SAMA CSF Consultation Proposal – Maturity Level 3

Version: 1.0

Date: 04-May-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

Contents

1. Executive Summary of CLIENT's requirements

The client requests to have the following services:

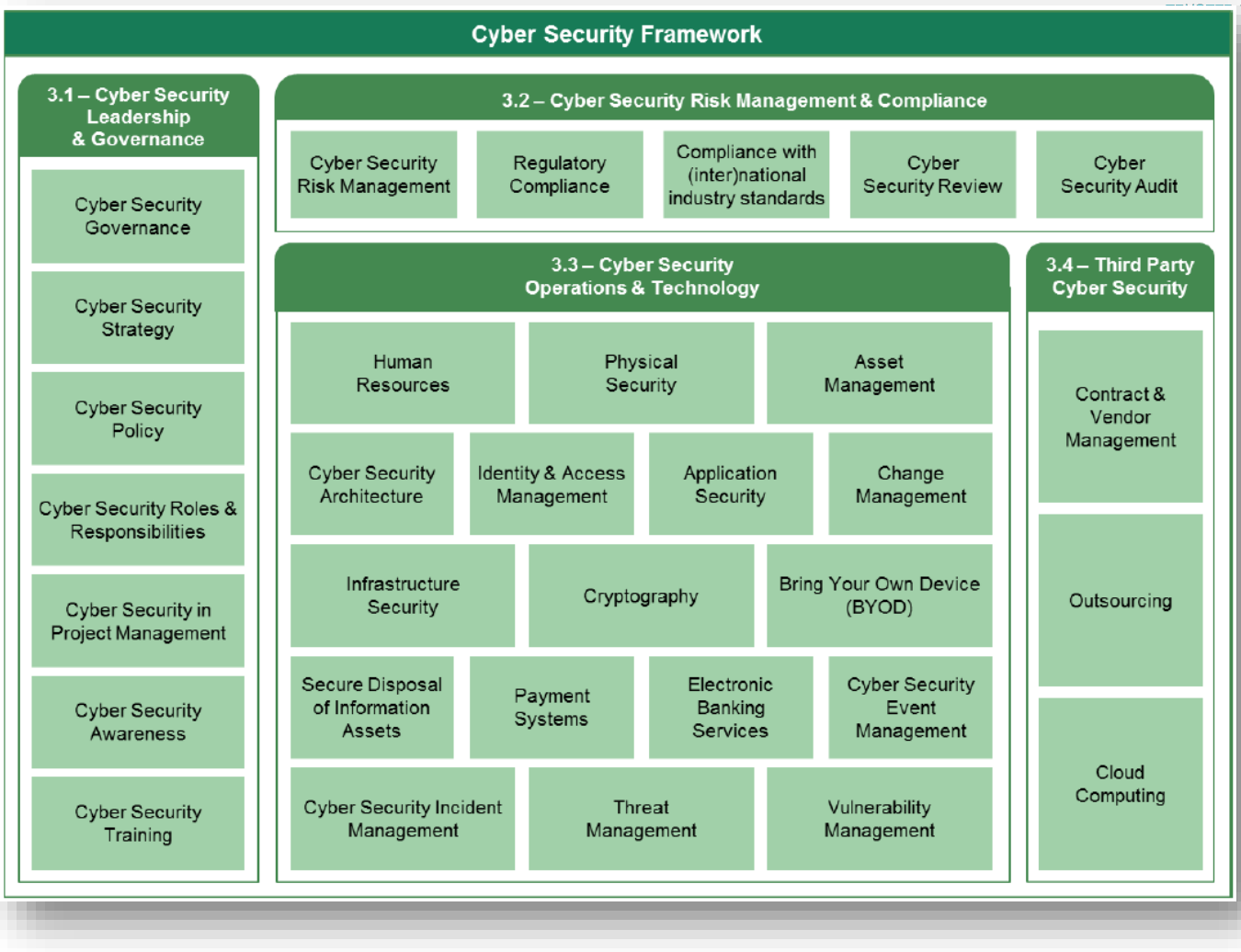
Consultation of SAMA Cybersecurity Framework to reach Maturity Level 3

SAMA established a Cyber Security Framework ("the Framework") to enable Financial Institutions affiliated with SAMA 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 objective of the Framework is as follows:

1. To create a common approach for addressing cyber security within the company.
2. To achieve an appropriate maturity level of cyber security controls within the company.
3. To ensure cyber security risks are effectively managed throughout the company.

The Framework is structured around four main domains as in figure 1 below:



1. Cyber Security Leadership and Governance.
2. Cyber Security Risk Management and Compliance.
3. Cyber Security Operations and Technology.
4. Third Party Cyber Security.

The cybersecurity maturity level will be measured with the help of a predefined cyber security maturity model. The cyber security maturity model distinguishes six maturity levels (0, 1, 2, 3, 4 and 5), which are summarized in the table below. To achieve levels 3, 4 or 5, a company must first meet all criteria of the preceding maturity levels.

