

Technical and Financial Proposal for CRF: 2023 Implementation

Version 1.0

Date: 19-05-2026 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
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 requirements	4
2. Project Benefits and Values	4
.3 Project management and implementation methodology	5
4. Knowledge Transfer	17
5. Weekly Project Progress Report	18
6. Resource, Quality and Communication Plans	19
7. Risk Register	20
8. Project Scope and Assumptions	21
.9 Company Information	22
.10 Certificates	23
.11 Previous Projects	25
12. Staff	32

1. Executive summary of client requirements

Trusted Vision Company is pleased to offer consulting services for the implementation Cybersecurity Regulatory Framework (CRF) for Service Providers in the Information and Communications Technology Sector.

We believe that our extensive experience in conducting similar consultation projects positions us among the elite consulting firms. This is further supported by our:

1. Balanced blend of international and local expertise in cybersecurity.
2. Efficient project execution approach, ensuring timely, professional, and high-quality outcomes.
3. Comprehensive knowledge and experience in designing and implementing solutions aligned with international standards and best practices.
4. Best consulting expertise to enhance cybersecurity.

2. Project Benefits and Values

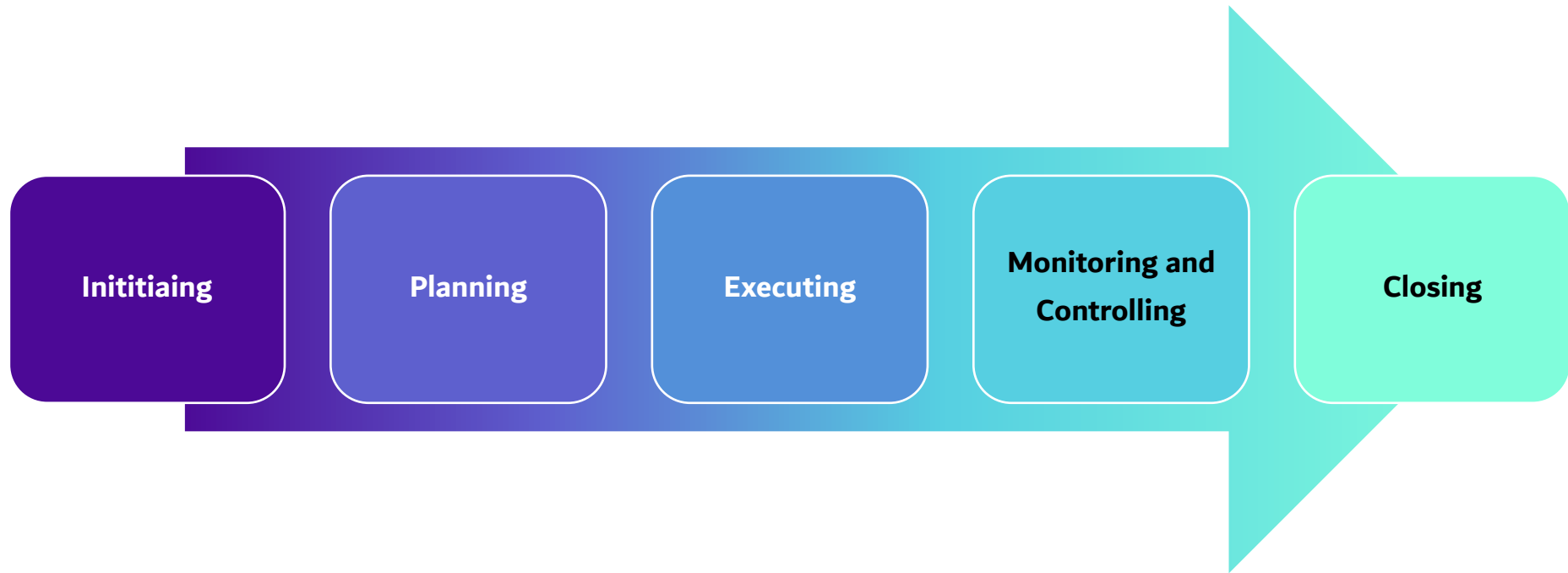
The implementation of the Cybersecurity Regulatory Framework (CRF) will provide significant strategic and operational value to the client. By aligning with CST's mandated cybersecurity requirements, the organization is expected to achieve the following key benefits:

