CMA Auditing Proposal

Version: 1.0

Date: 01-June-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

The Client requests independent Cybersecurity Audit Services against the Capital Market Authority (CMA) Cybersecurity Guidelines to assess the effectiveness of the organization's cybersecurity controls and determine its level of compliance with applicable regulatory requirements.

The CMA Cybersecurity Guidelines were issued by the Capital Market Authority (CMA) to support Capital Market Institutions (CMIs) in establishing effective cybersecurity controls that protect information assets, business operations, financial systems, and customer information from cybersecurity threats and risks.

The audit aims to:

- Assess the organization's compliance with the CMA Cybersecurity Guidelines.
- Evaluate the effectiveness and adequacy of implemented cybersecurity controls.
- Identify cybersecurity gaps, weaknesses, and areas for improvement.
- Assess cybersecurity governance, risk management, and operational security practices.
- Evaluate the organization's ability to protect the confidentiality, integrity, and availability of information assets.
- Provide management with an independent assessment of the current cybersecurity posture.
- Develop practical recommendations and a remediation roadmap to address identified findings.

The audit will assess the organization's cybersecurity posture across the four domains of the CMA Cybersecurity Guidelines:

1. Cybersecurity Governance
2. Cybersecurity Risk Management, Review and Audit
3. Operational Cybersecurity Controls
4. Third Party Cybersecurity

Figure (1)

2. Audit Methodology and Approach

To address the Client's requirements, our CMA Cybersecurity Audit methodology consists of five phases designed to evaluate compliance with the CMA Cybersecurity Guidelines and assess the effectiveness of cybersecurity controls across all applicable domains and subdomains.

Phase 0 – Audit Planning and Initiation

The objective of this phase is to establish the audit scope, identify stakeholders, define the audit approach, and collect preliminary information.

Activities

- Define audit scope and applicable CMA Cybersecurity Guideline requirements.
- Identify business units, processes, systems, applications, infrastructure, and third parties within scope.
- Develop audit work program and audit schedule.
- Request preliminary documentation and supporting evidence.
- Conduct kick-off meeting with management and key stakeholders.
- Establish communication and reporting channels.

Phase 1 – Cybersecurity Governance Assessment (Domain 4.1)

The objective of this phase is to assess the adequacy and effectiveness of cybersecurity governance practices.

Activities

- Assess Leadership and Responsibilities.
- Review Data Governance and Security controls.
- Review Cybersecurity Strategy and Policies.
- Assess Security Awareness and Training Programs.
- Evaluate Human Resources Cybersecurity controls.
- Verify compliance of governance documentation with CMA requirements.
- Conduct management interviews and evidence validation.

Phase 2 – Cybersecurity Risk Management, Review and Audit Assessment (Domain 4.2)

The objective of this phase is to assess the effectiveness of cybersecurity risk management and independent review mechanisms.

Activities

- Assess Cybersecurity Risk Management Framework.

- Review risk assessment methodology and risk registers.
- Evaluate risk treatment and monitoring processes.
- Assess Cybersecurity Review and Audit activities.
- Review audit findings management and corrective action tracking.
- Validate effectiveness of risk governance processes.

Phase 3 – Operational Cybersecurity Controls Assessment (Domain 4.3)

The objective of this phase is to evaluate the design and operating effectiveness of cybersecurity operational controls.

Activities

- Assess Cybersecurity Structure.
- Review Information and Technical Assets Management.
- Evaluate Infrastructure Security controls.
- Assess Identity and Access Management controls.
- Review Cybersecurity Threat Management processes.
- Assess Vulnerability Management practices.
- Evaluate Cybersecurity Event Logs Management.
- Review Cybersecurity Incident Management processes.

- Assess Encryption controls and key management practices.
- Evaluate Application Security controls.
- Review Change Management and Project Management controls.
- Assess Business Continuity Management controls.
- Evaluate Physical Security controls.
- Review Secure Disposal (Safe Destroying) controls.
- Assess BYOD security controls.
- Conduct technical control testing and evidence validation.

Phase 4 – Third Party Cybersecurity Assessment (Domain 4.4)

The objective of this phase is to assess cybersecurity controls related to external parties and service providers.

Activities

- Assess Contract and Suppliers Management controls.
- Evaluate Outsourcing security governance.
- Assess Cloud Computing security controls.
- Review third-party risk assessment processes.
- Review contractual cybersecurity requirements and service level agreements.

- Validate ongoing monitoring of third-party cybersecurity risks.

Phase 5 – Reporting and Recommendations

The objective of this phase is to communicate audit results and provide recommendations for remediation and continuous improvement.

Activities

- Consolidate audit observations and evidence.
- Perform compliance gap analysis against CMA requirements.
- Classify findings according to risk severity (Critical, High, Medium, Low).
- Develop practical recommendations and corrective actions.
- Prepare Executive Audit Report.
- Prepare Detailed Audit and Compliance Assessment Report.
- Present findings to management and relevant governance committees.

3. Audit mission Assumptions

- All deliverables shall be provided in English language.
- The audit shall be performed against the applicable requirements of the CMA Cybersecurity Guidelines.

- The Client shall provide timely access to relevant personnel, systems, facilities, documentation, and supporting evidence required to perform the audit.
- The Client shall assign a project coordinator to facilitate interviews, workshops, and evidence collection activities.
- The audit will be conducted through document review, interviews, walkthroughs, sampling, and control testing where applicable.
- The primary deliverables will include:

    - Executive Audit Report.
    - Detailed CMA Cybersecurity Compliance Assessment Report.
    - Gap Analysis Report.

4. 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)	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