TECHNICAL PROPSAL OF CONSULTING SERVICES RELATED TO THE IMPLEMENTATION OF THE PERSONAL DATA PROTECTION LAW AND REGULATIONS

Version 1.0

Date: 17-02-2026 AD

Prepared by: Trusted Vision for Cybersecurity

Contact Information

To inquire about this document and the information provided, you can contact the people mentioned in 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

Table of Contents

1. Executive summary of client requirements

Trusted Vision Company is proud to present its consulting services to support The entity in the full implementation of the Saudi Personal Data Protection Law, which was issued by Royal Decree No. (M/19) on September 2, 2021, and later amended by Royal Decree No. (M/148) on September 5, 2022 As part of the implementation of the Saudi Personal Data Protection Law and regulations project, we will comply with the National Data Index (NDI) and the personal data protection specifications issued by the National Data Management Office (NDMO 14), developed by the Saudi Data and Artificial Intelligence Authority (SDAIA). This commitment aims to enhance transparency and foster an organizational culture that prioritizes personal data protection, contributing to risk mitigation and ensuring comprehensive compliance across various operations and markets.

Figure 1 Personal Data Protection Law and Regulation

We believe that our experience in implementing similar projects places us among the elite consulting firms in addition to:

- A balanced blend of international and local expertise in cybersecurity
- An effective approach to project implementation to meet project requirements in a timely manner, in a professional and quality manner.
- Extensive knowledge and experience in implementing and designing solutions based on international standards and best practices.
- Best Consulting Expertise for Data Management and Personal Data Protection

We hope that our consulting services will meet the terms of competition and look forward to a mutual working relationship.

2. Project Objective

1. Implement Data Classification Controls (DCC) in alignment with National Cybersecurity Authority (NCA) regulations, ensuring proper categorization and handling of data according to sensitivity and criticality.
2. Ensure compliance with the Saudi Personal Data Protection Law and Regulations.
3. Evaluate the current information flow within the project scope and assess privacy implications and risks according to the Personal Data Protection Law.
4. Develop necessary plans for full compliance with the Saudi Personal Data Protection Law and Regulations, in accordance with local laws and the definitions of the National Data Management Office (NDMO). This includes identifying the required technical and procedural tools.
5. Raise awareness about legislative requirements and policies related to personal data protection within the organization.

3. Project Benefits

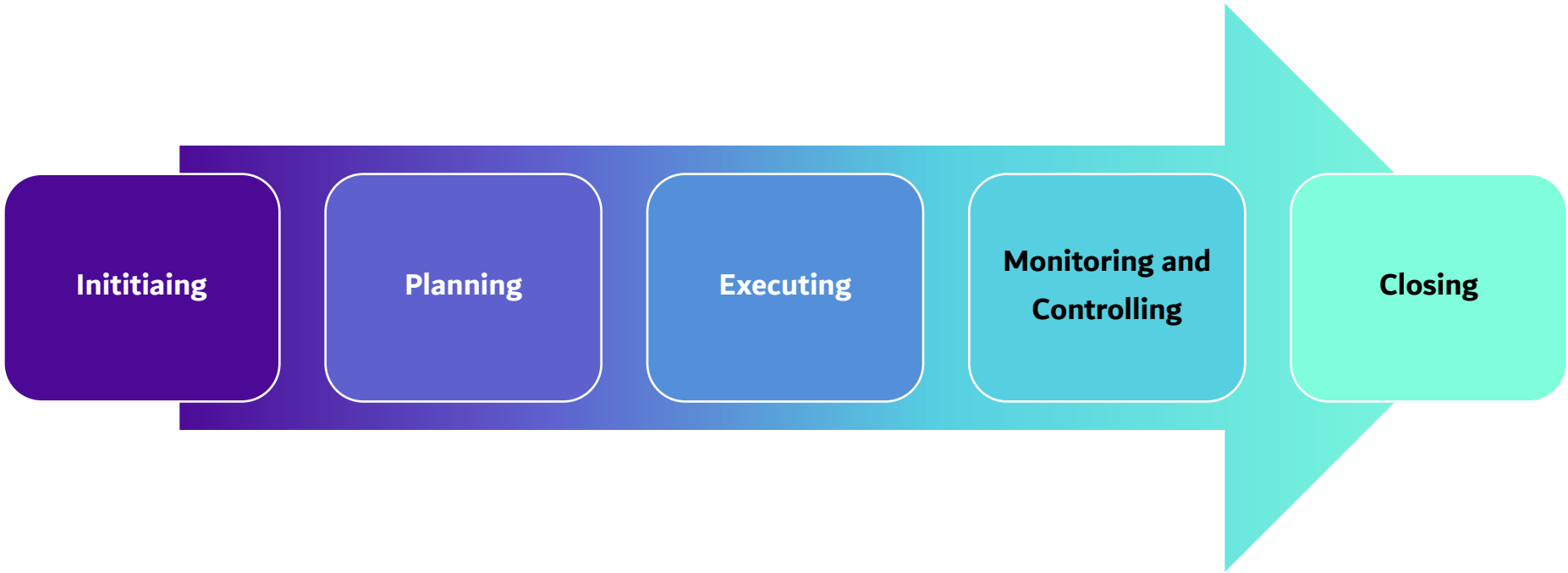
Through the implementation of this project, the organization will obtain the following benefits:

1. Achieve strict compliance with the National Data Management Office standards and the stipulated standards, ensuring that all operations meet both local and international regulatory expectations.
2. Significantly reduce risks and associated costs stemming from potential data breaches and cybersecurity threats by implementing robust data protection strategies and measures.