1. Achieve CST Compliance
2. Stronger Cybersecurity Posture
3. Reduced Cyber Risks
4. Higher Operational Resilience
5. Increased Customer Trust

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

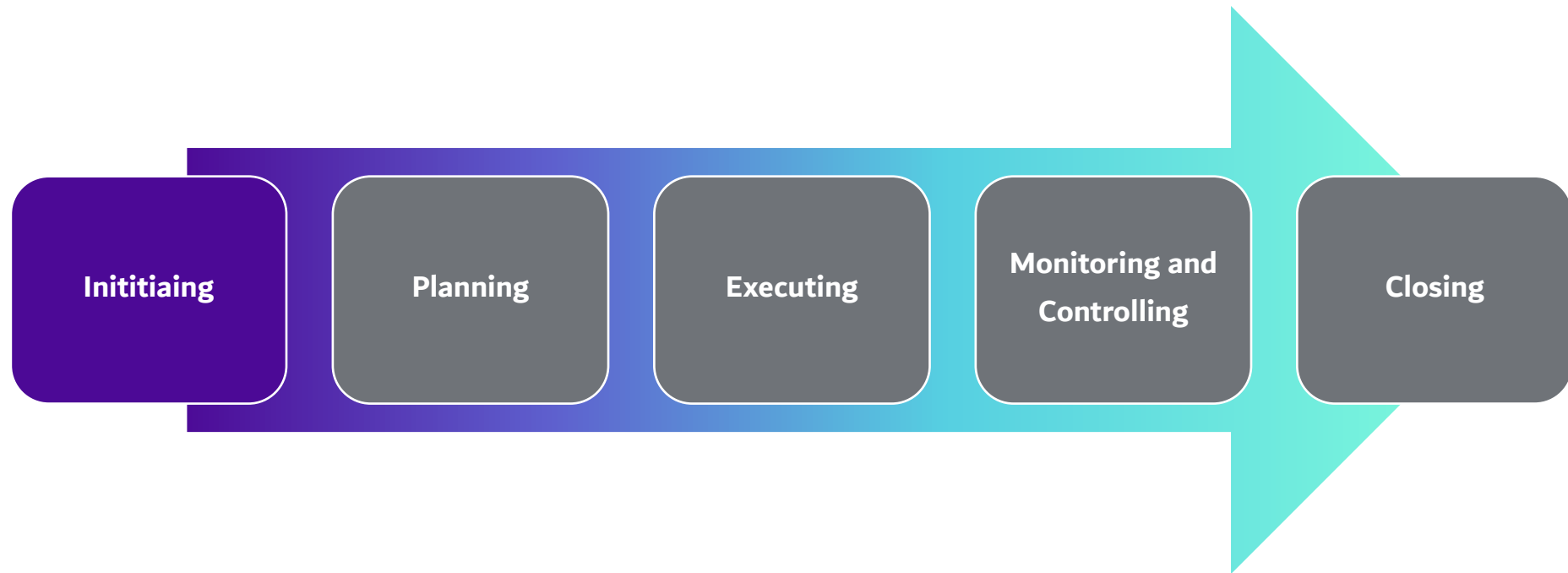
Note: Some documents may be combined and delivered to one document as needed and according to the requirements and circumstances of the entity.

3. Project management and implementation methodology



We at Trusted Vision follow the global project management methodology of the Project Management Institute (PMI) in terms of initiating, planning, executing, monitoring, and controlling, and closing.

