# NCA & CRF Auditing Proposal

**Version: 1.0**

**Date: 3-Feb-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,<br>Injaz Group Building, No. 6482, First Floor,<br>P.O. Box: 13247<br>Riyadh, Kingdom of Saudi Arabia |

TRUSTED VISION

## Contents

# 1. Executive Summary of CLIENT's requirements

The objective of this engagement is to support a fast-growing technology startup in achieving timely and successful regulatory attestation against the Saudi National Cybersecurity Authority (NCA) frameworks and the Cybersecurity Regulatory Framework (CRF).

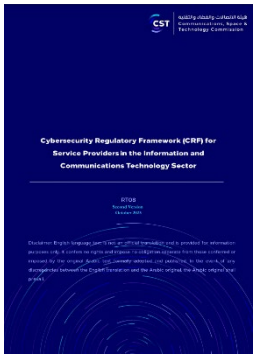
The National Cybersecurity Authority (NCA) has established a comprehensive set of cybersecurity frameworks to enable organizations operating within the Kingdom of Saudi Arabia to effectively identify, manage, and mitigate cybersecurity risks. To ensure the protection of information assets, critical systems, and digital services, the company is required to adopt and implement the NCA cybersecurity frameworks, including:

- ECC – Essential Cybersecurity Controls
- CCC – Cloud Cybersecurity Controls
- CSCC – Critical Systems Cybersecurity Controls
- DCC – Data Cybersecurity Controls
- TCC – Teleworking Cybersecurity Controls
- OSMACC – Organizations' Social Media Accounts Cybersecurity Controls









CST established a Cyber Security Framework (“the Framework”) to enable Institutions affiliated with CST to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the company must adopt the Framework.

The engagement will deliver an independent external validation of the organization’s current cybersecurity controls, building upon the results of the previously conducted internal/gap assessment. The focus will be on confirming control implementation and effectiveness, identifying remaining compliance gaps, and preparing regulator-ready documentation that demonstrates alignment with national cybersecurity obligations.

Given the client’s targeted deadline in early-mid March 2026, the project will be executed through an accelerated, risk-based approach designed to maximize coverage, efficiency, and regulatory alignment within a 5–6 week delivery window. The engagement will culminate in a comprehensive compliance validation report, a prioritized risk and remediation roadmap, and hands-on support throughout the regulatory attestation process.

Ultimately, this engagement will enable the client to demonstrate regulatory compliance with confidence, reduce exposure to cybersecurity and compliance risks, and establish a solid foundation for sustainable cybersecurity governance as the organization continues to scale.

We believe that our expertise in conducting similar data management projects positions us among the elite consulting firms in addition to our:

1. Long and in-depth expertise in designing and implementing similar projects.
2. A balanced mix of international and regional expertise in data consulting-related issues
3. Effective project implementation approach to address project requirements in a timely, professional, and quality manner
4. Extensive knowledge and expertise in implementing and designing solutions based on international standards and best practices.
5. Best-of-breed data management consulting expertise
6. Proven project management and implementation methodologies and approach

We hope our proposed services and approach meet your satisfaction, and we look forward to a mutual business relationship.

## 2. Project Benefits and Values

By implementing this project, the expected benefits and values will be the following.

1. Enhance compliance with NCA & CRF frameworks
2. Manages the assurance, integrity, security, value, and availability of data.
3. Increased customer and interested party satisfaction.
4. Reduced costs as a result of data breaches

## 3. Project Implementation Methodology

The table below holds the activities that will be conducted from Trusted Vision and the client:

| #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.** | • Review client-provided policies, standards, procedures, and technical evidence.<br>• Map existing controls to applicable NCA/CRF and related regulatory requirements.<br>• Conduct interviews/workshops with key stakeholders (IT, Security, Cloud, Operations, HR, etc.).<br>• Prepare consolidated Compliance Validation Report with findings and observations. | Provide existing policies, standards, procedures, and guidelines. | 1. Comprehensive Compliance Validation Report (CVR) for:<br>• ECC – Essential Cybersecurity Controls<br>• CCC – Cloud Cybersecurity Controls<br>• CSCC – Critical Systems Cybersecurity Controls<br>• DCC – Data Cybersecurity Controls<br>• TCC – Teleworking Cybersecurity Controls<br>• OSMACC – Organizations' Social Media |

| #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 |
|---|---|---|---|
| | | | Accounts Cybersecurity Controls<br>• CRF – Cybersecurity Regulatory Framework |
| **2.** | • Analyze validation findings to identify compliance and security gaps.<br>• Develop a centralized Risk Register with ownership and risk ratings.<br>• Validate gaps and risks with client stakeholders. | • Share prior gap assessment results (if exist)<br>• Provide configuration baselines and screenshots where required. | 2. Strategic Gap Analysis & Risk Register. |
| **3.** | • Define remediation options for each identified gap.<br>• Estimate remediation effort and complexity (high/medium/low).<br>• Sequence initiatives into phased roadmap.<br>• Align roadmap with regulatory deadlines and business priorities. | | 3. Prioritized Remediation & Transformation Roadmap. |
| **4.** | • Conduct internal readiness review before submission. | | 4. Regulatory Attestation & Audit Support Services. |

| #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 |
|---|---|---|---|
| | • Provide final attestation support and closure confirmation. | | |

# 4. Project Scope and Assumptions

## 4.1 Out of Scope

1. Implementing technology proof of concept or any technical solution
2. Any other service that has not been clearly mentioned in the previous section(s) shall be considered as out of scope.
3. Developing RFP for any solution or tool

## 4.2 Scope Assumptions

1. All deliverables will be in English Language
2. All activities will be conducted during the project timeline which is six weeks.
3. Each task will be performed during the project time; Trusted Vision is not responsible if the client has delayed any of the tasks or have any circumstances.
4. The proposal does not include any review of the submitted documents.

# 5. Terms and Conditions

1. This offer is valid for 1 month.
2. Attending meetings are mandatory for each party and stakeholder in this project.
3. Cooperation with the consultants is mandatory.

End of the Document