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

Version 2.0

Date: 23/Nov/2025 AD

Prepared by: Trusted Vision Cybersecurity Company

Contact Information

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

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

TRUSTED VISION

Table of Contents

1. Executive summary of client requirements

Trusted Vision is proud to offer comprehensive consulting services for the implementation of the Oman Personal Data Protection Law (PDPL) issued under Royal Decree No. 6/2022 and its Executive Regulation No. 34/2024, in alignment with the requirements of the Ministry of Transport, Communications and Information Technology (MTCIT) as the competent supervisory authority and taking into account the data protection and information security expectations of the Capital Market Authority (CMA) / Muscat Stock Exchange (MSX) applicable to listed companies.

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 ability in cybersecurity and data management.
- An effective approach to project implementation to meet project requirements on time, 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. Ensure compliance with the Omani Personal Data Protection Law and its Executive Regulation.
2. Evaluate the current information flow within the project scope and assess privacy implications and risks according to the Personal Data Protection Law.
3. Develop necessary plans for full compliance with the Omani Personal Data Protection Law and its Executive Regulation.
4. Raise awareness about legislative requirements and policies related to personal data protection within the organization.

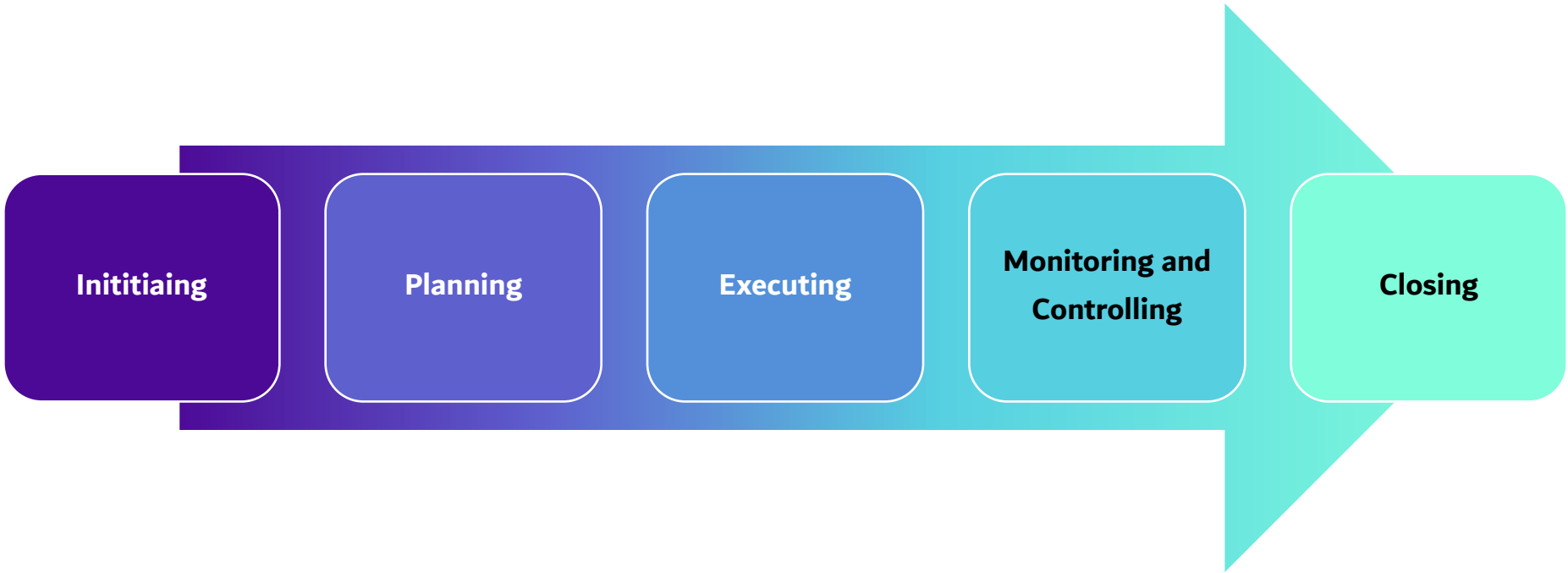
3. Project Benefits

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

1. Significantly reduce risks and associated costs stemming from potential data breaches and cybersecurity threats by implementing robust data protection strategies and measures.
2. Enhance transparency and accountability in data management.
3. Gain customers' trust in the secure processing of their personal.

