Technical Proposal for Supporting Compliance with New NCA DCC & CSCC Requirements and Validating ECC & MSOC Controls

Version 1.0

Date: 20-FEB-2026 AD

Prepared by: Trusted Vision for Cybersecurity

Contact Information

Please feel free to contact the following individuals for information about this document:

Name	Hashem Al-Azizi
Mobile Phone	+966-53-122-1580
Email	Hashem.azizi@trustedvision.biz
Address	Cordoba District, Saeed Bin Zaid Street, Injaz Group Building, No. 6482, First Floor, P.O. Box: 13247, Riyadh, Kingdom of Saudi Arabia

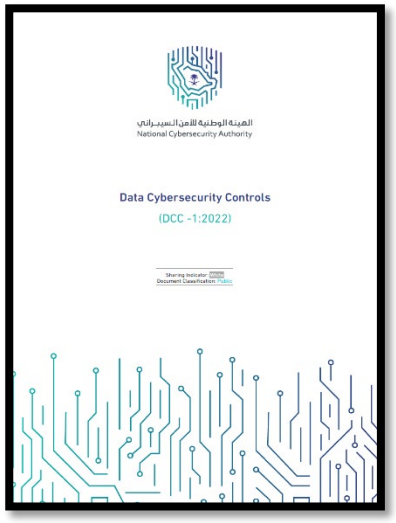
Contents

1. Executive summary of client requirements

TRUSTEDVISION will support the organization in addressing the newly introduced requirements of the National Cybersecurity Authority (NCA) related to the Data Cybersecurity Controls (DCC) and Cloud Cybersecurity Controls (CSCC). The scope of work includes conducting a comprehensive review and validation of the existing security controls and practices where compliance with the Essential Cybersecurity Controls (ECC) and Managed Security Operations Center (MSOC) requirements has already been achieved, ensuring continued alignment and identifying any gaps that require remediation or enhancement.

This structured approach will enable effective planning of the next steps and support the organization in achieving and sustaining full compliance with all applicable NCA frameworks and regulatory requirements

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority



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

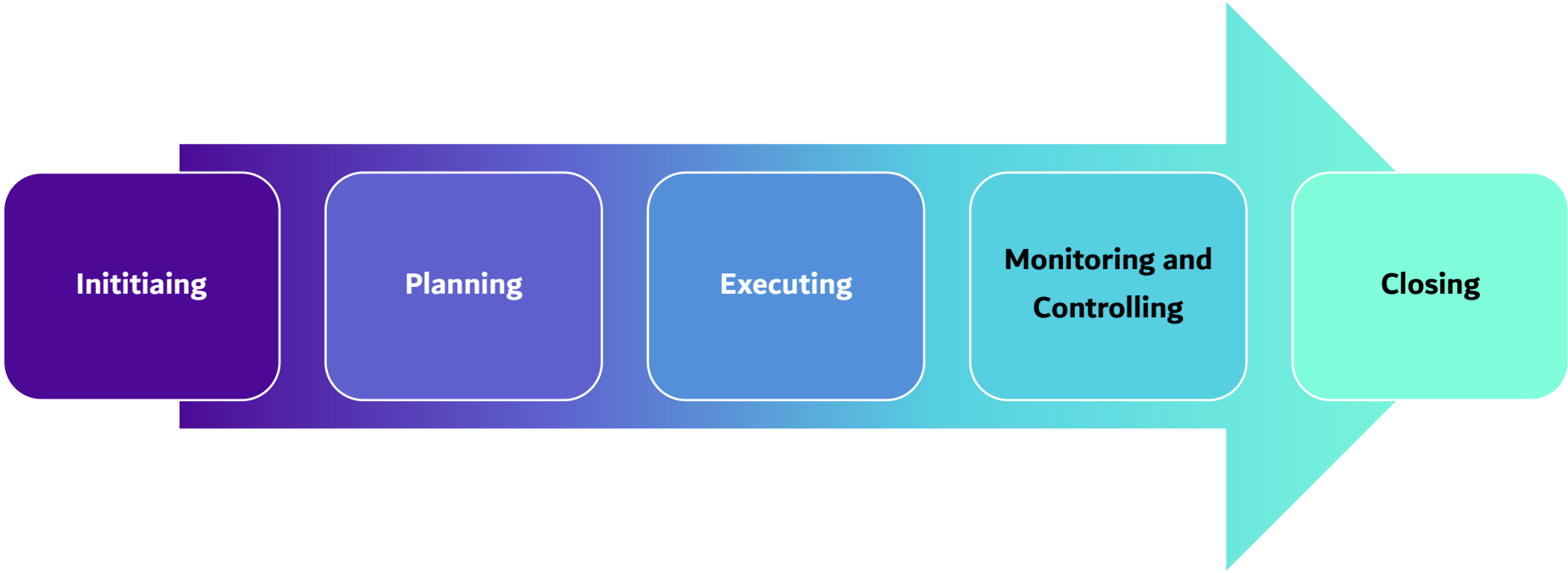
1. Balanced blend of international and local expertise in cybersecurity.
2. Efficient project execution approach, ensuring timely, professional, and high-quality outcomes.
3. Comprehensive knowledge and vast experience in designing and implementing solutions aligned with international standards and best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

2. Project Benefits and Values

By implementing this project, the organization is expected to realize the following benefits and added value:

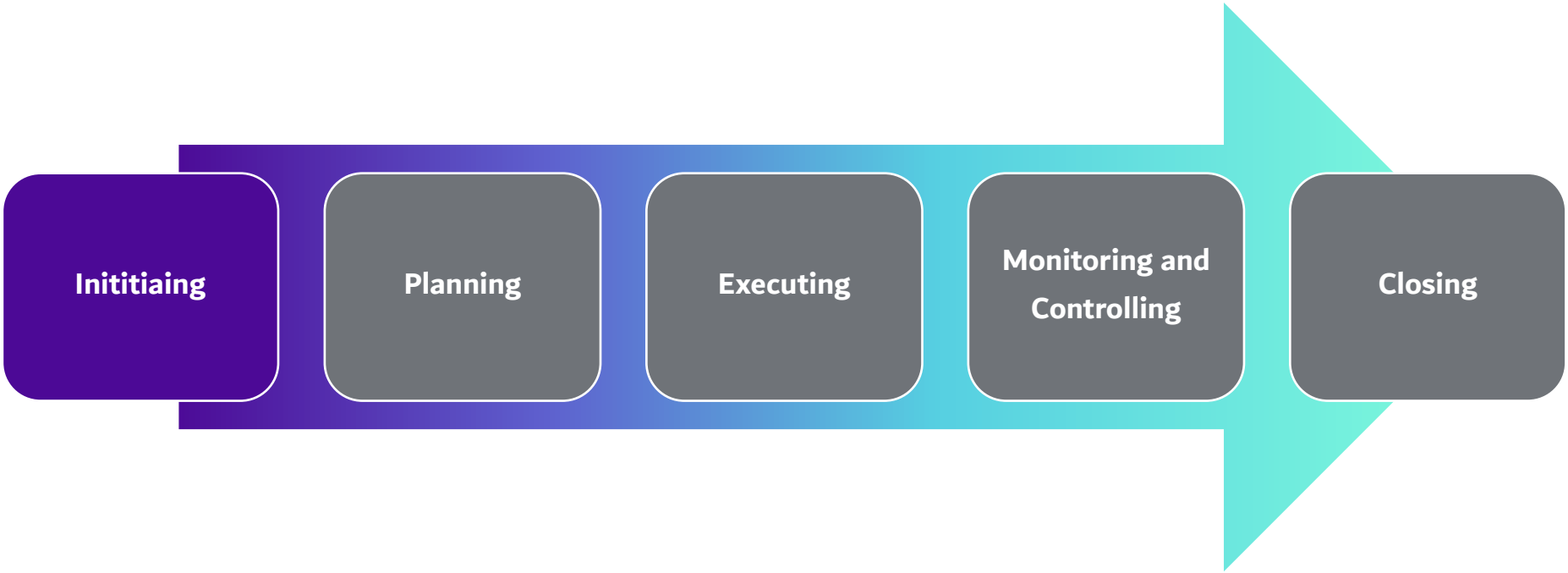
1. Strengthen and elevate compliance with the National Cybersecurity Authority (NCA) controls and applicable regulatory frameworks.
2. Enhance the overall cybersecurity posture and maturity level across the organization.
3. Increase competitive advantage by ensuring the confidentiality, integrity, availability, and value of data to effectively support strategic and operational decision-making.
4. Achieve greater efficiency and operational effectiveness through alignment with recognized international standards and best practices.
5. Reduce cybersecurity risks and minimize potential financial and reputational losses resulting from data breaches and security incidents.
6. Promote transparency, governance, and accountability in cybersecurity management and oversight

3. Project management and implementation methodology



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

3.1 Initiating Phase



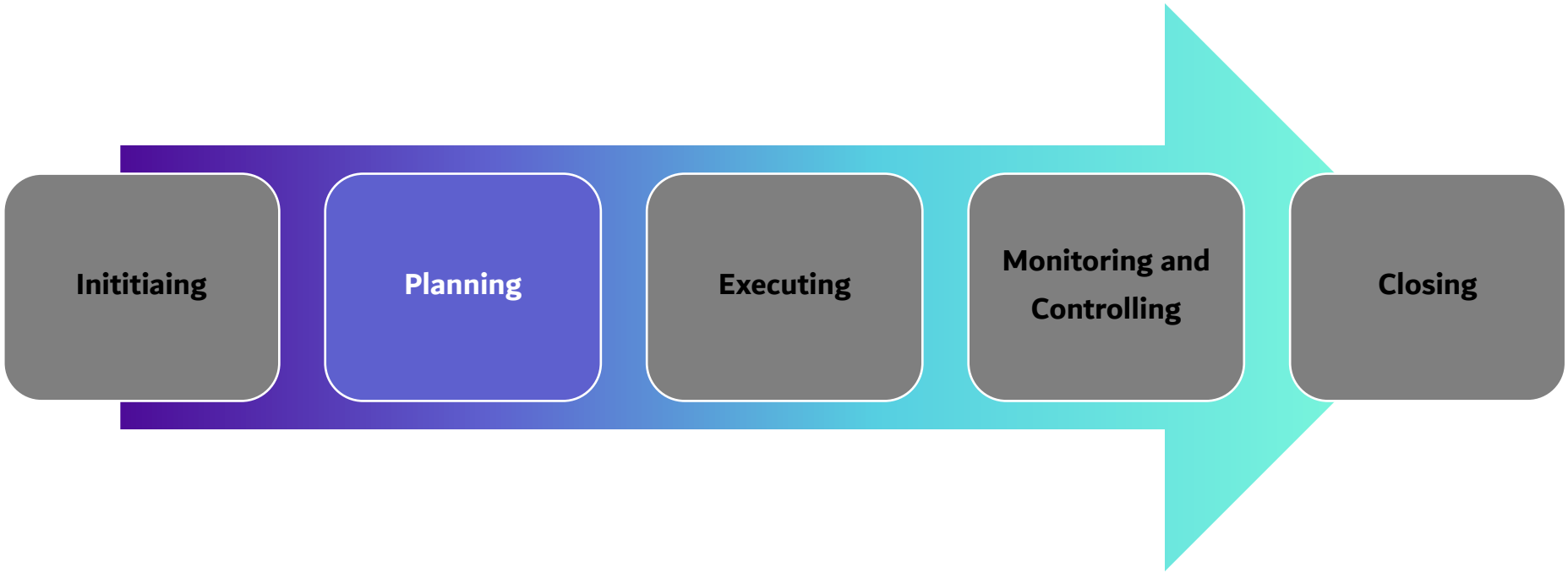
At this phase, the project is defined, and the project leader outlines their responsibilities, identifies key stakeholders, and conducts a current status assessment. This assessment aims to develop a comprehensive understanding of the entity's cybersecurity system, its compliance posture, and the associated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

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Preparing the project team	Assigning a project manager from the entity to work with the consultants	A team prepared to start the project

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
2.	Preparing to start the project and holding the kickoff meeting	Inviting the head of the entity and all department heads	Meeting minutes
3.	Develop Project Charter	Review and approve the project charter	Project Charter

3.2 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 cybersecurity framework, collecting all relevant documents available within the entity, evaluating its compliance posture, and identifying associated cyber risks.

