IT & CS Auditing Proposal

Version: 1.0

Date: 26-APRIL-2026

Prepared By:

Trusted Vision for Governance and Consultation

Contact Information

Please feel free to contact the following individuals for information about this document:

Name	Hashem Al-Azizi
Mobile Phone	+966-53-122-1580
Email	Hashem.azizi@trustedvision.biz
Address	Qurtuba District, Saeed Bin Zaid Street, Injaz Group Building, No. 6482, First Floor, P.O. Box: 13247 Riyadh, Kingdom of Saudi Arabia

TRUSTED VISION

Contents

1. Executive Summary of CLIENT's requirements

We are pleased to present this Technical Proposal in response to the Client's request for an independent IT and Cybersecurity Audit engagement. Our firm brings deep expertise in IT governance, systems assurance, and cybersecurity advisory , backed by a team of internationally certified professionals with a proven track record across government and regulated-sector clients in the Kingdom of Saudi Arabia and the wider region.

The objective of this engagement is to deliver an independent, risk-based assessment of the adequacy and operating effectiveness of the Client's IT governance framework, systems controls, and cybersecurity posture , benchmarked against leading international standards and applicable Saudi regulatory requirements, including e.g. **NCA ECC-2**, **SAMA CSF** (where applicable), **ISO/IEC 27001:2022**, **NIST CSF 2.0**, and the **Personal Data Protection Law (PDPL)**.

Our assessment will span eight defined control domains - from IT governance and access management through to ERP application controls and business continuity - providing the Client's management and Internal Audit function with:

- **Clear visibility** into the current state of IT and cybersecurity controls.
- **Risk-rated findings** classified as Critical, High, Medium, or Low - consistent with IIA standards and the Client's risk appetite.
- **Root cause analysis** for each identified gap, not merely a list of deficiencies.
- **Actionable recommendations** with ownership assignments, effort estimates, and a prioritized remediation roadmap.

We are committed to delivering this engagement with the highest standards of professional independence, objectivity, and confidentiality - and to ensuring that every output drives measurable improvement in the Client's security posture.

The audit aims to:

- Evaluate the design and operating effectiveness of IT and cybersecurity controls.

- Identify key risks, control gaps, and vulnerabilities across eight defined domains.
- Assess alignment with leading frameworks: e.g. COBIT 2019, ISO/IEC 27001:2022, NCA ECC-2, SAMA CSF, and PDPL where applicable.
- Provide practical, risk-rated, and implementable recommendations with a clear remediation roadmap.

We believe that our expertise in conducting similar IT and cybersecurity audits positions us among the leading professional services firms. Our value proposition is grounded in:

- Deep and in-depth expertise in designing and executing IT governance, access management, infrastructure security, and ERP controls reviews.
- A balanced mix of international and National expertise in regulatory compliance audit and consulting (ISO 27001, NCA ECC, SAMA CSF, PDPL).
- A rigorous, evidence-based audit methodology aligned with IIA standards, ISACA ITAF, and leading risk assessment frameworks.
- Effective project delivery - on time, on scope, and producing actionable outcomes for management.

2. Scope

The scope of this engagement covers, but is not limited to, the eight domains defined in the Request for Proposal. The table below summarizes the in-scope areas and specific control objectives for each:

#	Area	Scope Items
2.1	**IT Governance & Management**	IT organizational structure and roles; IT policies, procedures, and standards; IT strategy alignment with business objectives; IT risk management practices.
2.2	**Access Management (Logical Access Controls)**	User access provisioning and de-provisioning; role-based access and segregation of duties (SoD); privileged access management; periodic access reviews.

#	Area	Scope Items
2.3	IT Operations & Change Management	Change management processes (system changes, patches, releases); incident and problem management; IT service management practices.
2..4	IT Infrastructure & Security	Network security (firewalls, segmentation, VPNs); endpoint protection (antivirus, EDR); data protection controls; backup and recovery processes.
2.5	Cybersecurity Framework & Controls	Cybersecurity governance structure; security policies and standards; vulnerability management; penetration testing (optional scope).
2.6	Data Security & Privacy	Data classification and handling; data access controls; compliance with applicable regulations (e.g., PDPL).
2.7	Business Continuity & Disaster Recovery	IT disaster recovery planning; backup strategy and testing; business continuity integration.
2.8	Systems & Applications Controls (ERP Focus)	Key system controls (e.g., ERP environment such as Microsoft Dynamics); input, processing and output controls; interface and integration controls.

Note: Penetration testing (Section 3.5) is identified as optional scope. If included, it will be performed as a black-box or grey-box external/internal assessment and priced separately.

