorised incident response / managed services partner** for the proposed MXDR/XDR vendor.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.14	Structured onboarding & knowledge transfer plan (admin training, IR	Y	☐ Compliant	

	matrix & SLAs, communication channels, implementation QA) will be provided.		☐ Partially Compliant ☐ Not Compliant	
L1.15	All incident responders, SOC analysts and engineers assigned to ACC shall be **full-time employees of the Bidder** (single entity or JV member) (no outsourced resources).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L1.16	Bidder operates a **local SOC within Maldives** staffed with IR engineers and proposes to use it to deliver services to ACC. *(Added advantage – non-mandatory)*	N	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

5.10.2 LOT 2 – SIEM / Monitoring & Observability Stack & L3 Support

Technical Requirements Compliance Sheet

Bidder Name: _____

LOT 2 – SIEM / Monitoring & Observability Stack & L3 Support Services

Platform & Functional Requirements

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Reference
L2.1	Monitoring stack capable of ingesting, indexing & visualising logs/metrics from servers, network devices, security platforms & applications.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.2	Support observability for infrastructure metrics, application performance & log analytics in a unified interface.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.3	Provide **Application Performance Monitoring (APM)**, including traces, error rates, latency, throughput and service dependency/service map views.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.4	Provide **uptime / availability monitoring**, including endpoint/URL checks and synthetic probes with	Y	☐ Compliant ☐ Partially Compliant	

	alerting on unavailability or degraded performance.		☐ Not Compliant	
L2.5	Provide integrated dashboards and alerting that correlate **logs, metrics, APM and uptime** data (similar to leading observability platforms such as Elastic Observability or equivalent).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.6	Provide **case management** capability for investigations linked to relevant logs & events.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.7	Rule-based & behavioural alerting with configurable thresholds, correlation rules & notification channels.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.8	**Threat hunting** capabilities using flexible queries & dashboards.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.9	ML / advanced analytics for anomaly & outlier detection.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.10	Support multi-tenant or logically separated views (e.g. production vs test).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.11	Provide secure RBAC, audit logging & integration with identity provider (SSO/LDAP/MFA).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.12	Integrate with **LOT 1 MXDR** and **LOT 3 PAM/DAM** for central visibility & correlation.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

L2.13	SIEM / monitoring stack supports **hot, warm and archive data tiers** with policy-based movement of data between tiers.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.14	Solution provides an **effective data retention period of at least three (3) years** across hot, warm and archive tiers.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.15	Archive data tier can be stored in **encrypted object storage** (e.g. S3-compatible or equivalent) with encryption-at-rest and appropriate key management.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.16	System supports **automatic deletion / purge** of data after the configured archive retention period expires, enforcing data lifecycle policies.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Hardware & Deployment Requirements

Ref	**Requirement**	**Mandatory (Y/N)**	**Bidder Compliance (tick one)**	**Remarks / Proposal Reference**
L2.17	SIEM / search & analytics cluster is deployed on **a minimum of two (2) physical nodes** to provide high availability.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.18	**Each node** has at least **256 GB RAM**, **64 CPU cores** and provides **10 TB usable SSD storage** (after RAID) for SIEM data, with additional SSD disks configured as **hot spares**.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.19	Storage is provided on enterprise-grade SSDs with appropriate RAID configuration, and servers include redundant power supplies and network interfaces.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.20	SIEM / monitoring stack is deployed on **bare-metal servers** (no shared multi-tenant environment) within	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

	ACC's designated environment or as agreed with ACC.			
L2.21	Core SIEM / observability components (e.g. ingestion, indexing, API, UI) are deployed as **containers**, managed via a **container orchestration platform** (e.g. Kubernetes or equivalent) to support horizontal scalability and rolling upgrades.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.22	The architecture supports future **scale-out** by adding additional nodes and/or container instances with minimal downtime.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Implementation & Service Requirements – LOT 2

Ref	**Requirement**	**Mandatory (Y/N)**	**Bidder Compliance (tick one)**	**Remarks / Proposal Reference**
L2.23	Bidder will assign at least **one (1) dedicated SIEM / monitoring engineer** with hands-on experience deploying and operating the proposed search/analytics-based monitoring stack.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.24	Bidder will assign at least **one (1) DevOps engineer** with demonstrable experience in **container orchestration (e.g. Kubernetes or equivalent)** and operating **data analytics / search clusters**.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.25	Bidder will assign at least **one (1) cybersecurity engineer / analyst** with proven experience in **threat hunting, security monitoring and incident investigation** using SIEM or equivalent tools.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.26	Bidder will provide **L3 support services** for the monitoring stack with defined SLAs for incident response & performance tuning.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L2.27	Bidder will provide documentation, runbooks & basic user training for ACC IT/security staff.	Y	☐ Compliant ☐ Partially Compliant	