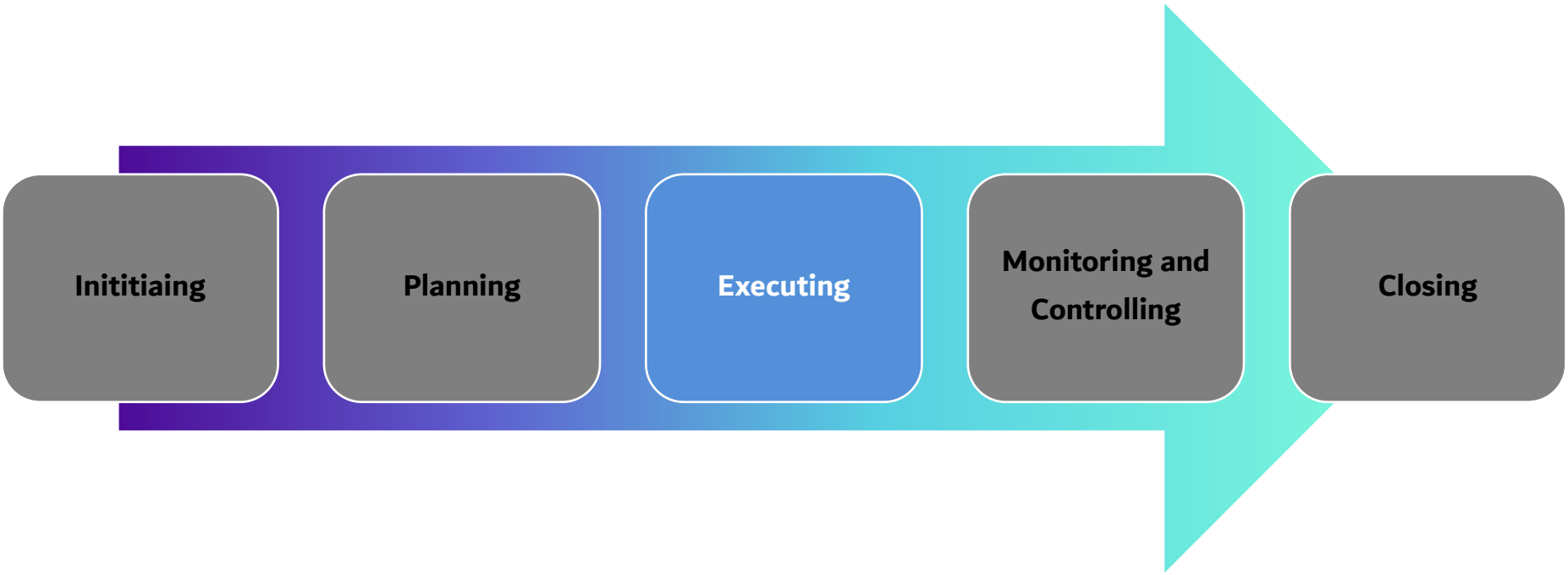
The table below contains the activities that will be carried out at this phase:

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Collect evidence and information related to cybersecurity requirements, including current cybersecurity governance documents: 1. Policies 2. Procedures 3. Cybersecurity Strategy, Digital Transformation, Data Management and IT 4. Frameworks 5. Technical Standards 6. Information and Technology Asset Registe	Submitting the required documents	Meeting minutes
2.	Conducting interviews with departments and stakeholders, including but not limited to: 1. General Department of Cybersecurity 2. General Department of Information Technology 3. General Department of Digital Transformation 4. Facilities Department 5. Administrative Affairs Department	• Coordinate interview appointments • Submit required documents	Meeting minutes
3.	Develop a project implementation plan	• Review and approve the project implementation plan	Project implementation plan

#	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
		• Allocate resources and budgets to complete the project	
4.	Study and assessment the current status of cybersecurity including the nature of the company's work, operations and activities of the departments and administrations.	Review and approve	Gap assessment report
5.	• Develop asset inventory • Identify national-level sensitive systems using the Sensitive Systems Identification Tool issued by the National Cybersecurity Authority (NCA), and periodically review the system sensitivity assessment. • Inventory all sensitive systems and their technical components, and review them at least annually or whenever significant changes occur. • Identify and maintain an inventory of privileged accounts with critical or sensitive access, including those capable of accessing or administering sensitive systems, and review them periodically	Review and approve	• Asset inventory • National Sensitive Systems Identification Report • Sensitive Systems Inventory Register • Privileged Accounts Register

#	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.	Develop comprehensive cybersecurity solutions matrix	Start purchasing cybersecurity tools and solutions	Cybersecurity solutions matrix

3.3 Executing Phase



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

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Develop / review (if exist) an integrated operational model for CLIENT's cybersecurity governance and operation, including the following:	Review and approval of documents	• Cybersecurity Operational Model Document

#	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. Analyzing and understanding CLIENT's internal and external context. 2. Understanding and analyzing the business operating model between CLIENT and external stakeholders and ensuring the cybersecurity governance model is aligned with it. 3. Understanding the details of CLIENT's existing or planned infrastructure, and taking this into account when building the cybersecurity governance model. 4. Determining the number, structure, responsibilities, and members of CLIENT's cybersecurity governance committees. 5. Developing templates for documenting committee meetings. 6. Develop a model to describe CLIENT's cybersecurity capabilities, in compliance with all relevant legislation. 7. Develop job descriptions for all positions within CLIENT's cybersecurity departments and divisions. 8. Develop RACI matrices for CLIENT's cybersecurity capabilities, services, and operations.		• Templates Document for Documenting Committee Meetings • Roles and Responsibilities Document for Cybersecurity at CLIENT, in accordance with relevant legislation, as well as the nature and context of CLIENT • Job Descriptions Document for all positions within the Cybersecurity Departments and Sections at CLIENT

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
2.	Develop / review (if exist) documents related to the cybersecurity system (policies, standards, procedures, and measurement indicators), including but not limited to: 1. Cybersecurity Oversight Committee Charter. 2. Acceptable Use. 3. Malware Protection. 4. Third-party Security Management. 5. Cybersecurity Logs and Incident Management and Monitoring. 6. Physical Security. 7. Cybersecurity Business Continuity. 8. Information Asset Management. 9. Data Classification and Protection. 10. Mobile and Personal Device Security Management. 11. Network and Communications Security. 12. Secure Development of Applications and Systems. 13. Identity Management and Access Control. 14. Encryption and Key Management. 15. Backup Management. 16. Cybersecurity Risk Management methodology based on developments in systems and	Review and approval of documents	Documents related to the cybersecurity system

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
	technologies, as well as relevant legislative and regulatory requirements. 17. Developing cybersecurity risk management log procedures 18. Technical Vulnerability Management Standards. 19. Cybersecurity Compliance Management Standards. 20. Developing and Improving Periodic Review and Audit Procedures 21. Cybersecurity Threat Management Standards. 22. A detailed program and plan for internal auditing (for at least one year). 23. Baselines Configuration standards for technical assets 24. Roadmap for other controls 25. Analysis and assessment of cybersecurity risks 26. Identify, assess, measure, and plan cyber risk remediation and reporting 27. Review and development of key elements of the operating model 28. Develop and build organizational structure and operational model strategies		

