NCA-ECC & DCC Consultation Proposal

Version 1.0

Date: 24-09-2025 AD

Prepared by: Trusted Vision Company for Cybersecurity

Contact Information

To inquire about this document and the information provided, you can contact the people mentioned on the table below:

Name	**Hashem Al-Azizi**
Phone Number	**+966-53-122-1580**
E-mail	**Hashem.azizi@trustedvision.biz**
Address	**Cordoba District, Saeed Bin Zaid Street** **P.O. Box 13247, Building No. 6482** **Riyadh - Kingdom of Saudi Arabia**

TRUSTED VISION

Contents

1. Executive Summary of CLIENT's requirements

The client requests consultation services covering

1. **The National Cybersecurity Authority Essential Cybersecurity Controls (NCA-ECC)**
2. **The National Cybersecurity Authority Data Cybersecurity Controls (NCA-DCC), in alignment with the Data Classification Standard issued by the National Data Management Office (NDMO).**

The ECC establishes the minimum cybersecurity requirements for information and technology assets to reduce risks arising from internal and external threats, while the DCC sets a comprehensive framework for protecting and managing data throughout its lifecycle, including classification, labeling, handling, storage, and disposal. Together, these controls align with industry's best practices, enhance regulatory compliance, and strengthen the organization's overall cybersecurity posture.

We believe that our extensive expertise in delivering similar cybersecurity and data management projects positions us among the leading consulting firms. This is further reinforced by:

1. Proven expertise in designing and implementing projects of similar scope and complexity.
2. A balanced mix of international and regional experience in addressing data consulting and cybersecurity challenges.
3. An effective project implementation approach that ensures requirements are addressed in a timely, professional, and high-quality manner.
4. Extensive knowledge of international standards and best practices, enabling the design and implementation of robust, future-ready solutions.
5. Best-in-class data management and cybersecurity consulting expertise tailored to organizational needs.
6. Proven methodologies and project management practices guarantee successful delivery and measurable results.

We are confident that our proposed services and approach will meet your expectations, and we look forward to building a long-term and mutually beneficial business relationship.

