Technical and Financial Proposal for Cybersecurity Compliance

Version 1.0

Date: 31-Aug-2025 AD

Prepared by: Trusted Vision for Cybersecurity

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

TRUSTED VISION

Contents

1. Executive summary of client requirements

Trusted Vision Company is pleased to offer consultation services for achieving compliance with National Cybersecurity Authority (ECC, DCC, TCC, CSCC, CCC-P, OSMACC) with an ongoing support service.

The project duration will be 12-Months.

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

1. Balanced blend of international and local ability in cybersecurity.
2. Efficient project execution approach, ensuring prompt, 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 ability to enhance cybersecurity.

2. Project Benefits and Values

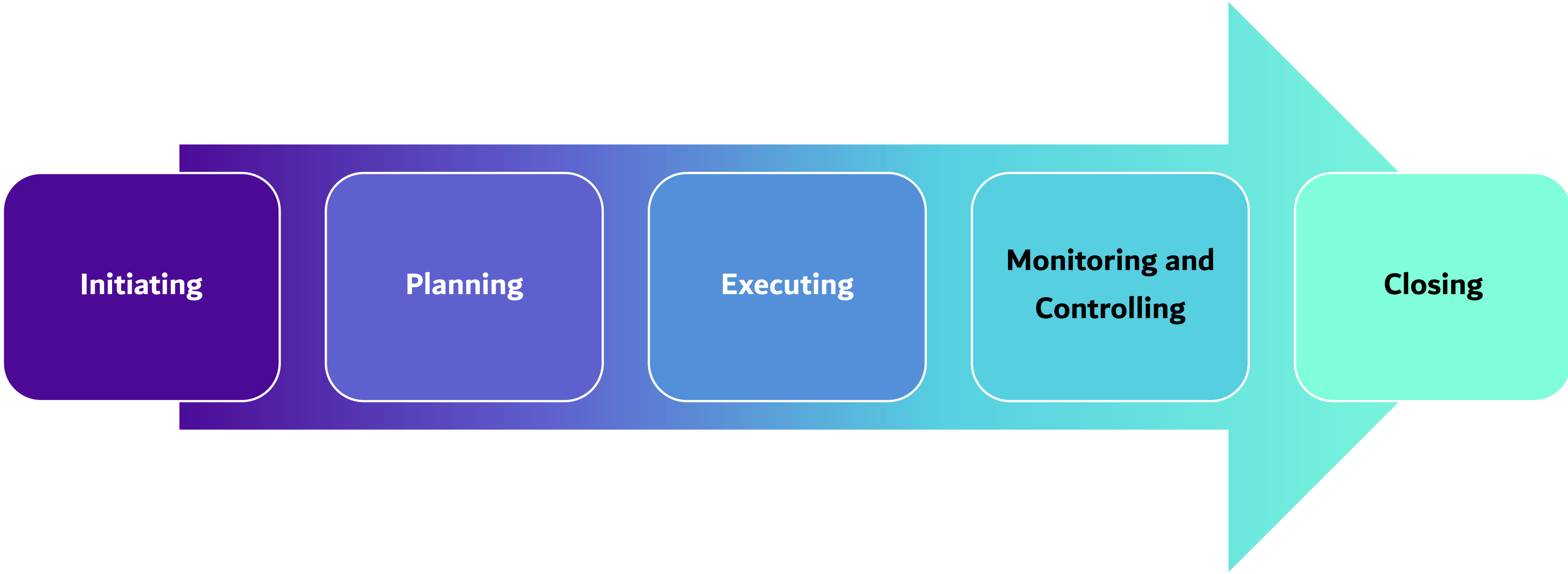
By implementing this project, the expected benefits and values will be the following:

1. Raise compliance with the National Cybersecurity Authority's controls for the entity.
2. Improve the cybersecurity system within the entity.
3. Increase competitive advantage by ensuring the safety, security, value, and availability of data to support business decisions.
4. Achieve economy and efficiency by applying international controls and standards.

