Technical Proposal for Proposal for Business Continuity and Cybersecurity Transformation

Version 1.0

30-Mrach-2026

Prepared by: Trusted Vision for Cybersecurity Company

Contact Information

For inquiries about this document and the information received, you can contact the persons listed in the table below:

Name	**Hashim Al , Azizi**
Phone Number	**+966-53-122-1580**
Email	**Hashem.azizi@trustedvision.biz**
Address	**Cordoba District, Said Bin Zaid Street,** **Enjaz Group Building, No. 6482, First Floor,** **P.O. Box: 13247,** **Riyadh, Saudi Arabia.**

Contents

1. Executive Summary of Client Requirements

The Client aims to engage a qualified vendor to enhance its Business Continuity Management System (BCMS) and Cybersecurity Framework in alignment with ISO 22301 and SAMA Cybersecurity Framework requirements.

The scope includes assessing the current state, identifying gaps, and developing required frameworks, policies, and plans such as BIA, TRA, BCP, and DRP. It also covers strengthening cybersecurity governance, conducting gap and maturity assessments, and establishing cyber risk management practices.

In addition, the project includes developing KPIs, KRIs, and dashboards for executive and board-level reporting, along with conducting training, awareness, and testing activities.

The overall objective is to improve compliance, strengthen resilience, enhance cybersecurity posture, and ensure continuity of critical services.

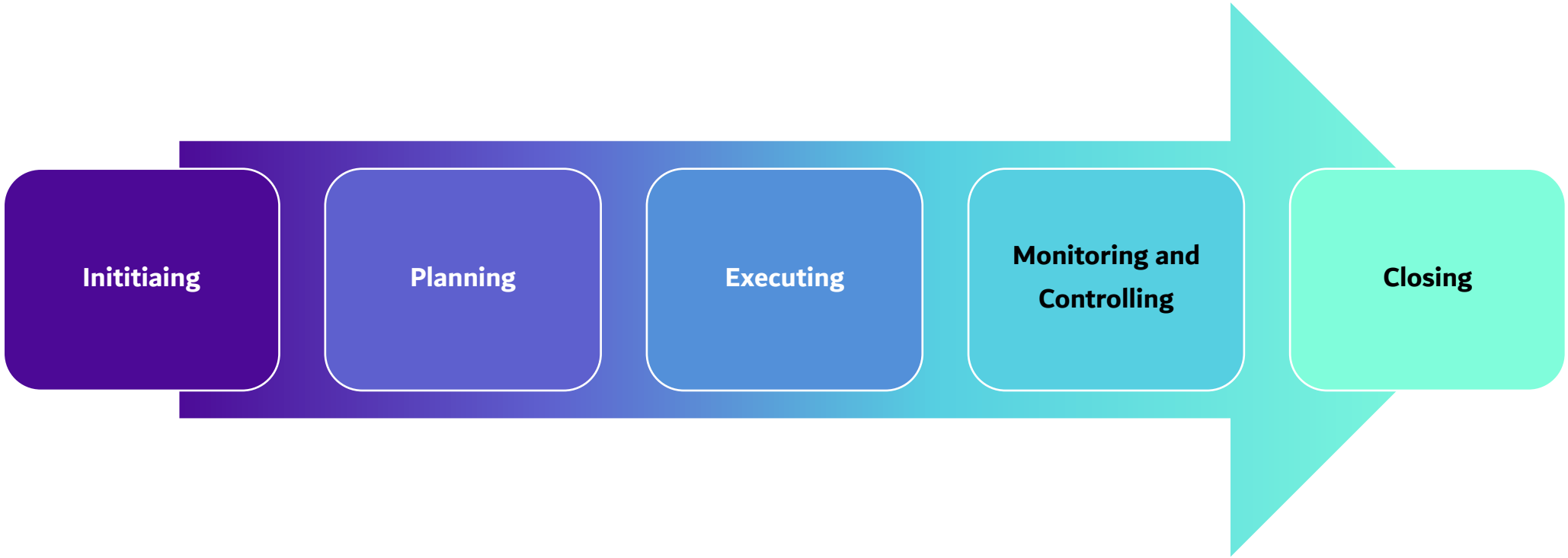
2. Project Objectives

The Business Continuity and Cybersecurity Consultancy Services Project aims to:

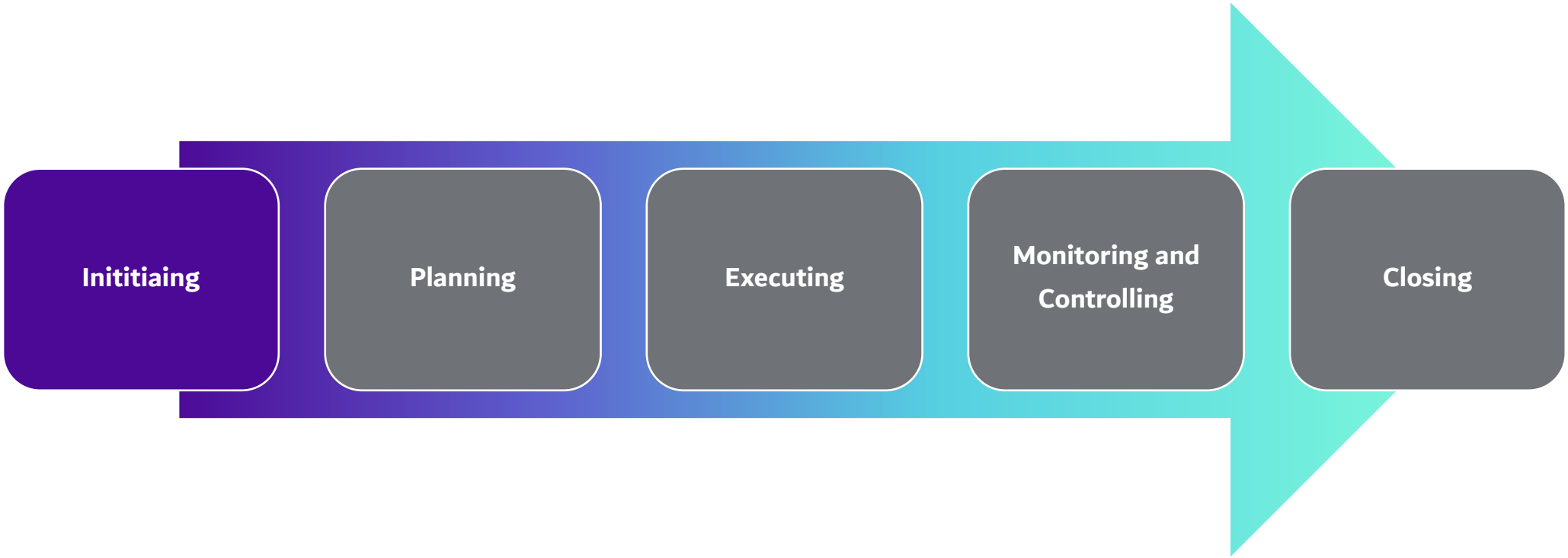
- Ensure compliance with Business Continuity and Cybersecurity regulatory requirements issued by the Saudi Central Bank (SAMA).
- Enhance the organization's ability to effectively respond to disruptions, disasters, and cyber risks.
- Protect critical assets, including employees, information, and operational systems.
- Strengthen business resilience through the implementation of BCMS, BCP, and DRP.
- Improve cybersecurity governance and risk management practices.
- Increase customer and stakeholder confidence through the organization's ability to maintain continuity of critical services.

