TERMS OF REFERENCE FOR

PROVISION OF IT AUDIT SERVICES FOR AASANDHA COMPANY LTD

Subject: TOR IT Audit Services 2025

Ref: **ASND/GA/IUL/2025/37**

Date: 26th November 2025

BACKGROUND

Aasandha Company Limited requires the services of a qualified and experienced firm to conduct an independent Information Technology (IT) Audit.

The purpose of this audit is to evaluate the effectiveness of the company's IT governance, risk management, internal controls, and operational efficiency.

The audit will be conducted in accordance with International Standards on Auditing (ISA), and other relevant frameworks such as ISO 27001.

OBJECTIVES

- The key objectives of this IT Audit are to:
- Assess the adequacy and effectiveness of IT governance, control, and compliance frameworks.
- Evaluate IT risk management practices and the effectiveness of mitigation controls.
- Review IT processes for efficiency, cost-effectiveness, and alignment with Aasandha's strategic objectives.
- Identify gaps and provide recommendations for improvement.

SCOPE OF WORK

The scope of the IT Audit will cover the following key areas:

1. Review of IT Governance Framework and Alignment with Business Strategy

Evaluate the overall IT governance structure to determine whether roles, responsibilities, decision-making authorities, and accountability mechanisms are clearly defined and effectively aligned with Aasandha's organizational strategy.

The review will include:

- Existence and adequacy of IT policies and procedures.
- Alignment of IT objectives and performance indicators with strategic and operational goals.
- Effectiveness of IT planning, budgeting, and project prioritization processes.
- Communication and reporting mechanisms between IT management and executive leadership.

2. Assessment of IT Risk Management Practices and Mitigation Measures

Assess the effectiveness of IT risk management processes implemented within the environment.

The audit will examine:

- Existence of an IT risk register and methodology for identifying, assessing, and prioritizing risks.
- Risk ownership, tracking, and escalation mechanisms.
- Mitigation measures for key risks such as cybersecurity, data integrity, business continuity (IT related), and system availability.
- Integration of IT risk management with enterprise-wide risk management frameworks.

3. Evaluation of Access Management and Data Protection Controls

Verify the adequacy and effectiveness of controls designed to protect access to critical systems, data, and information assets.

The review will include:

- Access provisioning and de-provisioning procedures, segregation of duties, and privilege management.
- Periodic user access reviews and approval workflows.
- Password and authentication policies (MFA, complexity, renewal frequency).
- Data classification and retention mechanisms and compliance with data protection regulations.
- Access restrictions for sensitive systems.

4. Review of Change Management, Software Update, and Version Control Processes

Examine processes governing system or application changes to ensure they are properly decided, tested, implemented, and documented.

The review will cover:

- Formal change management policy and process ownership.
- Evidence of change request approvals, test results, and rollback plans.
- Version control mechanisms for internally developed or customized software.
- Patch and update management processes to ensure timely application of vendor updates.
- Segregation of duties between development, testing, and deployment environments.

5. Assessment of Business Continuity (IT related) and Disaster Recovery Documentation and Testing

Review the adequacy of business continuity and disaster recovery plans related to IT operations.

The audit will assess:

Existence and completeness of Business Continuity (BCP) and Disaster Recovery (DRP) documents.

- Defined recovery objectives (RTO, RPO) and supporting backup strategies.
- Periodic testing and simulation exercises to validate readiness.
- Communication and escalation procedures during incidents.
- Post-incident reviews and updates to plans based on lessons learned.
- Reporting and analysis of recurring issues to inform process improvements.

6. Verification of Asset Management

Assess whether Aasandha maintains an accurate and updated inventory of IT assets.

The review will include:

Completeness and accuracy of IT asset registers, including hardware, software, and licenses.

- Controls for asset acquisition, movement, disposal, and protection.

7. Validation of Implementation of Recommendations from Cybersecurity Assessments

Review the actions taken by IT and management in response to recommendations made under prior cybersecurity assessments or penetration tests.