3. Strengthen compliance posture by adopting NCA Data Classification Controls (DCC), ensuring consistent protection and management of sensitive and critical information assets.
4. Enhance transparency and accountability in data management.
5. Gain customers' trust in the secure processing of their personal

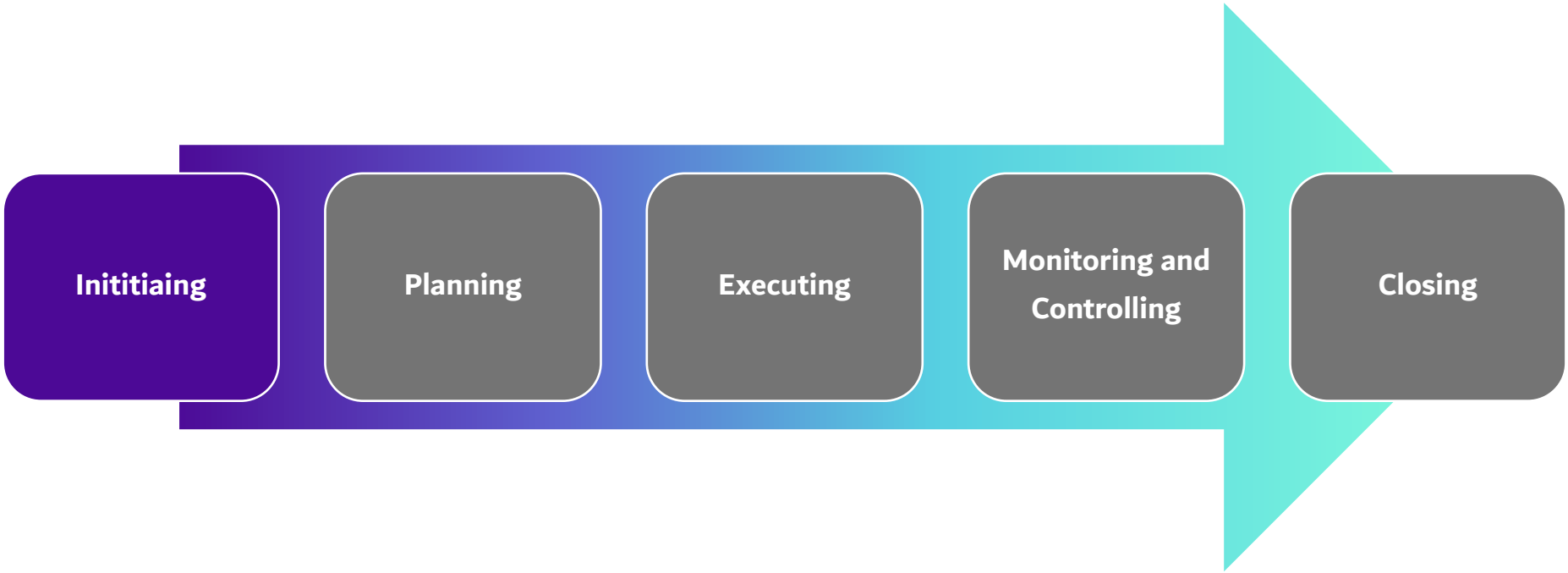
4. Project Implementation Methodology

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 together and delivered into one document as required and according to the requirements and circumstances of the entity.

4.1 Initiating Phase

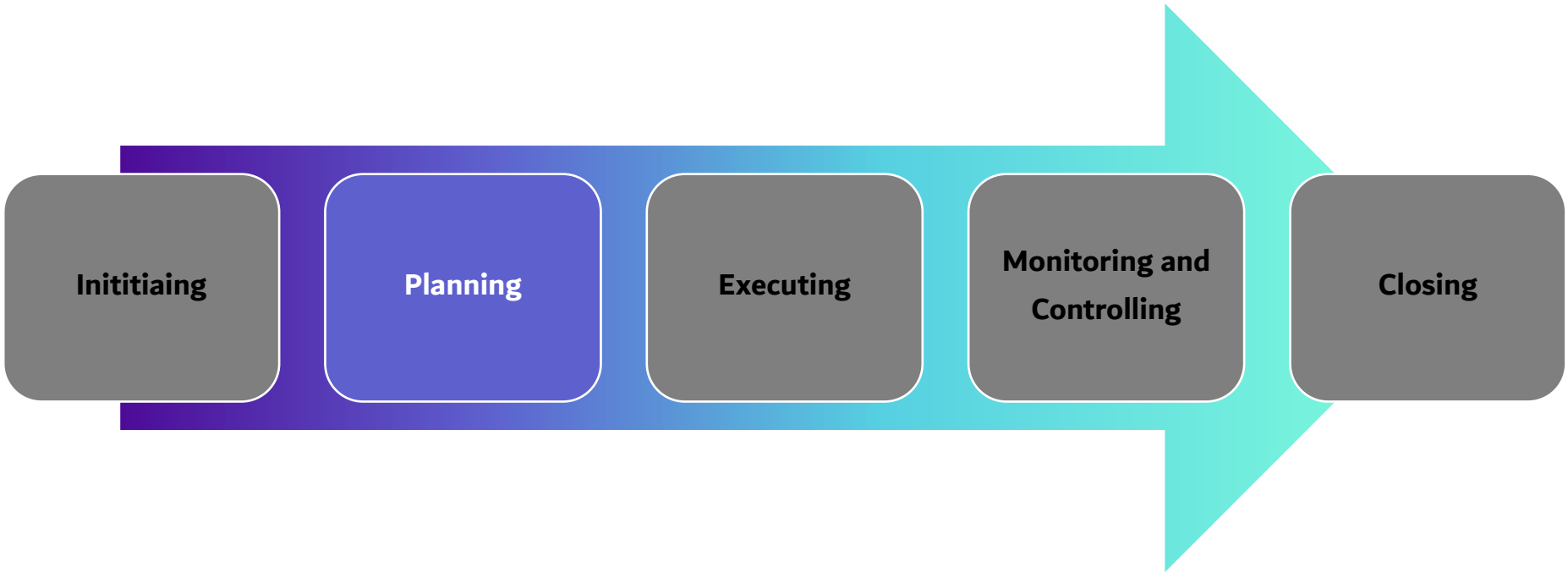


At this phase, the project is defined, and the project leader outlines their responsibilities which includes the project charter, includes restrictions and assumptions and preparing consultants to work at the entity's headquarters.