3. Project Management and Implementation Methodology

At Trusted Vision, we follow PMI's global project management methodology in terms of initiating, planning, executing, monitoring and controlling, and closing.



3.1 Getting Started

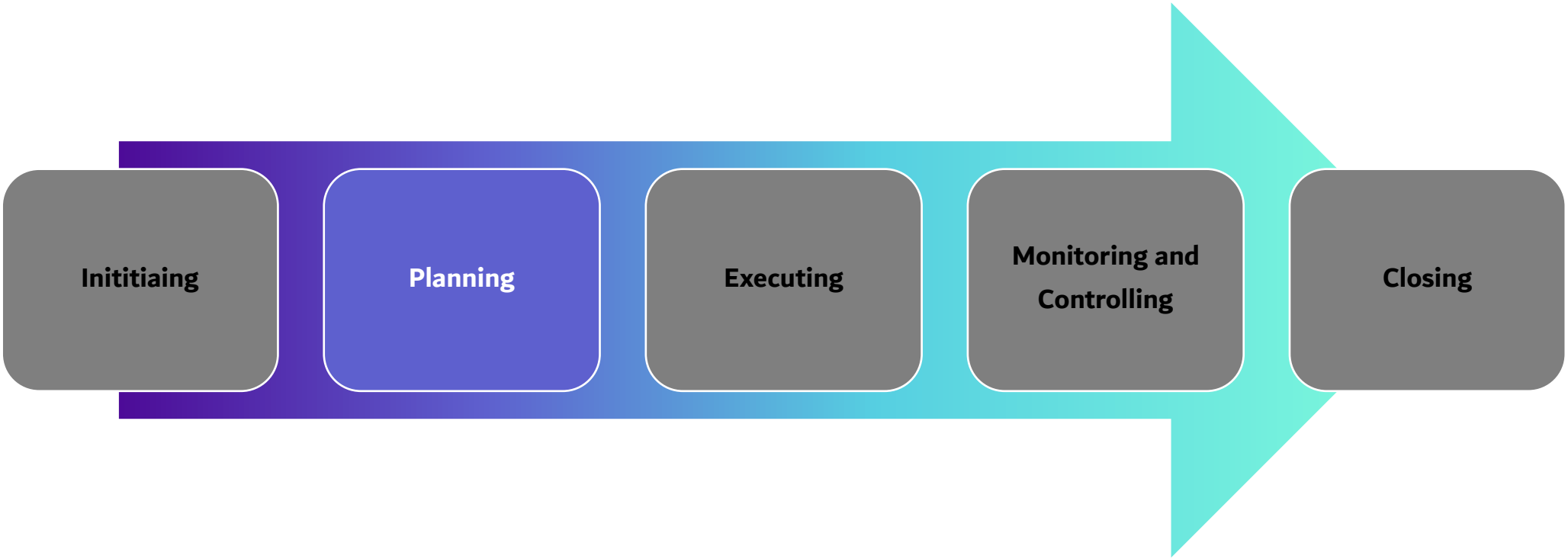


At this stage, the project is defined and the project leader defines its powers, the most important stakeholders, the most important expected risks, and the most important outputs, and this is written down in the project charter.

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

Number	Activities to be done by a reliable vision company	Activities to be carried out by the Entity	Completed Activities and Materials Delivered to the Entity
1	Project Team Preparation	• Designate a project sponsor, project steering committee, and project manager • **Appointment of a full-time person for business continuity (the project will only be successful with the provision of this person)** • Obtaining the project sponsor's commitment to business continuity	• List of consultants who will work on this project • A list of the names of the entity's employees who will be working with • A full-time business continuity person appointed by the entity

3.2 Planning Phase



In this stage, the scope is limited and the methods of work to reach the goals are determined, as well as the timetable, the project budget, and the most important outputs of this stage are determined, the project implementation plan that contains all the previous information. During which the following activities will be carried out.