The audit will verify:

- Status of recommendations.
- Effectiveness of corrective measures and remaining residual risks.
- Integration of cybersecurity assessment outcomes into IT governance and continuous improvement processes.

8. Review of Physical Environment Controls

Evaluate the adequacy and security of the physical IT environment, including server rooms, power, and cooling systems.

The review will assess:

- Physical access control to infrastructure.
- Compliance with environmental and safety standards.

9. Review of Cabling and Infrastructure Management

Evaluate cable management practices and infrastructure organization for safety, reliability, and documentation accuracy.

The audit will assess:

- Proper labeling, routing, and maintenance of network cabling.
- Adherence to cabling standards and data center setup best practices.
- Documentation and change tracking of network infrastructure.

10. Review of CCTV and Detector Systems

Examine the configuration, placement, and management of CCTV and environmental detector systems supporting IT facilities.

The audit will review:

- Adequacy of coverage, recording duration, and data retention policies.
- Integration of surveillance and detector systems (fire, temperature, motion) with IT infrastructure monitoring.
- Security and maintenance of recorded data.

11. Review of Data and Network Access Management & Privilege Escalation Controls

Assess how access rights to systems and network resources are managed, approved, and reviewed.

The review will cover:

- Enforcement of least privilege and segregation of duties.
- Controls for privilege escalation and unauthorized access attempts.
- Monitoring and audit trails of administrative access.

12. Review of IT Resource Allocation and Workforce Utilization

Evaluate how IT human resources and technical assets are allocated in relation to operational workload and organizational needs.

The audit will assess:

- Appropriateness of staffing levels and skill distribution.
- Alignment between assigned resources and company priorities.
- Effectiveness of task prioritization, performance monitoring, and workload balance to support service delivery.

13. Review of In-house software development process

- Assess the governance and controls over internally developed applications
- Verify adherence to secure coding standards and documentation requirements
- Evaluate processes for
    - Requirement gathering and approvals
    - Development environment security and segregation
    - Code review and test procedures
    - Version controls and release management
    - Check compliance with data protection and cyber security standards during development
    - Review post-deployment monitoring and maintenance

DELIVERABLES

The audit shall deliver:

- Comprehensive IT Audit Report with findings, recommendations, and management comments.
- Executive summary highlighting governance, risk, and compliance maturity levels.

DURATION

The duration of the engagement will be three (3) months from the date of commencement.

CONFIDENTIALITY

- The selected firm must sign a non-disclosure agreement with Aasandha Company Limited.
- All information obtained during the engagement shall be treated as strictly confidential and used solely for audit purposes.

REPORTING

The firm will report to the Internal Auditor from the Company as a primary focal who will facilitate further engagements on request.

ELIGIBILITY REQUIREMENTS

Vendors must comply with all of the following mandatory requirements:

- **REGULATORY & LEGAL COMPLIANCE**
    - Must submit a valid SME Certificate.
    - All proposed staff must be full-time employees of the company; outsourcing is not permitted.
    - Must submit valid business registration and current tax clearance certificates.
    - Must be willing to sign non-disclosure and confidentiality agreements.

- **TECHNICAL & CAPABILITY REQUIREMENTS**

    - All assessment and configuration work must be performed on-site at Aasandha premises. Remote VPN or direct access into Aasandha's core systems will not be permitted.
    - Must provide certifications of the members of engagement team.
    - Must provide a minimum of three (3) verifiable client references, preferably from companies of similar scale.
    - Delivery team must include a minimum of three (3) professionals with:
    - At least one Consultant with CISA or ISO 27001 Auditor/Implementer certification.

