TRUSTED VISION

SAMA AND NCA

CONSULTATION PROPOSAL

Version: 1.0

Date: 18-9-2024

Prepared By:

Trusted Vision for Governance and Consultation

Document Control

Item	Description
Document Title	SAMA AND NCA CONSULTATION PROPOSAL
File Name	SAMA AND NCA CONSULTATION PROPOSAL.docx
Author (s)	Hashem Al-Azizi
Classification	Confidential

Document Amendment Record

Version	Date	Remarks
1.0	18-9-2024	First Release

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	Cordoba District, Saeed Bin Zaid Street, Injaz Group Building, No. 6482, First Floor, P.O. Box: 13247, Riyadh, Kingdom of Saudi Arabia

Contents

1. Executive Summary of CLIENT's requirements

The client requests to have the following services:

1. **Consultation of Saudi Central Bank Cybersecurity Framework (SAMA-CSF).**
2. **Consultation of National Cybersecurity Authority Essential Cybersecurity Controls (NCA-ECC).**
3. **Consultation of National Cybersecurity Authority Cloud Cybersecurity Controls (NCA-CCC-Type Tenant (T)).**
4. **Consultation of National Cybersecurity Authority Teleworking Cybersecurity Controls (NCA-TCC).**
5. **Consultation of National Cybersecurity Authority Data Cybersecurity Controls (NCA-DCC).**
6. **Consultation of National Cybersecurity Authority Critical Systems Cybersecurity Controls (NCA-CSCC).**

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

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

2- Achieving compliance with NCA

3- Achieving compliance with SAMA

4- Improved decision-making by monitoring the overall cybersecurity governance, risk and compliance.

5- Increased competitiveness through improved customer satisfaction

6- Increased public trust through securing customer's data.

7- Manages the assurance, integrity, security, value, and availability of data.

8- Increased customer and interested party satisfaction.

9- Reduced costs as a result of data breaches

3. Project Implement Methodology and Approach

In order to address the Client's requirements, we have structured the project approach into phases as follows:

3.1 Baseline Phase

This is the first phase of the project, during which the following activities will take place.

Trusted Vision Activities		CLIENT Activities	
No	**Activity**	**No**	**Activity**
1	Mobilization of the project team	1	Nomination of the project coordinator and project steering committee
2	Information Gathering which includes. ○ Policies, Procedures, Forms ○ Asset register	2	Send all required documents to the consultants

	○ Technologies ○ Any related Doc's		
3	Develop project charter that elaborate the project scope, objectives, and project management processes	3	Review and approve project charter
4	Perform Kick-off meeting with all project stakeholders	4	Coordinate Project Kick-off meeting and ensure all stakeholders attendance
5	Conduct interviews with the project stakeholders to in order to (Agenda): • Understand their main activities and processes. • Understand and the critical infrastructure that their processes are dependent on • Understand Internal and External factors that affect their operation and cybersecurity. • Any signed agreements with third parties that entails cybersecurity controls. Stakeholders include all management levels listed below -but not limited to-: ○ Head of Company	5	Coordinate the interviews with all project stakeholders that are nominated by the consultant

	○ Risk Management Committee ○ Manufacturing Department ○ Head of IT Department ○ Head of Cybersecurity Department ○ Head of Human Resources ○ Head of Legal		
6	Develop a solution matrix sheet that includes the required solutions and tools to be brought to implement the NCA and SAMA controls	6	Review and approve the proposed solution matrix sheet that includes the required solutions and tools to be brought by the client to implement the cybersecurity controls
7	Understand company processes, business environment and its context	7	Engaging with vendors and third parties that provides the required cybersecurity solutions (based on NCA and SAMA) and conduct POCs with them and purchase the tools
		8	Acquire and implement all needed cybersecurity solutions and tools
		9	Obtain Top management commitment and buy-in with securing the budget towards implementing NCA and SAMA Controls

		10	Obtain IT Department commitment and buy-in to facilitate and prioritize the implementation of NCA and SAMA Controls
		11	Prepare an asset register and send it to the consultant
		12	Dedicate two (2) staff to work with the consultant to achieve the implementation of the project
8	Provide consultation on separating cybersecurity department from IT department	13	Separate cybersecurity department from IT department and allocate a separate budget for it
9	Conduct one 8 hours cybersecurity training for C-Levels and executives	14	Assign and attend the training by the cybersecurity C-Levels and executives

3.2 Develop Phase

This is the second phase of the project, during which the following activities will take place.

<table>
<tr><th colspan="2">Trusted Vision Activities</th><th colspan="2">CLIENT Activities</th></tr>
<tr><th>No</th><th>Activity</th><th>No</th><th>Activity</th></tr>
<tr><td>1.</td><td>Develop Cybersecurity strategy with roadmap</td><td>1.</td><td>Review and Implement the Cybersecurity strategy with roadmap</td></tr>
<tr><td>2.</td><td>Develop a committee charter and advise how to establish the cybersecurity committee</td><td>2.</td><td>Formalize cybersecurity committee and adopt its charter</td></tr>
<tr><td>3.</td><td>Develop the following cybersecurity documents, policies and procedures:<table><tr><td>Cybersecurity Roles and responsibilities for Internal Staff and Cloud computing parties including vendors + RACI Matrix</td><td>Cybersecurity Risk Management Methodology, Risk Register and Risk Assessment Forms + Defining acceptable risk levels for the cloud services</td></tr></table></td><td>3.</td><td>Review, adopt, publish and implement the following cybersecurity documents, policies and procedures:<table><tr><td>• Cybersecurity Roles and responsibilities for Internal Staff and Cloud computing parties including vendors + RACI Matrix</td><td>• Cybersecurity Risk Management Methodology, Risk Register and Risk Assessment Forms + Defining acceptable risk</td></tr></table></td></tr>
</table>