3.1 Initiating Phase



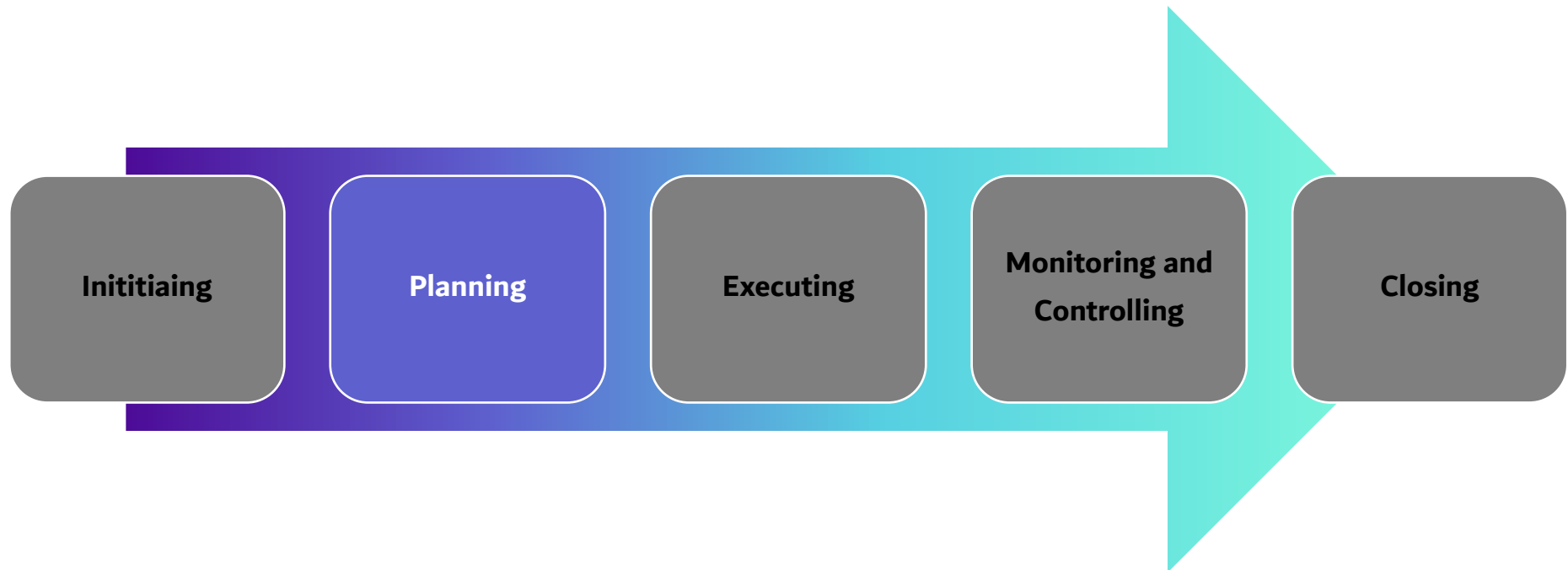
At this phase, the project is defined, and the project leader outlines their responsibilities, identifies key stakeholders.

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
2	Preparing to start the project and holding the kickoff meeting	Inviting the head of the entity and all department heads	Meeting minutes

#	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
3	Develop Project Plan	Review and approve the project plan	Project plan