5. Reduce risks and costs resulting from data breaches and cybersecurity risks.

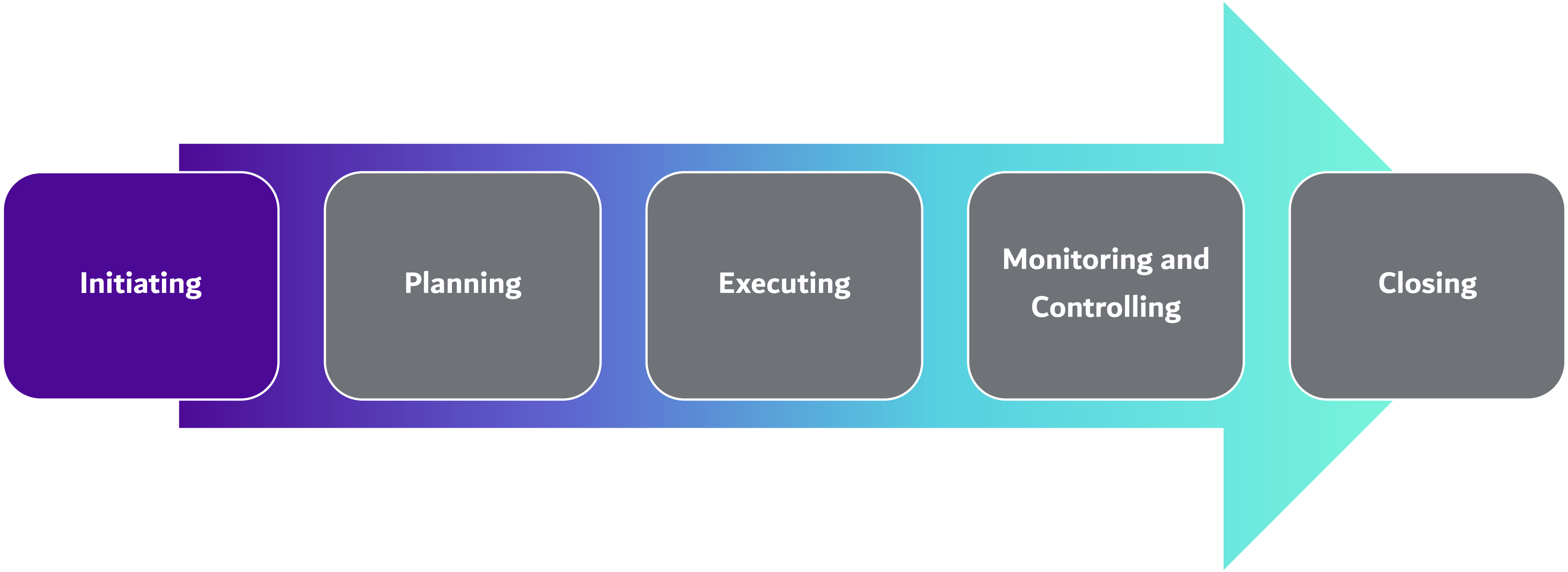
6. Enhance transparency and accountability in cybersecurity management.

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

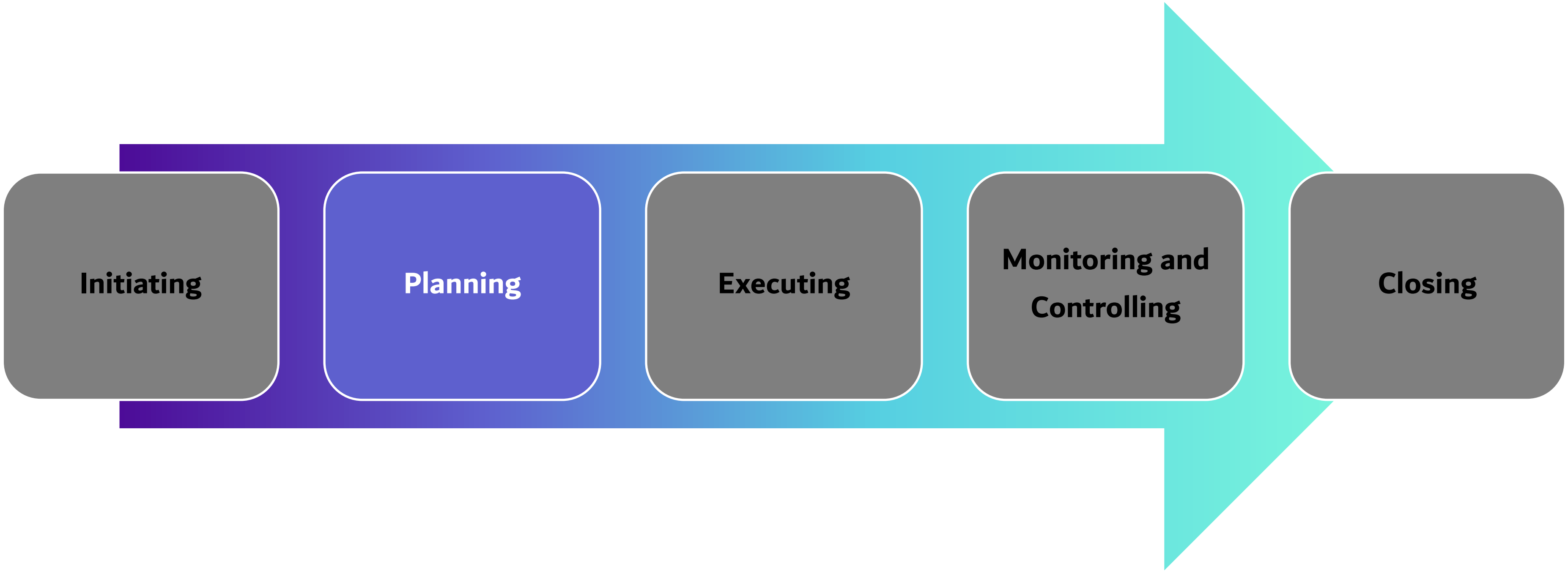


At this phase, the project is defined, and the project leader outlines their responsibilities, finds key stakeholders, and conducts a status assessment. This assessment aims to develop a comprehensive understanding of the entity's cybersecurity system, its compliance posture, and the associated cyber risks.

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
I-1	Preparing the project team	Assigning a project manager from the entity to collaborate with the consultants	3 Day	A team prepared to start the project
I-2	Preparing to start the project and holding the kickoff meeting	Inviting the head of the entity and all department heads	1 Day	Meeting minutes
I-3	Develop Project Charter	Review and approve the project charter	1 Day	Project Charter
I-4	Develop comprehensive cybersecurity solutions matrix	Purchasing cybersecurity tools and solutions	1 Day	Cybersecurity solutions matrix
I-5	Provide advice on purchasing technical tool/solutions	Purchase the technical tool/solutions	During the project period	Technical tools and solutions in place

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 finding associated cyber risks.