Maturity Level	Definition and Criteria	Explanation
0 - Non-existent	• No documentation. • There is no awareness of or attention for certain cyber security control.	Cyber security controls are not in place. There may be no awareness of the particular risk area or no current plans to implement such cyber security controls.
1 – Ad-hoc	• Cyber security controls are not or are partially defined. • Cyber security controls are performed in an inconsistent way. • Cyber security controls are not fully defined	• Cyber security control design and execution varies by department or owner. • Cyber security control design may only partially mitigate the identified risk and execution may be inconsistent.
2 - Repeatable but informal	• The execution of cyber security control is based on an informal and unwritten, though standardized, practice	• Repeatable cyber security controls are in place. However, the control objectives and design are not formally defined or approved. • There is limited consideration for a structured review or testing of a control
3 - Structured and formalized	• Cyber security controls are defined, approved, and implemented in a structured and formalized way. • The implementation of cyber security controls can be demonstrated.	• Cyber security policies, standards and procedures are established. • Compliance with cyber security documentation i.e., policies, standards and procedures are monitored, preferably using a governance, risk, and compliance tool (GRC). • key performance indicators are defined, monitored, and

		reported to evaluate the implementation.
4 - Managed and measurable	• The effectiveness of the cyber security controls is periodically assessed and improved when necessary. • This periodic measurement, evaluations and opportunities for improvement are documented.	• Effectiveness of cyber security controls are measured and periodically evaluated. • key risk indicators and trend reporting are used to determine the effectiveness of the cyber security controls. • Results of measurement and evaluation are used to identify opportunities for improvement of the cyber security controls.
5 - Adaptive	• Cyber security controls are subject to a continuous improvement plan.	• The enterprise-wide cyber security program focuses on continuous compliance, effectiveness, and improvement of cyber security controls. • Cyber security controls are integrated with enterprise risk management framework and practices. • Performance of cyber security controls are evaluated using peer and sector data.

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. Competitive cybersecurity 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.

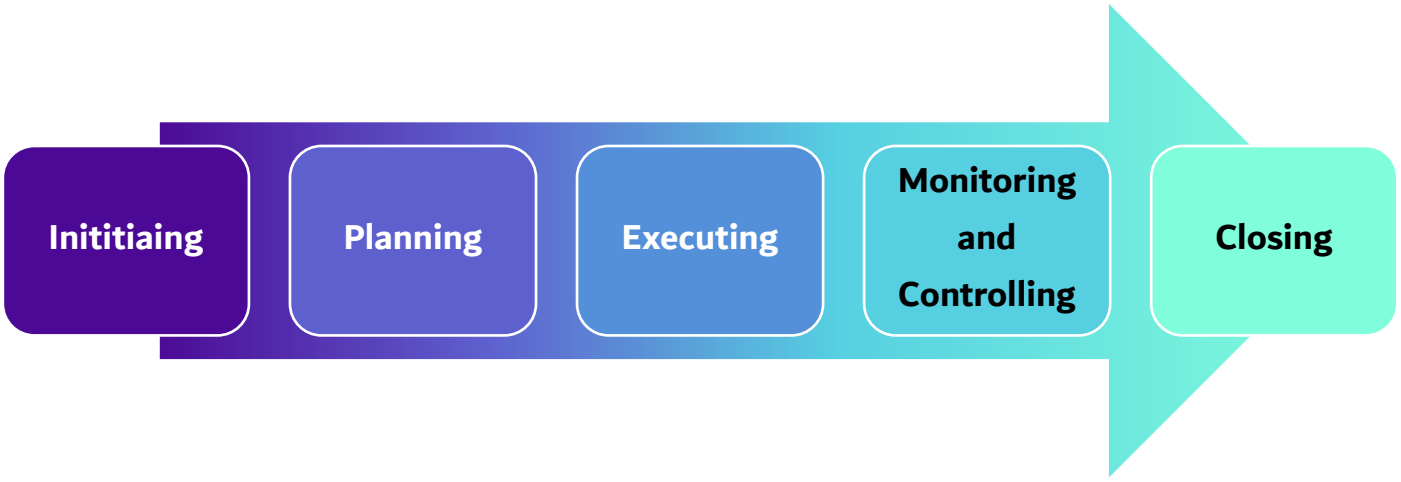
2. Project Benefits and Values

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

1. Alignment with national and international standards
2. Achieving compliance and maturity level 3 against SAMA Cybersecurity framework
3. Improved decision-making by monitoring the overall cybersecurity governance, risk, and compliance.
4. Increased competitiveness through improved customer satisfaction
5. Increased public trust through securing customer data.
6. Manages the assurance, integrity, security, value, and availability of data.
7. Increased customer and interested party satisfaction.
8. Reduced costs because of data breaches

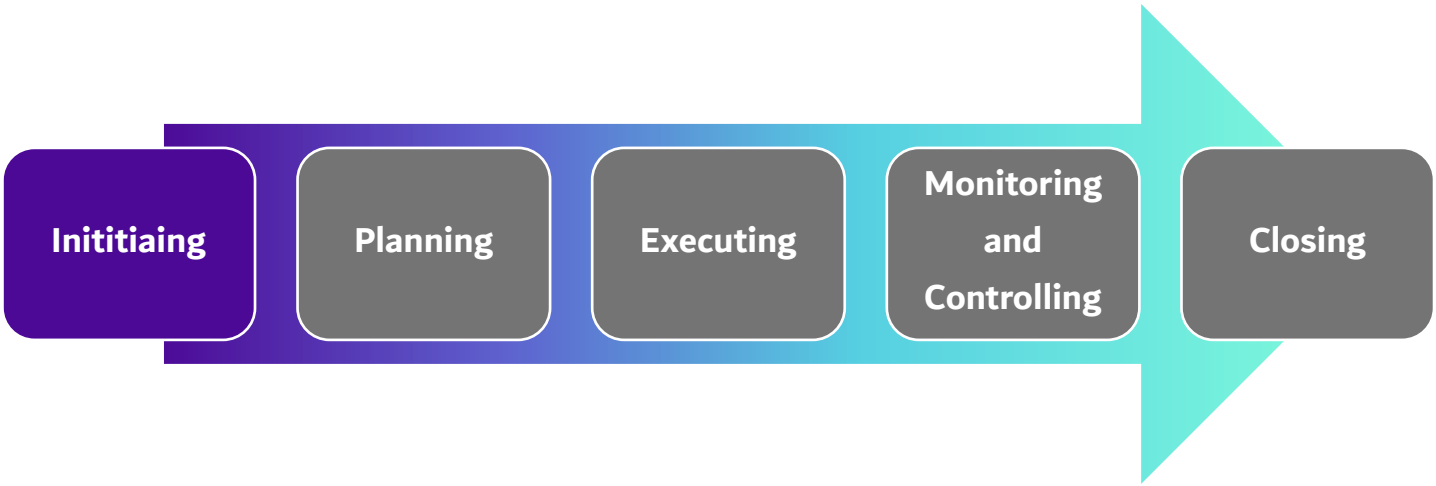
3. Project Implementation Methodology

At Trusted Vision Company, we follow the global project management method of the Project Management Institute (PMI) in terms of initiating, planning, executing, monitoring, and controlling, and closing.:



Note: Some documents may be combined and delivered into one document as needed and according to the requirements and circumstances of the entity.

4.1 Initiating Phase



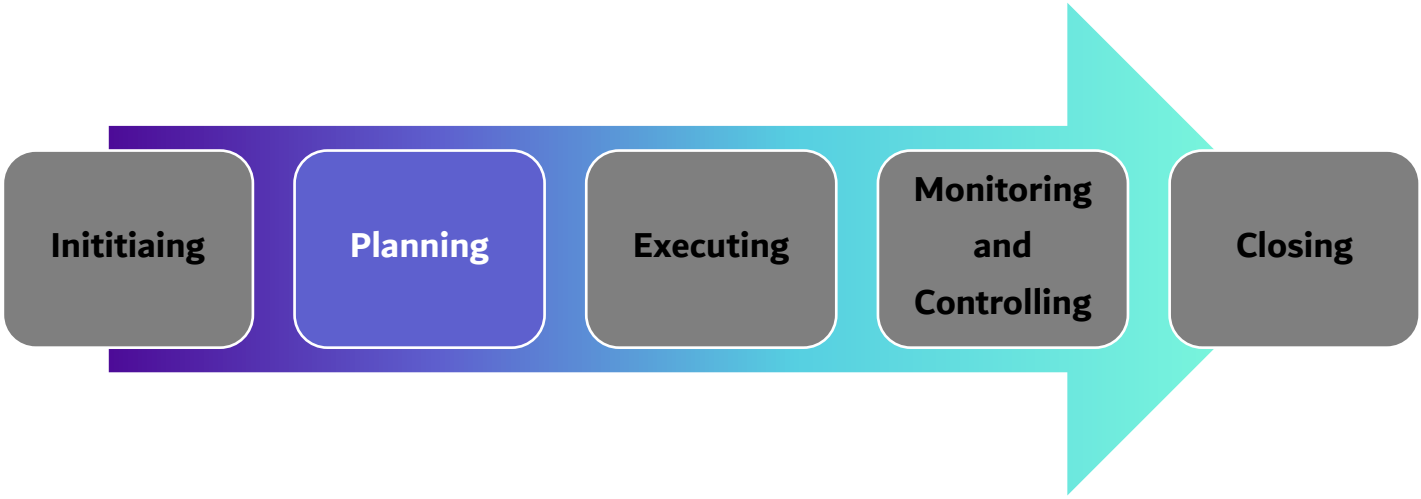
At this phase, the project is defined, and the project leader outlines their responsibilities which includes the project charter, includes restrictions and assumptions and preparing consultants to work at the entity's headquarters.

The table below lists the activities that will be conducted during this phase:

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.	Preparing the project team	• Nominate the project sponsor, project steering committee and project manager. • Obtain commitment from the project sponsor and executive management and take part in	• A list of the names of consultants who will work on this project. • A list of the names of the entity's employees who will

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
		enhancing data protection and privacy. • Allocating license officer from the entity to collaborate with consultants to achieve the implementation of the project.	be collaborating with them
2.	Develop SAMA Solution Matrix	• Acquire or purchase all required solutions mandated by SAMA	• Acquired Tools and solutions
3.	Develop Compliance Matrix between SAMA CSF, SAMA BCM,	• Review and Approve Compliance Matrix	• Compliance Matrix

4.2 Planning Phase



At this phase, various activities will be undertaken, including conducting a gap assessment to gain a comprehensive understanding of the entity, collecting all relevant documents available within the entity, evaluating its compliance posture.

The table below holds the activities that will be conducted at this phase:

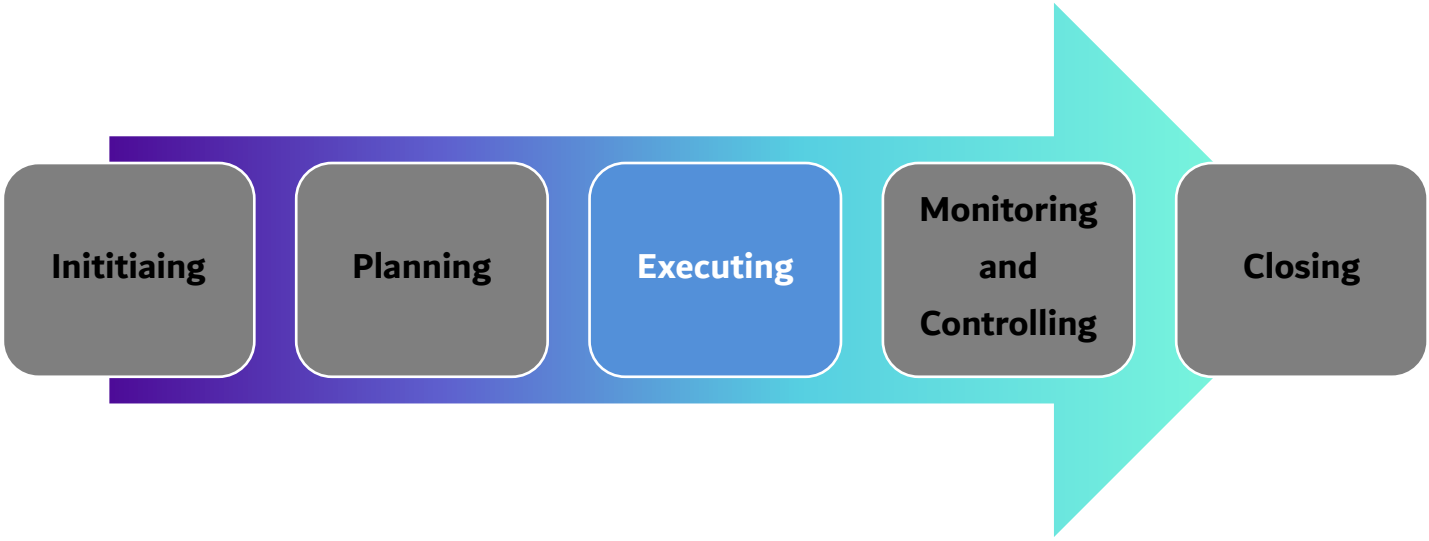
#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Preparing to start the project	• Invite all concerned and coordinate communication with them	Minutes Meeting
2.	Develop a project implementation plan (SAMA CSF project plan) that holds:	• Review and approval of the stakeholder's management plan.	Project implementation plan (PIP)

#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
	• Meeting with the concerned stakeholders. • Raising their awareness of the project • Scope of work • The requirements of the project and what is needed from them.		
3.	Collect, inventory, and review the following data: • The entity's business strategy • A list of general risks existing within the entity. • Roadmaps, information, and data management plans. • Review all systems and procedures related to data privacy, check	• Submit all required documents and information	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
	compliance with privacy regulations and document the results. • Any documents relevant to the above documents.		
4.	Conduct interviews with project stakeholders to understand their needs and expectations, including but not limited to: • Head of the organization • Information Technology Management • Data Management Office • HR department • The rest of the departments and departments within the entity	• Coordinating interviews with all departments.	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
5.	Assess the current situation, find gaps (technical, operational, and legal) internal systems, understand and study: • All data assets and their environment • Stages of processing data • Current cybersecurity management challenges • Clearly outline the scope of the project including the systems, standards, and processes that will be covered. • Reviewing the obligations of both the control party and the processing party. • Activities that can be assigned to external parties	• Send any required documents and give adequate answers to the consultants	Gap assessment report

4.3 Executing Phase:



At this phase, the project is implemented according to the plan set to obtain the expected outputs.

The table below holds the activities that will be conducted at this phase:

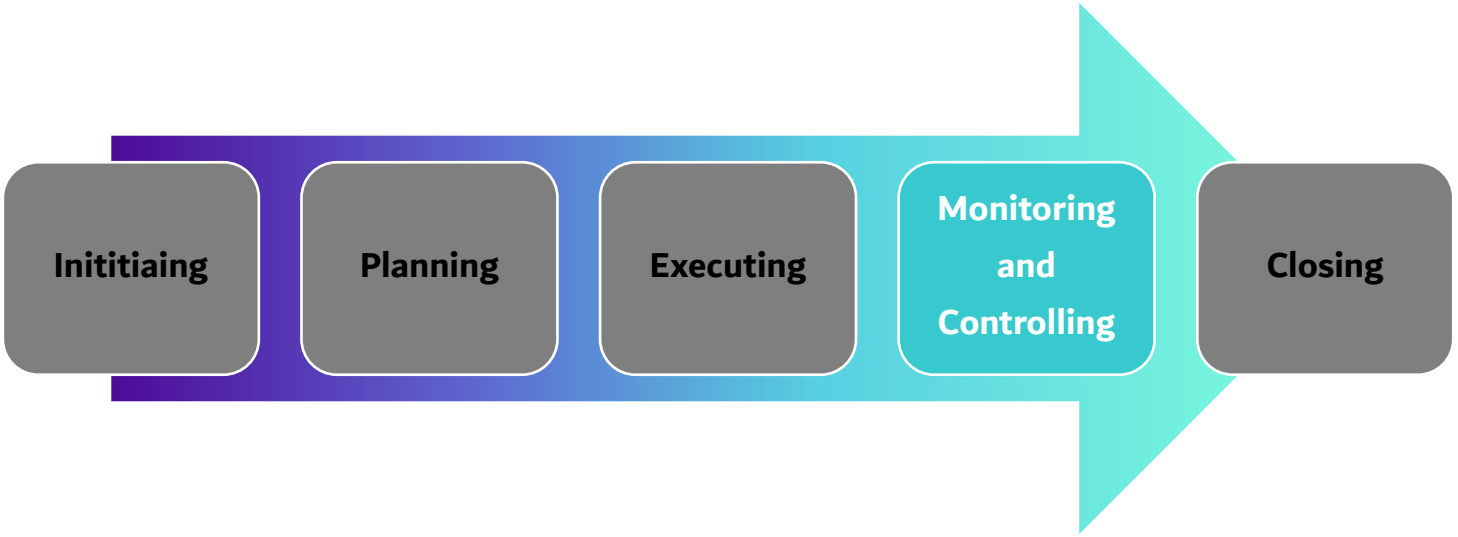
#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Review the existent documents and develop the missing cybersecurity documents, policies, and procedures including but not limited: 1. Cybersecurity strategy with roadmap 2. Cybersecurity Roles and responsibilities 3. Cybersecurity Risk Management Methodology	Review and approve all the deliverables	Cybersecurity Deliverables