PROPOSAL SUBMISSION REQUIREMENTS

Proposals **must** include the following:

1. **Company Profile** – including ownership, organizational structure, and years of operation.
2. **Evidence of Compliance** – SME certificate, police certifications, tax clearance, monitoring capability details.
3. **Relevant Experience** – details of at least three completed similar projects, with contactable references.
4. **Team Details** – CVs, certifications, and roles of proposed staff members (IT engineers, auditors and consultants clearly indicated).
5. **Deliverables and Timeline Confirmation** – aligned with relevant Section above.
6. **Commercial Proposal** – itemized pricing for the 3-month engagement, including any optional services.
7. **Declaration on Ethical Conduct and Fraud and Corruption** (filled and signed) - Anex 1

QUERIES

Please submit all queries or requests for clarification via email before **1400hrs, 07th December 2025** to:

Email: tender@aasandha.mv

Subject Header: Query on Audit Services

Unless notified by announcements or direct written communication, no changes will be allowed in the Bid Submission details or deadline.

REGISTRATION FOR BID

Vendors **must** send their Company name, contact person name, email, and number to tender@aasandha.mv before **03rd December 2025, 15:00hrs to register for the Bid submission.**

SUBMISSION OF BID PROPOSAL

Bid Submission Date: **10th December 2025**
Time: 10:00 HRS (via Microsoft Team)

Aasandha company will send a web meeting link to the provided email address for bid submission.

Vendors should send the bid document only when instructed to do so during the web meeting, via email to tender@aasandha.mv.

If the bid document exceeds 20MB in size, upload it to a cloud storage service (Google Drive, Dropbox, OneDrive) and share the link via email. Bid documents will not be accepted if the vendor does not attend the submission meeting or joins after the designated submission time

TERMS AND CONDITIONS

Consultant Access Control:

- Should it be required, Auditors will be provided only with the minimum required access (least privilege principle) on need basis.
- Access will be temporary, time-bound, and revoked immediately after contract completion.
- Remote connections into Aasandha's internal network are strictly prohibited.
- Access activities will be logged and monitored by Aasandha's IT team.

Vendor to declare at the start of work, the designated staff members of the company who would work in the project.

EVALUATION CRITERIA

Proposals will be evaluated on the following weighted criteria:

- **Price (40%)**
    - Competitive pricing and value for money.
    - Transparent breakdown of costs and services.
- **Experience (40%)**
    - Minimum of three (3) completed similar audits.
    - Strength and credibility of references provided.
- **Team Qualifications (20%)**

EVALUATION MATRIX

Criteria	**Weight**	**Scoring Guidelines**
Price	40%	Lowest-priced compliant proposal = highest score. Others scored proportionally.
Experience	40%	- 3 relevant projects = minimum compliance.
Team Qualifications	20%	- Meeting minimum certification requirements = baseline score.

Annex - 1

Declaration on Ethical Conduct and Fraud and Corruption

[The Bidder shall fill in and submit this form with the Bid]

We the undersigned confirm in the preparation of our Bid that:

1. Neither we, nor any of our employees, associates, agents, shareholders, consultants, partners or their relatives or associates have any relationship that could be regarded as a conflict of interest as set out in the Bidding Documents.

2. Should we become aware of the potential for such a conflict, will report it immediately to Aasandha Company Ltd.

3. That neither we, nor any of our employees, associates, agents, shareholders, partners, consultants or their relatives or associates have entered into corrupt, fraudulent, coercive or collusive practices in respect of our bid or proposal.

4. We understand our obligation to allow Aasandha Company Ltd to inspect all records relating to the preparation of our bid and any contract that may result from such, irrespective of if we are awarded a contract or not.

5. That no payments in connection with this procurement exercise have been made by us or our associates, agents, shareholders, partners or their relatives or associates to any of the staff, associates, consultants, employees, or relatives of such who are involved with the procurement process on behalf of Aasandha Company, Client or Employer.

6. We agree that Aasandha Company Ltd reserves the right to disqualify, suspend or terminate any contract or other arrangement between us and Aasandha Company ltd, with immediate effect and without liability, in the event it is discovered that we have submitted a fraudulent bid.

7. This declaration is in addition to, and does not replace or cancel, or operate as a waiver of, any terms of contractual arrangements between us and the Company.

Authorised Signature: _____

Name:

Title:

Company Stamp: