FAQ's

Provision of IT Audit Services.

1. Police Certificate Requirement

Police certificates would apply only to the staff deployed for the audit engagement and is to be submitted only after contract is awarded.

Intent: to ensure integrity and suitability of personnel by accessing sensitive IT environments of the company.

2. Clarification on "Monitoring Capability Details"

This refers to the bidder's internal audit methodologies — such as tools, approaches, and processes used to ensure quality and consistency. It does not refer to cybersecurity or system monitoring services. This engagement is not related to cybersecurity/SOC monitoring.

Intent: to ensure the vendor is capable of conducting a structured and controlled audit.

3. Evaluation Criteria – Experience (40%)

The TOR specifies that a bidder must have completed a minimum of three (3) relevant projects to be eligible. This minimum does not represent the full score.

Intent: To ensure that bidders have prior experience conducting IT audits of similar nature and can demonstrate capability, exposure, and understanding of comparable environments.

Mandatory:

- Three projects - Yes, mandatory for minimum eligibility
- Additional projects - Not mandatory, but add value and influence scoring

Scoring Formula:

Experience will be evaluated comparatively using the following proportional scoring method:

- Experience Score = (Vendor's Number of Relevant Projects ÷ Highest Number Submitted among all Bidders) × 40

This allows bidders with more experience to score proportionately higher.

4. Bid Submission Protocol in Case of Connectivity Failure

A contact number will be provided via email together with the bid submission meeting link. Vendors must contact the number to report any issues before the submission time. The meeting will begin 10 minutes prior to the submission time, so issues must be communicated before the submission time. The meeting will be held online via Microsoft Teams, with the screen shared throughout, and proposals will be opened during the meeting once all proposals are received.

Intent: fairness and equal opportunity for all bidders, and continuity.

5. Evaluation Criteria - Team Qualifications (20%)

Meeting the minimum certification requirements provides the baseline score of 10 points.

Intent: To ensure the team has essential foundational knowledge and professional credibility.

Additional relevant certifications will be scored at 5 points each, up to a maximum of two additional certifications (total 10 points).

Relevant certification:

CISA, CISM, CISSP, ISO/IEC 27001 Lead Auditor/Implementer, ITIL, Security+, CySA+, CEH, CCNA.

6. Definition of "Similar Scale"

Refers broadly to organizations with similar operational, system, or service complexity. Must meet at least one comparable criterion such as (but not limited to):

- Organizations with nationwide services
- 24/7 service operations
- Multi-site environments

Intent: to ensure bidders have handled environments of comparable complexity.

7. Optional Services

Optional services represent value-added offerings bidders may propose.

Intent: to allow bidders to propose enhancements without affecting mandatory evaluation.

8. Scope and Environment Details

a) Number and type of sites in scope (HQ, data centre(s), DR site, branches, third-party locations, etc.).

The audit scope covers Aasandha's IT operations, which include headquarters functions, core IT facilities (including data centre and disaster recovery arrangements), and selected operational locations, as relevant to the audit objectives. Specific site details will be confirmed during the planning phase after awarding to the winning party.

b) High-level inventory of:

i) Servers (physical/virtual)

ii) Databases and major business applications

iii) Network devices (firewalls, routers, switches, wireless controllers, etc.)

iv) Endpoints/users in scope

v) CCTV cameras and detector systems in scope

The Aasandha's IT environment includes a mix of physical and virtual servers, business-critical applications, databases, network and security infrastructure, end-user devices, and supporting systems such as CCTV and detectors. Detailed inventories will be made available during engagement execution.

c) Details of any cloud services to be included (e.g. O365, Azure, AWS, SaaS platforms).

We do have cloud and software-as-a-service platforms, which may be reviewed where relevant to ensure IT governance, access management, and risk, in line with the TOR scope. Specifics will be provided to the winning party.

d) Clarification on in-scope vs out-of-scope systems, subsidiaries, or vendors.

The scope of the audit is limited to what is defined in the TOR.

Systems and third-party services that support Aasandha's IT operations may be reviewed at a high level for governance and control purposes only.
Specific systems and detailed areas of review can be confirmed during the audit planning phase.

e) For in-house software development:

i) Approximate number of applications to be assessed

ii) Main technology stacks (web, mobile, APIs, databases, etc.)

iii) Whether secure code review and/or application vulnerability testing is expected

The audit is to review governance, SDLC processes, change management, and control mechanisms for internally developed systems. Secure code review, vulnerability testing, or penetration testing are not included under this IT Audit and not mentioned in the TOR.

9. Depth of Testing and Methodology Expectations

a) Whether vulnerability scanning of servers, endpoints, and network devices is expected, in addition to configuration review.

As per given TOR, vulnerability scanning is not required under this IT Audit. Focus is to be on configuration review, controls, governance, and compliance.

b) Whether web application, API, or mobile application security testing is required.

Application security testing is out of scope.

c) Confirmation if the focus is purely on configuration/compliance review or whether penetration testing is also in scope.

Penetration testing, exploitation, or adversarial testing activities are explicitly excluded from this engagement.

d) Any additional regulatory or local standards that must be considered.

The audit may consider applicable local regulatory requirements and recognized international best practices relevant to IT governance and controls.

e) Preferred risk rating model or confirmation that we may use our own standard (e.g. High/Medium/Low with defined criteria).

The auditor may apply their standard risk rating methodology.

f) Whether social engineering, phishing simulations, or staff awareness checks are included or explicitly excluded.

Social engineering exercises, phishing simulations, and staff testing are out of scope.

10. Documentation and Information Availability

a) Availability of the following documents at the start of the engagement:

i) IT and information security policies and procedures

ii) Network diagrams and data flow diagrams

iii) IT asset register (hardware, software, licenses)

iv) IT/enterprise risk register

v) Business Continuity Plan and Disaster Recovery Plan, including any defined RTO/RPO

vi) Previous IT/cybersecurity audits and penetration test reports, including status of recommendation implementation

b) Confirmation of whether these documents will be available before fieldwork begins or after the kick-off meeting.

The scope of this engagement includes review of IT governance. Therefore, it is the auditor's responsibility to check the existence and adequacy of related policies and procedures. Any required documents, (where available), including diagrams, asset registers, logs, and previous audit or assessment reports will be shared to the extent they exist, following commencement of the engagement and during the relevant phases.

11. On-Site Work and Logistics

We understand that all assessment and configuration review work must be performed on-site and that remote access is not permitted. In that context, please confirm:

a) Exact location(s) where the team will work.

b) Standard working hours and whether after-hours or weekend work is permitted for production-impacting activities.

c) Availability of:

i) A dedicated workspace for the audit team

ii) Network access for our laptops and security tools

iii) Facilities for temporary secure storage of exported logs/configuration files, if required

On-site audit activities will be conducted at designated Aasandha facilities as required. Standard working hours (0800 to 1600 hrs/weekdays) will apply, unless otherwise coordinated. A dedicated workspace maybe provided if requested.

d) Policy regarding:

i) Use of our own assessment tools and scripts within your environment

ii) Any restrictions on copying data/logs outside the environment (e.g. for offline analysis)

Logical access to IT facility (accompanied by a staff member from Company side) to be provided as necessary. Use of tools, scripts, or data extraction should be subject to prior notification/approval. Offsite storage of data or logs to be permitted with explicit authorization.

e) Any security induction, background checks, or specific access procedures required for our team.

Security inductions and access protocols will be communicated prior to fieldwork.

12. Deliverables, Format, and Review Process

a) Confirmation of the required deliverables, for example:

i) Detailed IT Audit report with findings and recommendations

ii) Executive summary for senior management/Board

iii) Risk heatmaps or maturity assessments, if desired

iv) Remediation roadmap with prioritisation and indicative timelines

b) Whether interim reports or periodic issue logs are required during fieldwork.

c) Expectations regarding presentations:

i) Number and type of presentations (technical vs executive)

ii) Audience (management, Board, Audit Committee, etc.)

d) Expected review cycle:

i) Draft report, comment period, and final report timelines

ii) Indicative time frame for management feedback on the draft.

Deliverables are clearly stated in the TOR. Auditors can use their own formats. Interim updates may be requested during fieldwork. At least one management-level presentation of findings is expected. Additional presentations may be requested, where necessary.

13. Project Timeline and Milestones

The TOR specifies a three-month duration from commencement. To plan resources effectively, kindly confirm:

a) Expected or target commencement date post-contract award.

b) Any hard deadlines for:

i) Completion of fieldwork

ii) Submission of the draft report

iii) Submission/presentation of the final report

c) Expected response times from your side for information requests, document reviews, and meeting scheduling.

Commencement date and detailed milestone timelines to be agreed with the successful bidder following contract award, once the bidder produces the proposed timeline to the Company

14. Commercial and Contractual Considerations

a) Confirmation that a fixed-price model for the full engagement is preferred, and whether you would like us to state explicit scope assumptions (e.g. maximum number of locations/systems).

Should quote a price for the full engagement.

b) Payment terms and preferred milestone structure.

Payment will be made after completion of the project. Prior to submitting the invoice, the final audit report must be shared with Aasandha Company.
The invoice may be submitted only after Aasandha Company has verified the final report and formally acknowledged that all required components of the audit have been completed.

c) Treatment of travel and accommodation (included in the lump sum or reimbursable).

All costs related to the engagement must be included in the proposed lump-sum price.

d) Any requirements regarding professional indemnity insurance and liability limitations.

e) Whether you use a standard contract template, and if there are any key clauses we should be aware of (e.g. IP ownership of deliverables, data protection obligations, confidentiality requirements).

A contract draft will be shared in adherence to the terms and in alignment with the TOR, and will be further discussed with the awarded party prior to commencement

15. Team Composition and Eligibility Requirements

a) Confirmation that only full-time employees of our firm may be deployed and whether:

i) Remote subject-matter experts (who do not access systems but review documents/deliverables) are permitted.

b) Any minimum onsite team size or minimum level of effort you expect to see in the proposal.

The core audit work is expected to be conducted by the bidder's proposed audit team. All proposed staff must be full-time employees of the company; outsourcing is not permitted.

No specific minimum team size is mentioned; bidders should propose a team appropriate to the scope and complexity of the assignment.