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

NO#	Reference	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.	N/A	Preparing the project team	• Nominate the project sponsor, project steering committee and project manager. • Obtain a commitment from the project sponsor and executive management and participate in enhancing data protection and privacy. • Allocating license officer from the entity to collaborate with consultants to achieve the implementation of the project.	• A list of the names of consultants who will work on this project • A list of the names of the entity's employees who will be working with them

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 PDPL, collecting all relevant documents available within the entity, evaluating its compliance posture, and identifying associated privacy risks.

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

#NO	Reference	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.		Develop a solution matrix sheet that includes the required solutions and tools to be brought to implement the NCA DCC Controls.	Review and approve the proposed solution matrix sheet that includes the required solutions and tools to be brought by the client to implement the cybersecurity controls	Solution matrix sheet
2.	PDP 1.1	Preparing to start the project	• Invite all concerned and coordinate communication with them	Minutes Meeting
3.	PDP 1.1	Develop a stakeholder's management plan. (in pptx format) that contains: • Meeting with the concerned stakeholders.	• Review and approval the stakeholder's management plan.	Stakeholders' management plan

#NO	Reference	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
		• Raising their awareness of the project • Scope of work • The requirements of the project and what is required from them.		
4.	PDP 1.1	Collect, inventory and review the following data: • The entity's business strategy • A list of general risks existing within the entity.	• Submit all required documents and information	Minutes Meeting

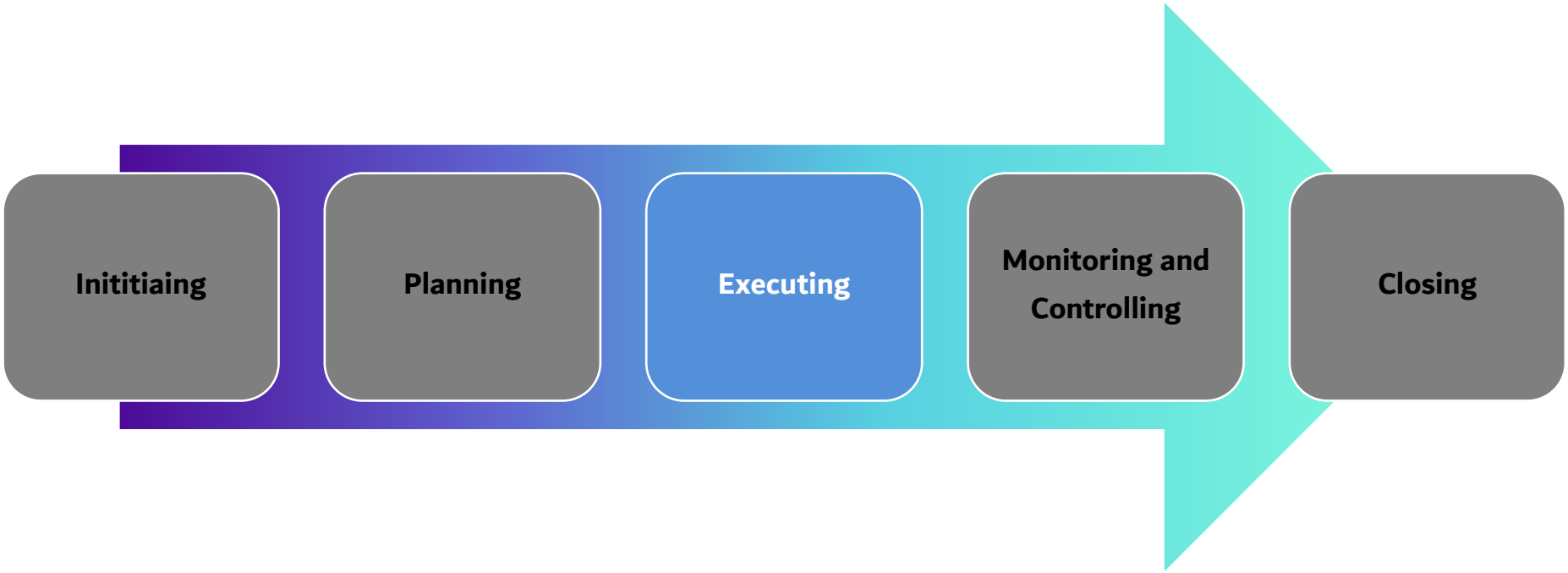
#NO	Reference	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
		• Roadmaps, information, and data management plans. • Review all systems and procedures related to data privacy, monitor compliance with privacy regulations and document the results. • Any documents relevant to the above documents.		
5.	PDP 1.1	Conduct interviews with project stakeholders to understand their needs	• Coordinating interviews with all departments.	Minutes Meeting

#NO	Reference	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
		and expectations, including but not limited to: • Head of the organization • Information Technology Management • Data Management Office • HR department • The rest of the departments and departments within the entity		

#NO	Reference	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
6.	PDP 1.1	Assess the current situation, identify gaps and the flow of personal data in internal systems, understand and study: • All personal data assets and their environment • Stages of processing personal data • Current personal data management challenges • Clearly outline the scope of the project including the systems,	• Send any required documents and provide adequate answers to the consultants	Understanding and studying the situation by consultants

#NO	Reference	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
		standards, processes and personal data that will be covered • Reviewing the obligations of both the control party and the processing party. • Analyze gaps and risks related to personal data protection • Activities that can be assigned to external parties		

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:

#NO	Reference	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.	DCC	Data Discovery and Classification 1. Perform data inventory to locate all data assets across systems (structured/unstructured). 2. Developing data classification policy, standard, and procedures. 3. Apply classification schema (e.g., Top Secret, Secret, Restricted, Public). Tag and categorize data based on sensitivity and business impact.	Fill Data inventory sheet approve Data classification policy, standard, and procedures. Classify The Data inventory sheet.	Data inventory sheet Data classification policy, standard, and procedures Data classification sheet
2.	PDP 1.2	Develop a personal data protection plan that meets the operational and strategic requirements of personal data protection in accordance with the Personal Data	Review and approve a personal data protection plan.	A personal data protection plan.