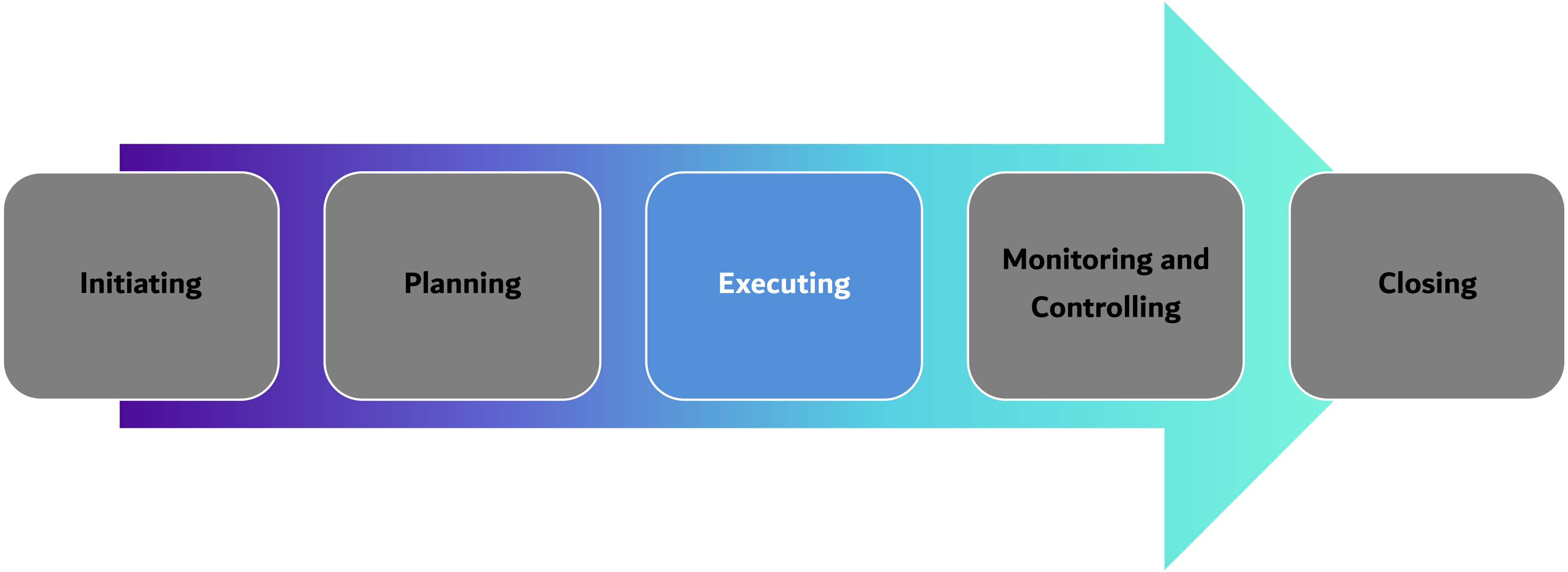
The table below has the activities that will be conducted at this phase:

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
P-1	Collect evidence and information related to cybersecurity requirements, including current cybersecurity governance documents: 1. Policies 2. Procedures 3. Cybersecurity Strategy, Digital Transformation, Data Management, and IT 4. Frameworks and methodologies 5. Technical Standards 6. Information and Technology Asset Register	Submitting the required documents	5 days	Meeting minutes
P-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	• Coordinate interview appointments. • Submit required documents	13 days	Meeting minutes

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
P-3	Develop a project implementation plan	• Review and approve the project implementation plan. • Allocate resources and budgets to complete the project	1 day	Project implementation plan
P-4	Gap assessment of the status of cybersecurity including the nature of the company's work, operations and activities of the departments and administrations. 1. ECC-2:2024: Assess baseline cybersecurity controls across CLIENT operations. 2. DCC: Evaluate secure classification, processing, and storage of sensitive data. 3. CSCC: Identify gaps in protecting critical systems. 4. CCC-T: Review compliance with cloud security requirements. 5. OSMACC: Assess operational systems and maintenance controls.	Review and approve gap assessment report	10 days	Gap assessment report

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	6. TCC: Evaluate telework security for external vendors and entities.			
P-5	Develop asset inventory including these standard (ECC-DCC-CCC-T-CSCC, TCC, OSMACC)	Review and approve asset inventory	12 days	Asset inventory
P-6	Conduct Cybersecurity Maturity Level Assessment on the following standard (ECC, DCC, CSCC, CCC-T, TCC, OSMACC)	Review and approve the following: • Maturity Level Assessment Maturity level Report	15 days	• Maturity Level Assessment • Maturity level Report
P-7	Maturity level assessment dashboard	Review and approve the Maturity Level Assessment Dashboard	5 days	Maturity Level Assessment Dashboard

3.3 Executing Phase



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

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
E-1	Developing and building a cybersecurity risk management methodology based on developments in systems and technologies, as well as relevant legislative and regulatory requirements.	Review and approve the cybersecurity risk methodology	10 days	• Cybersecurity Risk Management Methodology
E-2	Developing cybersecurity risk management register	Review and approve the cybersecurity risk register	5 days	• Cybersecurity Risk Management register
E-3	1. Perform a detailed risk assessment to identify risks, threats, and vulnerabilities within the compliance framework (including but not limited to social media, cloud service, third party, change management, technology projects). 2. Provide a Risk Assessment Report identifying threats, vulnerabilities, and associated risks. 3. Use a structured methodology aligned with cybersecurity frameworks.	Review and approve the following: • Risk Assessment • Risk Register • Risk Treatment Plan • Risk Assessment Report	30 Days	• Risk Assessment • Risk Register • Risk Treatments Plan • Risk Assessment Report