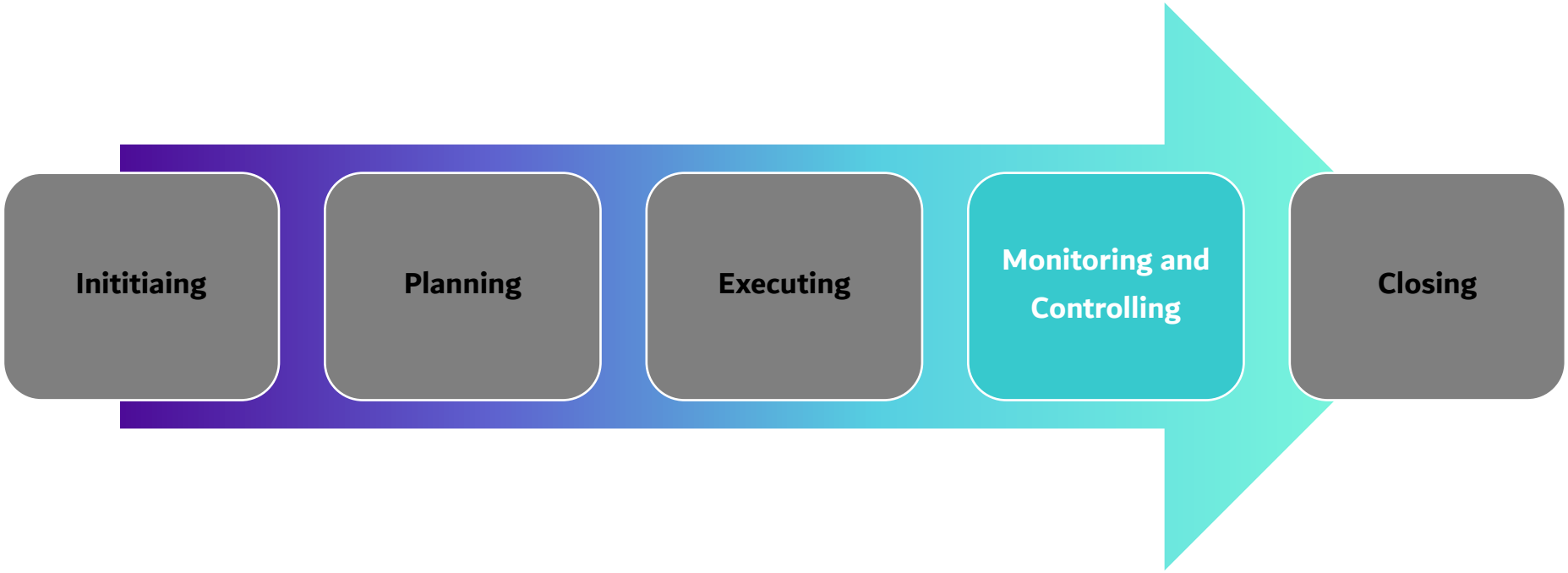
#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
	29. Identifying, Developing, and Reviewing Cybersecurity Roles and Responsibilities 30. Identify relevant regulation and standard and develop a plan to comply with it. 31. Build, develop and improve all baseline standards for technical systems.		
3.	Developing / review (if exist) an integrated cybersecurity strategy at CLIENT level, including the following: 1. Analyzing, understanding, and documenting CLIENT's internal and external context 2. Cybersecurity strategies in particular, such as SWOT, PESTEL, 3. Develop a unified cybersecurity controls framework for CLIENT, including at least NCA standards (DCC, CSCC, ECC), in addition to MSOC controls 4. Develop the integration of the cybersecurity strategy with CLIENT's business strategies 5. Develop a roadmap that includes all initiatives necessary to achieve the strategy's development objectives. Initiatives will be prioritized, and a detailed scorecard will be provided for each initiative.	Review and approval of documents	• CLIENT Cybersecurity Controls Framework. • An action plan document for implementing cybersecurity requirements, including how to implement NCA controls and CLIENT Cybersecurity Policies (how and to what extent to use external providers, and preferred activities to be performed internally) for all key cybersecurity organizational units, and work to implement the plan to achieve increased compliance with NCA controls. • CLIENT Cybersecurity Risk Register.

#	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. Developing KPI dashboards for cybersecurity governance 7. Reviewing cybersecurity requirements for company projects		• CLIENT Cybersecurity Strategy • Developing KPI dashboards for cybersecurity governance • Knowledge Transfer Workshops for all relevant CLIENT teams.

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

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

3.4 Monitoring and Controlling phase



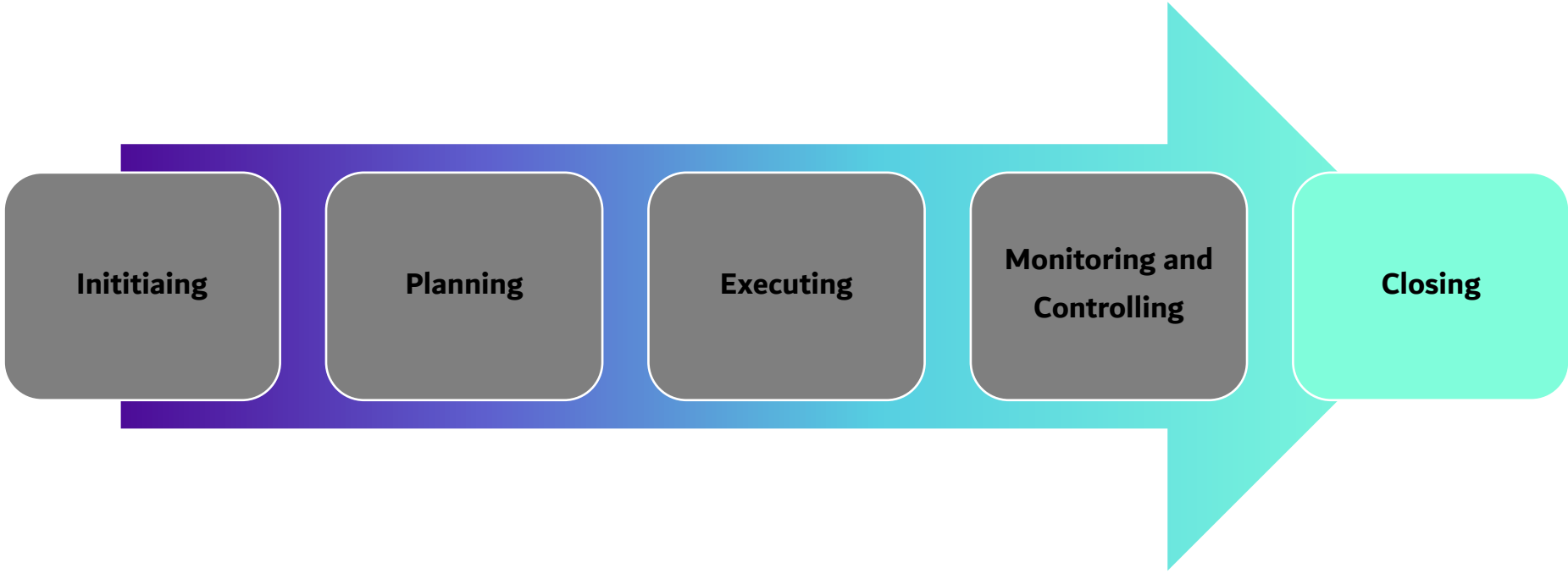
At this phase, project work is monitored, performance and changes are tracked, and all project deliverables are verified. The project objectives are achieved, and final approval of the deliverables is obtained.