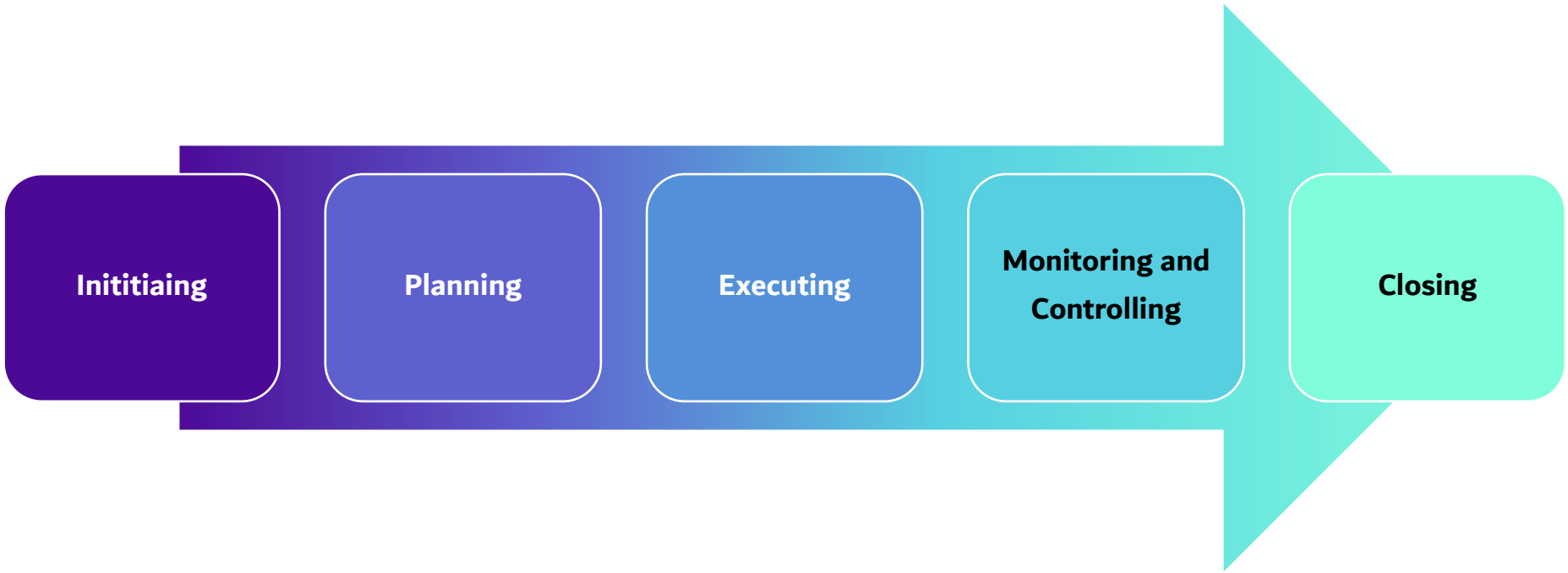
2. Project Benefits and Values

By implementing this project, the organization is expected to realize the following benefits and added value:

1. Alignment with national and international standards, ensuring consistency with globally recognized best practices.
2. Achieving compliance with NCA requirements, particularly the ECC and DCC frameworks.
3. Alignment with the Data Classification Standard issued by the National Data Management Office (NDMO), ensuring proper governance and protection of data throughout its lifecycle.
4. Enhanced decision-making through effective monitoring of cybersecurity governance, risk, and compliance.
5. Improved competitiveness driven by stronger customer satisfaction and trust.
6. Strengthened public confidence by ensuring the security and protection of customer data.
7. Effective data management, safeguarding assurance, integrity, security, value, and availability of information assets.
8. Higher satisfaction for customers and stakeholders by meeting their expectations for security and reliability.
9. Reduced financial and reputational costs associated with potential data breaches.

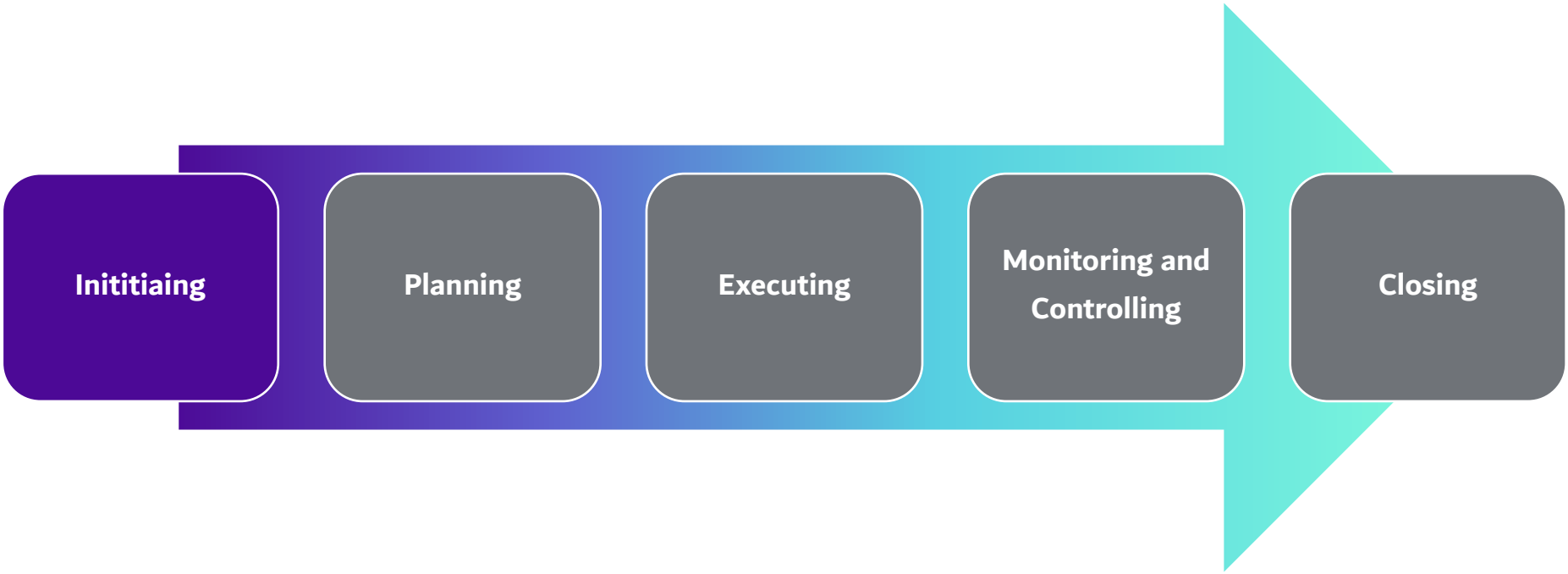
3. Project Implementation Methodology

At Trusted Vision Company, we follow the global project management methodology 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 required and according to the requirements and circumstances of the entity.