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	4. Risk Register: Document risks, their likelihood, impact, and mitigation strategies. 5. Update and review the Risk Management Methodology outlining how risks will be identified, assessed, and treated.			
E-4	Develop and Revise documents related to the cybersecurity management system (policies, standards, procedures, and measurement indicators), for NCA standards: ECC-DCC-CCC-T-CSCC, TCC, OSMACC and align them with regulations in KSA and global best practices (including but not limited to: 1. Cybersecurity Strategy for 3 years 2. Cybersecurity Oversight Committee Charter 3. Acceptable Use Policy 4. Malware Protection Policy 5. Data Storage and Disposal Policy and Procedure 6. Third-party Security Management	Review and approve all the cybersecurity documents	40 days	• Policies, standards, and procedures for NCA frameworks

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	7. Cybersecurity Incident Management 8. Cybersecurity Penetration Testing policy and procedure 9. Cybersecurity Event Logs and Monitoring Management 10. Physical Security Policy 11. Cybersecurity Business Continuity Policy 12. Cloud Computing and Hosting Policy 13. Information Asset Management 14. Data Classification and Protection Policy 15. Mobile and Personal Device Security Management 16. Network and Communications Security Process 17. Secure Development Lifecycle for Applications and Systems. 18. Identity Management and Access Management.			

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	19. Cybersecurity in Human Resources Policy and Procedure 20. Data and Information Policy 21. Encryption and Key Management. 22. Backup and Recovery Management. 23. Develop Root Cause Analysis corrective actions resulting from Cybersecurity incidents. 24. Incident escalation procedures 25. Technical Vulnerability Management Standards. 26. Cybersecurity Compliance Management Standards. 27. Developing and Improving Periodic Review and Audit Procedures 28. Cybersecurity Threat Management Standards 29. Program and plan for internal audit. 30. Web Application Security 31. Configuration Standards for Technical Assets			

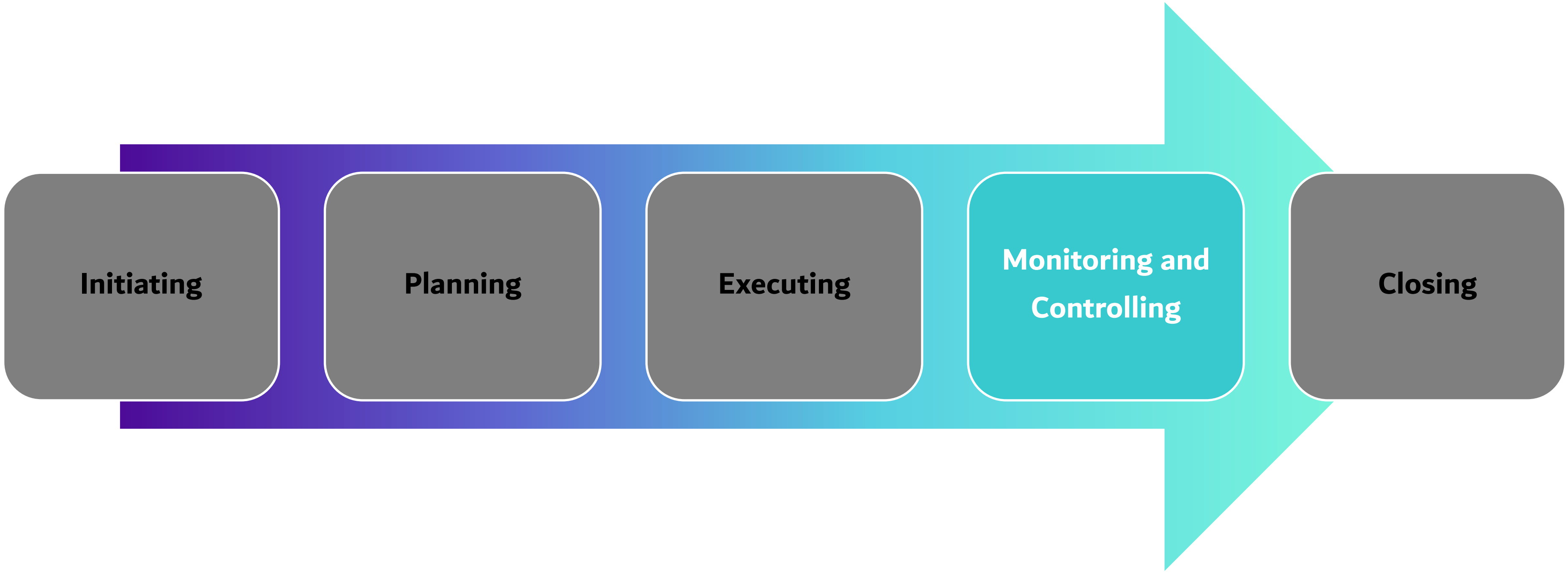
#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	32. Cybersecurity Projects Management Policy 33. Dashboards for cybersecurity 34. Third Party Risk Management Framework department 35. Establish monitoring processes to measure compliance with Cybersecurity frameworks. 36. Develop methodologies to track key performance indicators (KPIs) and compliance metrics.			
E-5	Develop the operating model and organizational structure Including: • Organization Chart • Cybersecurity Roles and Responsibilities • Job positions • SLAs • Communication Plan	Review and approve the operating model and organizational structure	7 days	Operating model and organizational structure