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1.	Develop and review (if exist) compliance matrix to ensure alignment of all cybersecurity controls in the regulations with the cybersecurity controls in the existing policies.	Review and approve compliance matrix	Compliance matrix

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
2.	Deliver specialized awareness lectures to raise awareness of cybersecurity in CLIENT	Coordinate meeting with stakeholders	Awareness workshop materials
3.	Awareness workshops on cybersecurity risks and document and data security will be held during the project	Coordinate meeting with stakeholders	Awareness workshop materials
4.	Providing recommendations, support, and follow-up on the implementation of technical security controls		
5.	Regularly follow up on cybersecurity management projects and programs	-	Meeting minutes
6.	Regularly monitoring the implementation of the cybersecurity strategy throughout the project		
7.	Provide a Bi-Weekly email on the progress	-	Project progress
8.	Coordinate for the management review	-	Meeting minutes
9.	Conduct internal audit for (DCC, ECC, CSCC and MSOC)	Collaboration with the internal auditor	Internal audit report
10.	Receive all project documents.	Approve all the documents	Receive all project data

3.5 Closing phase



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

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

#	Activities that must be conducted by the trusted vision company	Activities that must be conducted by the entity	Activities completed and materials delivered to the entity
1	Project sign-off	Sign off by the company's management	Project closure report

4. Knowledge Transfer

Knowledge transfer includes transferring knowledge from the consultant to the entity's employees and training with the aim of carrying out the work that the consultants were doing and enabling the Authority's employees to be able to carry out all the consultants' work with confidence and competence. Knowledge will be transferred to the entity's employees through the following schedule:

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

5. Weekly Project Progress Report

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

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

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

6. Resource, Quality and Communication Plans

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

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

The 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.

7. Risk Register

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

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

8. Approximate project implementation timeline

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

Phase		Weeks							
		1	2	3	4	5	6	7	8
1	Reviewing and validating the existing controls with ECC and MSOC requirements								
2	Implementation of DCC and CSCC								

9. Project Scope and Assumptions

Out of Scope of Work

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

Assumptions

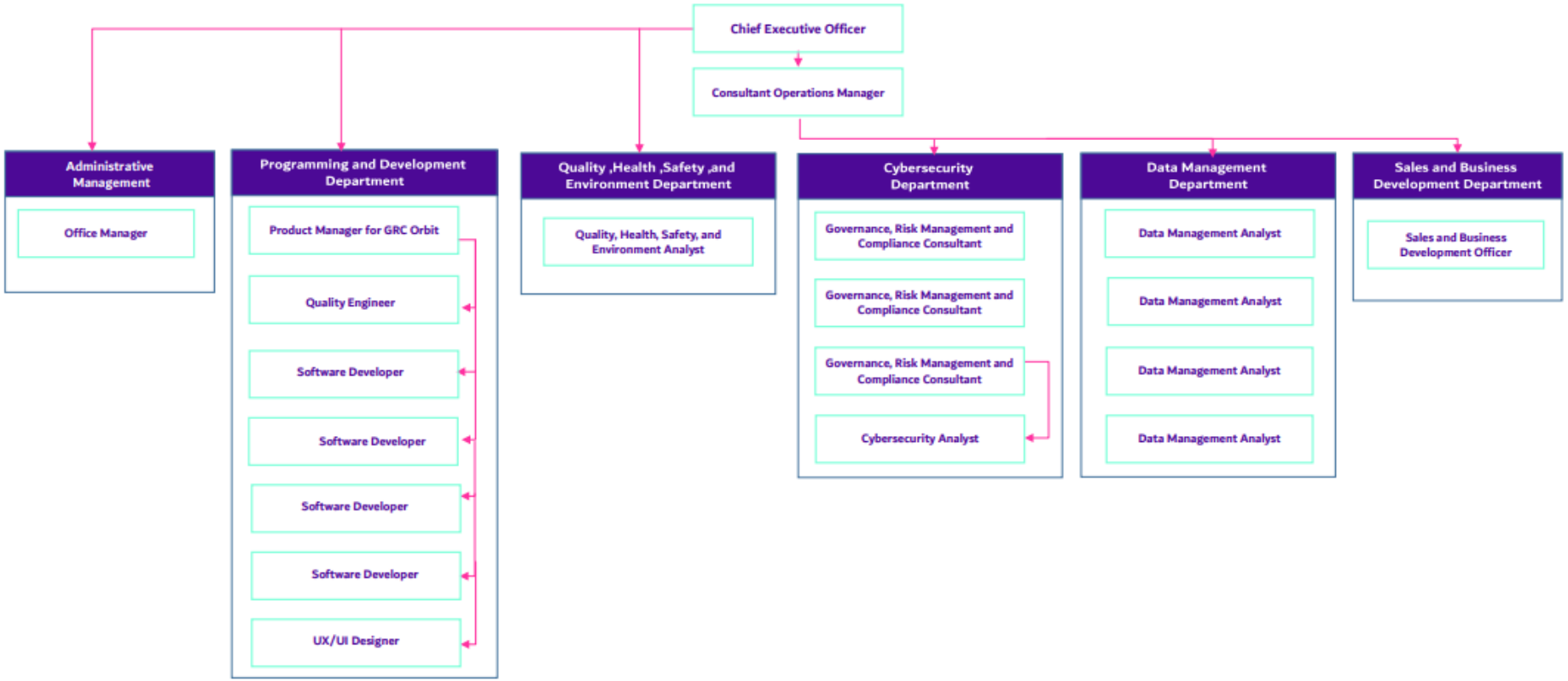
1. **All activities will take place during the project period only and the company has no relationship if there is any delay or lack of cooperation from the entity.**

2. **The company is not responsible for any delay caused by the entity.**
3. **Cooperation from the entity's departments and departments is mandatory for the success of the project.**
4. **The proposal includes only one review of the submitted documents.**
5. **Delivered documents will be reviewed for 3 days only.**
6. **Mode of Operation will be Hybrid (Online/Onsite)**
7. **An AI bot will be integrated to record and summarize conversations, aiming to assist consultants in improving and enhancing meeting minutes.**

8. **The company has the right to temporarily suspend the project if the payment is not made within two weeks from the date of issuing and sending the invoice to the entity.**

10. Company Information

Trusted Vision is a cybersecurity and data management consulting firm that provides full services in governance, risk, and compliance management, as well as solutions and training, to help entities meet their business requirements.



11. 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

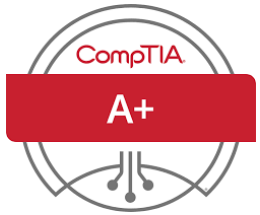

CompTIA
CSCP
Secure Cloud
PROFESSIONAL


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

12. 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)		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 مهام	1. Implement Aramco Cybersecurity Standard SACS-002 2. Develop relevant policies, procedures, and standards
11	Data Classification	Perfect Presentation	2P 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 SAMA CSF	Finzey		1. Conduct a comprehensive cybersecurity gap assessment. 2. Develop policies, procedures, and standards in alignment with the Saudi Central Bank (SAMA) Cybersecurity Framework. 3. Perform cybersecurity risk assessments for all information assets. 4. Establish and check cybersecurity performance indicators (KPIs.