3.2 Planning Phase

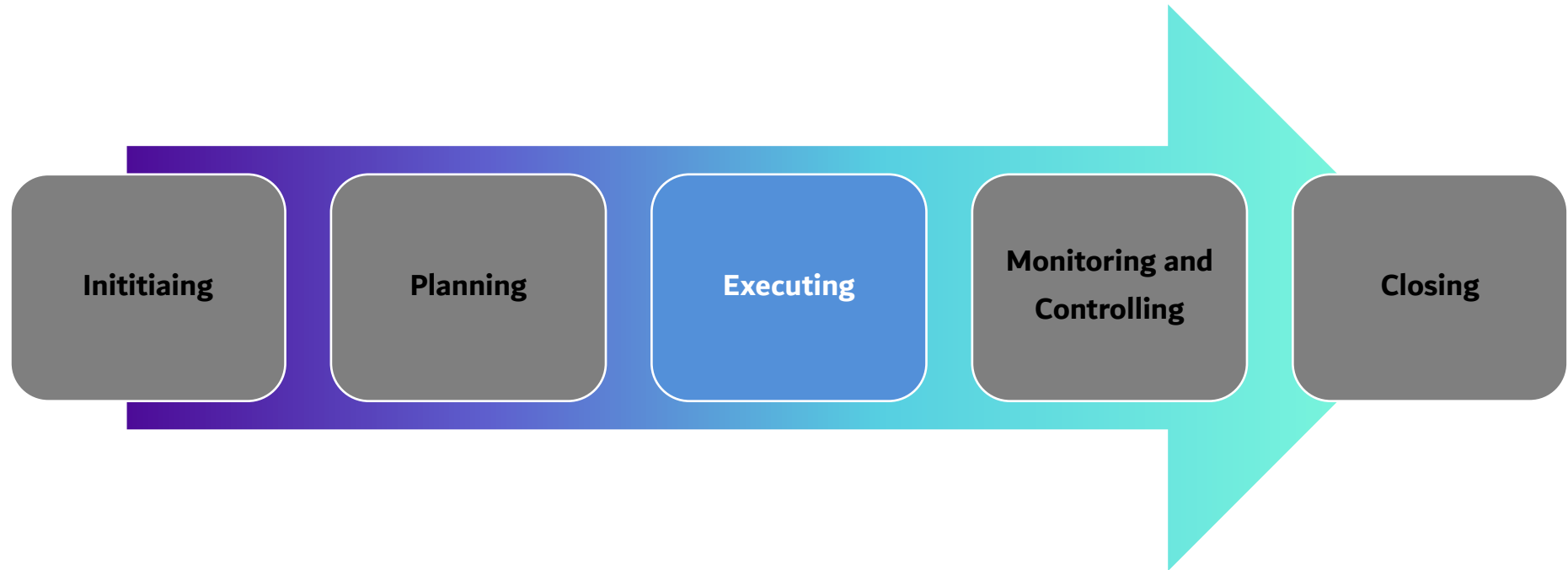


At this phase, various activities will be undertaken, including conducting a status assessment to gain a comprehensive understanding of the entity's cybersecurity framework, collecting all relevant documents available within the entity, evaluating its compliance posture, and identifying associated cyber 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 requirements, including current cybersecurity governance documents: • Policies • Procedures • Cybersecurity Strategy, Digital Transformation, Data Management and IT • Frameworks • Technical Standards • Information and Technology Asset Register	Submitting the required documents	Meeting minutes
2	Conducting interviews with departments and stakeholders, including but not limited to: 1. General Department of Cybersecurity 2. General Department of Information Technology 3. General Department of Digital Transformation 4. Facilities Department 5. Administrative Affairs Department	1. Coordinate interview appointments 2. Submit required documents	Meeting minutes
3	Conduct CRF Gap assessment plan (scope, tools, required access)	Review and approve the gap assessment plan	Approved gap assessment plan