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
E-6	Awareness Plan Document (for at least one year).	Review and approve the awareness plan document	3 days	Awareness Plan Document (for at least one year).
E-7	Awareness lectures to raise cybersecurity awareness	Review and approve the awareness lectures	5 days	Awareness lectures
E-8	Cybersecurity Awareness Program Document.	Review and approve the cybersecurity awareness program document	3 days	Cybersecurity Awareness Program Document.
E-9	Monitor and Mitigate Security Incidents by: • Lead the communication between SOC and internal team to remediate or Prevent security incidents. • Lead the Respond to crises between CLIENT team and SOC or IR team	Coordinate meetings with stakeholders	5 days	• Meeting minutes • Incident register

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 in one document as needed and according to the requirements and circumstances of the entity.

3.4 Monitoring and Controlling phase



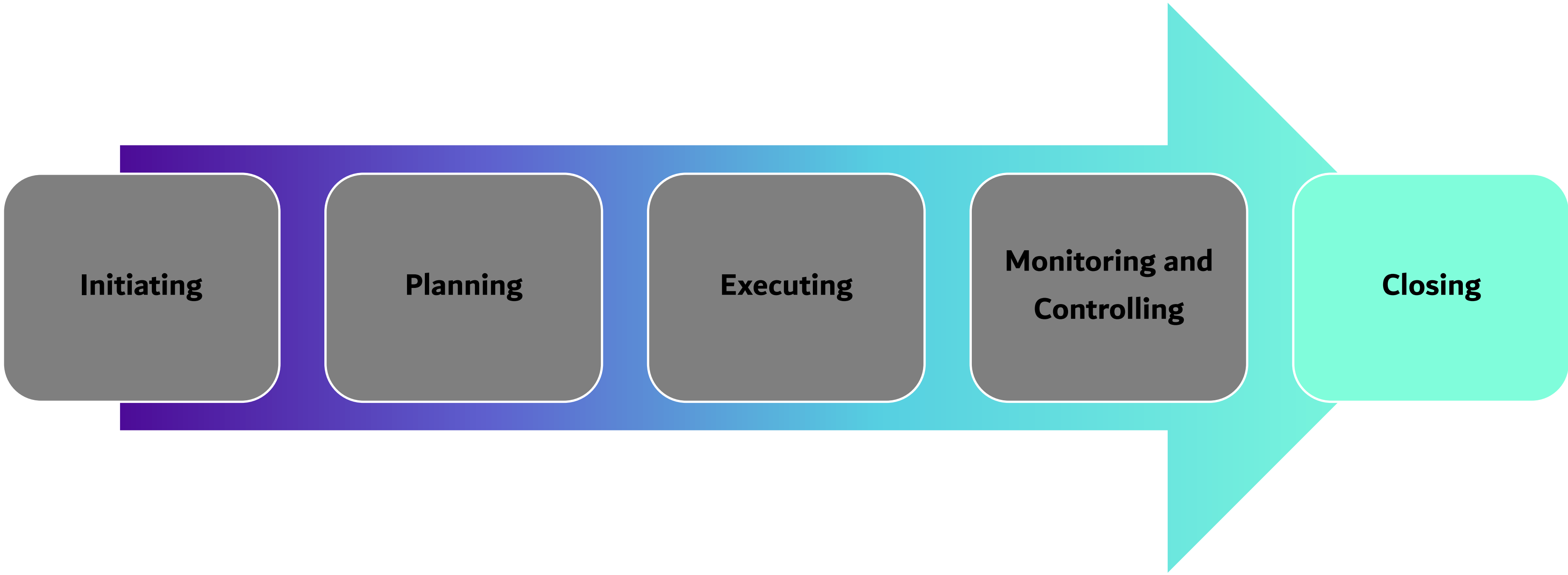
At this phase, project work is checked, performance and changes are tracked, and all project deliverables are verified. The project aims are achieved, and final approval of the deliverables is obtained.

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
M-1	Develop compliance matrix (mapping sheet) to ensure alignment of all cybersecurity controls in	Review and approval compliance matrix	7 days	Compliance matrix

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
	the regulations with the cybersecurity controls in the existing policies.			
M-2	Deliver specialized awareness session for: • Senior Management (1 Session) • IT Department (1 Session) • All Employees (1 Session)	Coordinate meeting with stakeholders	14 days	• Educational and awareness plan • Awareness workshop materials
M-3	Providing recommendations, support, and follow-up on the implementation of technical security controls and reducing cybersecurity risks.	Coordinate meeting with stakeholders	7 days	Meeting minutes
M-4	Track key performance indicators (KPIs) and compliance metrics.	Coordinate meeting with stakeholders	7 days	KPIs status report
M-5	Regularly perform internal audits, configuration reviews, and documentation assessments for (ECC, DCC, CSCC, CCC-T, TCC, OSMACC).	Collaboration with the internal auditor	24 days	Internal audit report

