Technical and Financial Proposal for Audit NCA-DCC

Version 1.0

Date: 12-11-2025 AD

Prepared by: Trusted Vision for Cybersecurity Company

Contact Information

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

Name	**Hashem Al-Azizi**
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**

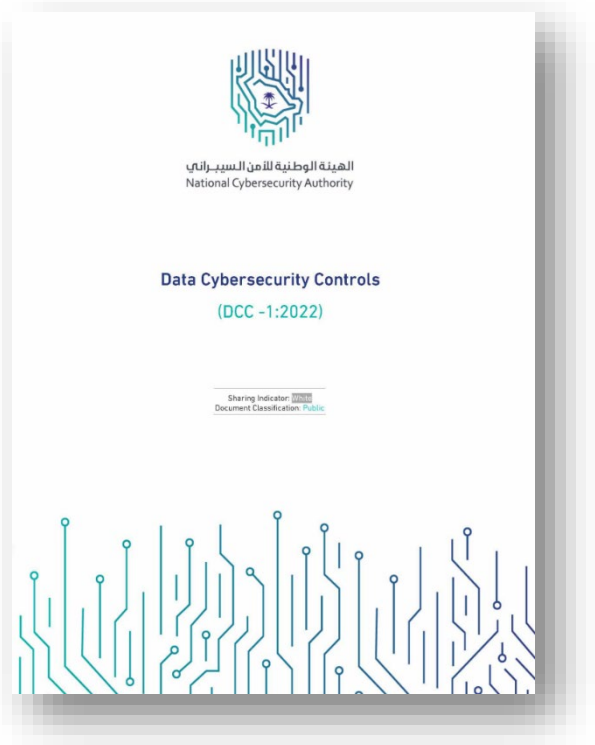
TRUSTED VISION

Table of Contents

1. Executive summary of client requirements

Trusted Vision Company is pleased to offer comprehensive consulting services for:

- Pre-Audit assessment for data cybersecurity controls NCA-DCC



TRUSTED VISION

We believe that our experience in implementing similar projects places us among the elite consulting firms in addition to:

- A balanced blend of international and local expertise in data management
- An effective approach to project implementation to meet project requirements in a timely manner, in a professional and quality manner.
- Extensive knowledge and experience in implementing and designing solutions based on international standards and best practices.
- Best Consulting Expertise for auditing.

We hope that our consulting services will meet the terms of competition and look forward to a mutual working relationship.

2. Project Implementation Methodology (Pre-Audit NCA-DCC)

Conduct pre-audit assessment for NCA-DCC evidence and deliver the pre-audit report.

Note: The cooperation of the entity and its employees is important, sensitive, and necessary to ensure the success of this project.

The project will be **over 7 days**, during which the following activities will be conducted.

NO#	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
1.	Conduct interviews with project stakeholders to understand their needs and expectations, including but not limited to: • Head of the organization • IT Management • Data management officer • HR department • The rest of the departments within the organization.	Conduct interviews with all the department.	Minutes Meeting

NO#	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
2.	Collect information about data system including all evidence of: • Data strategy • Roles and responsibilities document • Data protection policies • Data protection Procedures • Any other data processes and documents	Coordinate interviews and submit evidence to the auditor	Meeting Minutes
3.	Conduct a comprehensive pre-audit assessment for NCA-DCC evidence with corrective actions.	Review and approve the report	Pre-audit report for NCA-DCC evidence

3. Project scope and Assumptions

3.1 Outside the Scope of Work

1. Implementation or purchase of technical tools and solutions related to the application of the NCA-DCC.

2. Any other service not explicitly mentioned in the previous sections will be considered outside the scope of our work.

3.2 Assumptions

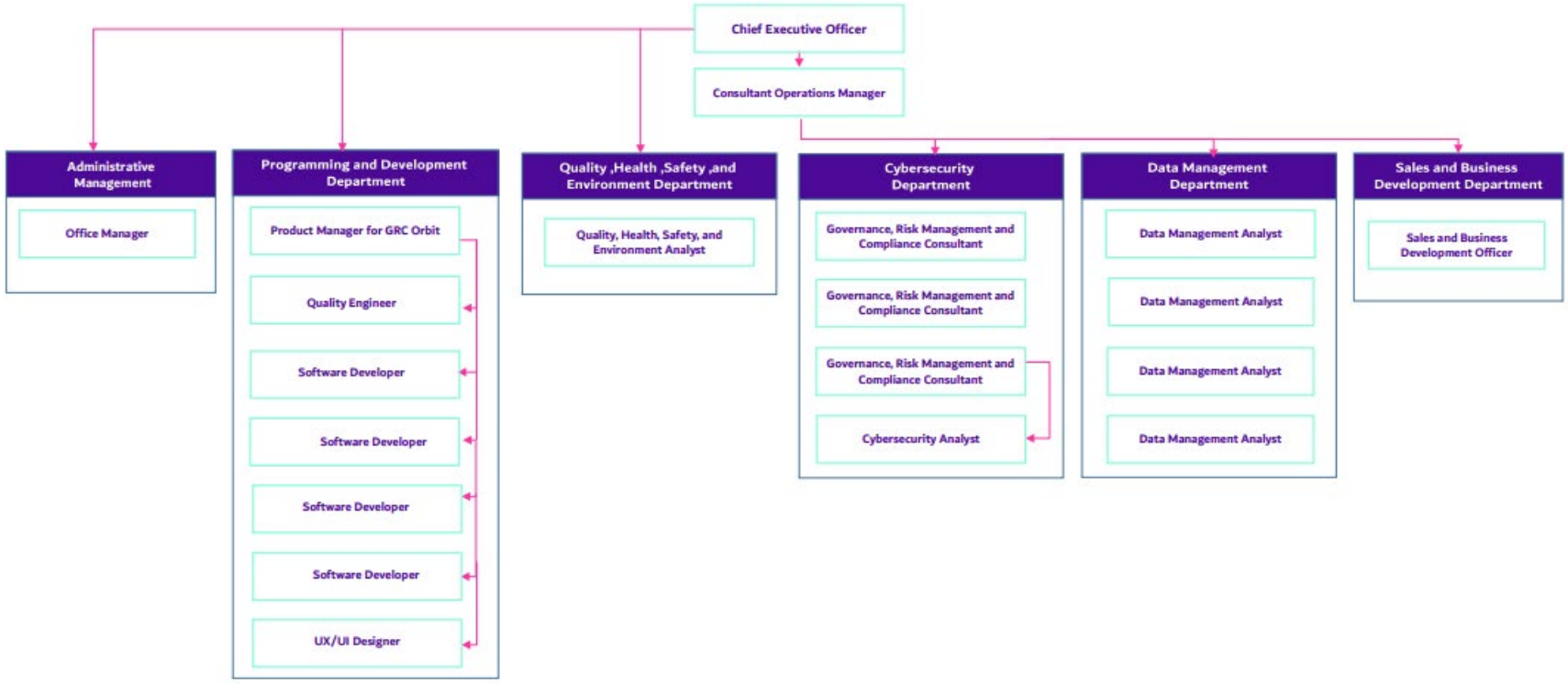
1. **All activities are assumed to occur within the designated project period. The company is not responsible for any delays or lack of cooperation on the client's side that may extend beyond this period.**

2. **The company is not responsible for any delay that occurs on the part of the entity.**

3. **Cooperation from the departments and departments of the entity is mandatory for the success of the project.**

4. Company Information

Trusted Vision is a data management and cybersecurity consulting firm that provides full services in governance, risk, and compliance management, as well as solutions and training, to help entities meet their business requirements. What sets us apart are the core values we espouse.



5. Certificates

Our team holds a variety of certifications, including:

PECB ISO/IEC 27001 SENIOR LEAD IMPLEMENTER

PECB ISO/IEC 27001 SENIOR LEAD AUDITOR

PECB ISO/IEC 27032 LEAD CYBERSECURITY MANAGER

PECB ISO/IEC 38500 LEAD IT CORPORATE GOVERNANCE MANAGER

PECB ISO 31000 LEAD RISK MANAGER

PECB ISO/IEC 27005 SENIOR LEAD RISK MANAGER

PECB DATA PROTECTION OFFICER

PECB ISO 22301 FOUNDATION

PECB ISO/IEC 20000 FOUNDATION

PECB ISO 45001 LEAD AUDITOR

PECB ISO 14001 LEAD AUDITOR

PECB ISO 9001 LEAD IMPLEMENTER

TRUSTED VISION

6. 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 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	Implementing a Business Continuity Management System SAMA BCM	ASIG Insurance Company	ACIG للتأمين بأمان	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
3	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

4	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
5	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
6	IT Systems Audit	Lebara Telecommunications Company	LEBARA ليبارا موبايل	IT Policies and Procedures Audit (General Technical Controls + Application Technical Controls)

7	ISO 27001 Information Security Standard Training	Energy Manufacturing and Services Company (Energy)	TAQA	Providing training in ISO 27001 information security standard
8	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
9	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
10	Saudi Aramco Cybersecurity Implementation	Maham	Maham	1. Implement Aramco Cybersecurity Standard SACS-002

				2. Develop relevant policies, procedures and standards
11	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
12	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

13	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
14	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
15	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

16	Implementation of the Personal Data Protection Law and Regulations (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
17	Implementation of the Personal Data Protection Law and Regulations (PDPL)	Hala Payment		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
18	Implementation of the Personal Data Protection	Mrna Finance		1. Limiting personal data and processing activities

	Law and 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
19	Implementation of SAMA CSF	Finzey	فينزي للتمويل FinZev Finance	1. Conduct a comprehensive cybersecurity gap assessment. 2. Develop policies, procedures, and standards in alignment with the Saudi Central Bank (SAMA) Cybersecurity Framework. 3. Perform cybersecurity risk assessments for all information assets. 4. Establish and check cybersecurity performance indicators (KPIs) 5. Development of a comprehensive Disaster Recovery (DR) Plan and Incident Response (IR) Plan
20	Implementation of the Personal Data Protection	Finzey		1. Limiting personal data and processing activities

	Law and Regulation (PDPL)		فينزي للتمويل FinZev Finance	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