4.1 Initiating Phase



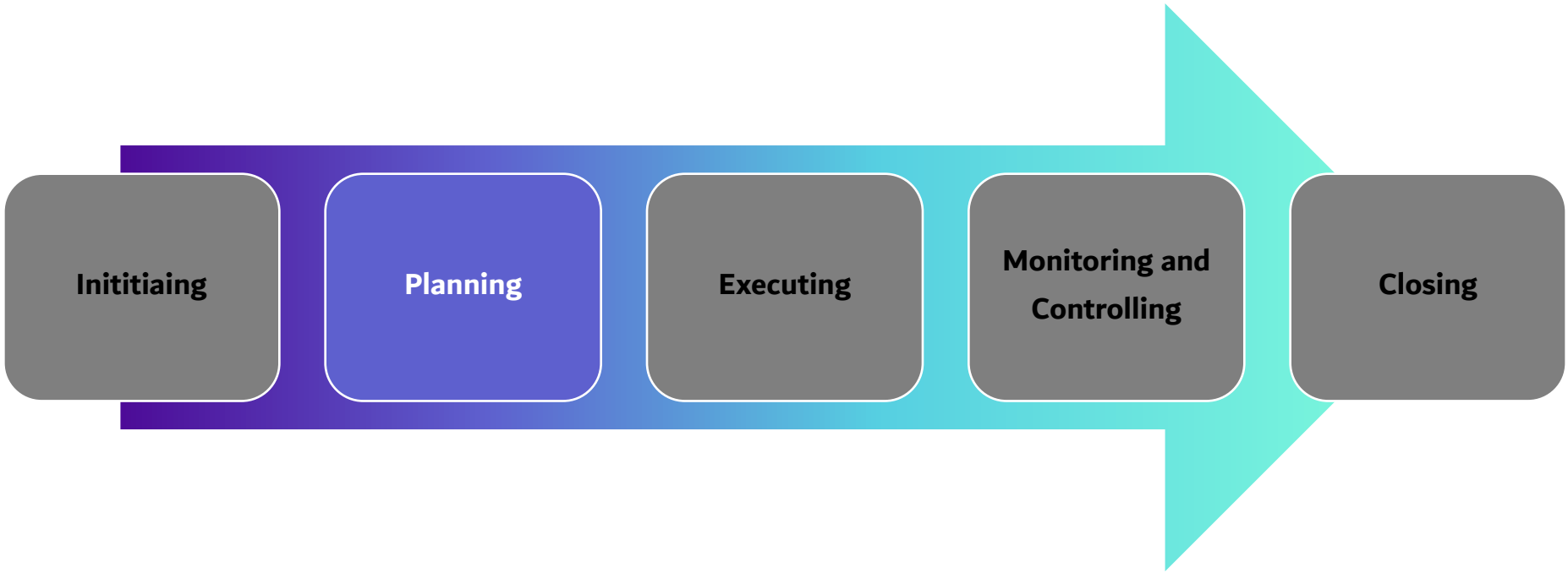
At this phase, the project is defined, and the project leader outlines their responsibilities which includes the project charter, includes restrictions and assumptions and preparing consultants to work at the entity's headquarters.

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

#	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	Assigning a project manager from the entity to work with the consultants	A team prepared to start the project

#	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	Preparing to start the project and holding the kickoff meeting	Inviting the head of the entity and all department heads	Meeting minutes
3	Develop Project Charter	Review and approve the project charter	Project Charter