3. Audit Methodology and Approach

To address the Client's requirements, we have structured the audit approach into phases as follows:

1. Phase 0: Planning and engagement

This will include Establish scope, objectives, resources, timelines and logistics; obtain stakeholder buy-in and mobilize the audit team.

Audit Activities	Key Outputs / Evidence
Confirm scope boundaries - business units, systems, data flows, locations, and in-scope third parties.	**Agreed Scope Charter**
Identify applicable regulatory requirements (NCA, SAMA, PDPL) and benchmark frameworks (COBIT, ISO 27001, NCA ECC, CIS Controls).	**Regulatory & Framework Mapping**
Assemble audit team and assign roles: engagement partner, IT auditors, cybersecurity specialist, ERP auditor, BCP/DR specialist, data privacy analyst.	**Team Assignment Matrix**
Agree timelines, evidence-request list, sampling approach, communication plan, and stakeholder interviews schedule.	**Project Initiation Pack**
Issue formal evidence request: policies, asset registers, risk register, architecture diagrams, past audit reports, contracts, recent test results.	**Evidence Request List**
Schedule kick-off meeting, site visits (if applicable), and system access windows for technical testing.	**Kick-off Meeting Minutes**

2. Phase 1: Baseline Assessment (Level 1 focus)

Aims to verify existence and basic operation of foundational controls the following domains

3.1 IT Governance & Management

Audit Activities	Key Outputs / Evidence
Review IT organizational chart, roles, responsibilities, and reporting lines; assess alignment with business objectives.	**IT Org Structure Assessment**
Evaluate completeness and currency of IT policies, procedures, and standards against framworks (e.g. COBIT 2019 and ISO 27001 Annex A.	**Policy Inventory & Gap List**
Assess IT risk management practices - risk identification, risk register maintenance, and integration with enterprise risk.	**IT Risk Register Review**
Interview IT leadership to assess strategic alignment, investment governance, and change advisory board operations.	**Interview Workpapers**

3.2 Access Management (Logical Access Controls)

Audit Activities	Key Outputs / Evidence
Review user access provisioning and de-provisioning procedures; sample 25 joiners/movers/leavers from the past 12 months.	**Joiners/Movers/Leavers Sample**
Evaluate role-based access controls (RBAC) and perform SoD conflict analysis using access matrix or GRC tool.	**SoD Conflict Report**
Review privileged access management - admin account inventory, PAM tool usage, session recording, and approval workflows.	**PAM Control Assessment**
Inspect evidence of periodic access reviews (quarterly or semi-annual); assess completeness and sign-off process.	**Access Review Evidence**

Audit Activities	Key Outputs / Evidence
Test MFA enforcement on critical systems: VPNs, admin consoles, cloud portals, email (M365/Google Workspace).	**MFA Testing Workpapers**

3.3 IT Operations & Change Management

Audit Activities	Key Outputs / Evidence
Review change management policy and process - request, impact assessment, testing, approval, and rollback capability.	**Change Management Walkthrough**
Sample 30 changes (including emergency changes) from ITSM tool; verify evidence of approval, testing, and UAT sign-off.	**Change Sample Testing Workpapers**
Assess incident and problem management processes - incident log review, SLA compliance, root cause analysis practices.	**Incident Log Review**
Evaluate IT service management maturity against (e.g. ITIL) best practices (service catalogue, capacity, availability management).	**ITSM Maturity Assessment**

3.4 IT Infrastructure & Security

Audit Activities	Key Outputs / Evidence
Review network architecture diagrams; assess firewall rule sets, network segmentation, DMZ design, and VPN configurations.	**Network Security Review**

Audit Activities	Key Outputs / Evidence
Inspect endpoint protection deployment coverage - antivirus/EDR agent inventory, update status, exclusion policies.	**Endpoint Protection Assessment**
Evaluate data protection controls - encryption at rest and in transit, DLP policy and alerting, media handling procedures.	**Data Protection Control Review**
Review backup and recovery processes - backup schedule, retention, offsite/cloud storage, and restore test evidence.	**Backup & Recovery Assessment**
Assess patch management - scanning tool outputs, patching SLAs, critical/high vulnerability remediation evidence.	**Patch Management Review**

3.5 Cybersecurity Framework & Controls

Audit Activities	Key Outputs / Evidence
Assess cybersecurity governance structure - CISO reporting line, security committee charters, and board reporting.	**Governance Assessment**
Review security policies and standards against frameworks (e.g NCA ECC-2 and ISO 27001:2022 Annex A - identify gaps.	**Gap Assessment Report**
Evaluate vulnerability management programme - scan frequency, tooling (e.g.Tenable/Qualys), remediation tracking, SLAs.	**Vulnerability Management Review**
[Optional] Conduct external/internal penetration test (black-box or grey-box) on agreed in-scope assets.	**Penetration Test Report (Optional)**