3.3 Executing Phase



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

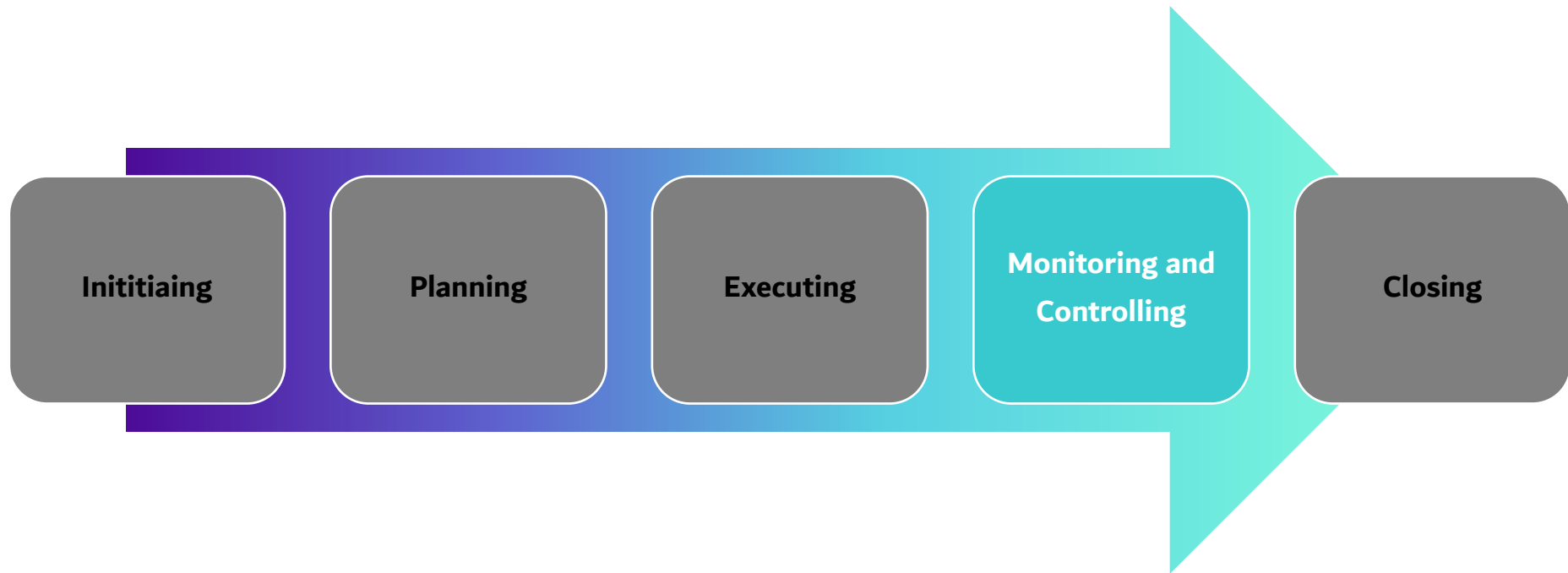
The table below contains the activities that will be carried out at this phase:

#	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	Perform cybersecurity risk assessment aligned with CRF requirements	Validate identified risks and provide missing information	Risk register & risk 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
2	Review and amend documents related to the cybersecurity system (policies, standards, procedures, and measurement indicators), including but not limited to: • Cybersecurity Oversight Committee Charter. • Acceptable Use. • Malware Protection. • ISMS Strategy • Third-party Security Management. • Cybersecurity Logs and Incident Management and Monitoring. • Physical Security. • Cybersecurity Business Continuity. • Information Asset Management. • Data Classification and Protection. • Mobile and Personal Device Security Management. • Network and Communications Security. • Secure Development of Applications and Systems. • Identity Management and Access Control. • Encryption and Key Management. • Backup Management. • Cybersecurity Risk Management.	Review and approval of documents	Documents related to the cybersecurity 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
	• Technical Vulnerability Management Standards. • Cybersecurity Compliance Management Standards. • Cybersecurity Internal Audit Management Standards. • Cybersecurity Threat Management Standards. • A detailed program and plan for assessing internal compliance with policies and procedures (for at least one year). • A detailed program and plan for internal auditing (for at least one year). • Baseline's Configuration standards for technical assets • Risk Assessment Report • Risk Register & Risk Treatment Plan		