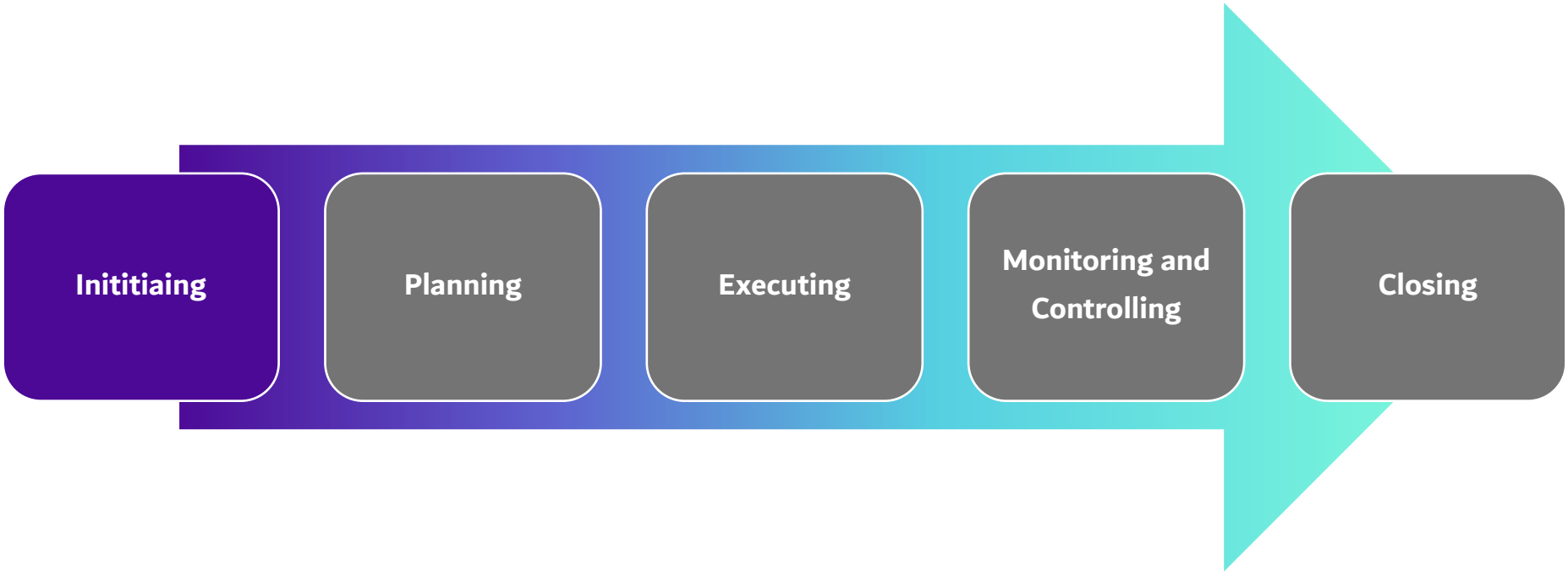
4. Project Implementation Methodology

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



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

4.1 Initiating Phase

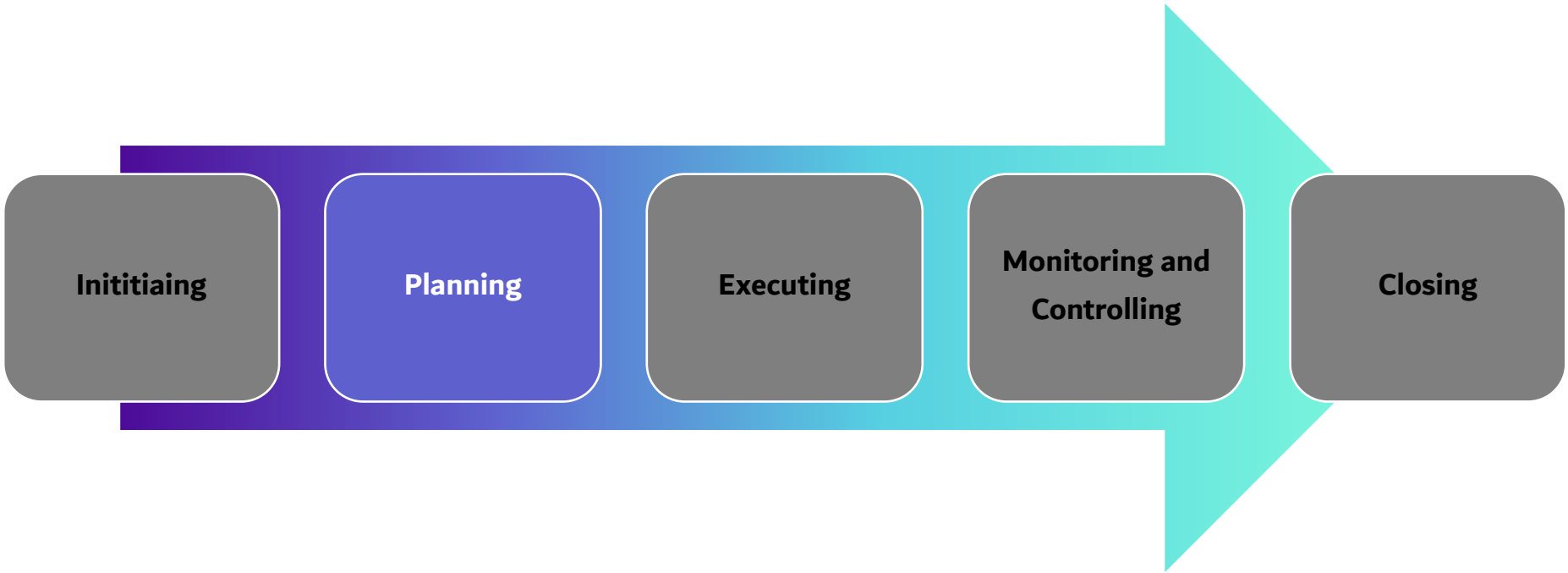


At this phase, the project is defined, and the project leader outlines their responsibilities which includes the project charter, includes restrictions and assumptions and preparing consultants to work at the entity's headquarters.

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

NO#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Preparing the project team	• Nominate the project sponsor, project steering committee, and project manager. • Obtain commitment from the project sponsor and executive management and take part in 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 collaborating with them

4.2 Planning Phase



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

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