				5. Development of a comprehensive Disaster Recovery (DR) Plan and Incident Response (IR) Plan

13. Staff

#	Name	Job Title	Education Level	Years of Experience	Experience
1	S.H	Governance and Risk Management (GRC)	Bachelor of Computer Engineering	6 Years	1. Manage and conduct operational and operational reviews in compliance with Saudi Arabian Oil Company (SAS 002), ISO 27001, NCA-ECC and NIST SP 800-53 cybersecurity requirements. 2. Manage and develop customized cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA and Saudi Arabian Oil Company Cybersecurity Standard. 3. Manage cybersecurity risks and conduct cybersecurity risk assessments and IT risk assessments by national and international standards.

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

					3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the organization's Information Security Management System based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.
3	G.H	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	3 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53.

					2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Manage cybersecurity risks and conduct cyber risk assessments and technology risk assessments against national and international standards. 4. Implement and audit the company's cybersecurity management system based on ISO 27001 and National Cybersecurity Authority (NCA-KSA). 5. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.

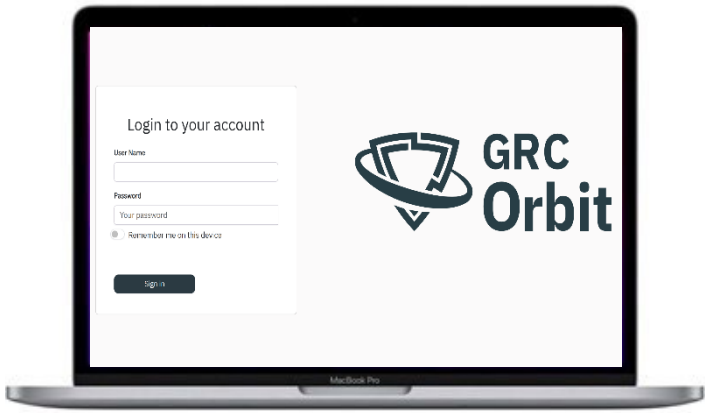
4	A. Y	Governance and Risk Management (GRC) Consultant	Master of Cybersecurity	2 Years	1. Manage and conduct operational and process reviews by Saudi Aramco Cybersecurity requirements (SACS-002) ISO 27001, NCA-ECC, and NIST SP 800-53. 2. Manage and develop cybersecurity governance policies and procedures in Arabic and English by ISO 27001, NIST, NCA, and Saudi Aramco Cybersecurity Standards. 3. Implement personal data protection law and regulations and conduct privacy risk assessments related to personal data.
5	I.A	Governance and Risk Management (GRC) Consultant	Bachelor of Software Engineering	15 Years	1. Design, implement, and oversee data governance frameworks, ensuring adherence to regulations such as SDAIA guidelines, and GDPR. 2. Develop data management strategies, policies, and initiatives aligned with organizational aims and best international practices.

					3. Establish and enforce data quality standards to enhance accuracy, integrity, and reliability. 4. Evaluate existing data processes and recommend enhancements to improve workflow efficiency. 5. Create dashboards and generate reports to support data-driven decision-making. 6. Collaboration and Coordination: Partner with IT, operations, and business units to align data strategies with organizational goals.
8	B. B	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Information Systems	1 Year	1. Finding and selecting datasets for publication as open data, ensuring compliance with regulatory and strategic aims. 2. Conducting assessments of data management maturity to find gaps and recommend improvements. 3. Developing Business Intelligence (BI) use cases and enhance user experience through data-driven insights.

					4. Designing and implementing plans, policies, and procedures for Master and Reference Data Management, Freedom of Information, Document and Content Management, and Data Value Realization in alignment with NDMO regulations.
9	B. A	Governance and Risk Management (GRC) Consultant	Bachelor of Computer Engineering	25 Years	1. Overseeing the design of information and communications systems 2. Overseeing the implementation of ISO 27001 certification 3. Overseeing the implementation of communications and data transmission projects 4. Overseeing the implementation of three fiber optic projects to ensure data transmission system security.

					5. Overseeing the implementation of LAN and WAN networks and ensuring data transmission system security. 6. Overseeing the implementation of the SCADA network

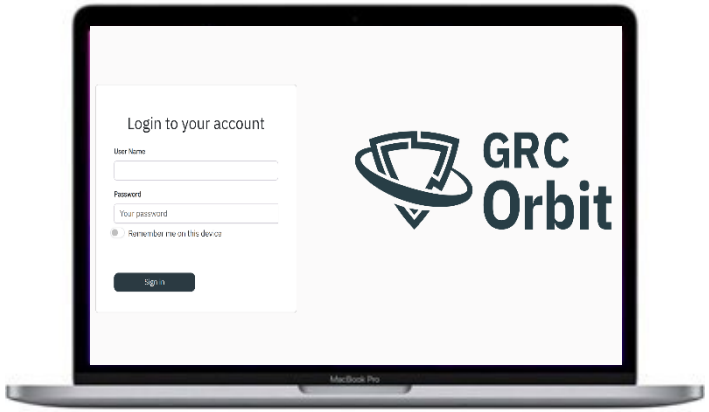
Technical Proposal for GRC Orbit System



ANNEX 1

Technical Proposal for

GRC Orbit System



ANNEX 1

Content

Table of Figures

Introduction

Trusted Vision Company is pleased to present its technical offer for the Governance, Risk Management and Compliance System “GRC Orbit”. This system has been designed to meet the needs of the Saudi market in particular and enable employees in the organization’s departments and divisions (especially the Cybersecurity Department) to monitor, manage, operate and audit governance, risk management and cybersecurity compliance operations and activities to ensure compliance with legislative, contractual and internal requirements and to ensure the effectiveness and automation of operations.

The GRC Orbit system can be used by all members of the organization and from various departments, and the focus is currently on the Cybersecurity Department, given that there are regulatory and legislative requirements that stipulate the creation of a department concerned with governance, risk management and cybersecurity compliance.

GRC Orbit system Objectives

Through the development of the GRC Orbit system, we aim to improve processes related to governance, risk management, and compliance by:

- Automating governance, risk management, and compliance processes.
- Eliminating the complex work files that burden cybersecurity employees by consolidating everything related to governance, risk management, and compliance (external standards and frameworks, policies, procedures, risks, auditing, compliance rates, follow-ups, performance indicators, task management) into the GRC Orbit system.
- Transferring the expertise of consultants in the field of governance, risk management, and compliance into the GRC Orbit system.
- Providing content related to cybersecurity, such as local and international standards, legislation, and information security risk elements.
- Eliminating Microsoft Excel files and follow-up emails with other departments.

3 GRC Orbit System Benefits

The following are the most important benefits and advantages obtained when acquiring this system:

- Managing all organizational risks (including cybersecurity risks and risks from other departments) according to the risk management methodology adopted within the organization.
- Addressing and following up on all organizational risks immediately.
- Enhancing the culture of governance and risk management within organizations.
- Strengthening the principle of accountability by assigning responsibilities to relevant parties and continuously monitoring them.
- Making decisions based on accurate and reliable information.
- Monitoring compliance with the policies and legislation that organizations adhere to (such as the requirements of the National Cybersecurity Authority, the Saudi Central Bank, Saudi Aramco, the Communications and Space Commission, and other bodies).
- Reducing the time taken to address cybersecurity incidents by monitoring them until they are resolved.
- Auditing internal policies or external standards and following up on cases of non-compliance with the relevant parties, involving them in the audit process.