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
1-	Preparing for the start of the project and having an opening meeting with stakeholders	Inviting all concerned and coordinating communication with them	Meeting Minutes
2-	Collect the following: • Business continuity policies, procedures, processes, templates and templates • Data records and technical assets • Roles, responsibilities and job descriptions • All Policies & Procedures Business Continuity Related Documents • The Entity's Work Strategy	Submit all required documents and information	Meeting Minutes

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity

	• List of general risks within the entity
	  • Contracts & Agreements
	  • Any information relevant to the above documents		

3-	Interviewing relevant parties in the project to understand their needs and expectations, but not limited to: • FAO President • Risk Management Committee • Information Technology Management • Cyber Security Management	• Coordinate interviews with all departments and departments	Meeting Minutes

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
	• Digital Transformation Management • Human Resources • Legal Affairs • The rest of the departments and departments within the entity		
4-	Assess the current situation, understand and study: • All data assets and environments • Business Continuity Management aligns with the direction of the entity	• Submit any required documents and provide adequate answers to the consultants	Understanding and studying the situation by consultants

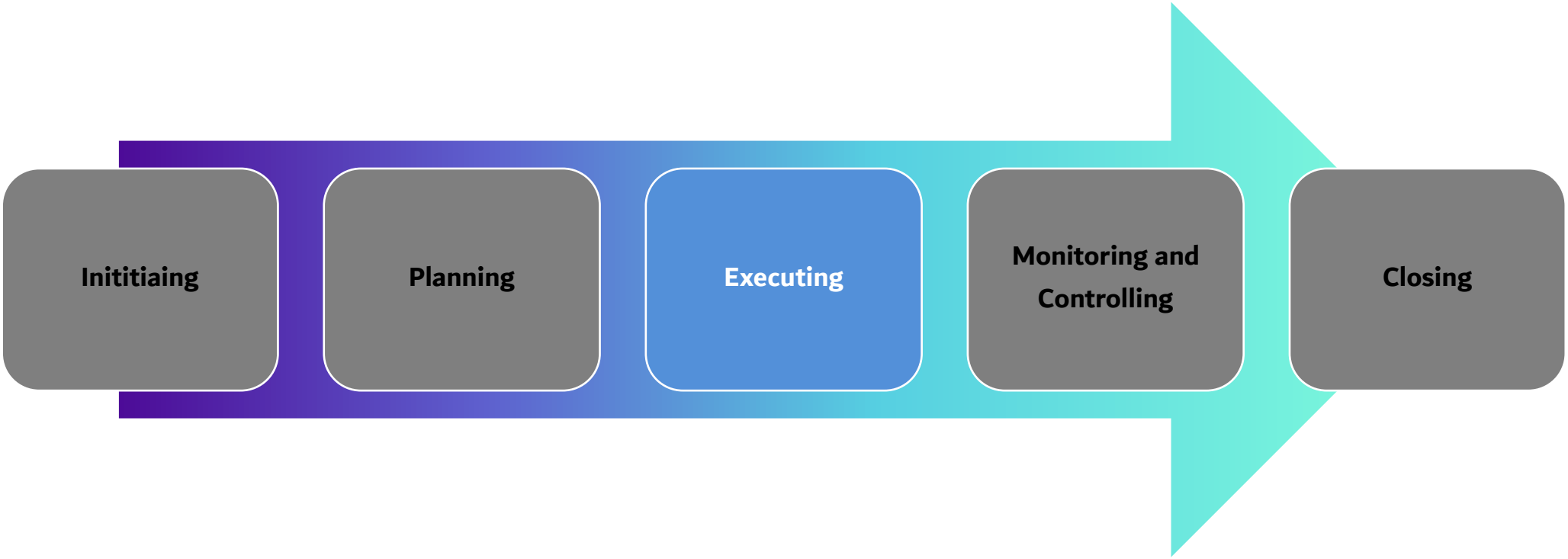
Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
	• Identify business continuity goals, KPIs,KRIs and needs along with stakeholder expectations. • Human Cadres and Organizational Structure in Business Continuity		
5-	Conduct gap Analysis of the Business Continuity against ISO 22301 and SAMA BCM and SAMA CSF	• Submit all required information and documents	• Gap Analysis Report
6-	Analyzing the internal and external context of the entity	• Review and approval of the internal and external context analysis document of the entity	• Analyzing the internal and external context of the entity

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
		• Coordination of meetings	
7-	Conducting business impact analysis with all departments (including all internal and external processes and procedures carried out by the entity, determining internal and external appropriations, and appointing staff for the processes and procedures that have been included).	• Review and Approval of the Business Impact Analysis and Risk Assessment Report • Coordination of meetings	Business Impact Analysis and Risk Assessment Report
8-	Developing a methodology to assess the impact of interruptions and assess risks related to business continuity in line with the entity's methodology	• Submit the general risk management methodology	

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
9-	Analyze the impact of business interruption using the Entity's approved Impact Impact Assessment Matrix according to the Entity's Impact and Risk Acceptance	• Coordination of meetings	
10-	Define the target period for the restoration of critical business services (RTO), the Recovery Point Objective (RPO) and the maximum acceptable downtime (MAO)	• Coordination of meetings	
11-	Assess and review the risks and threats to the continuity of the entity's business on an ongoing basis, and align them with the entity's approved institutional risk management methodology	• Coordination of meetings • Address all business continuity risks and procure High Availability solutions	

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
12-	Determine the maximum allowable time (MTDP) for business interruptions for products, services, processes, and activities, and the minimum level of service delivery.	• Coordination of meetings • Review and approval of risk assessment and impact analysis documents	• Meeting Minutes • Risk Assessments and Impact Analysis Documents • Risk Register
13-	Categorize the importance of suppliers, platforms, and applications and adhere to target recovery times	• Coordination of meetings	

3.3 Exeution Phase



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

The following activities will be carried out during this stage.

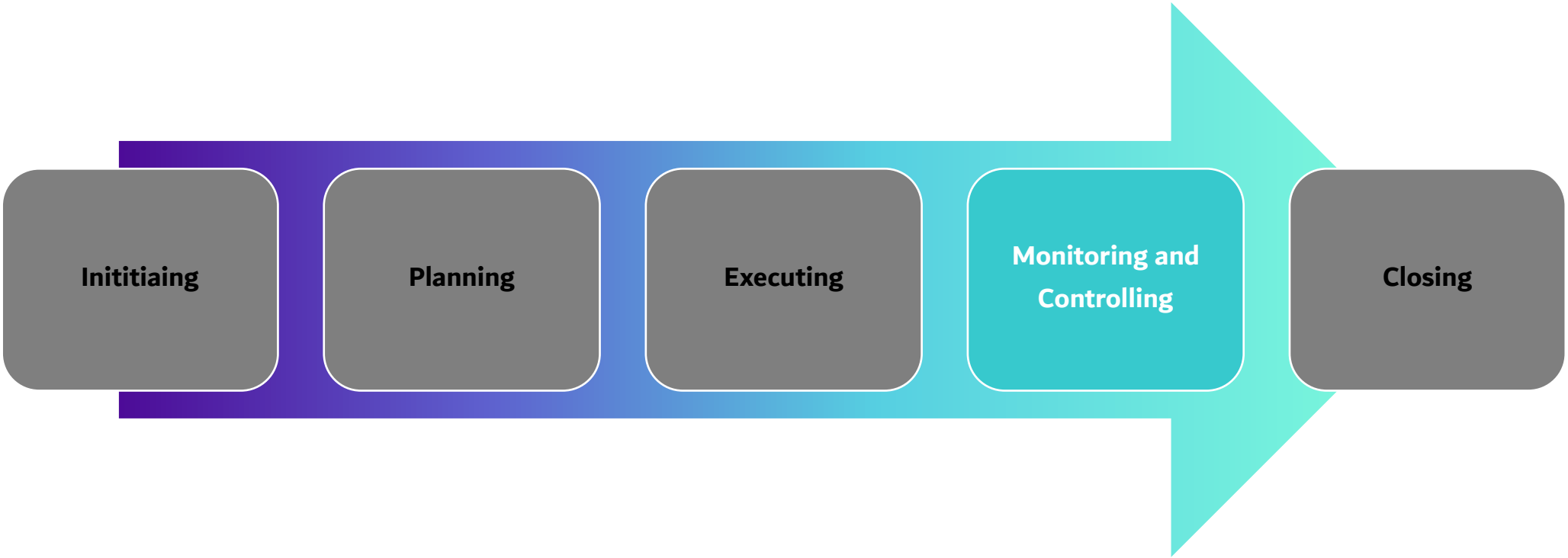
Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
1-	Advising on how to set up a business continuity module which includes: • Supervisory Committee Charter • Organizational Structure • Manpower needed for business continuity • Business Continuity Roles and Responsibilities	• Establishment of the Business Continuity Unit taking into account the recommendations of the consultant • Establishment of a Business Continuity Supervisory Committee • Organizational Structure Adjustment	• Supervisory Committee Charter • Organizational Structure • Manpower needed for business continuity • Business Continuity Roles and Responsibilities
2-	Review and improve the following business continuity governance documents: • Business Continuity Framework • Business Continuity Strategy • Business Continuity Policy	• Review and Approval of Business Continuity Governance Documents • Coordinate meetings to explain all business continuity governance documents	The following business continuity governance documents: • Business Continuity Framework • Business Continuity Strategy • Business Continuity Policy

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
	• Business Continuity Risk Management Methodology and Track • Periodic Business Continuity Review and Audit • Manage backups • Business Continuity Plans • Remote Work Policy • Business Continuity Awareness and Training Program • Communication and Media Plans • Disaster Recovery Plan • Crisis Management Plan • Change Management Methodology and Procedures • Develop the necessary response procedures		• Business Continuity Risk Management Methodology and Track • Periodic Business Continuity Review and Audit • Manage backups • Business Continuity Plans • Remote Work Policy • Business Continuity Awareness and Training Program • Disaster Recovery Plan • Crisis Management Plan • Change Management Methodology and Procedures • Necessary Response Actions

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
	• Required Reporting Forms for the Saudi Central Bank • Design a Cybersecurity Dashboard for executive management and board reporting • Develop or update Business Continuity Plans (BCP) for critical departments. • Develop or update IT Disaster Recovery Plans (DRP). • Business Continuity strategies for critical services • Update the Business Continuity Management Framework (BCM Framework). • Implement testing, exercises, and maintenance program (MOE). • Develop a Cybersecurity Risk Management Methodology and establish a Cyber Risk Register		• Required Reporting Forms for the Saudi Central Bank

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
	• Review and enhance the Cybersecurity Governance Framework. • Review and update Cybersecurity Policies and Procedures.		

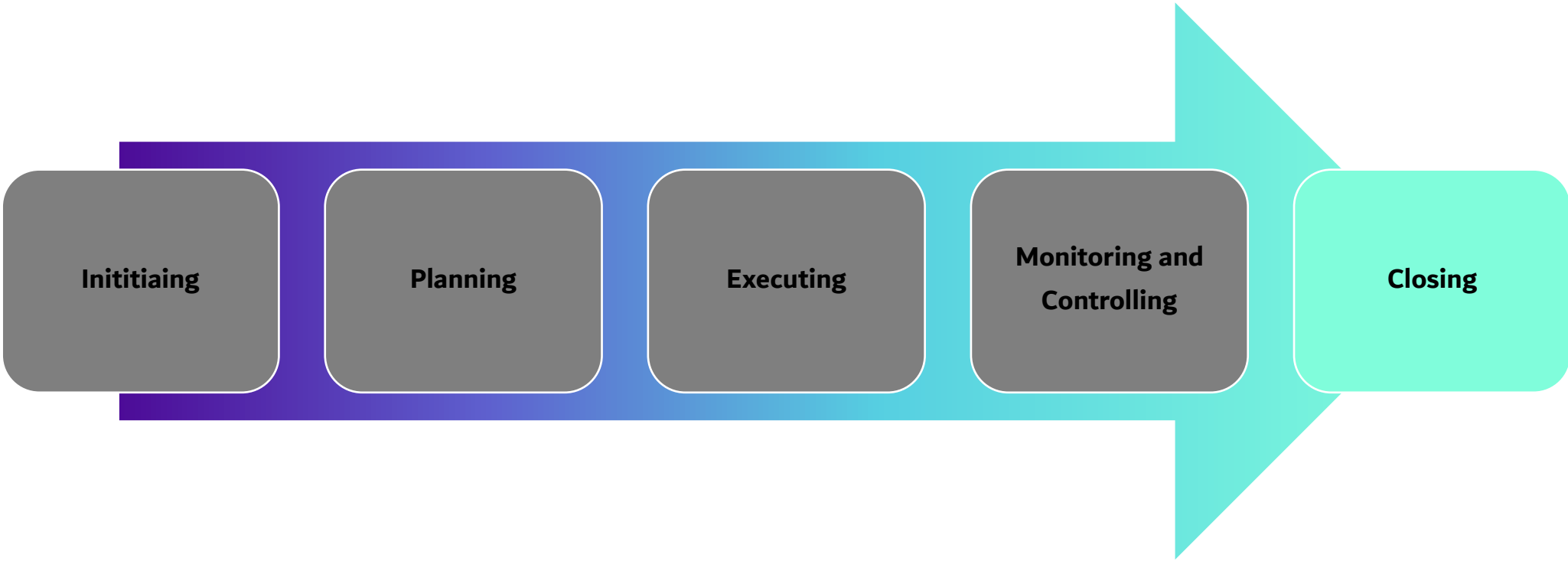
3.4 Monitoring and Control Phase



In this stage, the project works are monitored, performance and changes are monitored, and the project plan is amended according to the approved changes, if any, the most important outputs of this stage are business performance reports, changes, and updating the project plan. During which the following activities will be carried out.

Number	Activities to be done by a reliable vision company	Activities to be carried out by the Entity	Completed Activities and Materials Delivered to the Entity
1-	Supervise two exercises to measure the effectiveness of business continuity (over the duration of the project)	Exercise Coordination	Two exercises to measure the effectiveness of business continuity Note: The company has no relationship in case this office exercise is delayed for a time outside the duration of the project
2-	Send a weekly report on the progress of the project and the level of progress	View the weekly report and give feedback	Weekly report on the progress of the project and the level of progress
3-	Support certification readiness and continuous improvement and Conduct Internal audit of the Business Continuity System against ISO 22301	• Review and approve an internal audit report on the Business Continuity System • Working on the improvements and recommendations mentioned in the internal audit report on the business continuity system	Business Continuity System Internal Audit Report

3.5 Closing Phase



At this stage, all project outputs are verified, project objectives are achieved, lessons learned from the project are documented, final approval of project outputs is obtained, and the project closure is officially announced. During which the following activities will be carried out.

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
1-	Guiding and assisting the entity in implementing business continuity controls during the project period	Ensuring commitment and cooperation by all departments, especially the Information Technology Department, the Cyber Security Department, and the Digital Transformation Department in the entity.	Guiding and assisting the entity in implementing business continuity controls during the project period
2-	• Transfer of knowledge (as per the table in the next section) of everything related to the project documents and activities (will be periodically from the first day of the project) • Delivery of all documents and periodic processes	• Dedicate time and dedicate time to business continuity management • Receive all documents and periodic processes • Execute all works that will be received from the client	Transfer of knowledge of all things related to project documents

Number	Activities to be done by a reliable vision company	Activities to be carried out by the entity	Completed Activities and Materials Delivered to the Entity
3-	• Closure Model	• Signing the Project Termination Form	• Signed Project Termination Document • Project Closure Report • Lessons Learned Report

4. Knowledge Transfer

Knowledge transfer includes the transfer of knowledge from the consultant to the entity's employees and training in order to carry out the work that the consultants used to do and enable the Entity's employees to be able to carry out all the work of the consultants with confidence and capability.

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

What (Content)	When	From (Target Management)	How (Communication Channels)
Knowledge transfer to the cybersecurity team All documents and plans related to the project • Share and distribute documents and policies • Sharing information about new threats, attacks, and technologies • Dissemination of information through information exchange platforms • Apply best practices.	**Daily during all project cauldron**	• Lectures, Courses & Training Workshops • Threat Reports	• Video Meetings • In-person meetings

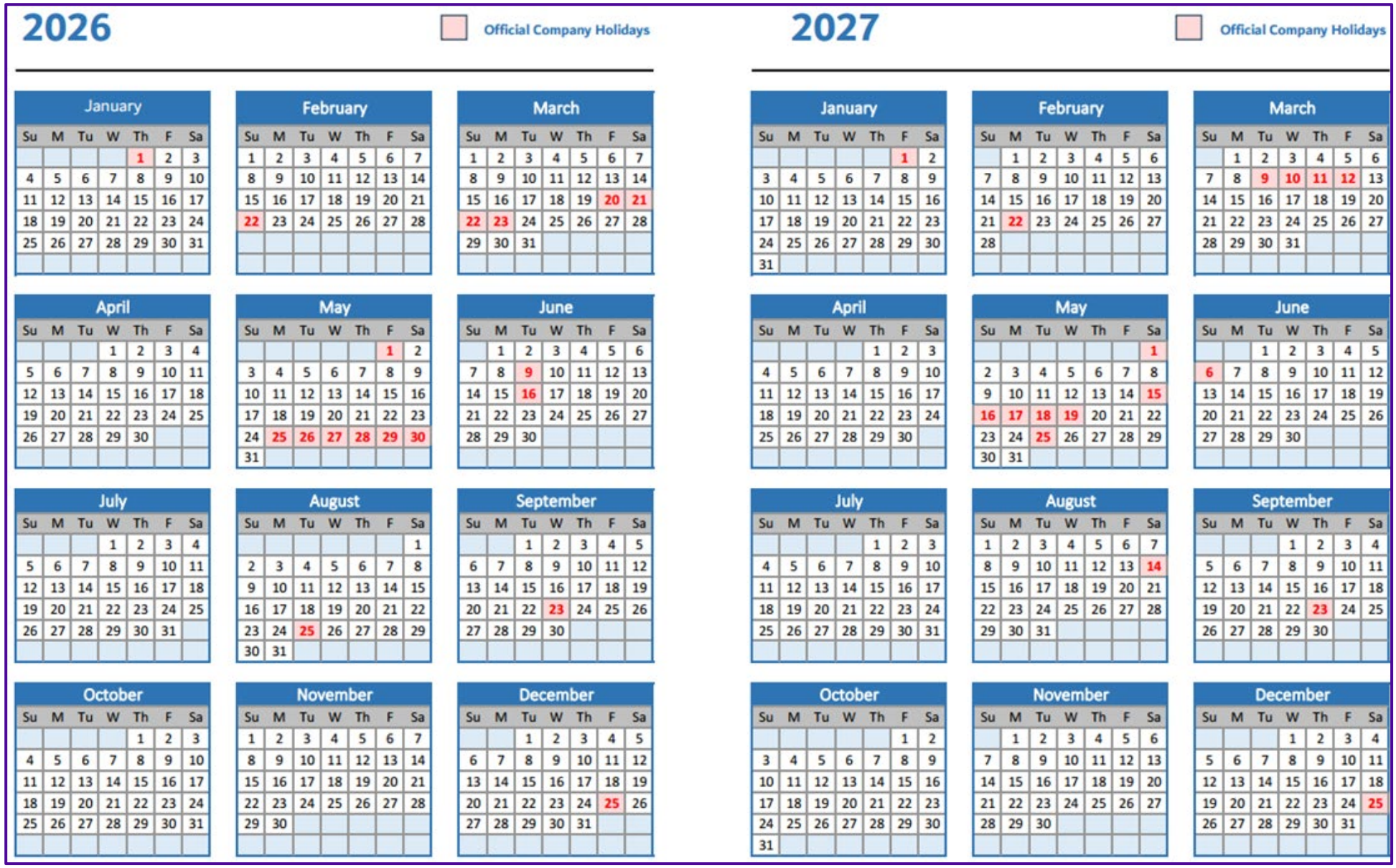
5. Weekly Project Workflow Report

The table below shows the progress of the project on a weekly basis to ensure that the objectives are achieved according to the planned timeline. The report is divided into four main themes:

1. Current Week's Achievements: Includes all activities and tasks completed during the week.
2. Next week's accomplishments: Identify tasks and activities planned to ensure continuity.
3. Challenges: Review obstacles that may affect the workflow, identifying areas that need to be addressed.
4. Recommendations: Provide suggestions to improve performance, reduce potential challenges, and ensure efficient operations.

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

6. Company Calendar



7. Resource Plans, Quality, and Communication

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

- In the resource plan, the available resources are listed, requirements and priorities are determined, and resources are distributed according to priorities.
- In a quality plan, quality standards are defined in order to be applied in the project, such as workflow methods, time required to review documents, and mechanisms for reviewing and approving documents.
- In the communication plan, the best ways to communicate according to the needs of the stakeholders are determined and the plan is written down and acted upon.

The mentioned plans are an important part of project management, and the aim is to determine how to prepare resources, manage quality, and communicate throughout the life of the project. It includes all stakeholder roles.

8. Project Duration

The total duration of the project is **7 months**, starting from the official project kickoff date.

The project timeline will be structured in alignment with the five standard phases of PMI as follows:

- **Initiation Phase:** Defining project objectives, stakeholders, and formal project approval
- **Planning Phase:** Developing detailed project plans including scope, schedule, resources, and risk management
- **Execution Phase:** Implementation, system development, integration, and delivery of project activities
- **Monitoring & Controlling Phase:** Continuous tracking of progress, performance, risks, and change management throughout the project lifecycle
- **Closing Phase:** Final delivery, client acceptance, documentation, and formal project closure

A detailed project schedule, including milestones, deliverables, and phase distribution across the 7-month timeline, will be provided upon project initiation.

		1	2	3	4	5	6	7
1	Business Continuity Management System (BCMS) in alignment with ISO 22301							
2	SAMA CSF requirements							

9. High-level risk

The most important high-level risks in the project are identified as in the table below

Number	Risk scenario	Overall Level	Controls for Dealing with Risk
1	The lack of cooperation of the employees of the entity and consequently the delay in the entertainment is dead	high	1- Allocating a project manager from the entity and discharging him to work with consultants 2- Giving a letter and an order from the entity holder to all departments to cooperate with consultants to ensure the completion of the project within the specified time
2	The entity's dissatisfaction with the submitted documents	Medium	Developing and activating a quality plan between the company and the entity
3	Resignation of a consultant during the work of the project	Low	1- Provision of other consultants for reserve by the company

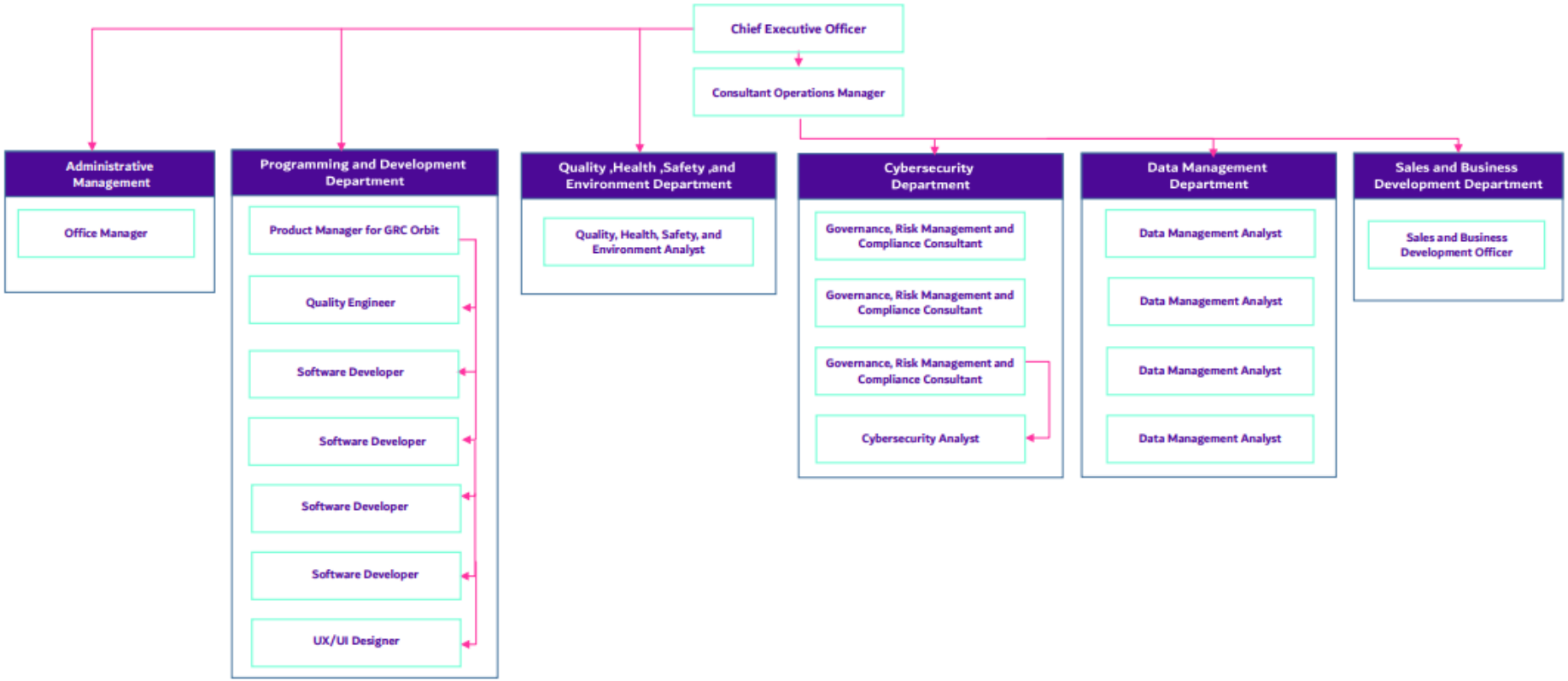
10. Project Management

During the project period (six months), the consultants will submit basic project management documents, which include:

- Schedules and minutes of meetings
- Project Status Reports

11. Company Information

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



12. Certifications

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


PECB
ISO 9001
LEAD AUDITOR


ITIL
FOUNDATION


CompTIA
CCAP
Cloud Admin
PROFESSIONAL


CompTIA
CSCP
Secure Cloud
PROFESSIONAL


CompTIA
Data+


CompTIA
Cloud+


CompTIA
CySA+


CompTIA
Network+


CompTIA
A+


CompTIA
Security+


CNSS


FORTINET
NSE
1
ASSOCIATE


FORTINET
NSE
2
ASSOCIATE


FORTINET
NSE
3
ASSOCIATE


FORTINET
NSE
4
PROFESSIONAL


C|EH
Certified Ethical Hacker


paloalto
NETWORKS
PCCSA


paloalto
NETWORKS
PCNSA

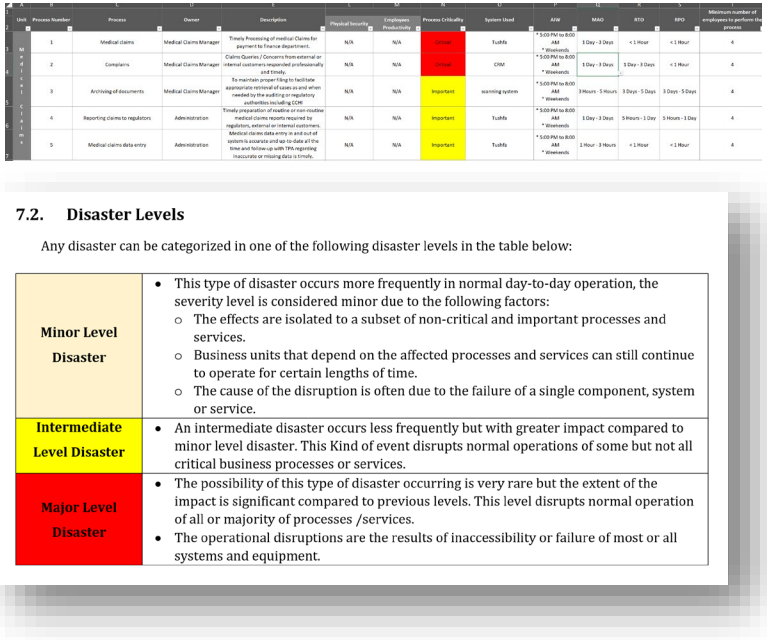

paloalto
NETWORKS
PCNSE


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA
CYBER+INFRASTRUCTURE


ASSOCIATE
CERTIFIED

13. Previous Projects Implemented

Many projects have been implemented by dealing with various entities in different countries and multiple environments and we always seek to implement the best practices and standards in order to achieve the best results required

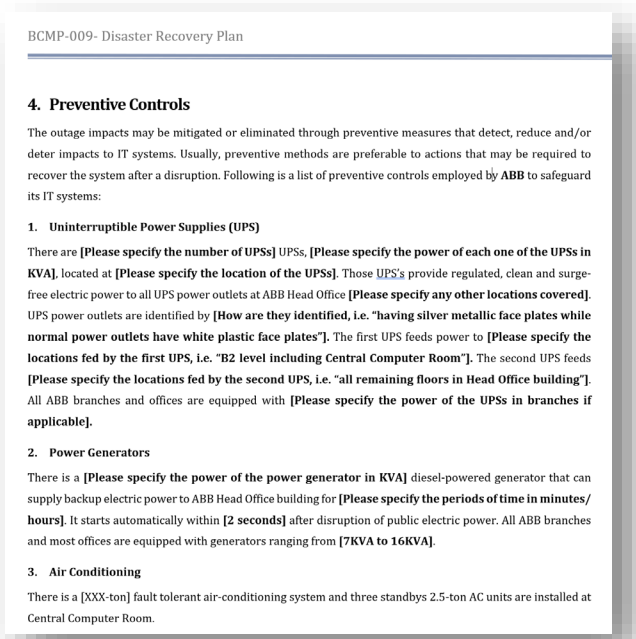
Project Number	Project Name	Name of the customer or beneficiaries	Picture of the project	Project Description
1	Business Continuity Project	**Entity in the Oil and Gas Sector**		• Establishing a Business Continuity Management System • Developing relevant policies, procedures and standards • Define and implement a business impact analysis • Conduct a Business Continuity Risk Assessment • Define the Restore Time Objective (RTO) and Restore Point Objective (RPO) • Developing a Business Continuity Strategy • Developing Business Continuity Plans

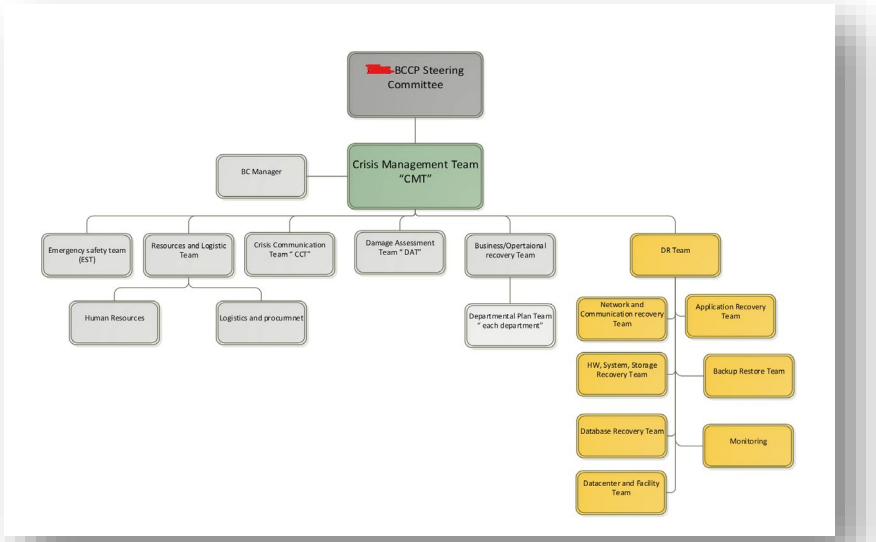
7.2. Disaster Levels

Any disaster can be categorized in one of the following disaster levels in the table below:

Minor Level Disaster	• This type of disaster occurs more frequently in normal day-to-day operation, the severity level is considered minor due to the following factors: ○ The effects are isolated to a subset of non-critical and important processes and services. ○ Business units that depend on the affected processes and services can still continue to operate for certain lengths of time. ○ The cause of the disruption is often due to the failure of a single component, system or service.
Intermediate Level Disaster	• An intermediate disaster occurs less frequently but with greater impact compared to minor level disaster. This Kind of event disrupts normal operations of some but not all critical business processes or services.
Major Level Disaster	• The possibility of this type of disaster occurring is very rare but the extent of the impact is significant compared to previous levels. This level disrupts normal operation of all or majority of processes /services. • The operational disruptions are the results of inaccessibility or failure of most or all systems and equipment.

				• Define performance metrics and KPIs •

2	**Company in the Insurance Sector**			• Gap Analysis • Studying the Status Quo • Impact analysis and business continuity risk assessment • Developing a Business Continuity Strategy • Business Continuity Policy Development • Developing a Business Continuity Framework and Supporting Documents


BCCP Steering Committee
BC Manager
Crisis Management Team "CMT"
Emergency safety team (EST)
Resources and Logistic Team
Crisis Communication Team " CCT"
Damage Assessment Team " DAT"
Business/Opertaional recovery Team
DR Team
Human Resources
Logistics and procumnet
Departmental Plan Team " each departmere"
Network and Communication recovery Team
Application Recovery Team
HW, System, Storage Recovery Team
Backup Restore Team
Database Recovery Team
Monitoring
Datacenter and Facility Team

14. Staff

Number	Name	Job position	Academic Level	Years of Experience	Expertise
1	B. A	Business Regulation, Governance and Risk Management (GRC) Advisor to the CEO	Master of Computer Engineering	25 years	• SAMA csf maturity level 3 - Finzey company • SCADA Implementation – GASCO • Supervised the implementation of SCADA systems, ensuring secure and efficient control infrastructure for natural gas operations. • Optical Fiber Projects – GASCO • Led the execution of optical fiber infrastructure for enhanced communication reliability across GASCO's operational zones. • Smart City Design Review – Libya • Reviewed and validated smart city design proposals to ensure alignment with modern telecom and security standards. • ISO 27001 Implementation – Smicolon • Contributed to the implementation of ISO 27001 framework for information security management in a European tech company. • LAN/WAN Network Implementation – GASCO • Managed the deployment of LAN/WAN networks, ensuring robust connectivity and communication across GASCO's facilities in Suez.

2	A. A	Governance & Risk Management Consultant (GRC)	Bachelor of Computer Engineering	2 Years	• ISO 27001 Compliance Policy Development (Genelle) Contribution to the preparation and development of information security policies and procedures for Genelle to achieve compliance with the ISO/IEC 27001 standard. This included identifying required security controls, documenting operational and procedural policies, and ensuring the alignment of the technical environment with the standard's requirements, supporting data protection and enhancing the company's readiness for certification. • NCA-DCC Implementer and Auditor (EXPRO) • NCA-DCC Auditor (HRSD) • CRF Auditor (Emdad Digital)

15. Vendor Cybersecurity Obligations – Compliance Table

#	Requirement	Compliance Status
1	The Vendor shall comply with all applicable cybersecurity regulations and directives issued by relevant authorities	FULLY COMPLIANT
2	The Vendor shall support cybersecurity audits, due diligence, and risk assessments conducted by the Client	FULLY COMPLIANT
3	The Vendor shall implement data protection controls including encryption and data segregation	FULLY COMPLIANT
4	The Vendor shall implement network and system security controls including firewalls and intrusion protection	FULLY COMPLIANT
5	The Vendor shall ensure continuous logging and monitoring of systems and security events	FULLY COMPLIANT
6	The Vendor shall ensure that no data is stored outside the Kingdom of Saudi Arabia	FULLY COMPLIANT
7	The Vendor shall ensure all integrated systems are free from vulnerabilities	FULLY COMPLIANT

#	Requirement	Compliance Status
8	The Vendor shall implement cybersecurity policies and procedures aligned with regulatory requirements	FULLY COMPLIANT
9	The Vendor shall notify the Client at least 30 days prior to any major system changes	FULLY COMPLIANT
10	The Vendor shall immediately notify the Client in case of any cybersecurity incident	FULLY COMPLIANT
11	The Vendor shall remove all access rights upon completion of services or contract termination	FULLY COMPLIANT
12	The Vendor shall ensure protection and privacy of data at all times	FULLY COMPLIANT
13	Any changes in policies must not reduce the level of data protection agreed with the Client	FULLY COMPLIANT