#NO	Reference	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
		Protection Policy issued by the National Data Management Office.		
3.	PDP.5.1	Developing a Record of Processing Activities (ROPA).	Review and approve the Record of Processing Activities (ROPA).	Record of Processing Activities (ROPA).
4.	PDP.1.2	Website Privacy Policy and Cookie Policy.	Review and approve the Website Privacy Policy and Cookie Policy.	Website Privacy Policy and Cookie Policy
5.	PDP.1.2	Data Protection and Privacy Policy (Handling Personal Data and Compliance with PDPL Principles including	Review and approve the Data Protection and Privacy Policy.	Data Protection and Privacy Policy.

#NO	Reference	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
		Privacy by design and default and data minimization guidelines).		
6.	PDP.3.1	Personal Data Breach Notification Template	Review and approve the personal data breach notification template	Personal Data Breach Notification Template
7.	PDP.2.1	Development of Personal Data Protection Training Plan	Review the personal data protection training plan.	Personal Data Protection Training Plan
8.	PDP.4.2	• Document of Roles and Responsibilities Related to Personal Data Protection • Target Operating Model (TOM)	Review and approve the document outlining roles and	Document of Roles and Responsibilities Related to Personal Data Protection

#NO	Reference	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
			responsibilities related to personal data protection.	
9.	PDP.4.3	Privacy Risk Assessment Policy and Procedures - DPIA	Implementing the Privacy Risk Assessment Policy and Procedures.	Privacy Risk Assessment Policy and Procedures - DPIA
10.	PDP.4.3	(DPIA) Impact Assessment Template	Review and approve the Data Protection Impact Assessment (DPIA) template.	(DPIA) Impact Assessment Template
11.	PDP.4.1	Reporting and Approval Policy and Procedures	Implementing policies and procedures for managing consents.	Reporting and Approval Policy and Procedures

#NO	Reference	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
12.	PDP.4.1	Consent Collection Template	Review and approve the consent collection template.	Consent Collection Template
13.	PDP.4.2	Data Subject Rights Management Procedures (Procedures for Handling Data Subject Requests including Access, Correction, Erasure, and Restriction of Processing Requests	Implementing procedures and plans for managing data subject rights.	Data Subject Rights Management Document.
14.	PDP.4.2	Record of Personal Data Subject Requests	Review and approve the record of data subject requests.	Record of Personal Data Subject Requests
15.	PDP.4.2	Data Subject Requests Template	Review and approve the data subject request template.	Data Subject Requests Template

#NO	Reference	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
16.	PDP.1.2	Data Sharing Policy and Procedure	Review and approve the data sharing policy and procedures.	Data Sharing Policy and Procedure
17.	N/A	Data Processing and Sharing Agreement for supplier contracts (Controller-to-Controller and Controller-to-Processor)	Review and approve the data processing and sharing agreement.	Data Processing and Sharing Agreement
18.	PDP.1.2	Third-party supplier privacy risk management procedure and register (up to 5 records)	Review and approve the third-party compliance procedures for the personal data protection system.	Third-Party Compliance Document for the Personal Data Protection System.

#NO	Reference	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
19.	PDP.1.2	Third-Party Compliance Assessment Template	Review and approve the third-party compliance assessment template.	Third-Party Compliance Assessment Template
20.	PDP.1.2	Record of Disclosure and Sharing Activities Documentation	Review and approve the record of disclosure and sharing activities documentation.	Record of Disclosure and Sharing Activities Documentation
21.	DP.1.2	Internal Disclosure/Sharing Cases Assessment	Review and approve the assessment of internal disclosure/sharing cases.	Internal Disclosure/Sharing Cases Assessment

#NO	Reference	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
22.	N/A	Data Sharing Template and Attachment on the Website.	Review and approve the data sharing template and its attachment on the website.	Data Sharing Template and Attachment on the Website.
23.	PDP.3.2	Process for Managing Data Breach Handling.	Review and approve the process for managing data breach handling.	Document for Managing the Data Breach Handling Process.
24.	PDP.3.2	Data Breach Notification Template.	Review and approve the Data Breach Notification Template.	Data Breach Notification Template

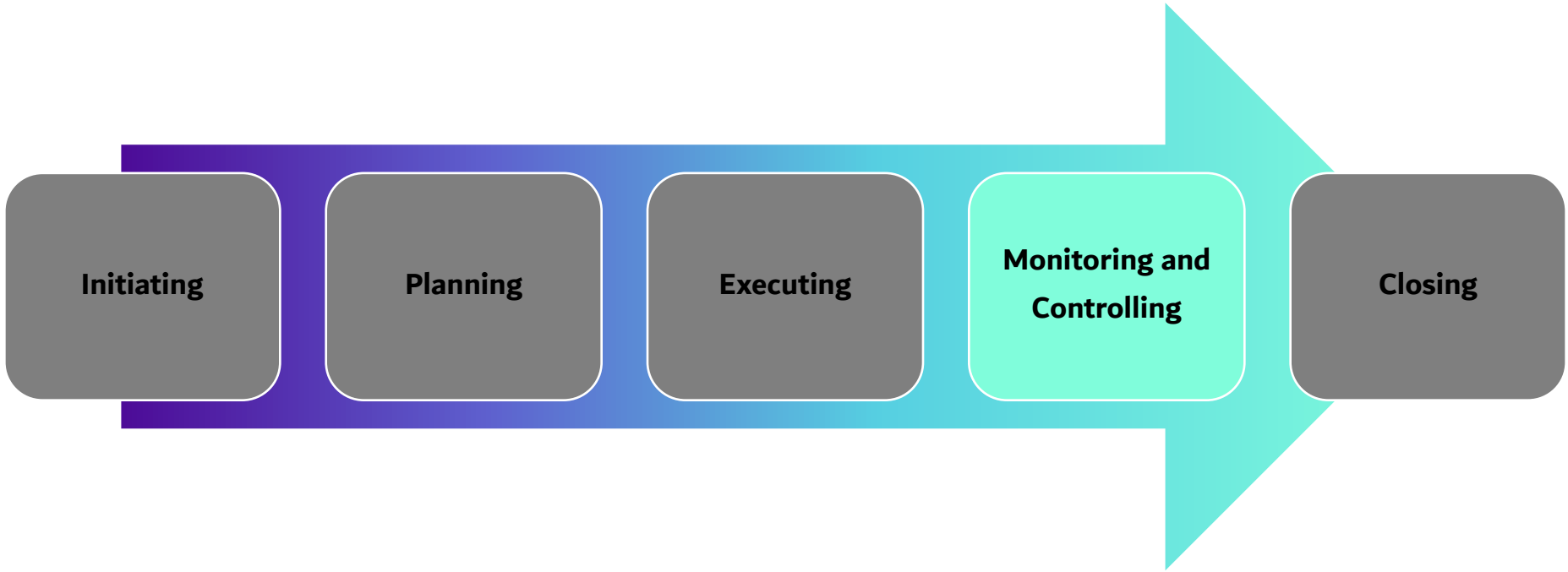
#NO	Reference	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
25.	PDP1.2	Access Storage and Disposal Policy and Procedures.	Review and approve the Access Storage and Disposal Policy and Procedures.	Access Disposal Policy and Procedures.
26.	PDP.1.2	Data flow map.	Review and approve the data flow map.	Data flow map.
27.	PDP.4.4	Internal compliance monitoring report.	Review and approve the internal compliance monitoring report.	Internal compliance monitoring report.
28.	PDP.5.1	Consolidated Record of Compliance Audit Logs.	Review and approve the compliance audit logs.	Compliance audit logs.

#NO	Reference	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
29.	PDP.2.1	Preparing educational awareness materials on how to protect personal data.	Coordination with all departments and divisions.	Awareness Tests and Understanding Assessment Presentations
30.	N/A	Implementation plan for the personal data protection law and regulation.	Review and approve the implementation plan.	Implementation plan for the personal data protection system and regulation.
31.	N/A	Dashboard for Displaying Data and Information in Graphical Interfaces.	Review and approval.	Dashboard

#NO	Reference	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
32.	PDP.4.1	Advising on How to: • Document Data Processing Activities and Create Detailed Records (ROPA) for All Data Processing Activities, Including the Purpose of Processing and Legal Basis • Notify the Regulatory Authority in Case of a Personal Data Breach • Document Compliance Audit Logs for a Reasonable Period of No Less Than 24 Months in a Consolidated Record	1. Documenting Data Processing Activities and Creating Detailed Records for All Data Processing Activities, Including the Purpose of Processing, Legal Basis, Data Retention Periods, and Third-Party Data Transfers.	1. Notifying the Regulatory Authority in Case of a Personal Data Breach 2. Documented Data Processing Activities 3. Personal Data Protection Compliance Audit Logs for a Reasonable Period of No Less Than 24 Months in a Consolidated Record

#NO	Reference	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
		• Document Privacy Risk Assessment - Impact Assessment	2. Notifying the Regulatory Authority in Case of a Personal Data Breach. 3. Documenting Compliance Audit Logs for a Reasonable Period of No Less Than 24 Months in a Consolidated Record.	

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 project objectives are achieved, and final approval of the deliverables is obtained.

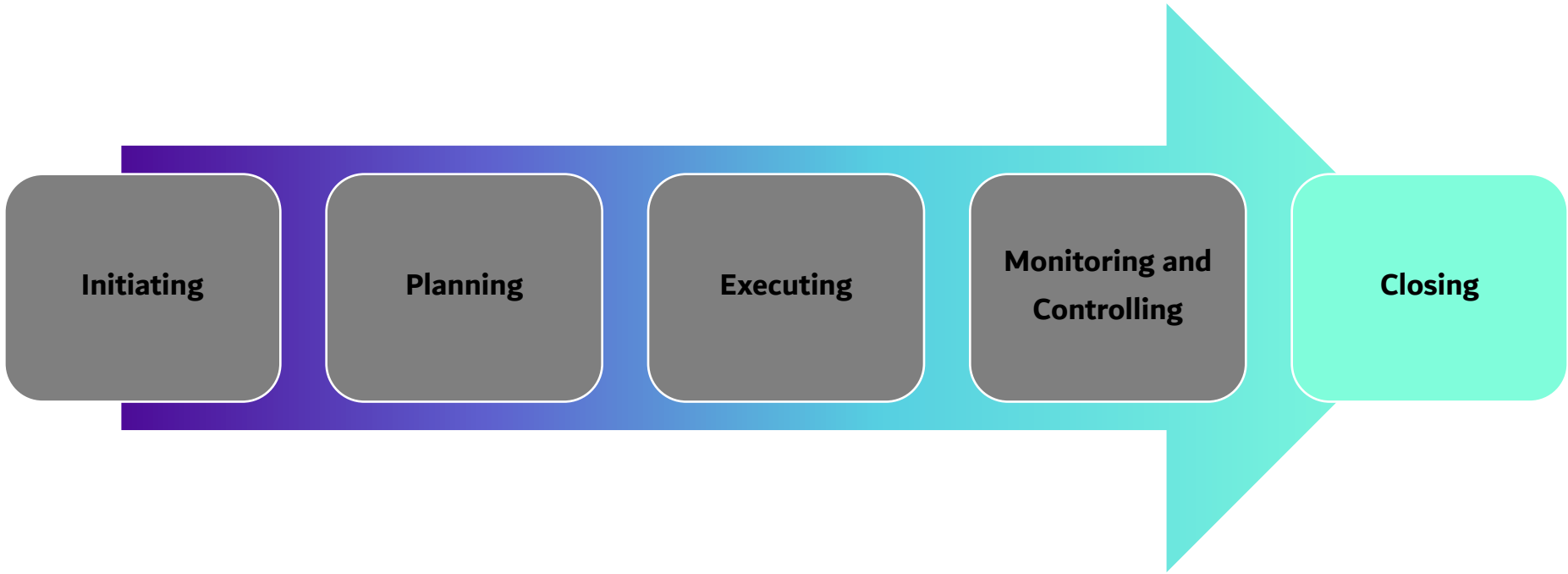
The table below also contains the activities that will be carried out at this phase:

#NO	Reference	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.	PDP.1.2	Activating and adhering to the prepared policies and procedures.	Implementing the policies, procedures, plans, tools, and strategies that have been provided.	Approved data management and governance processes.
2.	PDP4.2	Creating and documenting data rights management processes to support data subject rights.	Managing data rights.	Data rights management processes.
3.	PDP.2.1	Supervising the implementation of security measures to protect personal data.	Implementing security measures to protect personal data.	Implementing security measures to protect personal data.
4.	PDP.4.4	Developing any remaining documents.	Reviewing and approving the documents.	Approved documents.

5.	PDP.2.1	Providing guidance and improvements on any topics related to personal data protection (during the project period).	Reviewing, approving, and applying the guidelines.	Approved guidelines.
6.	PDP.1.2	Supervising meetings related to personal data protection tools and solutions during the project period with suppliers and providing appropriate advice on solutions and data management tools suitable for the entity.	Coordinating and attending meetings on data management solutions with suppliers.	Selecting the best data management solutions and tools suitable for the organization
7.	PDP.4.4	Conducting compliance audits, reviews, and improvements related to personal data protection and data protection standards and plans.	Reviewing and approving personal data protection audit reports, standards, and data protection plans.	Approved audit reports on data protection, personal data protection standards, and plans.

8.	PDP4.4	Developing corrective plans to ensure full compliance with the personal data protection system and working on them during the project period.	Reviewing and approving corrective plans to ensure full compliance with the personal data protection system.	Corrective plans to ensure full compliance with the personal data protection system to be worked on during the project period.
9.	N/A	Sending a weekly report on the project progress and level of advancement.	Reviewing the weekly report and providing feedback.	Weekly report on the progress of the project and level of advancement.

4.5 Closing Phase:



At this phase, will be conduct knowledge transfer to the employees.

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

#NO	Reference	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.	N/A	Guiding and assisting the entity in implementing the Personal Data Protection System and Regulations during the project period	Ensure commitment and cooperation from all departments, especially the IT Department and the Data Management Office in the entity	Guiding and assisting the entity in implementing the Personal Data Protection System and its regulations during the project period
2.	N/A	Transferring knowledge (according to the schedule in the following section) regarding everything related to the project documents and activities (this will be on a regular basis from the first day of the project)	Allocate time and availability from the Data Management Office	Transferring knowledge of everything related to the project documents

5. Knowledge Transfer Plan

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

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

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

6. Weekly Project Progress Report

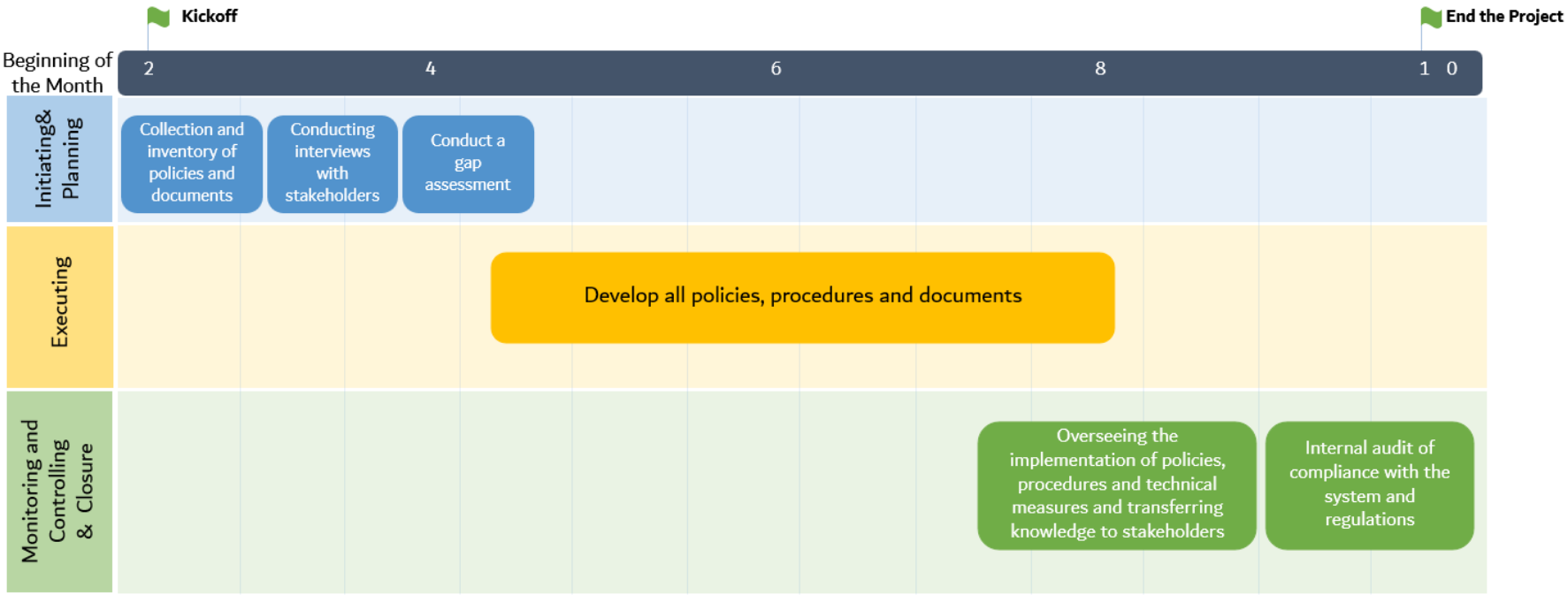
The table below shows the project progress on a weekly basis to ensure that the objectives are met according to the planned schedule. The report is divided into four main sections:

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			

7. Approximate project implementation timeline

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



8. Resource, Quality and Communication Plans

In the planning 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.

9. Project Management

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

- Schedules and minutes of meetings
- Project status reports

10. 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

11. Project Scope and Assumptions

11.1 Out of Scope of Work

1. Implementing or purchasing technical tools and solutions related to the implementation of the Personal Data Protection Law and Regulations

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

11.2 Assumptions

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

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

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

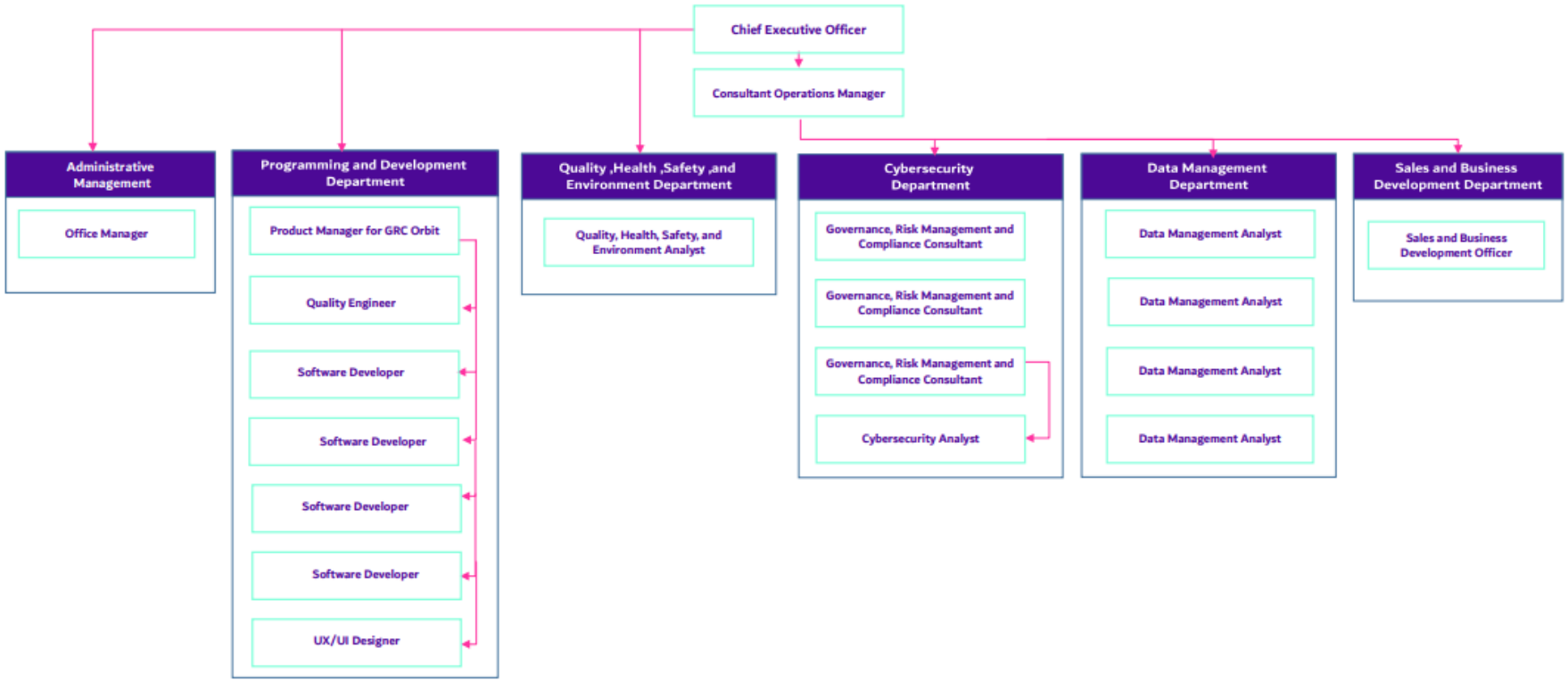
4. **An AI bot will be integrated to record and summarize conversations, aiming to assist consultants in improving and enhancing meeting minutes.**