4 GRC Orbit System Feature

Main features of the GRC Orbit system

The GRC Orbit system has features that make it a leader in the field of governance, risk management and compliance:

- Supports Arabic and English interfaces
- Supports governance documents in Arabic and English in the same document
- Comprehensive Dashboards in governance, risk management and compliance
- Measurements for performance indicators
- Ability to integrate with the Active Directory system
- Ability to integrate with the Multi-Factor Authentication feature
- Ability to integrate with the organization's File Management System
- Ability to deal with the organization's email system Email Gateway
- Providing an API to integrate the system with other systems.
- Integration with vulnerability detection systems
- The ability to install the system on the company's internal servers or on a Saudi cloud service provider
- The ability to remind tasks that have an expiration date and the reminder will be after the end of the task time (every two or three days or a week), and it will also be optional according to the system settings
- The ability to audit internal controls (organizational policies, procedures and standards) and external controls (global and local standards and frameworks)
- Create a report that shows the status of the controls in each standard.

5 Project Timeline and Key Milestones

The following table outlines the proposed work plan and project timeline

Phase	Main Tasks	Deliverables	Estimated Duration

1. Analysis & Preparation Phase	- Requirements analysis - Define project scope and target systems - Identify relevant stakeholders	- GAP Analysis Document - Project Plan - RACI Matrix	1–2 weeks
2. GRC Solution Design	- Design workflows - Customize reports and forms - Define governance, risk, and compliance models - Design integration with other systems	- Functional and Technical Solution Design Document - API Integration Design Document	2–3 weeks
3. Installation & Configuration	- System installation (On-Prem or Cloud) - Initial configuration setup - Integrate with authentication (LDAP) - User and permission setup	- System ready for operation - Basic configuration documentation	1–2 weeks
4. Integration with Other Systems	- Identify integration methods and connect with other systems	- Effective integration with other systems - Unified data models	2–3 weeks
5. Training	- Train end-users - Prepare training materials and user manuals	- Trained users able to operate the system - User manual	1–2 weeks
6. Launch & Pilot Operation	- Official system launch - Pilot run under supervision - Provide direct support	- System running in production environment - Feedback and improvement notes	2–4 weeks
7. Post-Go-Live Support	- Ongoing technical support - Performance monitoring and enhancement - Incident and issue handling	- Post-Go-Live Support Plan (SLA) - Performance and issue tracking log	Ongoing

6 GRC Orbit System Modules

6.1.1 Governance Module

The Governance Module consists of global and local standards and frameworks, policies, procedures, internal standards, and provides a workflow for reviewing, approving, and publishing documents.

Full support for multiple legislative and regulatory frameworks

The system provides all local and global standards, which are continuously updated by our consulting team, with a focus on local standards and frameworks related to the Kingdom of Saudi Arabia, such as:

- National Cybersecurity Authority Controls: NCA-ECC, DCC, TCC, OTCC, OSMACC, CCC
- Saudi Central Bank Frameworks: SAMA CSF, BCM, ITG
- CMA Cybersecurity Guidelines
- Communications and Space Commission Controls: CST Cybersecurity
- Aramco Third Party Cybersecurity Standard: SACS-002
- ISO 27001:2022
- NIST – CSF
- Data Governance Controls issued by the Data Management Office (Priority 1+2+3)
- We provide the standards required by clients, whether local or global, so that organizations can measure compliance, monitor the status of controls, and take the necessary measures to ensure that the requirements of these standards are met.

Fig 1 Standards Added in the GRC Orbit System

Flexibly Add and Publish Internal Policies and Procedures

The system allows the addition of internal policies, procedures, and regulatory standards specific to the organization, and makes it easy to publish them to the relevant parties. This creates a transparent regulatory environment where everyone can access approved policies, enhancing overall compliance and facilitating adherence to controls and guidelines.

Manage Multiple Controls and Standards and Link Them to Regulatory Frameworks

The system enables the creation of security controls and linking them to the appropriate regulatory frameworks, with the ability to assign control owners and define periodic audit schedules. This capability helps monitor teams' adherence to the required controls and facilitates the periodic verification process, strengthening confidence in the level of security and compliance.

A Dedicated Mechanism for Collecting Feedback and Conducting Group Reviews

The system provides an effective mechanism for collecting feedback from different departments through policy review tasks, allowing each department to add its feedback on each control. This feedback is then shared with other departments to enable a comprehensive group review process. The system also retains all feedback attached to policies, ensuring thorough documentation and easy reference to comments and recommendations.

Dynamic Workflow for Obtaining Approvals from Multiple Administrative Positions or Specialized Committees

The system provides a flexible and efficient workflow that allows obtaining approvals from multiple administrative positions or through specialized committees, such as the Cybersecurity Committee. It also enables the determination of a specific quorum for completing approval from the committee, ensuring the implementation of policies and procedures agreed upon by all concerned parties and aligned with security requirements and organizational structure.

Integrated Management of Policy Versions and Updating Them with a Flexible Workflow

The system facilitates effective management of policy versions, allowing policies to be amended and a customized workflow for review and approval to be applied. Once amendments are approved, old versions are automatically archived, and new versions are published, ensuring that the latest versions are available to relevant parties while maintaining historical documentation of previous amendments for review and continuous compliance.

Update Notifications

The system sends alerts or notifications when policies are updated or new policies are added, ensuring that all employees are informed of the changes.