4.2 Planning Phase



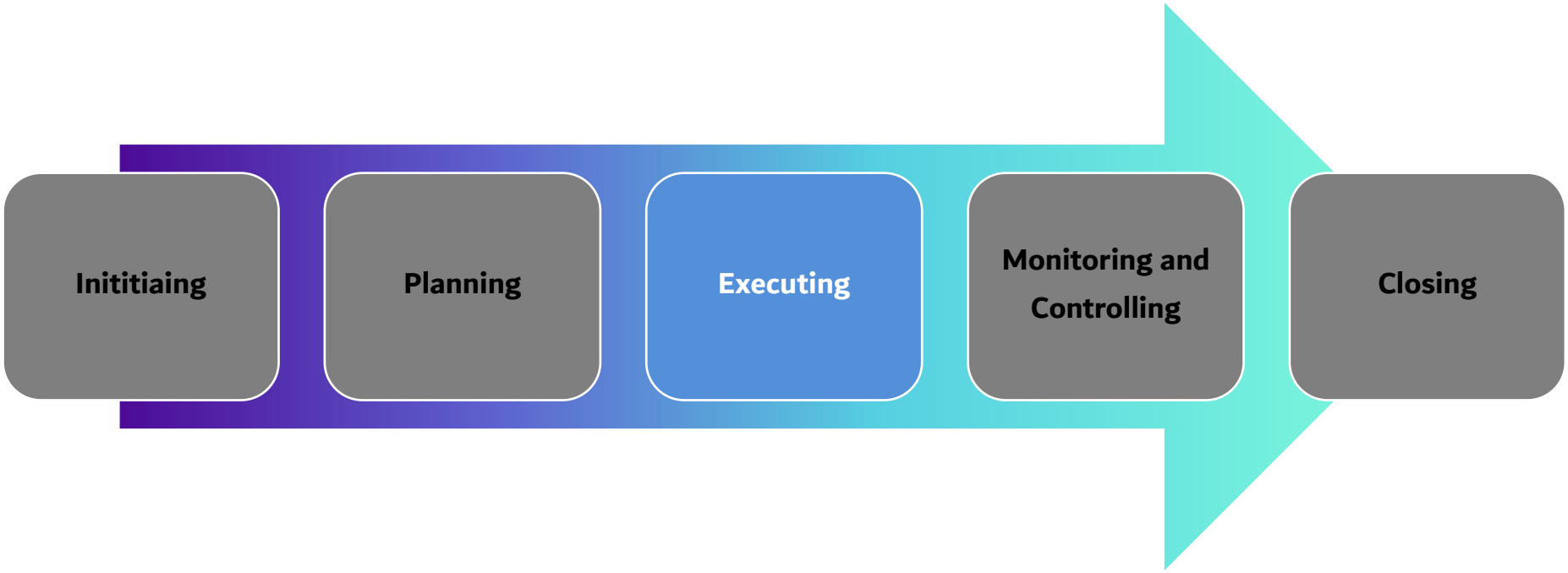
At this phase, various activities will be undertaken, including conducting a current status assessment to gain a comprehensive understanding of the entity's cybersecurity framework, collecting all relevant documents available within the entity, evaluating its compliance posture, and identifying associated cyber risks.

The table below contains the activities that will be carried out at this phase:

#	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	Collect evidence and information related to cybersecurity and data requirements, including current cybersecurity governance documents: • Policies • Procedures • Cybersecurity Strategy, Digital Transformation, Data Management and IT • Frameworks • Technical Standards • Information and Technology Asset Registe	Submitting the required documents	Meeting minutes
2	Conducting interviews with departments and stakeholders, including but not limited to: 1. Head of Company 2. Risk Management Committee 3. Manufacturing Department 4. Head of IT Department 5. Head of Cybersecurity Department 6. Head of Human Resources	• Coordinate interview appointments • Submit required documents	Meeting minutes
3	Develop a solution matrix sheet that includes the required solutions and tools to be brought to implement the NCA ECC , DCC Controls.	Review and approve the proposed solution matrix sheet that includes the required solutions and tools to	Solution Matrix Sheet

#	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
		be brought by the client to implement the cybersecurity controls	
4	Conduct detailed assessments against ECC & DCC controls, analyze compliance status, identify gaps, and develop a prioritized remediation roadmap with timelines.	Provide access to policies, procedures, systems, and relevant stakeholders for interviews and evidence collection.	Comprehensive Gap Assessment Report, Remediation Roadmap with priorities and timelines.