3.6 Data Security & Privacy

Audit Activities	Key Outputs / Evidence
Review data classification policy and handling procedures; sample data assets to verify labelling and protection controls.	**Data Classification Assessment**
Assess data access controls - least privilege for sensitive data stores (databases, SharePoint, file shares, cloud storage).	**Data Access Control Review**
Evaluate PDPL compliance readiness - personal data inventory,ROPA, lawful basis, consent management, data subject rights, data breach procedures.	**PDPL Compliance Assessment**

3.7 Business Continuity & Disaster Recovery

Audit Activities	Key Outputs / Evidence
Review IT Disaster Recovery Plan (DRP) - scope, RTO/RPO targets, recovery procedures, BIA , BCP , and last review date.	**DRP& BCM Document Review**
Assess backup strategy - coverage, frequency, retention, immutability, and evidence of successful restore tests.	**Backup Strategy Assessment**
Review integration of IT DR requirements into the Business Continuity Plan (BCP); assess annual BCP/DR exercise evidence.	**BCP/DR Exercise Evidence Review**
Conduct a tabletop exercise scenario (ransomware or major system outage) with IT and business stakeholders.	**Tabletop Exercise Report**

3.8 Systems & Applications Controls (ERP Focus - Microsoft Dynamics)

Audit Activities	Key Outputs / Evidence
Review ERP (Dynamics) access controls - role assignments, admin accounts, SoD in financial modules (AP, AR, GL, payroll).	**ERP Access & SoD Review**
Assess input, processing, and output controls - interface reconciliation, batch job monitoring, error handling, audit trails.	**Application Controls Workpapers**
Evaluate interface and integration controls - API security, data validation, error logging for key system integrations.	**Integration Controls Assessment**
Review ERP change management - transport/deployment controls, approval workflows, and segregation of development/production.	**ERP Change Management Review**

3. Phase 2 : Operationalization & Effectiveness (Level 2 focus)

Aims to assess that controls are not only present but are operationalized, automated where appropriate, and effective in detection/prevention . examples according to the frameworks e.g.

Audit Activities	Key Outputs / Evidence
Review and test monitoring and detection capabilities - SIEM rules, alerting, log retention policies, and tuning evidence.	**SIEM & Detection Capability Review**
Evaluate vulnerability management effectiveness - patch prioritization rationale, SLA compliance, remediation ticket evidence.	**Vuln. Mgmt. Effectiveness Testing**
Review secure development lifecycle (SDLC) artefacts and code/security testing evidence for applications in scope.	**SDLC Controls Assessment**

Audit Activities	Key Outputs / Evidence
Test incident response readiness - examine past incidents, timelines, root-cause analysis; run one tabletop exercise.	**IR Readiness Report & Tabletop**
Deeper third-party risk review - due diligence questionnaires, security audit reports, SLA compliance, ongoing monitoring.	**Third-Party Risk Assessment**
Examine configuration management and deployment pipelines for security controls, hardening baselines, and rollback capability.	**Config & Pipeline Controls Review**
Re-performance tests: e.g. privileged account provisioning, restore from backup, vulnerability scan of sampled assets.	**Technical Re-Performance Evidence**

4. Phase 3: Maturity & Continuous Improvement (Level 3 focus)

Aims to assess whether the organization has mature practices: continuous measurement, threat-informed improvements, automation/orchestration and resilient operations.

Audit Activities	Key Outputs / Evidence
Review KPIs, security dashboards, and executive reporting - confirm continuous measurement and management oversight.	**KPI & Metrics Review**
Validate integration of threat intelligence into detection and response processes	**Threat Intelligence Assessment**
Evaluate advanced testing programme - red/blue/purple team exercises, continuous penetration testing, application security automation.	**Advanced Testing Programme Review**
Review programme governance for continual improvement - lessons-learned processes, investment prioritisation, repeatable remediation.	**Improvement Programme Assessment**

Audit Activities	Key Outputs / Evidence
Confirm demonstrable improvements over time - metrics trending, reduced MTTR, reduced critical vulnerability backlog.	**Performance Trending Evidence**

5. Phase 4: Reporting & Remediation Oversight

Deliver consolidated audit outcomes and ensure remediation planning and tracking.