#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
	4. Risk Register and Risk Assessment Forms 5. Cybersecurity in Project Management 6. Cybersecurity in Human Resources 7. Cybersecurity Awareness and Training program 8. Cybersecurity in Asset Management Policy and Procedure 9. Identity and Access Management Policy and Procedure 10. Information Systems and Information Processing Facilities Protection Policy and Procedure 11. Email Protection Policy and Procedure 12. Network Security Policy and Procedure 13. Mobile Devices Security Policy and Procedure 14. Data and Information Protection Policy and Procedure 15. Cryptography Policy and Procedure		

#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
	16. Backup and Recovery Management Policy and Procedure 17. Vulnerability Management and Patch Management Policy and Procedure 18. Cybersecurity Event Logs and Monitoring Management Policy and Procedure 19. Cybersecurity Incident and Threat Management Policy and Procedure 20. Cybersecurity in Physical and Environmental Policy and Procedure 21. Web Application Security Policy and Procedure 22. Cybersecurity requirements for business continuity management Policy and Procedure 23. Developing response plans for cybersecurity incidents 24. IT disaster recovery plan		

#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
	25. Cybersecurity requirements for Third party Policy and Procedure 26. Cybersecurity requirements for cloud computing Policy and Procedure 27. Cybersecurity requirements for Industrial Controls Systems Policy and Procedure Secure coding standards 28. Secure usage policy for users 29. Cybersecurity in change management Policy and Procedure 30. Cybersecurity Architecture 31. Cyber Security Review and Audit 32. Cybersecurity Audit Manual 33. Technologies configuration standards		

4.4 Monitoring and Controlling Phase:



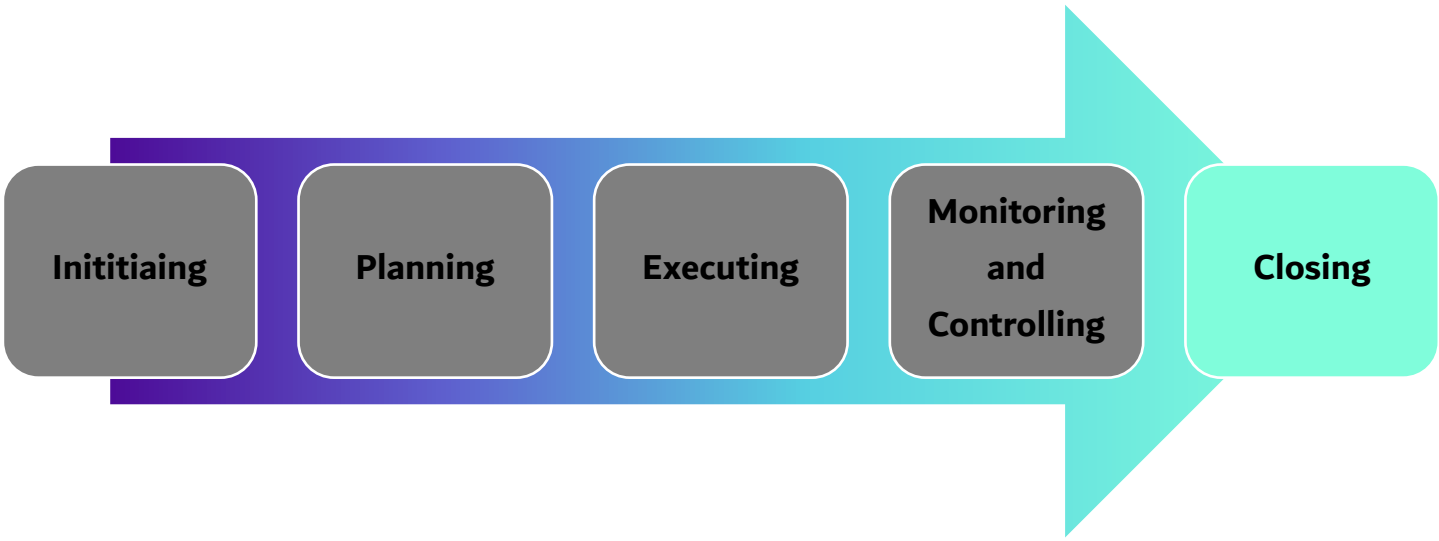
At this phase, project work is checked, performance and changes are tracked, and all project deliverables are verified. The project aims are achieved, and final approval of the deliverables is obtained.

The table below also holds the activities that will be conducted at this phase:

#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.	Activating and adhering to the prepared policies and procedures.	Implementing the policies, procedures, plans, tools, and strategies that have been provided.	Approved cybersecurity department and governance processes.
2.	Developing any remaining documents.	Reviewing and approving the documents.	Approved documents.

3.	Providing guidance and improvements on any topics (during the project period).	Reviewing, approving, and applying the guidelines.	Approved guidelines.
4.	Conducting compliance audits, reviews, and improvements	Reviewing and approving SAMA CSF audit reports	Approved audit report
5.	Sending a weekly report on the project's progress and level of advancement.	Reviewing the weekly report and providing feedback.	Weekly report on the progress of the project and level of advancement.
6.	Review Third-Party, IAM, HR, Risk Management and Encryption Controls and apply needed configuration.		Fully complied with SAMA regulations.

4.5 Closing Phase:



At this phase, we will conduct knowledge transfers to the employees.

The table below also holds the activities that will be conducted over 5 days at this phase:

#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.	Ongoing guidance and support including consultation on legal interpretations, best practices, and regulatory expectations for the entity.	Ensure commitment and cooperation from all departments, especially the cybersecurity, IT Department	Guiding and aiding the entity during the project period

#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.	Transferring knowledge (according to the schedule in the following section) about everything related to the project documents and activities (this will be on a regular basis from the first day of the project)	Allocate time and availability from the Data Management Office	Transferring knowledge of everything related to the project documents
3.	Project closure	Approve the report	Project closure report

4. Knowledge Transfer Plan

Knowledge transfer includes transferring knowledge from the consultant to the entity's employees with the aim of conducting the work that the consultants were doing and the ability to do it with confidence.