4.3 Executing Phase



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

The table below contains the activities that will be carried out at this phase:

#	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 data inventory and mapping across the company's technical systems and departments, with a focus on both personal and sensitive data.	Perform Data Impact Assessment (at the levels of national interest, authority's interest, individuals, and environment).	Comprehensive Data Inventory Record

#	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	Develop documents related to the cybersecurity and data management system (policies, standards, procedures, and measurement indicators), including but not limited to: • Cybersecurity Strategy for 3 years • Cybersecurity Oversight Committee Charter • Acceptable Use Policy • Malware Protection Policy • Data Storage and Disposal Policy and Procedure • Third-party Security Management • Cybersecurity Incident Management • Cybersecurity Penetration Testing policy and procedure • Cybersecurity Event Logs and Monitoring Management • Physical Security Policy • Cybersecurity Business Continuity Policy • KPI's • Cloud Computing and Hosting Policy • Information Asset Management • Data Classification and Protection Policy • Mobile and Personal Device Security Management	Review and approval of documents	Documents related to the cybersecurity and data system

#	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
	• Network and Communications Security Process • Secure Development Lifecycle for Applications and Systems. • Identity Management and Access Management. • Cybersecurity in Human Resources Policy and Procedure • Data and Information Policy • Encryption and Key Management. • Backup and Recovery Management. • Cybersecurity Risk Management methodology (Policy, Procedure, Treatment report, Register) covers these standard (ECC-DCC) • Develop Root Cause Analysis corrective actions resulting from Cybersecurity incidents. • Cybersecurity Risk Register • Technical Vulnerability Management Standards. • Cybersecurity Compliance Management Standards. • Developing and Improving Periodic Review and Audit Procedures • Cybersecurity Threat Management Standards • Retention and Destruction Policy		

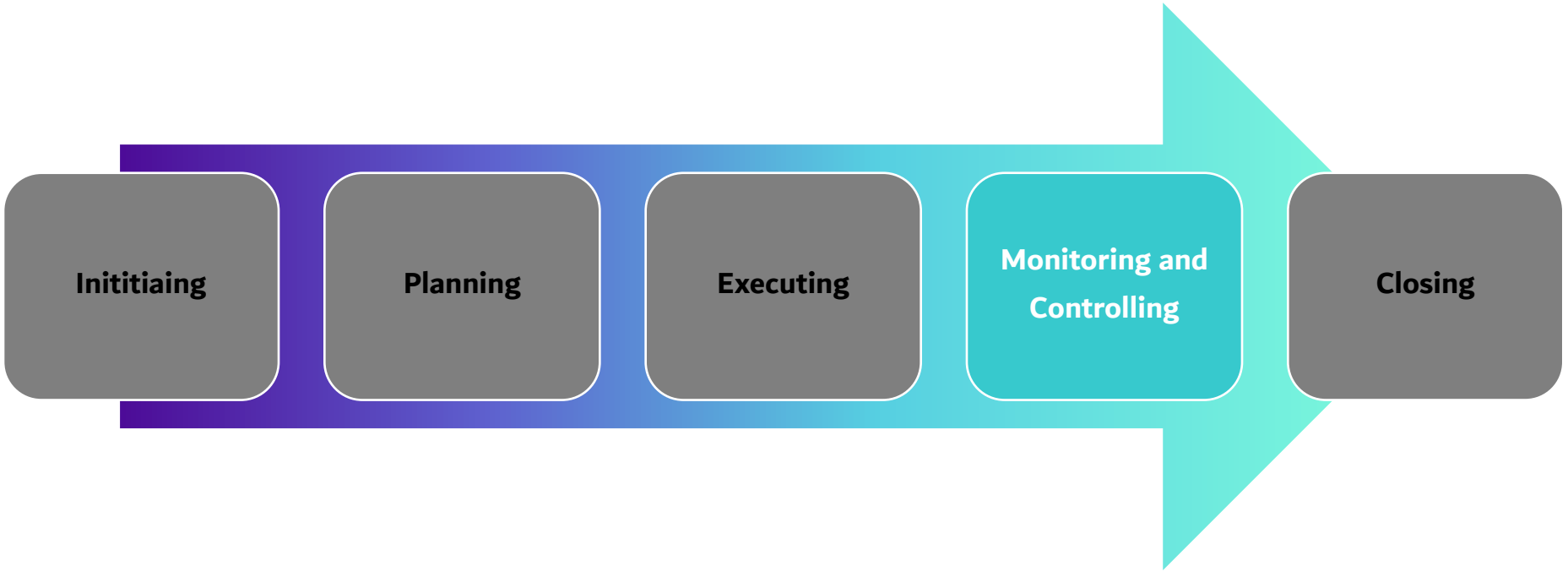
#	Activities that must be conducted by the Trusted Vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity

	• Program and plan for internal audit.
	• Web Application Security
	• Configuration Standards for Technical Assets
	• Cybersecurity Projects Management Policy
	• Cybersecurity Roles and Responsibilities (ECC-DCC)
	• List of Employees with Access to Secrete and Top-Secret Data
	• List of Storage Assets Handling Restricted, Secrete, or Top-Secret Data
	• Data Sharing Procedure Template with Third Parties
	• Develop the operating model and organizational structure Including:
	  ○ Organization Chart
	  ○ Cybersecurity Roles and Responsibilities
	  ○ SLAs
	  ○ Communication Plan		

3	Identify and assess critical business functions, processes, and evaluate the potential impact of their disruption across different threat scenarios (cybersecurity incidents, natural disasters, engineering/development failures).	Provide information on critical business functions, processes, and dependencies.	Critical Business Functions & Impact Assessment Report.

#	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	Conduct a comprehensive risk assessment covering internal and external threats to critical operations and IT systems.	Provide access to systems, documentation, and relevant stakeholders.	Risk Assessment Report with identified threats and vulnerabilities.

4.4 Monitoring and Controlling Phase



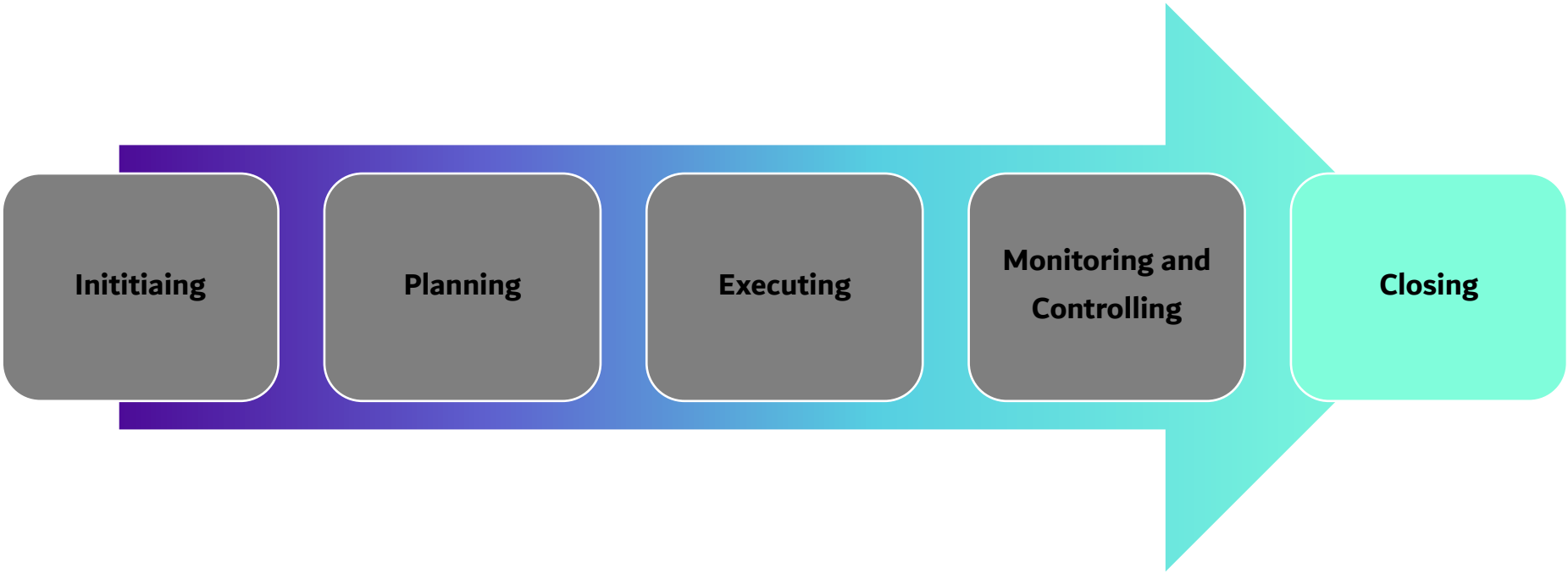
At this phase, project work is monitored, performance and changes are tracked, and all project deliverables are verified.