3.4 Monitoring and Controlling phase



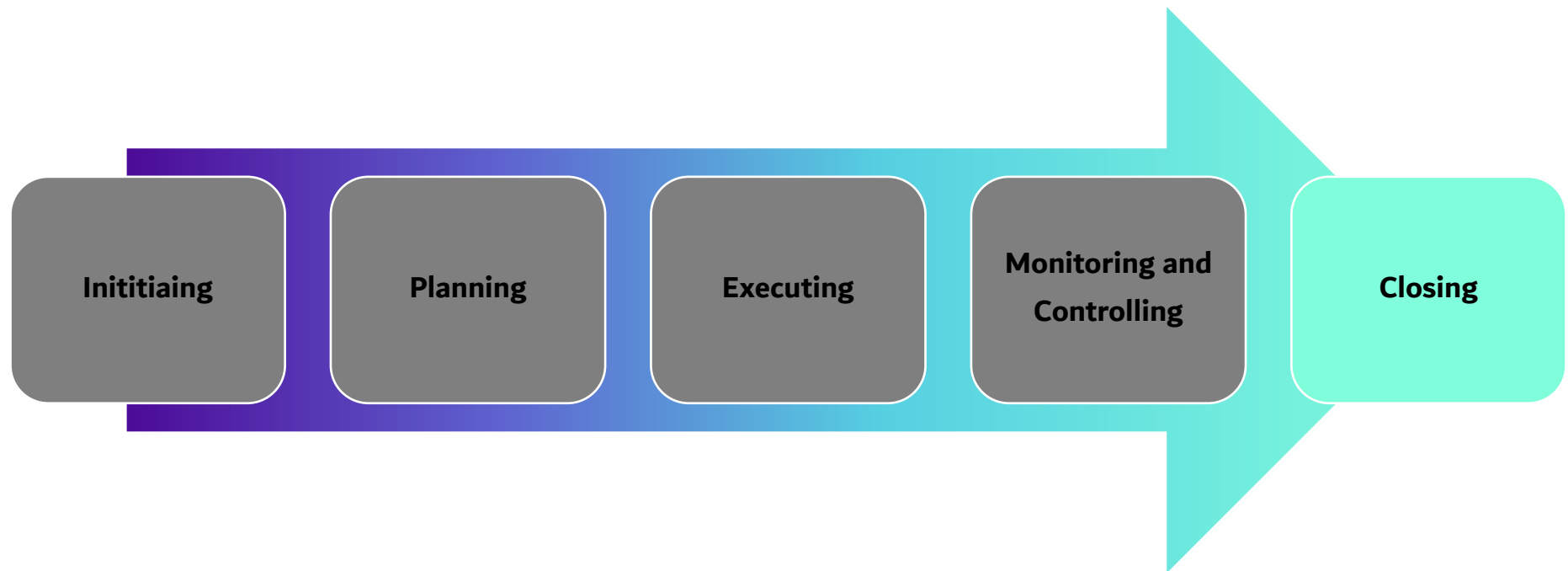
At this phase, project work is monitored, performance and changes are tracked, and all project deliverables are verified. The project objectives are achieved, and final approval of the deliverables is obtained.

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	Conduct Cybersecurity awareness workshops for all company employees	Coordinate meeting with stakeholders	Awareness workshop materials

#	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	Validate implemented controls (technical and documentation validation)	Provide access for validation	Control validation report
3	Support preparation for Management Review (objectives status, risks, non-conformities, corrective actions, improvement opportunities)	-	Meeting minutes

3.5 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	Conduct a formal project handover, including documentation, processes, and responsibilities	Acknowledge handover and assume ownership	Handover documentation pack

#	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	Close all project activities, finalize contracts, and archive project records	Approve project closure	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	Daily	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 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