Audit Activities	Key Outputs / Evidence
Consolidate Phase 1–3 findings into a single draft final report with executive summary and detailed technical appendices.	**Draft Final Audit Report**
Classify all findings (Critical, High, Medium, Low);	**Findings Register with Risk Ratings**
Propose remediation actions , assign proposed owners and target dates.	**Remediation actions**
Issue draft report to management and allow 10 business days for management responses and agreed remediation plans.	**Management Response Template**
Present findings to executive stakeholders and governance bodies (CISO, risk committee, board as required).	**Management Presentation (PowerPoint)**
Incorporate management responses into final report; issue signed final audit report.	**Final Audit Report**

4. Deliverables

The consultant will provide the following deliverables during the engagement:

#	Deliverable	Target Date	Trigger	Milestone
1	Phase 0 - Project Initiation Pack (Scope charter, test plan, stakeholder register, evidence request list)	Week 1	Kick-off meeting	**Project Initiation**
2	Phase 1 - Baseline Assessment Report (Governance, access, infrastructure, physical, third-party - Level 1)	Weeks 2–3	Fieldwork start	**Fieldwork**
3	Phase 2 - Operationalization Assessment Report (SIEM, vuln. mgmt., IR readiness, change mgmt., SDLC etc - Level 2)	Weeks 3–5	Phase 1 accepted	**Fieldwork**
4	Phase 3 - Maturity & Continuous Improvement Report (KPIs, threat intel, automation, ---)	Week 5	Phase 2 accepted	**Fieldwork**
5	Draft Final Report (Exec. summary, all findings, risk ratings, root causes, recommendations)	Week 5	Phase 4 complete	**Draft Report**
6	Management Presentation (Board/CISO deck with top risks and remediation roadmap)	Week 5	Draft accepted	**Presentation**
7	Final Report (Incorporating management responses and agreed remediation plans)	Week 6	Comments received	**Final Report**

5. Team Structure

The following specialists are proposed for this engagement. All team members hold relevant international certifications and have direct experience in IT and cybersecurity audit engagements:

#	Name	Role
1	Lead auditor	Lead Auditor & Project Sponsor
2	**IT Auditor**	IT auditing and assessment
3	**Cybersecurity Specialist**	CS Security auditing and assessment
4	**Data Privacy Specialist**	Data Security & PDPL Compliance

6. Audit mission Assumptions

1. All deliverables will be provided in English language.

2.The client will provide timely access to all required documentation, systems, and key personnel .

3.The main deliverable will be a comprehensive Final Audit Report covering all eight scope domains, with an executive summary, findings register, risk ratings, root causes, management responses, and remediation roadmap.

4.Client personnel (IT, security, and business stakeholders) will be available for interviews and walkthroughs as scheduled during fieldwork weeks.

5.Attending kick-off and status meetings is mandatory for both parties and relevant stakeholders.

6. Penetration testing is treated as optional scope. If required, it will be scoped, priced, and authorized separately via a standalone rules-of-engagement document.

7. The Project shall be executed and delivered in full as a single indivisible work package,

7. Previous Projects

Many projects have been implemented by dealing with various parties in different countries and multiple environments, and we always strive to implement the best practices and standards in order to achieve the best required results.

Project No.	Project Name	Client Name	Logo	Project Description
1	Implementation of the SAMA CSF Cybersecurity Framework	Gulf Union and Al Ahlia Insurance Company	إتحاد الخليج للتأمين التعاوني GULF UNION COOPERATIVE INSURANCE CO.	1. Developing cybersecurity policies, procedures and standards issued by the Saudi Central Bank 2. Conducting a Cybersecurity Risk Assessment on information systems, assets and processes 3. Developing key performance indicators and key risk indicators for operations (KPIs, KRIs) 4. Performing process monitoring
2	CRF Audit	EMDAD DIGITAL		IT Policies and Procedures Audit (General Technical Controls + Application Technical Controls)
3	IT Systems Audit	Lebara Telecommunications Company	LEBARA ليبارا موبايل	IT Policies and Procedures Audit (General Technical Controls + Application Technical Controls)
4	SAMA BCM AUDIT	FINZEY FINANCE	فينزي للتمويل FinZey Finance	SAMA BCM Policies and Procedures ,plans (BCP, DRP ,

				crisis ,and IRP)AND Strategy Audit (General Technical Controls + Application Technical Controls)
5	Implementing a Business Continuity Management System SAMA BCM	ASIG Insurance Company		1. Establish a Business Continuity Management System 2. Develop relevant policies, procedures and standards 3. Define and implement a Business Impact Analysis 4. Conduct a Business Continuity Risk Assessment 5. Define a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO) 6. Develop a Business Continuity Strategy 7. Develop Business Continuity Plans 8. Define Performance Metrics and KPIs
6	Implementation of Business Continuity and Disaster Recovery Program	Energy Manufacturing and Services Company (TAQA)		1. Establish a Business Continuity Management System 2. Develop relevant policies, procedures and standards 3. Define and implement a Business Impact Analysis 4. Conduct a Business Continuity Risk Assessment 5. Define a Recovery Time Objective (RTO) and a