The table below also contains the activities that will be carried out at this phase:

#	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	Supervise the implementation of the governance cybersecurity and data strategy, policies, procedures and standards.	Implement all governance cybersecurity strategy, policies, procedures and standards	-

#	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	Provide ongoing guidance and support during implementation of ECC and DCC requirements.	Ensure coordination with internal teams and provide necessary information and access.	Continuous Support Records and Progress Reports.
3	Awareness sessions for: • Senior Management (2 Sessions) • IT Department (2 Sessions) • All Employees (4 Sessions)	Nominate participants and ensure attendance of relevant staff.	Training Sessions, Training Materials, and Attendance Records.
4	Conduct internal audit against NCA-ECC and NCA-DCC requirements, identify gaps, and provide recommendations for corrective actions.	Facilitate access to systems, documents, and staff required for the internal audit process.	Internal Audit Report covering ECC & DCC compliance gaps and recommendations.
5	Develop awareness campaigns and compliance handbooks to promote adoption of cybersecurity policies and practices.	Distribute materials internally and support awareness initiatives.	Awareness Campaign Materials and Compliance Handbook.
6	Provide a Bi-Weekly email on the progress	-	Project progress

4.5 Closing phase



At this phase, the project closure report is signed, and the project is officially closed.

The table below contains the activities that will be carried out at this phase:

#	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	Project sign-off	Sign off by the company's Management	Project closure report

4. Knowledge Transfer

Knowledge transfer includes transferring knowledge from the consultant to the entity's employees and training with the aim of carrying out the work that the consultants were doing and enabling the Authority's employees to be able to carry out all the consultants' work with confidence and competence. Knowledge will be transferred to the entity's employees through the following schedule:

How (communication channels)	From (target management)	when	what (content)
• Video meetings • In-person meetings • E-mail	Cybersecurity (if applicable) or relevant department	On a daily basis	All documents and plans related to the project

5. Weekly Project Progress Report

The table below shows the project progress on a weekly basis to ensure that the objectives 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: Identify the tasks and activities planned to be implemented to ensure continuity.
3. Challenges: Review obstacles that may affect the workflow, identifying 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. Resource, Quality and Communication Plans

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

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

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

7. 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 work with the consultants 2. Giving a message and order from the authorized person to all departments regarding 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

8. Project Scope and Assumptions

Out of Scope of Work

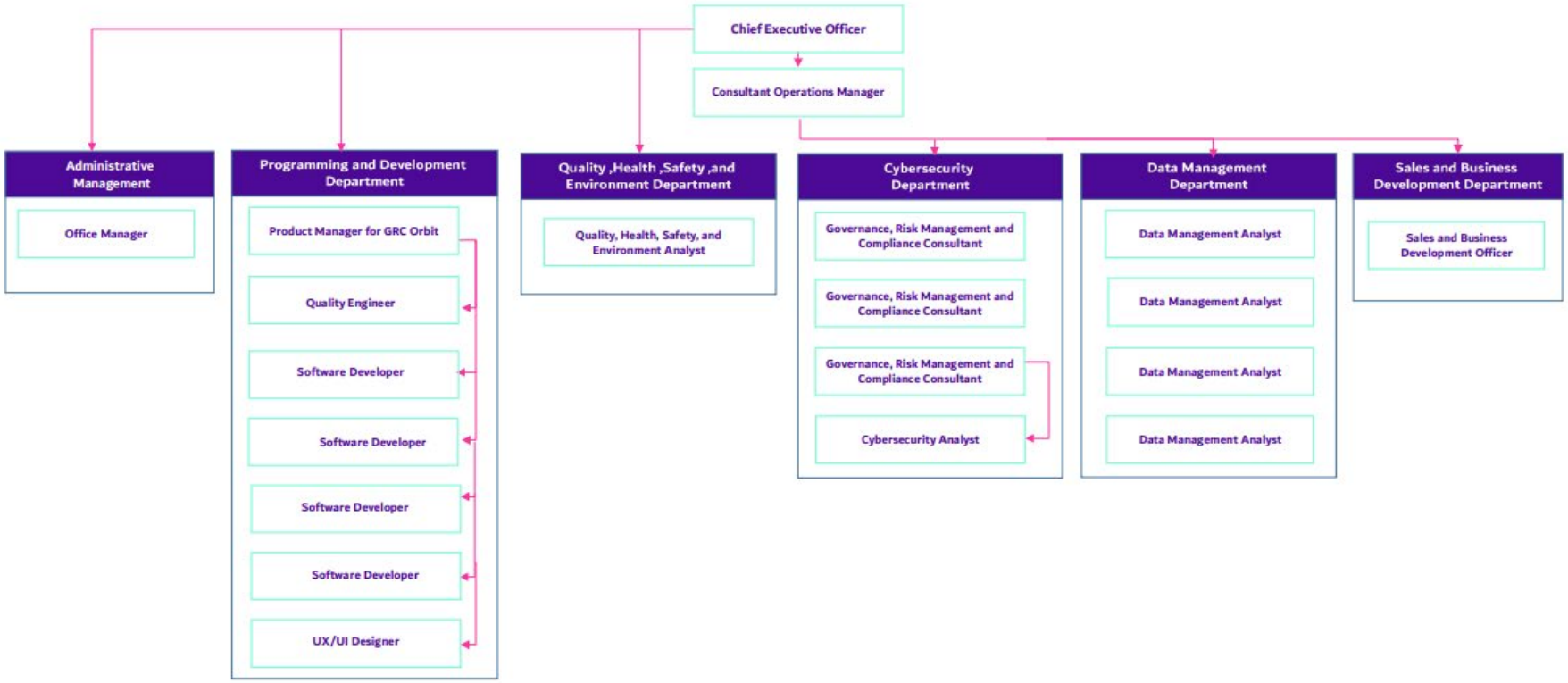
1. Implementing or purchasing technical tools and solutions related to the implementation of the NCA-ECC, DCC
2. Any other service not clearly mentioned in the previous sections will be considered outside the scope of work.