3.5 Closing phase



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

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

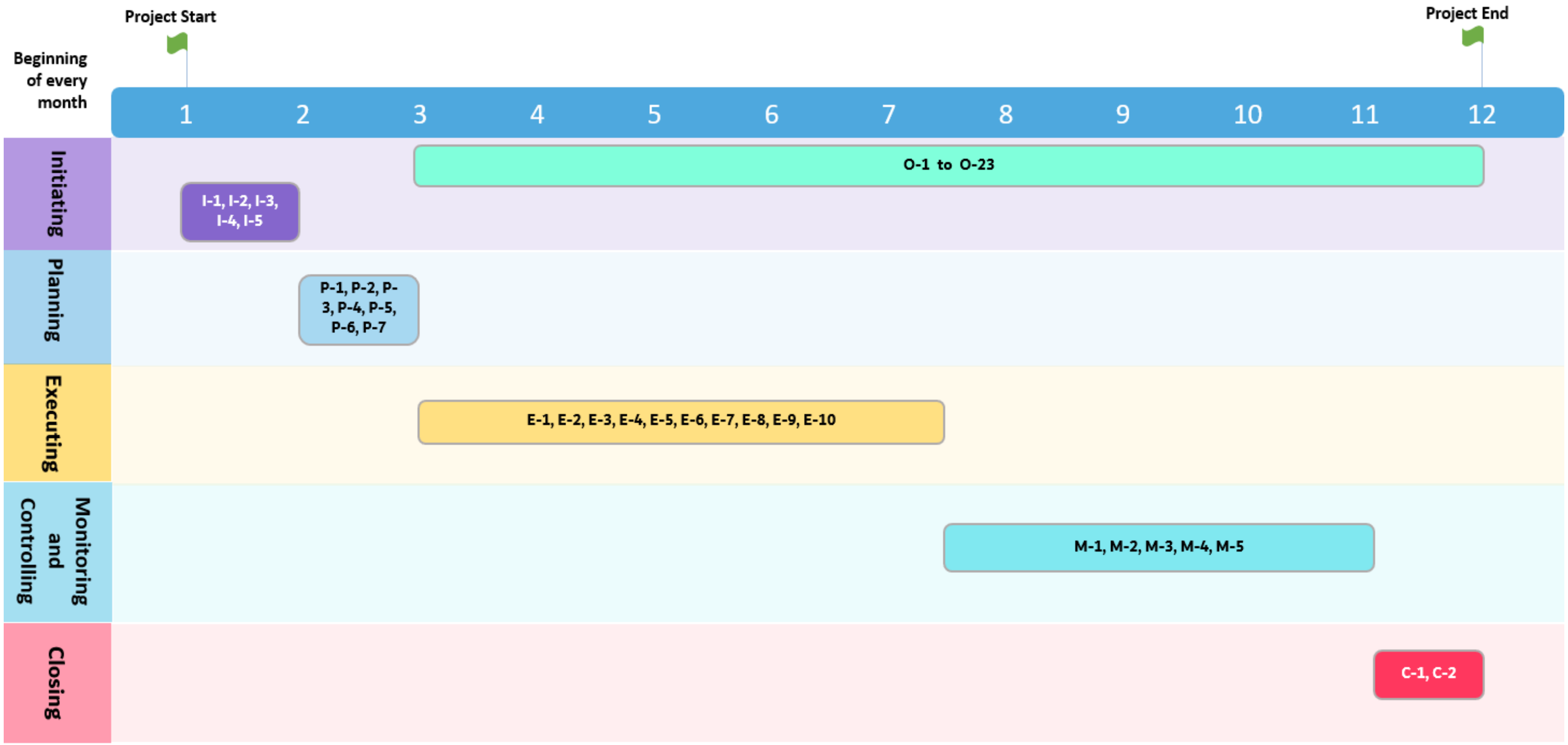
#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Tentative Timeline	Activities completed and materials delivered to the entity
C-1	Receive all project documents.	Approve all the documents	5 Days	Received all project data
C-2	Project sign-off	Sign off by the company's management	5 days	Project closure report

4. Ongoing Activities

No.	Process	Phases
O-1	Assess user authentication systems (e.g., user registration, password management, and account recovery).	Periodically
O-2	Evaluate privileged access management systems and provide recommendations for improvement.	Periodically
O-3	Assess patch management for systems, applications, and devices and provide recommendations.	Periodically
O-4	Evaluate multi-factor authentication (MFA) for remote access and recommend enhancements.	Periodically
O-5	Assess advanced email protection technologies and mechanisms and provide recommendations.	Quarterly
O-6	Update, review, and deliver cybersecurity awareness and training programs for stakeholders.	Quarterly
O-7	Assess the implementation and effectiveness of cybersecurity encryption systems and recommend improvements.	Periodically
O-8	Review secure configurations and hardening processes for systems and devices and provide recommendations.	Periodically
O-9	Evaluate the effectiveness of advanced persistent threat (APT) protection against Zero-Day Malware and recommend enhancements.	Quarterly
O-10	Measure performance indicators and cybersecurity maturity levels and provide actionable insights.	Every 6 Months
O-11	Monitor and report on compliance Key Performance Indicators (KPIs) and recommend corrective actions.	Periodically
O-12	Assess the separation and encryption of data stored on mobile devices and BYOD systems and recommend improvements.	Quarterly
O-13	Ensure the continuity of cybersecurity systems and procedures and recommend enhancements.	Periodically