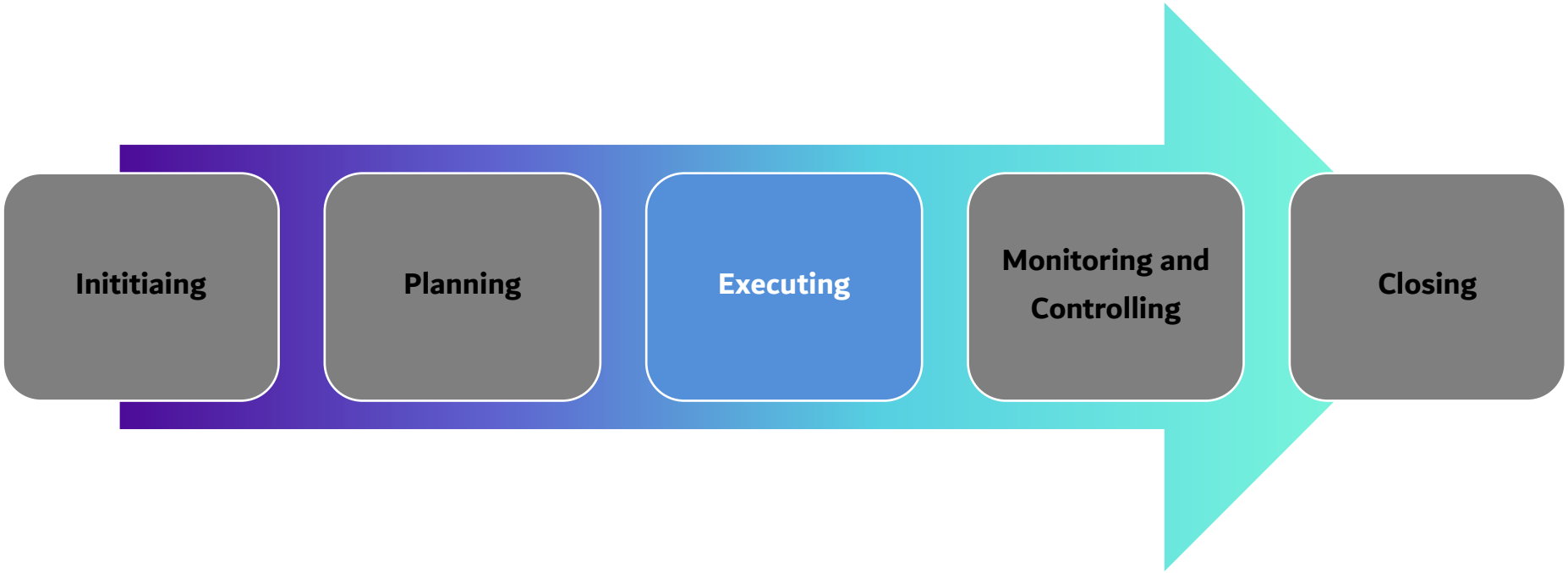
#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Kick-off meeting	• Invite all concerned and coordinate communication with them	Minutes Meeting
2.	Develop a project implementation plan (PDPL project plan) that holds: • Meeting with the concerned stakeholders. • Raising their awareness of the project • Scope of work • The requirements of the project and what is needed from them.	• Review and approval of the stakeholder's management plan.	Project implementation plan (PIP)

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
3.	Collect, inventory, and review the following data: • The entity's business strategy • A list of general risks existing within the entity. • Roadmaps, information, and data management plans. • Review all systems and procedures related to data privacy, check compliance with privacy regulations and document the results. • Any documents relevant to the above documents.	• Submit all required documents and information	Minutes Meeting

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
4.	Conduct interviews with project stakeholders to understand their needs and expectations, including but not limited to: • Head of the organization • Information Technology Management • Data Management Office • HR department • The rest of the departments and departments within the entity	• Coordinating interviews with all departments.	Minutes Meeting

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
5.	Review the PDPL governance model for the client: • Analyze current organizational structure • Define PDPL roles, responsibilities, and reporting lines • Share the proposed model for client review	• Provide organizational information and required documents • Nominate staff for PDPL roles	• Roles and responsibilities • Reporting lines and structure
6.	Assess the current situation, find gaps (technical, operational, and legal) and the flow of personal data in internal systems, understand and study	Send any required documents and give adequate answers to the consultants	Gap assessment report

4.3 Executing Phase:



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

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

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Develop a personal data protection plan	Review and approve a personal data protection plan.	Personal data protection plan.
2.	Perform discovery of personal data processing activities across key business units, systems, applications, and third parties. Current-State Assessment & Data Inventory	Review and approve the activities	Discovery for personal data processing
3.	Developing a Record of Processing Activities (ROPA), includes: • data inventory	Review and approve the Record of Processing Activities (ROPA).	Record of Processing Activities (ROPA).

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
	• covering purposes • categories of data • data subjects • Recipients • and legal basis.		
4.	Highlight any processing that may require MTCIT permits/approvals (e.g., certain categories of sensitive personal data or high-risk processing, as defined in the PDPL framework)	Review and approve the processing	Personal data processing activities

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
5.	Website Privacy Policy and Cookie Policy.	Review and approve the Website Privacy Policy and Cookie Policy.	Website Privacy Policy and Cookie Policy
6.	Data Protection and Privacy Policy (Handling Personal Data and Compliance with PDPL Principles including Privacy by design and default and data minimization guidelines).	Review and approve the Data Protection and Privacy Policy.	Data Protection and Privacy Policy.
7.	Personal Data Breach Notification Template	Review and approve the personal data breach notification template	Personal Data Breach Notification Template
8.	Development of Personal Data Protection Training Plan	Review the personal data protection training plan.	Personal Data Protection Training Plan

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
9.	• Document of Roles and Responsibilities Related to Personal Data Protection • Target Operating Model (TOM)	Review and approve the document outlining roles and responsibilities related to personal data protection.	Document of Roles and Responsibilities Related to Personal Data Protection
10.	Privacy Risk Assessment Policy and Procedures - DPIA	Implementing the Privacy Risk Assessment Policy and Procedures.	Privacy Risk Assessment Policy and Procedures - DPIA
11.	(DPIA) Impact Assessment Template	Review and approve the Data Protection Impact Assessment (DPIA) template.	(DPIA) Impact Assessment Template
12.	Reporting and Approval Policy and Procedures	Implementing policies and procedures for managing consents.	Reporting and Approval Policy and Procedures

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
13.	Consent Collection Template	Review and approve the consent collection template.	Consent Collection Template
14.	Data Subject Rights Management Procedures (Procedures for Handling Data Subject Requests include Access, Correction, Erasure, Grievance Redressal, and Restriction of Processing Requests	Implementing procedures and plans for managing data subject rights.	Data Subject Rights Management Document.
15.	Record of Personal Data Subject Requests	Review and approve the record of data subject requests.	Record of Personal Data Subject Requests
16.	Data Subject Requests Template	Review and approve the data subject request template.	Data Subject Requests Template

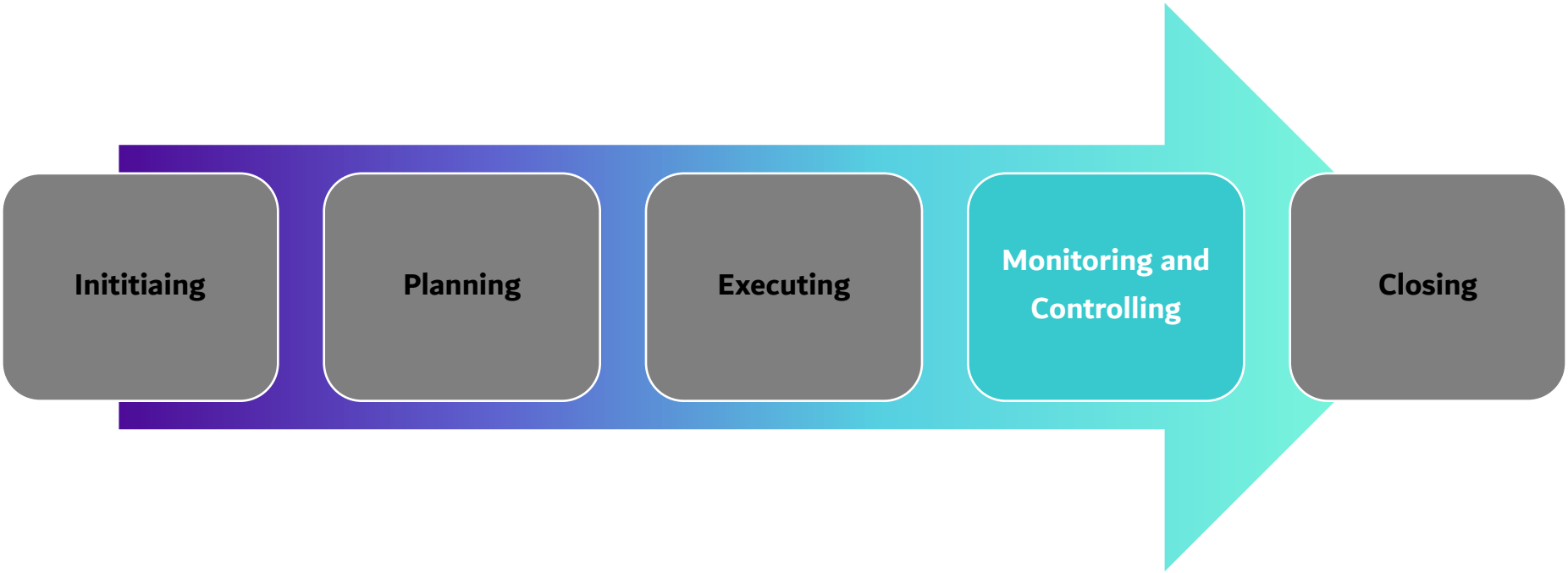
#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
17.	Data Sharing Policy and Procedure	Review and approve the data sharing policy and procedures.	Data Sharing Policy and Procedure
18.	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
19.	Third-Party Compliance Assessment Template	Review and approve the third-party compliance assessment template.	Third-Party Compliance Assessment Template
20.	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

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
21.	Internal Disclosure/Sharing Cases Assessment	Review and approve the assessment of internal disclosure/sharing cases.	Internal Disclosure/Sharing Cases Assessment
22.	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.	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.	Data Breach Notification Template	Review and approve the Data Breach Notification Template.	Data Breach Notification Template

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
25.	Retention and Disposal Policy and Procedures.	Review and approve the Access Storage and Disposal Policy and Procedures.	Access Disposal Policy and Procedures.
26.	Preparing educational awareness materials on how to protect personal data. (including PDPL principles, data protection responsibilities, and regulatory requirements)	Coordination with all departments and divisions.	Awareness Tests and Understanding Assessment
27.	Implementation plan for the personal data protection law and regulation.	Review and approve the implementation plan.	Implementation plan for the personal data protection law and regulation.

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
28.	Vendor due diligence Template	Review and approve the Vendor due diligence Template	Vendor due diligence Template

4.4 Monitoring and Controlling Phase:



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

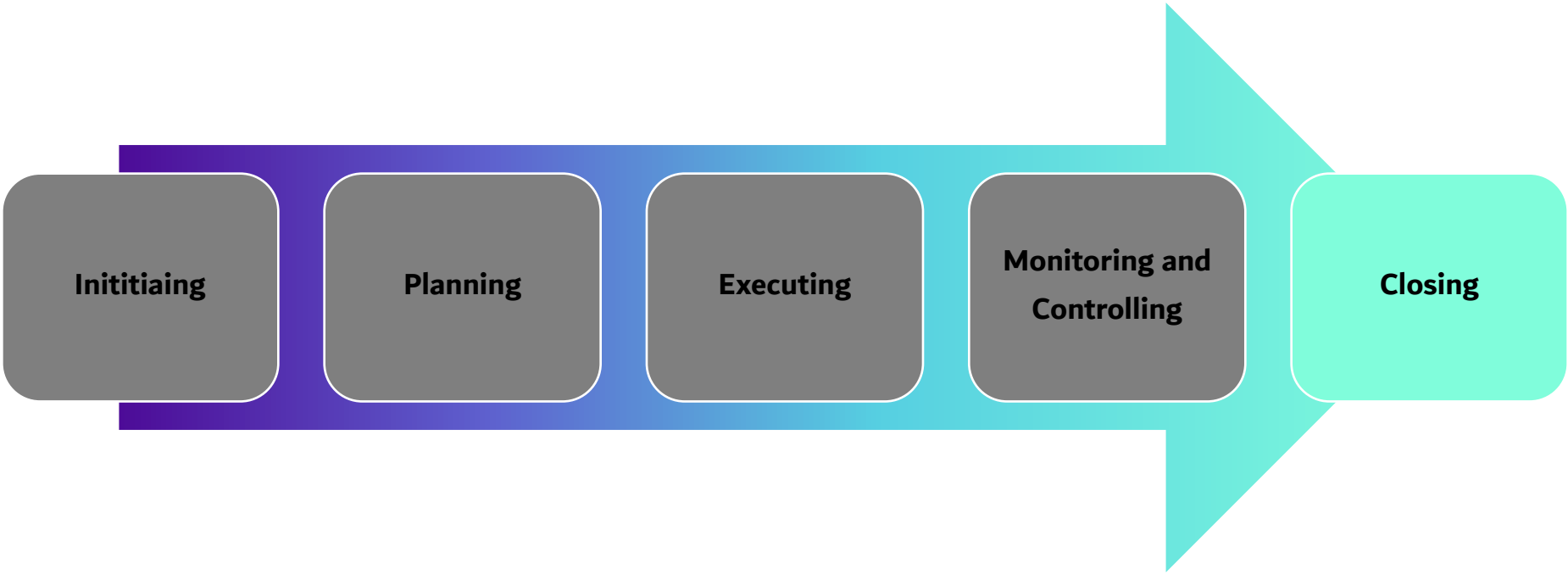
The table below also holds the activities that will be conducted at this phase:

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Activating and adhering to the prepared policies and procedures.	Implementing the policies, procedures, plans, tools, and strategies that have been provided.	Approved data management and governance processes.
2.	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	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 Personal Data Protection Compliance Audit Logs for a Reasonable Period of No

	• Document Compliance Audit Logs for a Reasonable Period of No Less Than 24 Months in a Consolidated Record • 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.	Less Than 24 Months in a Consolidated Record
3.	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.	Developing any remaining documents.	Reviewing and approving the documents.	Approved documents.
5.	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.	Supervising meetings related to personal data protection tools and solutions during the project period with suppliers and giving proper 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.	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.	Developing corrective plans to ensure full compliance with the personal data protection law and working on them during the project period.	Reviewing and approving corrective plans to ensure full compliance with the personal data protection law.	Corrective plans to ensure full compliance with the personal data protection law to be worked on during the project period.
9.	Sending a weekly report on the project's progress and level of advancement.	Reviewing the weekly report and providing feedback.	Weekly report on the progress of the project and level of advancement.

4.5 Closing Phase:



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

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

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Provide advisory support including consultation on legal interpretations, best practices, and regulatory expectations for the entity in implementing the Personal Data Protection law and Regulation	Ensure commitment and cooperation from all departments, especially the IT Department and the Data Management Office in the entity	Guiding and aiding the entity in implementing the Personal Data Protection law and its regulation during the project period
2.	Transferring knowledge (according to the schedule in the following section) about everything related to the project documents and activities (this will be on a regular basis from the first day of the project)	Allocate time and availability from the relevant department	Transferring knowledge of everything related to the project documents

#NO	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
3.	Post-Implementation Support (Optional)	Coordination with all departments and divisions.	PDPL post-implementation support for a period of up to 12 months
4.	Conduct close-out meeting	• Review the final project outcomes and confirm acceptance. • Provide feedback. • Approve closure of the project activities.	Project Close-Out Report, including: • Summary of work completed • Final deliverables list

5. Knowledge Transfer Plan

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

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

How (communication channels)	From (target management)	when	what (content)
• Video meetings • In-person meetings • E-mail	Data management office (if applicable) or relevant department	Daily	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 aims are met according to the planned schedule. The report is divided into four main sections:

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

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

7. Resource, Quality and Communication Plans

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

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

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

8. Project Management

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

- Schedules and minutes of meetings
- Project status reports

9. Risk Register

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

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

10. Project Scope and Assumptions

10.1 Out of Scope of Work

1. Implementing or buying 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 earlier sections will be considered outside the scope of work.