				Recovery Point Objective (RPO) 6. Develop a Business Continuity Strategy 7. Develop Business Continuity Plans 8. Define Performance Metrics and KPIs
7	Implementation of ISO 27001 and basic cybersecurity controls (ECC, CCC, DCC, OSMACC, TCC)	Energy Manufacturing and Services Company (TAQA)		1. Establish a cybersecurity management system 2. Develop a cybersecurity strategy and operational model 3. Develop relevant policies, procedures and standards 4. Ensure compliance with the National Cybersecurity Authority frameworks ECC, CCC, DCC, OSMACC, TCC 5. Ensure compliance with ISO 27001 6. Conduct internal audits on the National Cybersecurity Authority frameworks and ISO 27001 7. Obtain ISO 27001 certification
8	Audit and Oversee the Implementation of NCA-ECC Essential Cybersecurity Controls	Sovereign Government Entity		1. Improve governance documents (cybersecurity strategy, cybersecurity roles and responsibilities, cybersecurity policies) 2. Audit of core cybersecurity controls NCA-ECC

9	ISO 27001 Information Security Standard Training	Energy Manufacturing and Services Company (Energy)	TAQA	Providing training in ISO 27001 information security standard
10	Data Management and Governance Strategy	King Abdulaziz Public Library		1. Conduct gap analysis on the national data governance and management framework 2. Study the current situation 3. Develop a data management strategy 4. Develop an open data plan 5. Publish six open data sets on the Saudi National Data Platform
11	Implementation of ISO 27001 Information Security Standard	Genelle	genelle	1. Establish an information security management system 2. Develop relevant policies, procedures and standards 3. Ensure compliance with ISO 27001 4. Conduct remediation activities and resolve findings 5. Obtain ISO 27001 certification
12	Saudi Aramco Cybersecurity Implementation	Maham	Maham	1. Implement Aramco Cybersecurity Standard SACS-002 2. Develop relevant policies, procedures and standards

13	Data Classification	Perfect Presentation	شركة العرض المتقن Perfect Presentation	1. Collect and classify all data 2. Develop policies, procedures and standards related to data classification and protection
14	Implementation of ISO 27001 Information Security Standard and Basic Cybersecurity Controls (ECC, CCC, DCC, OSMACC, TCC)	National Community Development Program (Tanmia)	تنمية البرنامج الوطني للتنمية المجتمعية في المناطق	1. Establish a cybersecurity management system 2. Develop a cybersecurity strategy and operational model 3. Develop relevant policies, procedures and standards 4. Ensure compliance with the National Cybersecurity Authority frameworks ECC, CCC, DCC, OSMACC, TCC 5. Ensure compliance with ISO 27001 6. Conduct internal audits on the National Cybersecurity Authority frameworks and ISO 27001 7. Obtain ISO 27001 certification
15	Cybersecurity Risk Management	Sovereign Government Entity		1. Develop a cybersecurity risk management methodology and align it with the overall risk management methodology 2. Conduct a cybersecurity risk assessment on information assets + third parties + material changes + technical projects + operations

16	NCA-ECC and CCC-P	Nashirnet		1. Establish a cybersecurity management system 2. Develop policies, procedures and standards for cloud computing controls and ECC + CCC core controls for service providers 3. Conduct cybersecurity risk assessments for projects and products 4. Conduct internal audits 5. Develop and measure performance indicators
17	Data Classification and Modeling	King Abdulaziz Public Library		1. Develop data log 2. Classify data 3. Develop data modeling plan and perform modeling for library systems
18	Implementation of the Personal Data Protection Regulation (PDPL)	Aljaber Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy 3. Developing consent management processes 4. Conducting audits of data processing activities 5. Conducting awareness workshops on personal data protection
19	Implementation of the Personal Data Protection	Hala Payment		1. Limiting personal data and processing activities

	Regulation (PDPL)			2. Developing policies, standards and procedures related to data privacy 3. Developing consent management processes 4. Conducting audits of data processing activities 5. Conducting awareness workshops on personal data protection
20	Implementation of the Personal Data Protection Regulation (PDPL)	Mrna Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy 3. Developing consent management processes 4. Conducting audits of data processing activities 6. Conducting awareness workshops on personal data protection

End of the Document