Knowledge will be transferred to the entity's employees through the following table:

How (communication channels)	From (target management)	when	what (content)
• Video meetings • In-person meetings • E-mail	Cybersecurity Department (if applicable)	Daily	All documents and plans related to SAMA CSF

5. Weekly Project Progress Report

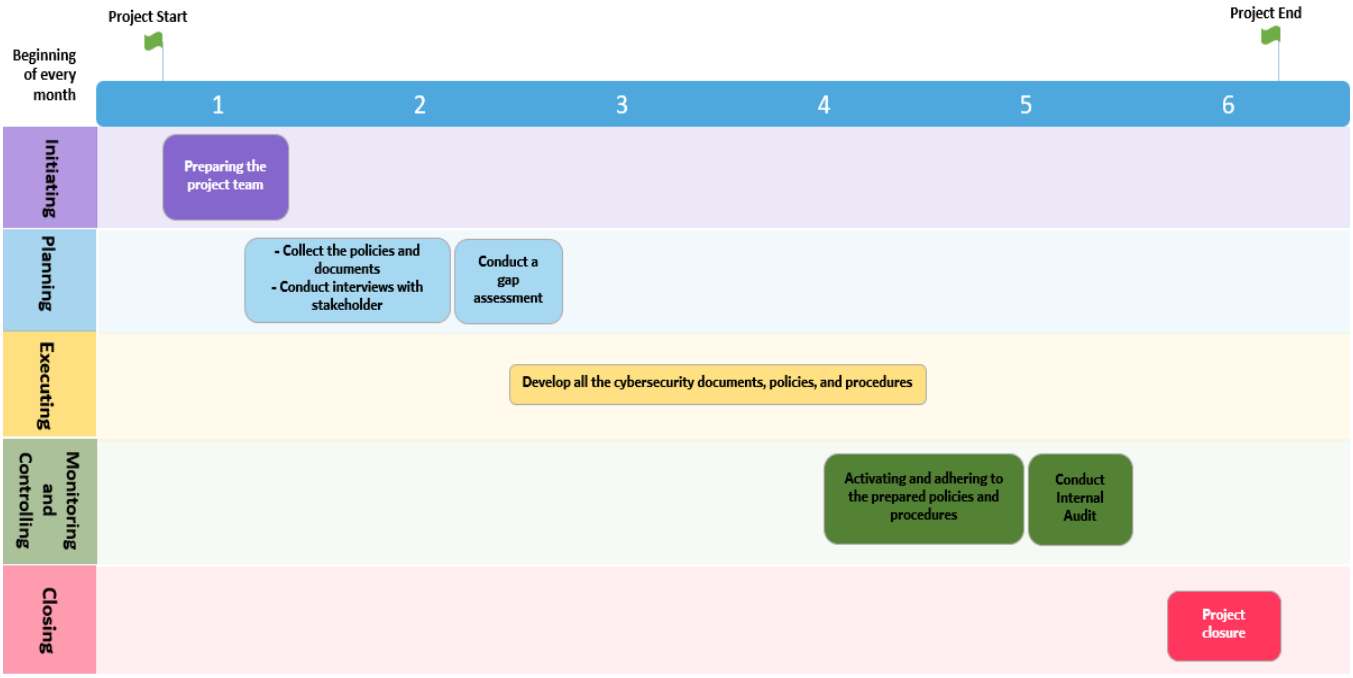
The table below shows the project progress on a weekly basis to ensure that the aims are met according to the planned schedule. The report is divided into four main sections:

1. Current Week Achievements: Includes all activities and tasks completed during the week.
2. Next Week Achievements: Find the tasks and activities planned to be implemented to ensure continuity.
3. Challenges: Review obstacles that may affect the workflow, finding areas that need solutions.
4. Recommendations: Provide suggestions to improve performance, reduce potential challenges, and ensure operational efficiency.

Project Name		xx		
Project Manager (x)		xx	Project Manager (Trusted Vision)	xx
Achievements for the past week (18-08-2024 To 22-08-2024)	1			
	2			
	3			
To be achieved next week (25-08-2024 To 29-08-2024)	1			
	2			
	3			
Challenges and outstanding issues	1			
Recommendations	1			
	2			

6. Approximate project implementation timeline

This is the approximate project timeline; it may vary based on business needs.



7. Resource, Quality and Communication Plans

In the planning phase, the project manager makes a set of plans to implement the project in the best practical way, including a resource plan, a quality plan, and a communication plan, as follows:

1. In the resource plan, the available resources are found, requirements are decided, priorities are decided, and resources are distributed according to priorities.
2. In the quality plan, quality standards are decided for application in the project, such as workflow methods, time needed to review documents, and mechanisms for reviewing and approving documents.
3. In the communication plan, the best methods of communication are decided according to the needs of stakeholders, and the plan is written down and implemented.

The plans are an important part of project management, and their purpose is to decide how to prepare resources, manage quality, and how to communicate during the life of the project. They include all the roles of stakeholders.

8. Project Management

During the project period, consultants will provide basic project management documents. These documents include:

- Schedules and minutes of meetings
- Project status reports

9. Risk Register

The most important risks related to the project and the controls for dealing with them have been identified as in the table below.