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. **The proposal includes only one review of the submitted documents.**
5. **Delivered documents will be reviewed for 3 days only.**
6. **This project will be implemented within 6 months.**
7. **An AI bot will be integrated to record and summarize conversations, aiming to assist consultants in improving and enhancing meeting minutes**
8. **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.**

9. Company Information

Trusted Vision is a cybersecurity and data management 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.



10. Certificates

Our team holds a variety of certifications, including:


PECB
ISO 9001
LEAD AUDITOR


ITIL
FOUNDATION


CompTIA
CCAP
Cloud Admin
PROFESSIONAL

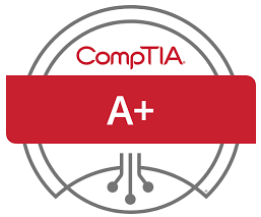

CompTIA
CSCP
Secure Cloud
PROFESSIONAL


CompTIA
Data+


CompTIA
Cloud+


CompTIA
CySA+


CompTIA
Network+


CompTIA
A+


CompTIA
Security+


CNSS


FORTINET
NSE
1
ASSOCIATE


FORTINET
NSE
2
ASSOCIATE


FORTINET
NSE
3
ASSOCIATE


FORTINET
NSE
4
PROFESSIONAL


C|EH
Certified Ethical Hacker


paloalto
NETWORKS
PCCSA


paloalto
NETWORKS
PCNSA


paloalto
NETWORKS
PCNSE


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA
CYBER+INFRASTRUCTURE


ASSOCIATE
CERTIFIED

11. 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	Implementing a Business Continuity Management System SAMA BCM	ASIG Insurance Company	ACIG التأمين أمان	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)		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		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 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 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 SAMA CSF	Finzey		1. Conduct a comprehensive cybersecurity gap assessment. 2. Develop policies, procedures, and standards in alignment with the Saudi

			فينزي للتمويل FinZev Finance	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

12. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	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.

					1. Overseeing the implementation of the SCADA network
2	S.H	Governance and Risk Management (GRC)	Bachelor of Computer Engineering	6 Years	2. 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. 3. 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. 4. Manage cybersecurity risks and conduct cybersecurity risk assessments and IT risk assessments by national and international standards.

					5. Implement and review the organization's Information Security Management System by ISO 27001 and the National Cybersecurity Authority (NCA-KSA) 6. Managing and implementing the organization's business continuity management system according to ISO 22301
3	E. A	Governance and Risk Management (GRC) Consultant	Master of Cyber security	6 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.
4	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.
5	R. Y	Governance and Risk Management (GRC) Consultant	Bachelor 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.
6	B. B	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Information Systems	2 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.