10.2 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.**

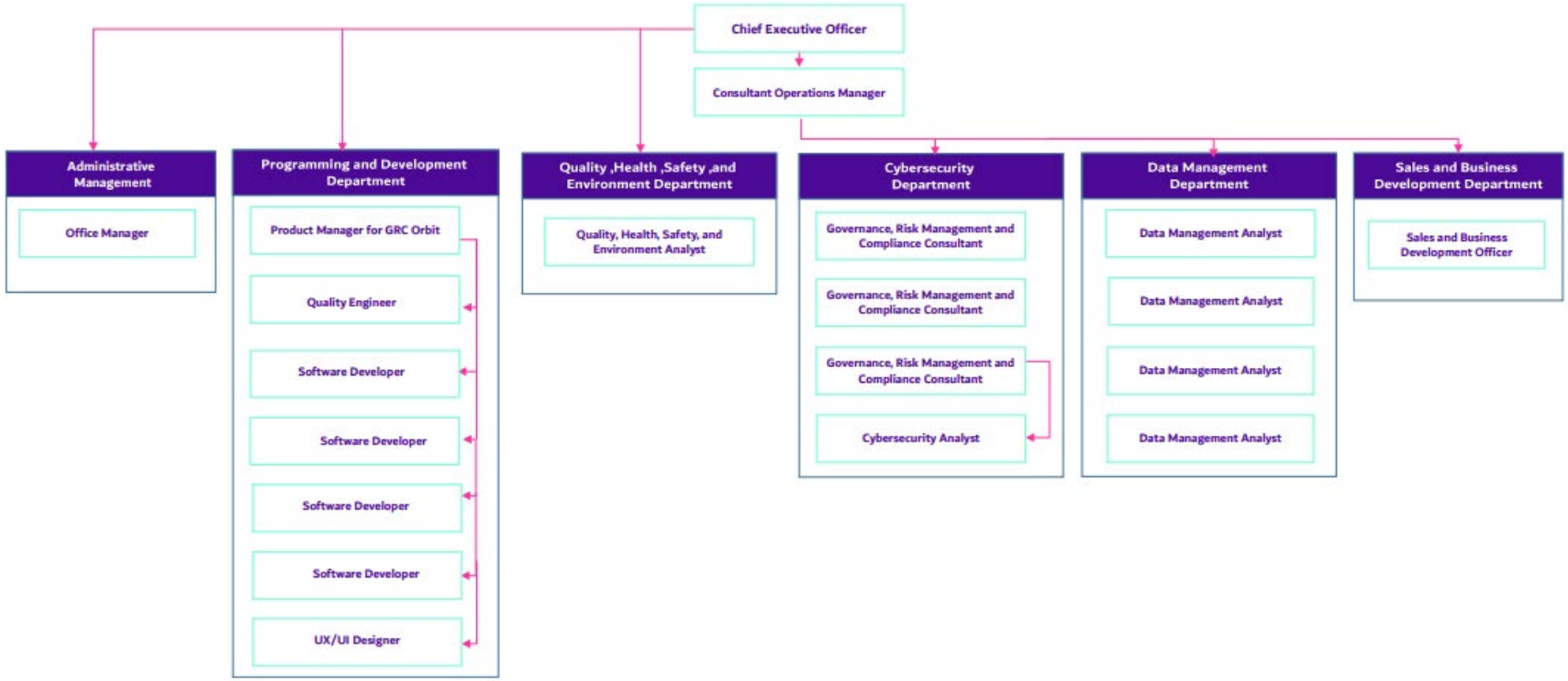
3. **Cooperation from the entity's departments and departments is mandatory for the success of the project.**

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

5. **The project will be executed over 2 months.**

11. Company Information

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



12. 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+
CNSS
FORTINET
NSE
1
ASSOCIATE
FORTINET
NSE
2
ASSOCIATE
FORTINET
NSE
3
ASSOCIATE
FORTINET
NSE
4
PROFESSIONAL
C|EH
Certified Ethical Hacker
paloalto
NETWORKS
PCCSA
paloalto
NETWORKS
PCNSA
paloalto
NETWORKS
PCNSE
CISA
CYBER+INFRASTRUCTURE
ASSOCIATE
CERTIFIED

13. Earlier Projects

Many projects have been implemented by dealing with various parties in different countries and multiple environments, and we always strive to implement the best practices and standards to achieve the best required results.

Project No.	Project Name	Client Name	Logo	Project Description
1	Implementation of the SAMA CSF Cybersecurity Framework	Gulf Union and Al Ahlia Insurance Company	إتحاد الخليج للتأمين التعاوني GULF UNION COOPERATIVE INSURANCE CO.	1. Developing cybersecurity policies, procedures and standards issued by the Saudi Central Bank 2. Conducting a Cybersecurity Risk Assessment on information systems, assets, and processes 3. Developing key performance indicators and key risk indicators for operations (KPIs, KRIs) 4. Performing process monitoring
2	Implementing a Business Continuity Management System SAMA BCM	ASIG Insurance Company	ACIG للتأمين 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. 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)	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	شركة العرض المتقن 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)	تنمية البرنامج الوطني للتنمية المجتمعية في المناطق	1. Establish a cybersecurity management system. 2. Develop a cybersecurity strategy and operational model. 3. Develop relevant policies, procedures, and standards. 4. Ensure compliance with the National Cybersecurity Authority frameworks ECC, CCC, DCC, OSMACC, TCC 5. Ensure compliance with ISO 27001 6. Conduct internal audits on the National Cybersecurity Authority frameworks and ISO 27001 7. Obtain ISO 27001 certification
13	Cybersecurity Risk Management	Sovereign Government Entity		1. Develop a cybersecurity risk management method and align it with the overall risk management method. 2. Conduct a cybersecurity risk assessment on information assets + third parties + material changes + technical projects + operations