			☐ Not Compliant	
L2.28	All engineers and support staff providing SIEM / monitoring and L3 support services are **full-time employees of the Bidder** (single entity or JV member) (no outsourced resources).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

5.10.3 LOT 3 – PAM & DAM Platform

Technical Requirements Compliance Sheet

Bidder Name: _____

LOT 3 – Privileged Access Management & Database Activity Monitoring

Platform Requirements

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Reference
L3.1	Provide proposed PAM & DAM platform and associated licences/subscriptions suitable for ACC.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.2	Support centralised, secure credential vault with password rotation & approval workflows.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.3	Platform is **agentless** and operates using **outbound-only connectivity** (no inbound firewall rules, VPNs or endpoint agents).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.4	Provide **built-in data masking & tokenisation** of sensitive data as native features (no third-party masking tools).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.5	Delivered as a **single unified platform** for PAM, fine-grained	Y	☐ Compliant	

	app/data authorisation, DAM & central audit under one console.		☐ Partially Compliant ☐ Not Compliant	
L3.6	Support **Just-in-Time (JIT) access** with time-bound approvals & automatic privilege revocation; integrated approvals via email/Teams/Slack or similar.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.7	Provide secure vendor & break-glass access using credential abstraction, with full auditing of sessions & actions.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.8	Support **least-privilege** policies for human users, workload identities & automation/AI identities within one policy framework.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.9	Provide **real-time DAM** across hybrid & multi-cloud with policy-based detection and responses (alert, block, mask, tokenise).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.10	Support cloud & on-prem deployment, connecting via outbound-only connectivity (no site-to-site VPNs or inbound internet).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.11	Provide **tamper-evident audit logs** for privileged sessions, DB activity, policy changes, approvals & JIT workflows with export in standard formats.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.12	Underlying platform (incl. any SaaS control plane) holds an active **SOC 2 Type II or equivalent** attestation.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.13	Support session recording, monitoring & keystroke logging for privileged sessions with searchable playback.	Y	☐ Compliant ☐ Partially Compliant	

			☐ Not Compliant	
L3.14	Provide RBAC, policy-based approvals & integration with identity providers (SSO, MFA).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.15	Provide dashboards & reports for privileged activity, DB activity & compliance reporting.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Implementation & Service Requirements – LOT 3

Ref	**Requirement**	**Mandatory (Y/N)**	**Bidder Compliance (tick one)**	**Remarks / Proposal Reference**
L3.16	At least **one (1) engineer** with hands-on experience deploying the proposed PAM & DAM platform in enterprise environments.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.17	Bidder is an **authorised partner** for the proposed PAM & DAM platform.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.18	Implementation team includes at least **one (1) engineer** with security certifications (e.g. CISA, eCPPT, vendor PAM certs) or equivalent.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.19	Bidder will configure initial policies, roles, connectors & integrations as agreed with ACC.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.20	Bidder will deliver admin/operator training and provide full handover documentation & runbooks.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

L3.21	All PAM & DAM engineers, consultants and technical staff assigned to ACC are **full-time employees of the Bidder** (single entity or JV member) (no outsourced resources).	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L3.22	Bidder has successfully implemented and supported a **PAM and/or DAM solution** for at least **one (1) government ministry/agency or state-owned enterprise based in the Maldives**, and will provide a reference letter or completion certificate with contact details.		☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

5.10.4 LOT 4 – Edge Security Platform

Technical Requirements Compliance Sheet

Bidder Name: _____

LOT 4 – Edge security platform providing DNS, WAF, Bot Detection and DDoS Protection

Platform Requirements

Ref	Requirement	Mandatory (Y/N)	Bidder Compliance (tick one)	Remarks / Proposal Reference
L4.1	Provide an integrated, enterprise-grade, cloud-delivered edge security platform including authoritative DNS, WAF, bot detection/management and DDoS protection for ACC's internet-facing services.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.2	Provide highly-available Anycast authoritative DNS with low-latency resolution, support for common DNS record types (A/AAAA/CNAME/TXT, etc.) and management via web portal and API.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.3	Provide a WAF with built-in protection against OWASP Top 10 and common web exploits, including virtual patching, IP reputation filtering, geolocation-based controls and custom rule sets.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.4	Provide always-on L3–L7 DDoS detection and mitigation for web applications, with automatic attack detection and rate-based protection to maintain service availability during volumetric and application-layer attacks.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.5	Provide bot detection and management capabilities to distinguish between legitimate automation and malicious bots, including support for challenge/response, JavaScript and behavioural challenges.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