5. **The project will be complete over 10 months.**

12. Company Information

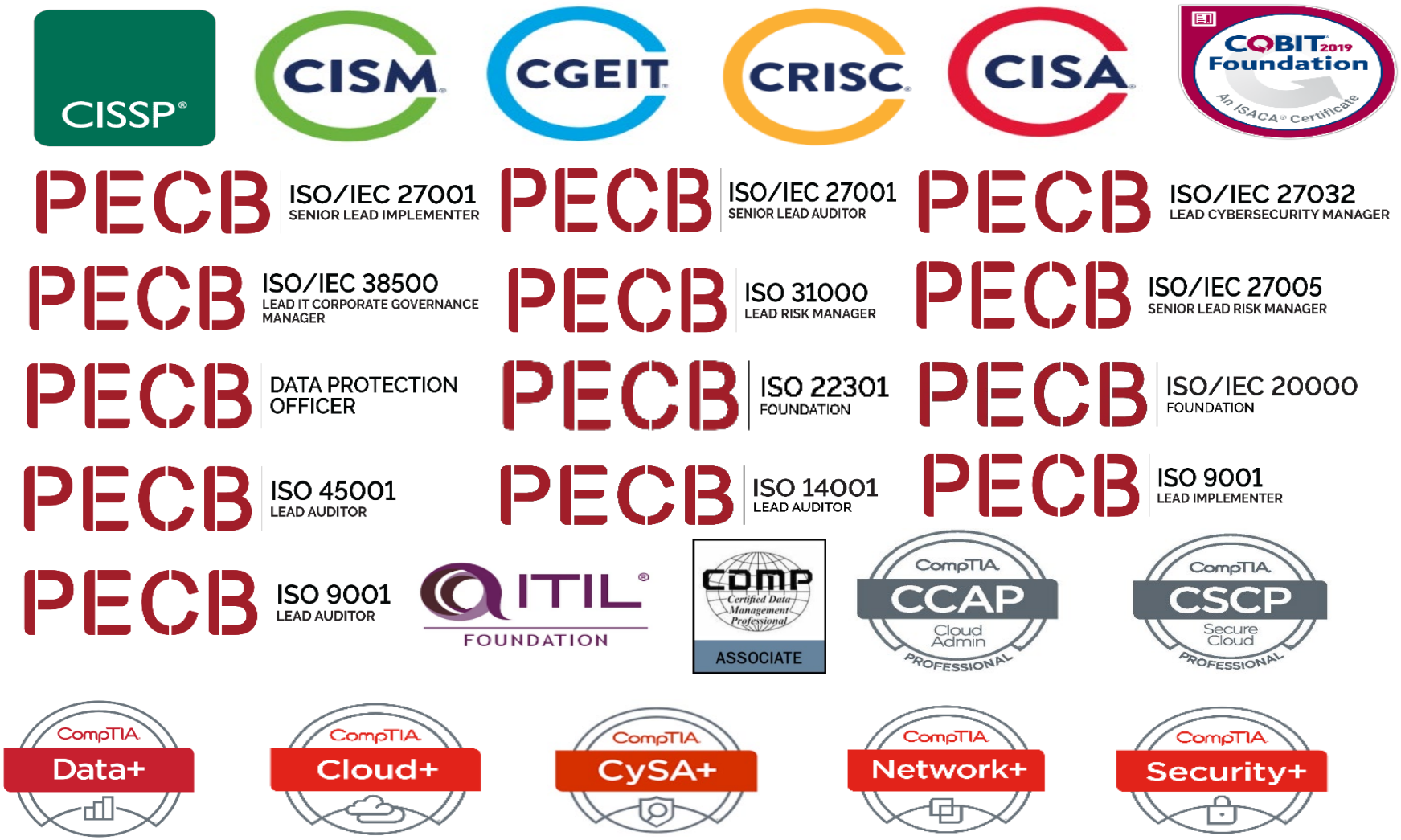
Trusted Vision is a data management and cybersecurity consulting firm that provides full services in governance, risk, and compliance management, as well as solutions and training, to help entities meet their business requirements. What sets us apart are the core values we espouse.

Organizational Structure



13. Certificates

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



14. 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 للتأمين بأمان	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	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	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)	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

15. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	H.A	Governance , Compliance Risk Management (GRC) and Data Management Advisor	Bachelor of Computer Engineering	11 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 in accordance with ISO 27001, NIST, NCA and Saudi Arabian Oil Company Cybersecurity Standard. 3. Manage cybersecurity risks and conduct cybersecurity risk assessments and IT

					risk assessments in accordance with national and international standards. 4. Implement and review the organization's Information Security Management System in accordance with 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 in accordance with 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 in accordance with 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).
3	G.H	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	3 Years	1. Manage and conduct operational and process reviews in accordance with 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 in accordance with 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).
4	A.Y	Governance and Risk Management (GRC) Consultant	Master of Cybersecurity	1 Years	1. Manage and conduct operational and process reviews in accordance with 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 in accordance with ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards.
5	I.A	Data Management Senior 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 objectives 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.
6	H.A	Data Management Analyst	Bachelor of Data Analysis	2 Years	1. Identifying and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic objectives. 2. Conducting assessments of data management maturity to identify gaps and recommend improvements. 3. Developing Business Intelligence (BI) use cases and enhancing 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.
7	B.H	Data Management Analyst	Bachelor of Artificial Intelligence	2 Years	1. Developing data sharing policies and request models, as well as establishing internal and external agreements to ensure compliance and effective governance. 2. Designing mechanisms to improve data integration across systems, enhancing the seamless flow of data and ensuring its quality when shared between entities. 3. Identifying data quality standards and dimensions, and customizing rules to

					ensure data accuracy, completeness, and consistency. 4. Developing procedures for addressing data quality issues, creating plans for quality monitoring, and designing corrective measures to resolve identified issues, ensuring continuous improvement. 5. Developing policies and procedures for data structuring, ensuring organization and optimization of data according to established standards. 6. Designing comprehensive plans for data modeling and structuring to enhance data integration across systems and improve usability and analysis capabilities.

					7. Familiarity with the fundamentals of preparing analytical reports and dashboards to support strategic decision-making at various organizational levels. 8. Designing and reviewing dashboards to ensure they deliver accurate and valuable insights, with a focus on enhancing user experience and ease of access to data.
8	B.B	Data Management Analyst	Bachelor of Computer Information Systems	1 Year	1. Identifying and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic objectives. 2. Conducting assessments of data management maturity to identify gaps and recommend improvements.

					3. Developing Business Intelligence (BI) use cases and enhancing 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.