O-14	Enhance protection levels, monitor tools for endpoint devices, and escalate issues with recommendations.	Periodically
O-15	Participate in and escalate issues to CLIENT and relevant entities with actionable recommendations.	As Needed
O-16	Conduct knowledge transfer sessions to the CLIENT Team.	As Needed
O-17	Regularly identify, assess, and manage cybersecurity risks to protect information and technology assets in line with policies, procedures, and regulations. Provide risk mitigation recommendations.	Periodically
O-18	Perform vulnerability assessments of systems and networks to identify deviations from acceptable configurations or policies.	Periodically
O-19	Analyze cybersecurity controls and assess their effectiveness, providing recommendations for enhancement.	Quarterly
O-20	Perform comprehensive configuration reviews, and documentation assessments to identify gaps, ensure compliance, and recommend enhancements.	Semi-annually
O-21	Monitor and assess the use of vulnerability assessment tools and techniques, providing recommendations for optimization.	As Needed
O-22	Assess and monitor systems like Active Directory, firewalls, databases, and cloud platforms, providing recommendations for improvement.	As Needed
O-23	Conduct comprehensive Cybersecurity Architecture review and document the findings and recommendations, Measure effectiveness of defense-in-depth and Security by Design architecture and recommend improvements.	Semi-annually

5. Aproximate Implementation plan



6. Knowledge Transfer

Knowledge transfer includes transferring knowledge from the consultant to the entity's employees and training with the aim of conducting the work that the consultants were doing and enabling the Authority's employees to be able to conduct 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 protection of personal data

7. Weekly Project Progress Report

The table below shows the project progress on a weekly basis to ensure that the goals 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			

8. Resource, Quality and Communication Plans

In the initiating phase, the project manager makes a set of plans to implement the project in the best workable 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 figured out, priorities are figured out, and resources are distributed according to priorities.
2. In the quality plan, quality standards are figured out 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 figure out how to prepare resources, manage quality, and how to communicate during the life of the project. They include all the roles of stakeholders.

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

Out of Scope of Work

1. Implementing or buying technical tools and solutions related to the implementation of the cybersecurity standard.

2. Any other service not clearly mentioned in the earlier 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 documents sent.**

5. **Delivered documents will be reviewed for 3 days only.**

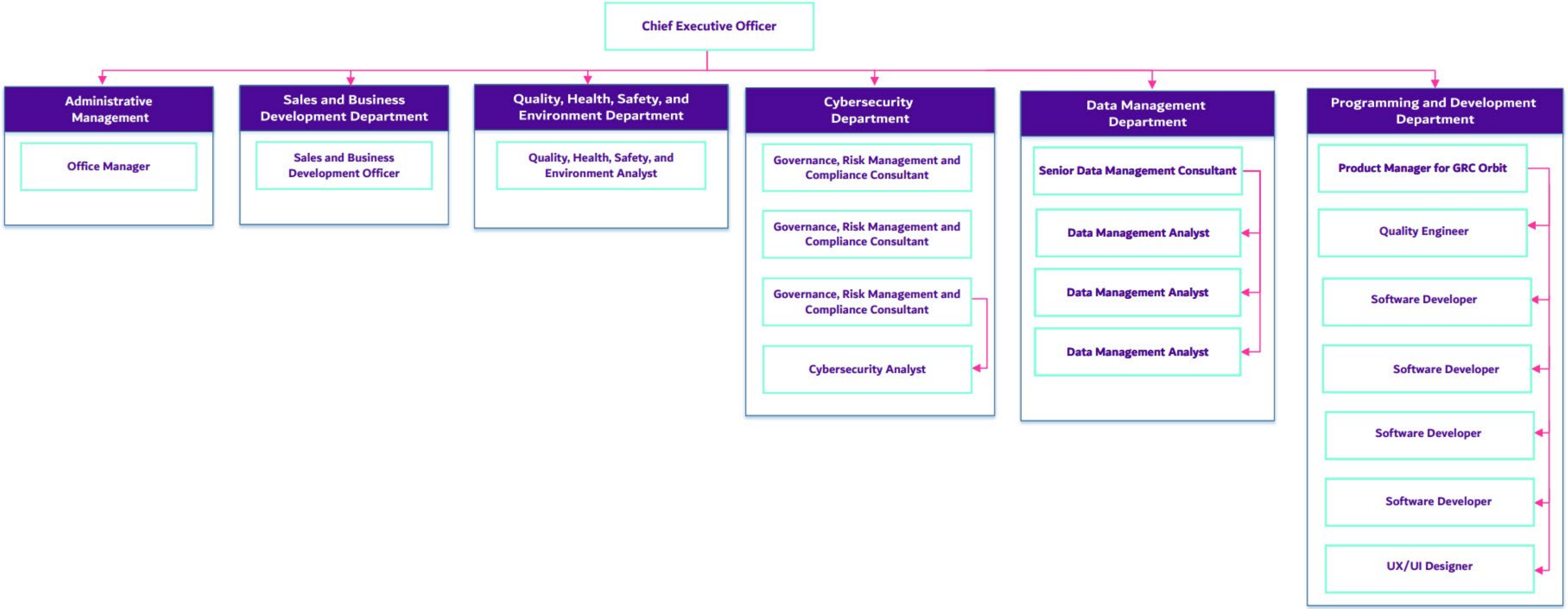
6. **The project will be executed over 12 months.**

7. **An AI bot will be integrated to record and summarize conversations, aiming to aid 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.**

11. 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.