Danger number	Risk scenario	Total level	Controls for dealing with risk
1	Lack of cooperation from the entity's employees, resulting in a delay in deliveries	high	1- Allocating a person from the entity and assigning him to collaborate with the consultants 2- Giving a message and order from the authorized person to all departments about the necessity of cooperating with the consultants to ensure the completion of the project within the specified time
2	The entity is not satisfied with the documents delivered	middle	Developing a quality plan and activating it between the company and the entity
3	One of the consultants resigned during the project work	low	Providing other consultants as backup by the company

10. Project Scope and Assumptions

4.6 Out of Scope of Work

1. Implementing or buying technical tools and solutions related to the implementation of SAMA CSF.

2. Any other service not clearly mentioned in the earlier sections will be considered outside the scope of work.

4.7 Assumptions

1. **All activities will take place during the project period only and the company has no relationship if there is any delay or lack of cooperation from the entity.**

2. **The company is not responsible for any delay caused by the entity.**

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

4. **An AI bot will be integrated to record and summarize conversations, aiming to aid consultants in improving and enhancing meeting minutes.**

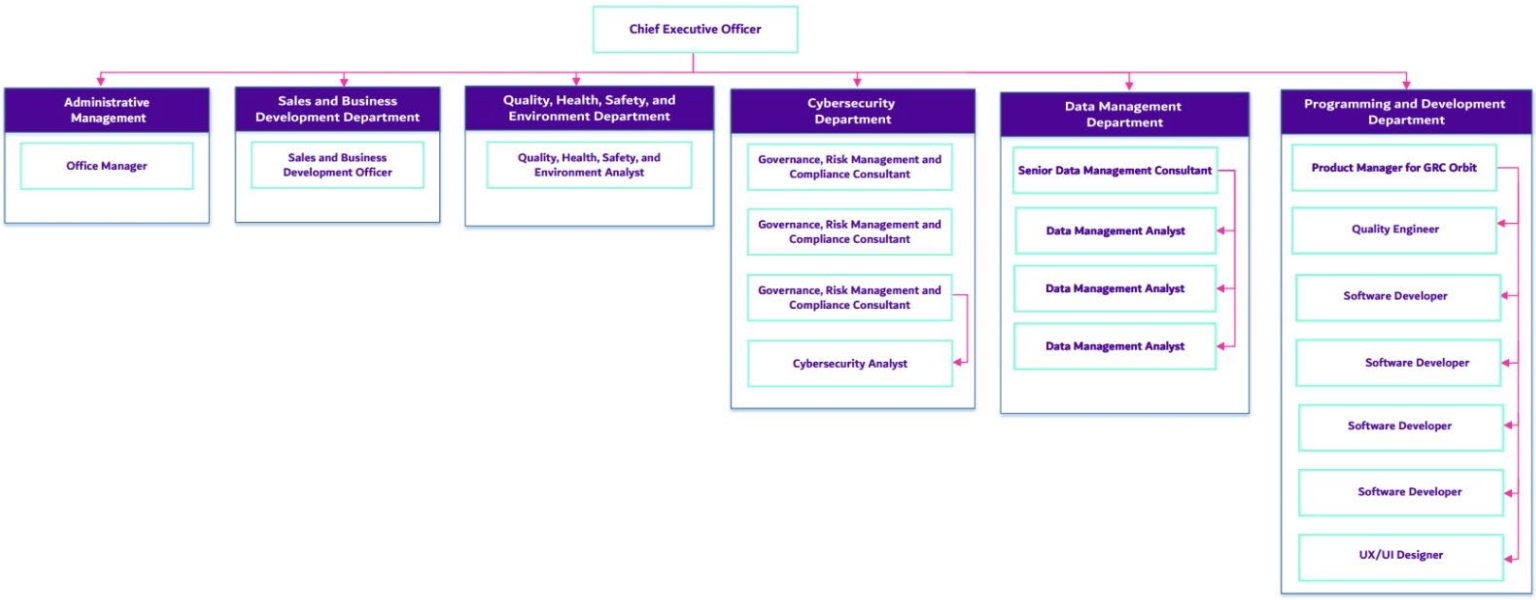
5. **All deliverables to the client will have 3 days period for their review and approval, if the time is due without any official reply, it is considered as approved deliverable.**

