ECC & PDPL AUDITING PROPOSAL

Version: 1.0

Date: 9-March-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

1. Contents

2. Executive Summary of CLIENT's requirements

Trusted Vision Company is proud to offer comprehensive audit services covering compliance with the Personal Data Protection Law (PDPL), issued under Royal Decree No. (M/19) on September 2, 2021, and amended by Royal Decree No. (M/148) on September 5, 2022, in addition to the Essential Cybersecurity Controls (ECC – 2: 2024) Audit.

As part of the Saudi PDPL compliance audit, we evaluate alignment with the National Data Index (NDI) and the personal data protection controls issued by the National Data Management Office (NDMO 14), developed by the Saudi Data and Artificial Intelligence Authority (SDAIA). Our audit approach assesses the effectiveness of governance frameworks, identifies compliance gaps, and provides actionable recommendations to strengthen data protection practices. This structured evaluation enhances transparency, promotes accountability in personal data handling, mitigates regulatory and operational risks, and ensures comprehensive compliance across operations and markets.

In response to the client's request, we also provide audit services for the Essential Cybersecurity Controls (ECC – 2: 2024), developed by the National Cybersecurity Authority (NCA). The ECC framework consists of:

- 4 Cybersecurity Main Domains
- 28 Cybersecurity Subdomains
- 110 Cybersecurity Controls

The ECC requirements apply to all governmental and semi-governmental organizations within the Kingdom of Saudi Arabia. The primary objective of these controls is to establish the minimum cybersecurity requirements for information and technology assets, based on industry-leading practices. Compliance with ECC helps organizations minimize cybersecurity risks arising from both internal and external threats, while strengthening overall security posture and resilience.

Figure 1 Personal Data Protection Law and Regulations

شكل (١): المكونات الأساسية للضوابط

Figure (1)

3. Scope

1. The scope of this Audit is to conduct ECC audit will include:

1. **Governance**: Policies, governance structure, roles, training, audit logs of policy changes, board reporting, compliance registers.
2. **Cybersecurity Defense**
    - Asset Management : Asset inventory completeness, classification, lifecycle processes, disposal records
    - Identity and Access Management
    - Information Systems and Information Processing Facilities Protection
    - Email protection
    - Network Security Management
    - Mobile devices security
    - Data and Information Protection
    - Cryptography
    - Backup and Recovery Management
    - Vulnerability management
    - Penetration Testing
    - Events logs and monitoring management
    - Cybersecurity Incident and Threat Management
    - Physical security : Access controls, CCTV logs, visitor records, environmental controls, media handling, site access reviews
    - Web Application Security
3. **Cybersecurity Resilience Aspects of Business Continuity Management (BCM)**
    - business continuity and recovery capabilities.
    - Business Continuity Management (BCM)
    - Cybersecurity Disaster Recovery
    - Crisis Management
    - Resilience Testing and Exercises

4. **Third-Party and Cloud Computing Cybersecurity**

Inventory of suppliers, contract clauses, due diligence records, audit/assessment reports, SLAs, exit plans and data residency evidence data residency

2. PDPL audit will include:

Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity

Collect and compile evidence, information, policies, procedures, processes, forms, and templates related to the protection and privacy of personal data. • Activity logs, data logs, and technical asset logs. • Roles and responsibilities. • The organization's business strategy. • A list of general risks within the organization. • Roadmaps, information, and personal data management plans. • Review all systems and procedures related to data protection, monitor compliance with personal data protection, and document the results. • Any information relevant to the above documents. • Conduct interviews with relevant project stakeholders to understand their needs and expectations, including but not limited to: • Information Technology Department • Data Management Office • Human Resources • Other departments and divisions within the organization.	• Submit all required documents and information • Coordinate interviews with all departments and sections • Submit any required documents and provide adequate answers to consultants • Review and provide feedback on the processing plan • Review and provide feedback on the draft internal audit report for the Personal Data Protection System and Regulations	Meeting minutes Auditors' understanding and analysis of the situation Remediation plan Internal audit of the personal data protection system and regulations

• Review, audit, and identify gaps in the documentation related to the personal data protection system and regulations, including: • Personal data assets and environment • Stages of personal data processing • Current personal data management challenges • Personal data protection risk assessment plan • Change management plan or as appropriate to the organization's approved change management framework • Review the obligations of both the data controller and the data processor. • Activities that can be delegated to external parties. • Issuing a draft internal audit report for the personal data protection system and regulations.		

4. Audit Methodology and Approach

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

4.1 Phase 0: Planning and engagement

This will include Establish scope, objectives, resources, timelines and logistics; obtain stakeholder buy-in

Phase Activities:

- ✓ Confirm scope boundaries (business units, systems, data, locations, third parties).
- ✓ Identify target control level(s) and applicable regulatory requirements.
- ✓ Assemble audit team and assign roles (lead auditor, technical specialists, physical security, third-party assessor).
- ✓ Agree timelines, sampling approach, communication plan and evidence access.
- ✓ Request initial documentation package (policies, asset registers, risk register, contracts, architecture diagrams, recent test reports).
- ✓ Schedule interviews, site visits and testing windows.