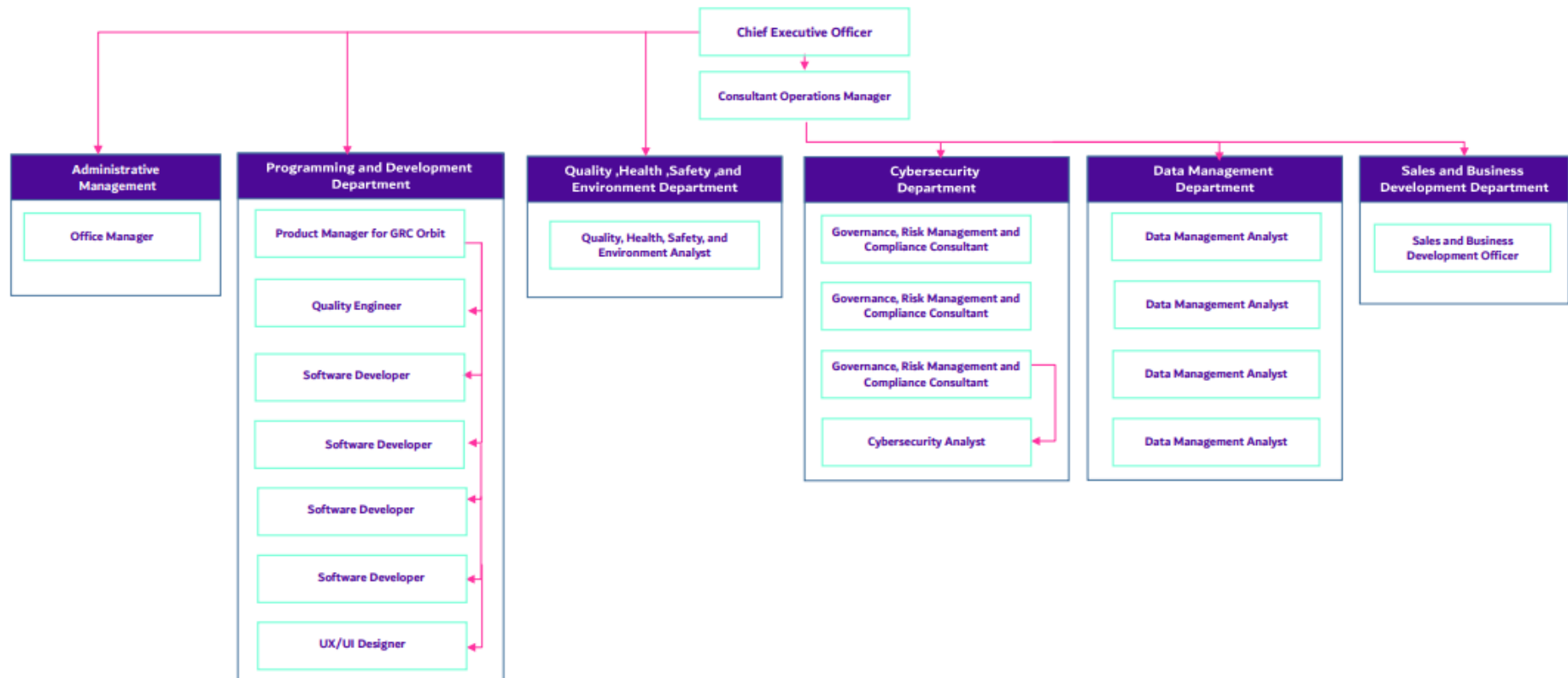
1. Implementing or purchasing technical tools and solutions related to the implementation of the CRF:2023.
2. Any other service not clearly mentioned in the previous sections will be considered outside the scope of work.

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. Delivered documents will be reviewed for 3 days only.
5. This project will be implemented within 2 months.
6. An AI bot will be integrated to record and summarize conversations, aiming to assist consultants in improving and enhancing meeting minutes.
7. 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/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

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+



FEATINET
NSE 1
ASSOCIATE

FEATINET
NSE 2
ASSOCIATE

FEATINET
NSE 3
ASSOCIATE

FEATINET
NSE 4
PROFESSIONAL

CEH
Certified Ethical Hacker

paloalto
NETWORKS
PCCSA

paloalto
NETWORKS
PCNSA

paloalto
NETWORKS
PCNSE

CISA
CYBER+INFRASTRUCTURE
SECURITY AGENCY

COMP
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 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		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		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. 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		IT Policies and Procedures Audit (General Technical Controls + Application Technical Controls)
7	ISO 27001 Information Security Standard Training	Energy Manufacturing and Services Company (Energy)		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) Regulation	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 5. Conducting awareness workshops on personal data protection
19	Implementation of SAMA CSF	Finzey		1. Conduct a comprehensive cybersecurity gap assessment.

			 فينزي للتمويل FinZev Finance	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
--	--	--	---	---

12. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	S.	Governance and Risk Management (GRC)	Bachelor of Computer Engineering	6 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
--	--	--	--	--	--

10	E.A	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.
----	-----	--	----------------------------	---------	--