12. Certificates

- CISSP®
- CISM®
- CGEIT®
- CRISC®
- CISA®
- COBIT 2019 Foundation – An ISACA® Certificate

- 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+

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

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 التأمين أمان أسيج	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		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 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	مرنة للتمويل	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	فينزي للتمويل FinZev Finance	1. Conduct a comprehensive cybersecurity gap assessment. 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

14. Staff

#	Name	Job Title	Responsibilities	Qualifications and soft skills
1	S.H	Governance and Compliance Specialist	1. Ensures an organization's cybersecurity program complies with applicable requirements, policies and standards. 2. Update and implement and maintain cybersecurity governance and policies aligned with national regulations. 3. Conduct compliance assessments, coordinate audits, and prepare detailed compliance reports. 4. Update, Develop and deliver cybersecurity awareness and training programs for stakeholders. 5. Track and report on compliance Key Performance Indicators (KPIs) to ensure alignment with regulatory updates. 6. Identify alternative cybersecurity strategies to address organizational security objectives .	1. Bachelor's degree in Cybersecurity, Information Technology, or a related field. 2. Minimum of 5 years of experience in cybersecurity governance, compliance, or policy development. 3. Certifications such as: ▪ Certified Information Systems Auditor (CISA) 4. Certified Cybersecurity Manager (CISM) 5. Certified in Risk and Information Systems Control (CRISC) 6. ISO 27001 Lead Implementer or Auditor 7. Strong understanding of national and international cybersecurity regulations and frameworks.

			7. Promote and demonstrate the value of cybersecurity to stakeholders within an organization . 8. Advocate cybersecurity related topics with senior management, to ensure the organization's strategic goals include cybersecurity . 9. Monitor how effectively cybersecurity policies, principles and practices are implemented in the delivery of planning and management services . 10. Participate in the development or modification of cybersecurity program plans and requirements . 11. Provide policy guidance to cybersecurity management, staff and users . 12. Advocate cybersecurity risks and posture to senior management . 13. Evaluate cybersecurity aspects of supplier selection and proposition.	8. Excellent communication and stakeholder management skills. **Soft Skills:** • Strong analytical and problem-solving skills. • Excellent communication and report-writing abilities. • Ability to work independently and collaboratively in a team environment

2	B. A	**Risk and Controls Assessment consultant**	1. Identifies, assesses and manages an organization's cybersecurity risks to protect its information and technology assets in line with organizational policies and procedures and related laws and regulations. 2. Performs vulnerability assessments of systems and networks. Identifies where they deviate from acceptable configurations or applicable policies. Measures effectiveness of defense-in-depth architecture against known vulnerabilities. 3. Experience in evaluating effectiveness, design, implement, fine-tune and enhance full and partial end-to-end business continuity of digital-based business services with a lot of components and complex net of interdependencies. 4. Experience in calculating, fine-tuning and reach agreement on Business Impact Assessment (BIA)	1. Bachelor's degree in Cybersecurity, Information Technology, or a related field. 2. Minimum of 10 years of experience in cybersecurity risk management, technical controls, or incident response. 3. Certifications such as: ▪ Certified Information Systems Security Professional (CISSP) 4. Certified Ethical Hacker (CEH) 5. Certified Cybersecurity Manager (CISM) 6. GIAC Security Essentials (GSEC) 7. Certified Cloud Security Professional (CCSP) 8. Strong technical expertise in vulnerability management, SOC operations, and incident response. **Soft Skills:** • Strong analytical and problem-solving skills.

			outputs: Priority Tiers, RPOs and RTOs for various business and operations services. 5. Identify, assess, and manage cybersecurity risks, including the development of risk treatment plans. 6. Analyzes cybersecurity controls and assesses their effectiveness 7. Oversee vulnerability scans and the implementation of cybersecurity technical controls. 8. Monitor and test Security Operations Center (SOC) and incident response plans. 9. Maintain cybersecurity aspects of business continuity plan and track risk-related metrics. 10. Perform assessments of security controls to ensure compliance with company policies, industry standards (ISO 27001, NIST, CLIENT), and regulatory requirements. Review and validate security configurations for critical systems, including	• Excellent communication and report-writing abilities. • Ability to work independently and collaboratively in a team environment

			Active Directory, firewalls, servers, and network devices. 11. Evaluate security configurations of systems such as Active Directory, databases, and cloud platforms. Provide actionable recommendations to enhance system security configurations. 12. Assess and improve the quality of security-related documentation, including policies, procedures, and guidelines. And make sure that the periodic technical assessment is compliant with CLIENT' Governance. 13. Review technical and administrative security controls to verify effective implementation. Identify gaps and recommend remediation measures. 14. Identify and assess cybersecurity risks in systems and processes. Support the development and tracking of mitigation plans.	

			15. Collaborate with cross-functional teams, including IT, compliance, and risk management, to enhance security practices. Assist in preparing reports and presentations for management and auditors. 16. will be responsible for performing comprehensive assessments, configuration reviews, and documentation assessments to ensure robust cybersecurity controls across our systems and networks. This role focuses on identifying gaps, ensuring compliance with regulations standards, and recommending enhancements to strengthen CLIENT’s security posture. 17. Configure and handle vulnerability assessment tools and techniques. 18. Assessment and configuring systems like Active Directory, firewalls, databases, and cloud platforms… etc.	

TRUSTED VISION