L4.6	Support TLS termination at the edge with modern cipher suites/protocols, automated certificate lifecycle management and support for both platform-managed and customer-provided certificates.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.7	Support fine-grained security policies (per hostname, path, API, application) including rate limiting, IP allow/deny lists, geofencing, header-based rules and API protection features.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.8	Provide centralised logging and export of DNS, WAF, bot and DDoS events to ACC's SIEM/SOC via API, syslog or supported log streaming mechanisms.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.9	Provide Role-Based Access Control (RBAC) for administrative users, with granular roles for authentication.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.10	Provide detailed analytics and reporting for traffic, performance, security events and policy effectiveness, with configurable dashboards for ACC operations and management teams.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

Implementation & Service Requirements – LOT 4

Ref	**Requirement**	**Mandatory (Y/N)**	**Bidder Compliance (tick one)**	**Remarks / Proposal Reference**
L4.11	Assign at least **one (1) engineer** with hands-on deployment experience in the proposed edge security platform (DNS, WAF, DDoS, bot management) to the project.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.12	Project team to include at least one (1) engineer holding relevant	Y	☐ Compliant	

	security/network certifications (e.g. web security certifications, network/security professional certifications).		☐ Partially Compliant ☐ Not Compliant	
L4.13	Design and configure initial DNS, WAF, DDoS and bot management policies for all in-scope applications, including migration of existing DNS zones and definition of security and performance/caching policies.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.14	Develop and execute a cutover and rollback plan to transition ACC's applications to the new edge security platform with minimal downtime and validated rollback procedures.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.15	Integrate the platform with ACC's SIEM/SOC tooling for centralised log ingestion and alerting.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.16	Perform comprehensive testing (functional, performance and security, including representative attack simulations and failover testing) prior to go-live, and provide documented test results.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.17	Provide training and handover for ACC technical and operations staff, including as-built diagrams, configuration documentation, runbooks and incident response playbooks related to the edge security platform.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	
L4.18	All engineers, consultants and technical staff assigned to ACC under this LOT shall be full-time employees of the Bidder (single entity or JV member). Outsourcing or use of third-party personnel is not permitted.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

L4.19	Bidder shall have successfully implemented and supported an edge security and/or WAF/DNS protection solution for at least one (1) government ministry/agency or state-owned enterprise in the Maldives, and shall provide a reference letter or completion certificate (in English or Dhivehi) including client name, scope, duration and contact person.	Y	☐ Compliant ☐ Partially Compliant ☐ Not Compliant	

BID SUBMISSION FORM

Tender Reference Details

Tender Title:

Reference Number:

Bidder Information

Business Name:

Address:

Phone Number:

Email Address:

Business Registration Number:

Financial Offer and Validity

LOT	**Description**	**3-Year Total Price (MVR)**
LOT 1	MXDR with ITDR & MDR	
LOT 2	SIEM / Monitoring & Observability Stack & L3 Support	
LOT 3	PAM & DAM Platform	
LOT 4	Edge Security Platform	
Grand Total (3 Years) MVR (including GST):	—	
Grand Total Amount in Words:		

Bid Validity Period (Bids shall remain valid for a minimum period of six (6) months):

Authorized Signatory

Name of Authorized Signatory:

Title / Designation:

ID Ca‌rd Number:

Signature:

Date:

Company Stamp / Seal:

BID DECLARATION FORM

Bid Reference No: .....

Project / Procurement Title: .....

1. Bidder Details

Name of Bidder (Individual / Company): .....

Business Registration Number: .....

Address: .....

Telephone Number: .....

Email Address: .....

2. Declaration

- We have examined and fully understood the bidding documents and instructions issued by the Anti-Corruption Commission.
- All information provided in this bid is true, accurate, and complete.
- We confirm that we are not bankrupt, in liquidation, blacklisted, or in conflict of interest.
- We agree to be bound by the bid and accept all conditions stated in the bidding documents.
- We acknowledge that false or misleading information may result in disqualification or legal action.

3. Authorized Signatory

Name: .....

Designation: .....

National ID / Passport No: .....

Signature: .....

Date: .....

Company Seal: .....