6. **The project will be executed over 6 months.**

11. Company Information

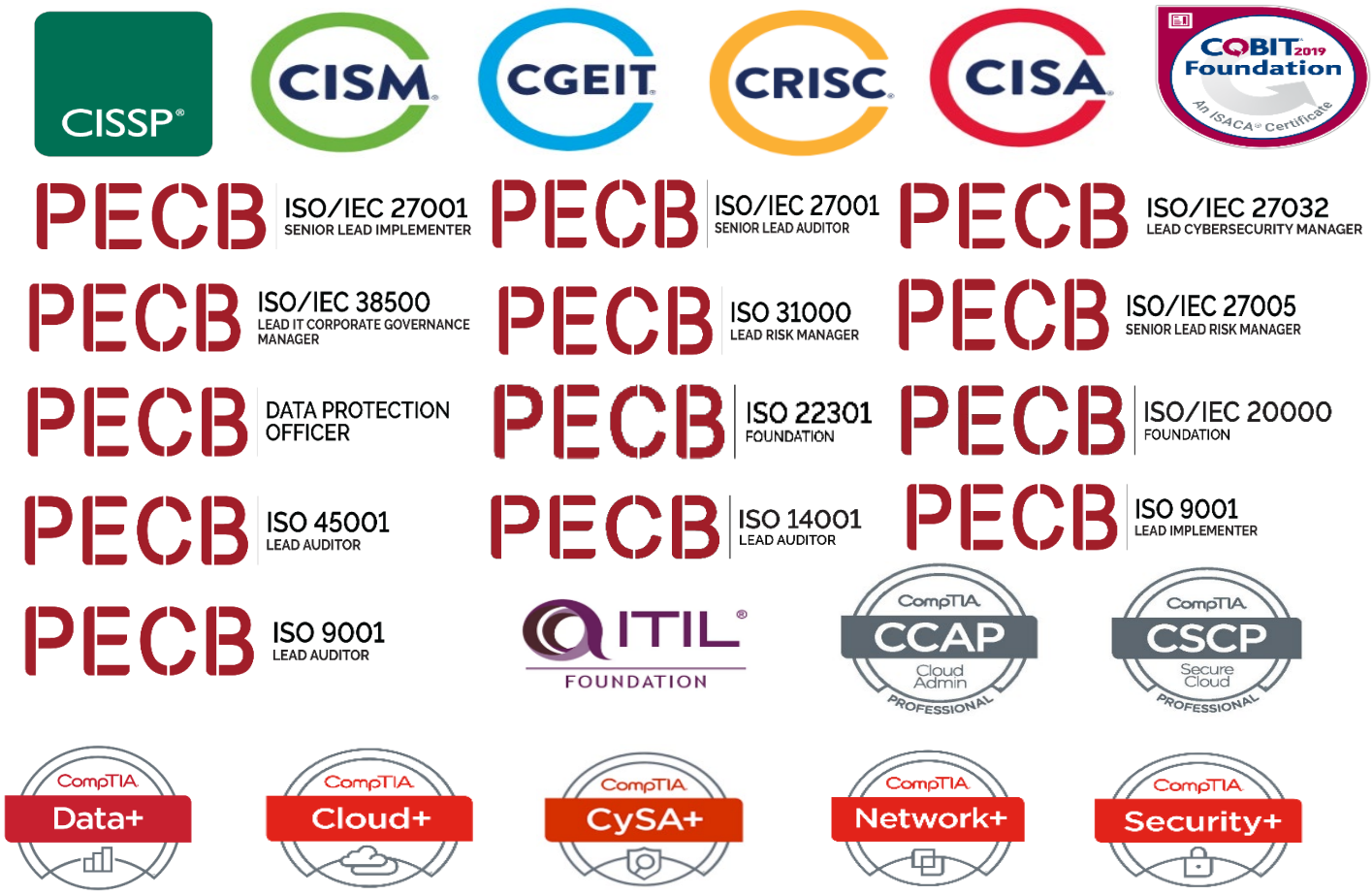
Trusted Vision is a data management and cybersecurity consulting firm that provides full services in governance, risk, and compliance management, as well as solutions and training, to help entities meet their business requirements. What sets us apart are the core values we espouse.

Organizational Structure



12. Certificates

Our team holds a variety of certifications, including the following:



13. Earlier 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	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. Developing 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. Developing 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)		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 بارا 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	مكتبة الملك عبدالعزيز العامة	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		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		1. Implement Aramco Cybersecurity Standard SACS-002 2. Develop relevant policies, procedures, and standards
11	Data Classification	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)		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 method and align it with the overall risk management method. 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 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
17	Implementation of the Personal Data Protection Regulation (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 Regulation (PDPL) Regulation	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
19	Implementation of the SAMA CSF Cybersecurity Framework	FinZey	فينزي للتمويل FinZey Finance	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

14. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	H. A	Business Regulatory, Governance and Risk Management (GRC) Advisor to the CEO	Bachelor of Computer Engineering	13 Years	1. Manage and conduct operational and operational reviews in compliance with Saudi Arabian Oil Company (SAS 002), ISO 27001, NCA-ECC and NIST SP 800-53 cybersecurity requirements. 2. Manage and develop customized cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA and Saudi Arabian Oil Company Cybersecurity Standard. 3. Manage cybersecurity risks and conduct cybersecurity risk assessments and IT risk assessments by national and international standards.

					4. Implement and review the organization's Information Security Management System by ISO 27001 and the National Cybersecurity Authority (NCA-KSA) 5. Managing and implementing the organization's business continuity management system according to ISO 22301
2	B. A	Governance and Risk Management (GRC) Consultant	Master of Cyber security	2 Years	1. Manage and conduct operational and business reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and

					Saudi Aramco Cybersecurity Standards. 3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the organization's Information Security Management System based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.
3	G.H	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	3 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001,

					NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the company's cybersecurity management system based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and

					regulations and conduct privacy risk assessments related to personal data.
4	A. Y	Governance and Risk Management (GRC) Consultant	Master of Cybersecurity	2 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.

5	I.A	Governance and Risk Management (GRC) Consultant	Bachelor of Software Engineering	15 Years	1. Design, implement, and oversee data governance frameworks, ensuring adherence to regulations such as SDAIA guidelines, and GDPR. 2. Develop data management strategies, policies, and initiatives aligned with organizational aims and best international practices. 3. Establish and enforce data quality standards to enhance accuracy, integrity, and reliability. 4. Evaluate existing data processes and recommend enhancements to improve workflow efficiency. 5. Create dashboards and generate reports to support data-driven decision-making. 6. Collaboration and Coordination: Partner with IT, operations, and business units to align data strategies with organizational goals.
8	B. B	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Information Systems	1 Year	1. Finding and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic aims.

					2. Conducting assessments of data management maturity to find gaps and recommend improvements. 3. Developing Business Intelligence (BI) use cases and enhance user experience through data-driven insights. 4. Designing and implementing plans, policies, and procedures for Master and Reference Data Management, Freedom of Information, Document and Content Management, and Data Value Realization in alignment with NDMO regulations.
9	B. A	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	25 Years	1. Overseeing the design of information and communications systems 2. Overseeing the implementation of ISO 27001 certification

					3. Overseeing the implementation of communications and data transmission projects 4. Overseeing the implementation of three fiber optic projects to ensure data transmission system security. 5. Overseeing the implementation of LAN and WAN networks and ensuring data transmission system security. 6. Overseeing the implementation of the SCADA network