PDPL-Specific Additions:

- ✓ Identify personal data processing activities within scope (data types, data subjects, purposes, storage locations, cross-border transfers).
- ✓ Request Record of Processing Activities (RoPA), privacy policies, consent forms, DPIA/PIA documentation.
- ✓ Identify sensitive personal data processing and applicable additional safeguards.
  Review third-party processors handling personal data and request Data Processing Agreements (DPAs).
- ✓ Map regulatory obligations based on guidance issued by the National Data Management Office (NDMO)

Phase 1: Baseline Assessment (Level 1 focus)

Aims to verify existence and basic operation of foundational controls required for Level 1.

Phase Activities:

- ✓ Document and policy review (governance, acceptable use, incident response, backup).
- ✓ Validate asset inventory and classification for critical assets.
- ✓ Review identity & access controls (user/provisioning flows, MFA on critical systems, privileged access controls).

- ✓ Confirm basic technical controls: patch management process, baseline configurations, backups and restore evidence, endpoint protection.
- ✓ Physical security walkthroughs of primary sites and data centers.
- ✓ Initial third-party inventory and review of contracts for critical suppliers.
- ✓ Sample testing (config inspection, log checks, access reviews).
- ✓ Conduct stakeholder interviews for control of ownership and operation.

PDPL-Specific Additions:

- ✓ Review existence and approval of data protection and privacy policies.
- ✓ Verify data classification includes personal and sensitive personal data categories.
- ✓ Confirm existence of data retention and destruction procedures.
- ✓ Review mechanisms for obtaining and recording data subject consent (where required).
- ✓ Verify existence of data breach response and regulatory notification procedures.
- ✓ Confirm availability of channels to support data subject rights (access, correction, deletion, withdrawal of consent).

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.

Phase Activities:

- ✓ Review and test monitoring and detection capabilities (SIEM rules, alerting, retention, tuning).
- ✓ Evaluate vulnerability management (scanning, patch prioritization, remediation SLAs) and review remediation tickets.
- ✓ Review secure development lifecycle artifacts and code/security testing for applications in scope.
- ✓ Test incident response readiness: examine past incidents, timelines, root-cause analysis, and run at least one tabletop exercise.

- ✓ Deeper third-party risk assessments: review due diligence, security questionnaires, audit reports, SLAs and ongoing monitoring.
- ✓ Examine change management, configuration management, and deployment pipelines for controls and rollback capability.
- ✓ Reperformance tests: privileged account provisioning, restore from backup, run a vulnerability scan on sampled assets.

PDPL-Specific Additions:

- ✓ Test effectiveness of Data Subject Access Request (DSAR) handling process.
- ✓ Review and evaluate DPIAs conducted for high-risk processing activities.
- ✓ Assess implementation of data minimization and purpose limitation principles.
- ✓ Test encryption, masking, anonymization, or pseudonymization controls where applicable.
- ✓ Evaluate cross-border data transfer compliance mechanisms.
- ✓ Review staff awareness and privacy training effectiveness.

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.

Phase Activities:

- ✓ Review KPIs, dashboards and executive reporting to confirm continuous measurement and management oversight.
- ✓ Validate integration of threat intelligence into detection and response processes.
- ✓ Assess automation/orchestration (SOAR playbooks, automated patching, automated response workflows).
- ✓ Evaluate advanced testing (red/blue/purple team exercises, continuous penetration testing, application security automation).
- ✓ Review program governance for continual improvement: lessons-learned processes, investment

prioritization, repeatable remediation execution.

- ✓ Confirm demonstrable improvements over time (metrics trending, reduced MTTR, reduced vulnerability backlog).
- ✓ Conduct live simulations or full-scale incident response exercises where feasible.

PDPL-Specific Additions:

- ✓ Review privacy KPIs (number of DSARs, response timelines, breach incidents, compliance metrics).
- ✓ Assess effectiveness and independence of Data Protection Officer (if appointed).
- ✓ Evaluate integration of privacy risk into enterprise risk management.
- ✓ Review automation tools used for privacy management and compliance tracking.
- ✓ Confirm periodic internal reviews or independent assessments of PDPL compliance.

Phase 4: Reporting & Remediation Oversight

Deliver consolidated audit outcomes and ensure remediation planning and tracking.

Phase Activities:

- ✓ Consolidate Phase 1–3 findings into a single final report with executive summary and detailed technical appendices.
- ✓ Classify findings (Critical, High, Medium, Low), propose remediation actions, assign owners and target dates.
- ✓ Present findings to executive stakeholders and governance bodies (CISO, risk committee, board as required).
- ✓ Establish remediation tracking process; schedule follow-up validation reviews or re-testing for high/critical items.
- ✓ Provide a roadmap to achieve the next control level where gaps exist.

PDPL-Specific Additions:

- ✓ Provide a structured PDPL compliance remediation roadmap.

- ✓ Recommend periodic PDPL compliance reassessment and continuous monitoring mechanisms.

5. Proposed Schedule

Phase	Duration (WEEKS) Hybrid works
ECC audit	2
PDPL audit	2

6. Audit mission Assumptions

1. All deliverables will be in English Language
2. The main deliverables will be Audit report for ECC framework.
3. The company will nominate SPOC for audit coordination.
4. The company will guarantee and facilitate access to all required resources.

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