Cybersecurity in Project Management and Change Management	Cybersecurity in Human Resources which includes: • Integrating NDA in their job contracts • Screening for cybersecurity staff and high privilege positions (1)
Cybersecurity Awareness and Training program	Cybersecurity in Asset Management Policy and Procedure
Identity and Access Management Policy and Procedure	Information Systems and Information Processing Facilities Protection Policy and Procedure

• Hire Saudi in the cybersecurity	levels for the cloud services. • Communicate risk levels to the CSTs (if applicable) • Periodic Monitoring risk register
Cybersecurity in Project Management and Change Management	Cybersecurity in Human Resources which includes: • Integrating NDA in their job contracts • Screening for cybersecurity staff and high privilege positions (1) and any staff that have access to cloud technology stack • Require all staff to read

Email Protection Policy	Network Security Policy and Procedure
Mobile Devices Security Policy and Procedure	Data and Information Protection Policy and Procedure
Cryptography Policy, standard and Procedure	Backup and Recovery Management Policy and Procedure
Bring your own device policy	Cybersecurity Event Logs and Monitoring Management Policy and Procedure
Vulnerability Management and Patch Management Policy and Procedure	Cybersecurity in Physical and Environmental Policy and Procedure

	and sign all cybersecurity governance documentation
Cybersecurity Awareness and Training program	Cybersecurity in Asset Management Policy and Procedure
Identity and Access Management Policy and Procedure	Information Systems and Information Processing Facilities Protection Policy and Procedure
Email Protection Policy	Network Security Policy and Procedure
Mobile Devices Security Policy and Procedure	Data and Information Protection Policy and Procedure

Cybersecurity Incident and Threat Management Policy and Procedure	Cybersecurity requirements for business continuity management Policy and Procedure
Web Application Security Policy	IT disaster recovery plan
Developing response plans for cybersecurity incidents	Cybersecurity requirements for cloud computing Policy and Procedure
Cybersecurity requirements for Third party Policy and Procedure	Secure coding standards
Cybersecurity requirements for Industrial Controls Systems Policy and Procedure	Cybersecurity in change management Policy and Procedure

Cryptography Policy, standard and Procedure	Backup and Recovery Management Policy and Procedure
Bring your own device policy	Cybersecurity Event Logs and Monitoring Management Policy and Procedure
Vulnerability Management and Patch Management Policy and Procedure	Cybersecurity in Physical and Environmental Policy and Procedure
Cybersecurity Incident and Threat Management Policy and Procedure	Cybersecurity requirements for business continuity management Policy and Procedure

Secure usage policy for users	Cybersecurity requirements in SLAs
Cybersecurity Architecture	Electronic Banking Services policy

Web Application Security Policy	IT disaster recovery plan
Developing response plans for cybersecurity incidents	Cybersecurity requirements for cloud computing Policy and Procedure
Cybersecurity requirements for Third party Policy and Procedure	Secure coding standards
Cybersecurity requirements for Industrial Controls Systems Policy and Procedure	Cybersecurity in change management Policy and Procedure
Secure usage policy for users	Cybersecurity requirements in SLAs and contract
Cybersecurity Architecture	Electronic Banking Services policy

4.	Develop configuration standards (network devices, endpoints, applications, Storage Networks, etc.) for technology assets owned by the client	4.	Review, adopt, publish and implement configuration standards

(1)Need to define what is highly privilege positions.

3.3 Supervise and Assist

This is the third phase of the project, during which the following activities will take place.

Trusted Vision Activities	
No	Activity
1.	Supervise the implementation of NCA and SAMA Controls
2.	Conduct Cybersecurity awareness workshops (for onboarded and current staff)
3.	Dedicate 1 resource from Trusted Vision to fully work on supervision and assist in implementing the SAMA and NCA controls

CLIENT Activities	
No	Activity
1.	Review and approve the External Cybersecurity Audit report
2.	Coordinate Cybersecurity awareness workshops
3.	Facilitate the implementation of the NCA and SAMA Controls (especially the IT Department)

3.4 Audit

Trusted Vision Activities		CLIENT Activities	
No	Activity	No	Activity
1.	Perform Internal Cybersecurity Audit report	1.	Review and approve the Internal Cybersecurity Audit report
2.	Conduct Cybersecurity awareness workshops (for onboarded and current staff)	2.	Coordinate Cybersecurity awareness workshops

4. Project Scope and Assumptions

4.1 Out of Scope

1. Implementing technology proof of concept
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.

3. Client will be committed to the Project Timeframe and will take the responsibility if any delay has occurred from their side.

4. Cooperation from executives, departments heads and all Client staff shall be demonstrated and be committed to the timeline of this project.

5. 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.

6. Compliance with any other regulation(s) or law is the responsibility of the client.

7. The proposal includes only one review of the submitted documents.

8. • An AI bot will be added to record and summarize conversations, aiming to assist consultants in improving and developing meeting minutes.

9. The company has the right to temporarily suspend the project if the payment is not made within two weeks from the date of issuing and sending the invoice to the entity.

5.1 Terms and Conditions

1. This offer is valid for 1 month.
2. Payment Terms are to be on monthly basis throughout the project period (24 months).
3. The client has the right to stop or exit from the contract at any stage in any month, and there will be no extra fees to be paid after.
4. All services scope of work as per the technical proposal.
5. Attending meetings are mandatory for each party and stakeholder in this project.
6. Cooperation with the consultants is mandatory.
7. All deliverables to the client will have 3 working days period for their review and approval, if the time is due without any official reply, it is considered as approved deliverable.
8. The proposal includes only one review of the submitted documents.

End of the Document