14	NCA-ECC and CCC-P	Nashirnet		1. Establish a cybersecurity management system. 2. Develop policies, procedures, and standards for cloud computing controls and ECC + CCC core controls for service providers. 3. Conduct cybersecurity risk assessments for projects and products. 4. Conduct internal audits. 5. Develop and measure performance indicators
15	Data Classification and Modeling	King Abdulaziz Public Library		1. Develop data log. 2. Classify data. 3. Develop data modeling plan and perform modeling for library systems
16	Implementation of the Personal Data Protection Regulation (PDPL)	Aljaber Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy. 3. Developing consent management processes 4. Conducting audits of data processing activities

				5. Conducting awareness workshops on personal data protection
17	Implementation of the Personal Data Protection Regulation (PDPL)	Hala Payment		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy. 3. Developing consent management processes 4. Conducting audits of data processing activities 5. Conducting awareness workshops on personal data protection
18	Implementation of the Personal Data Protection Regulation (PDPL) Regulation	Mrna Finance		1. Limiting personal data and processing activities 2. Developing policies, standards and procedures related to data privacy. 3. Developing consent management processes 4. Conducting audits of data processing activities 6. Conducting awareness workshops on personal data protection

19	Implementation of the SAMA CSF Cybersecurity Framework	Finzey		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) 5. Performing process monitoring
20	Implementation of the Personal Data Protection Regulation (PDPL) Regulation	Finzey		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

14. Staff

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

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

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

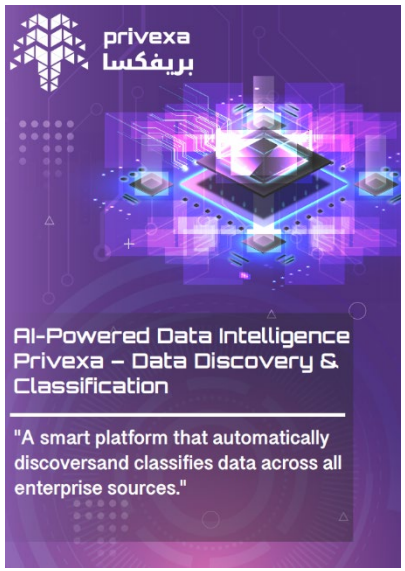
					ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against 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	R. Y	Governance and Risk Management (GRC) Consultant	Bachelor of Cybersecurity	1 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.

8	B. B	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Information Systems	2 Year	1. Finding and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic aims. 2. Conducting assessments of data management maturity to find gaps and recommend improvements. 3. Developing Business Intelligence (BI) use cases and enhance user experience through data-driven insights. 4. Designing and implementing plans, policies, and procedures for Master and Reference Data Management, Freedom of Information, Document and Content Management, and Data Value Realization in alignment with NDMO regulations.

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

15. Annex (1): Privexa Tool (Data Discovery & Classification Tool)



Solution Overview

AI-powered solutions for data discovery & classification

Supercharge your data governance and privacy programs with Privexa — the intelligent platform that discovers, indexes, and classifies sensitive data across files, databases, email systems, cloud repositories, and more.

Privexa supports all enterprise data types (structured and unstructured) in full alignment with NCA-DCC Data Cybersecurity Controls.

Data Discovery & Classification

Privexa delivers fast, accurate, and automated intelligence across all enterprise data — enabling complete visibility and compliance with minimal effort

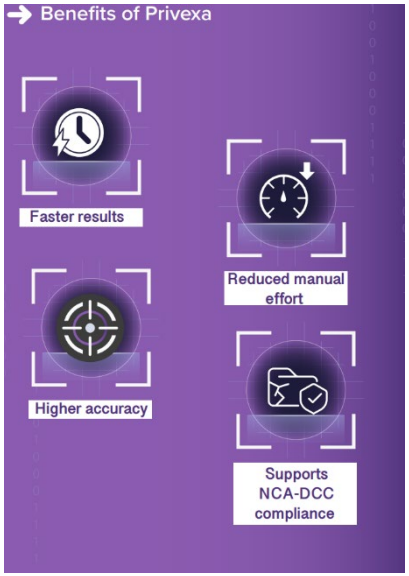
Data Discovery

- Fast identification of sensitive data across all sources
- High-accuracy contextual detection
- No rules, no training, no manual scanning

Data Classification

- Automated and consistent classification
- Context-aware intelligence
- Scalable and customizable policies

Benefits of Privexa



Conclusion

Welcome to Privexa

Privexa is an end-to-end data intelligence platform designed to help organizations discover, understand, and secure their data with speed and precision. Our AI-powered capabilities enhance compliance, reduce risk, and empower teams with trusted, actionable insights.

Try Privexa Today

Schedule a demo to explore how Privexa's discovery and classification engine can transform your organization's data security and compliance strategy.

privexa
بريفكسا