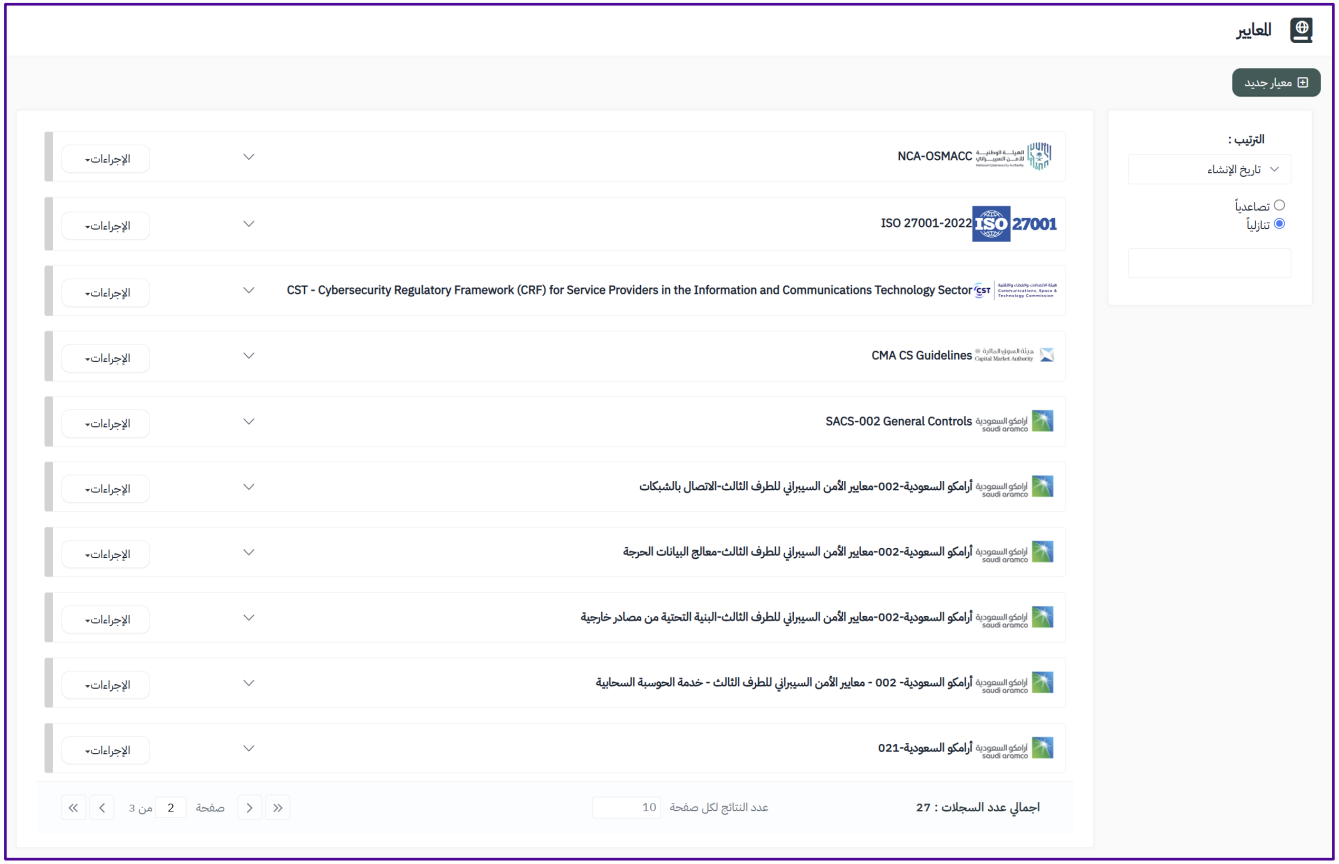


Fig 2 Examples of local and international standards are added to the system.

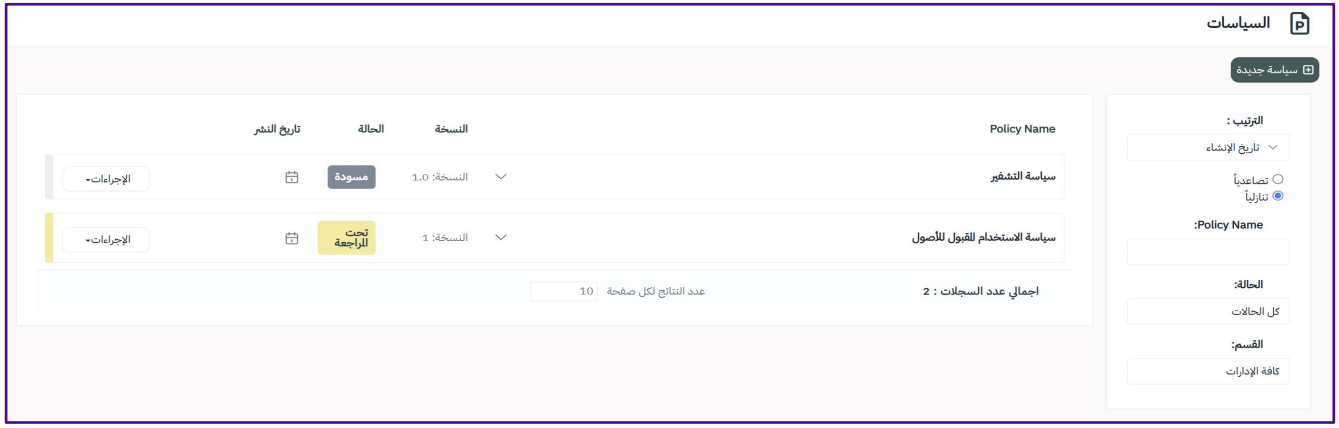


Fig 3 Examples of internal policies added to the system

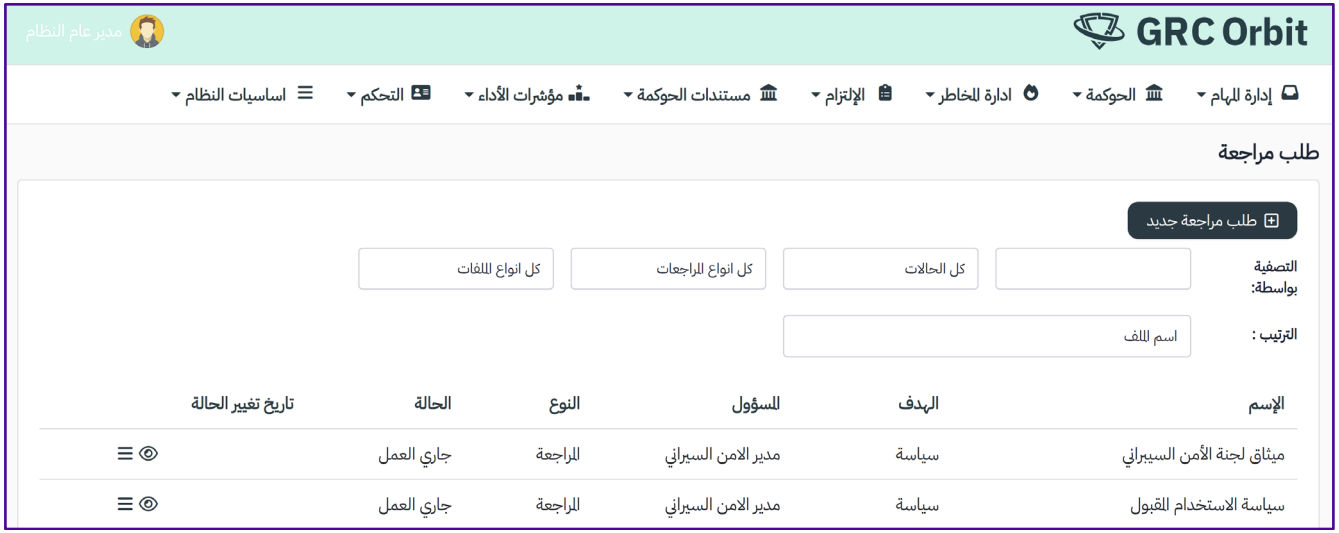


Fig 4 Examples of internal policies and procedures

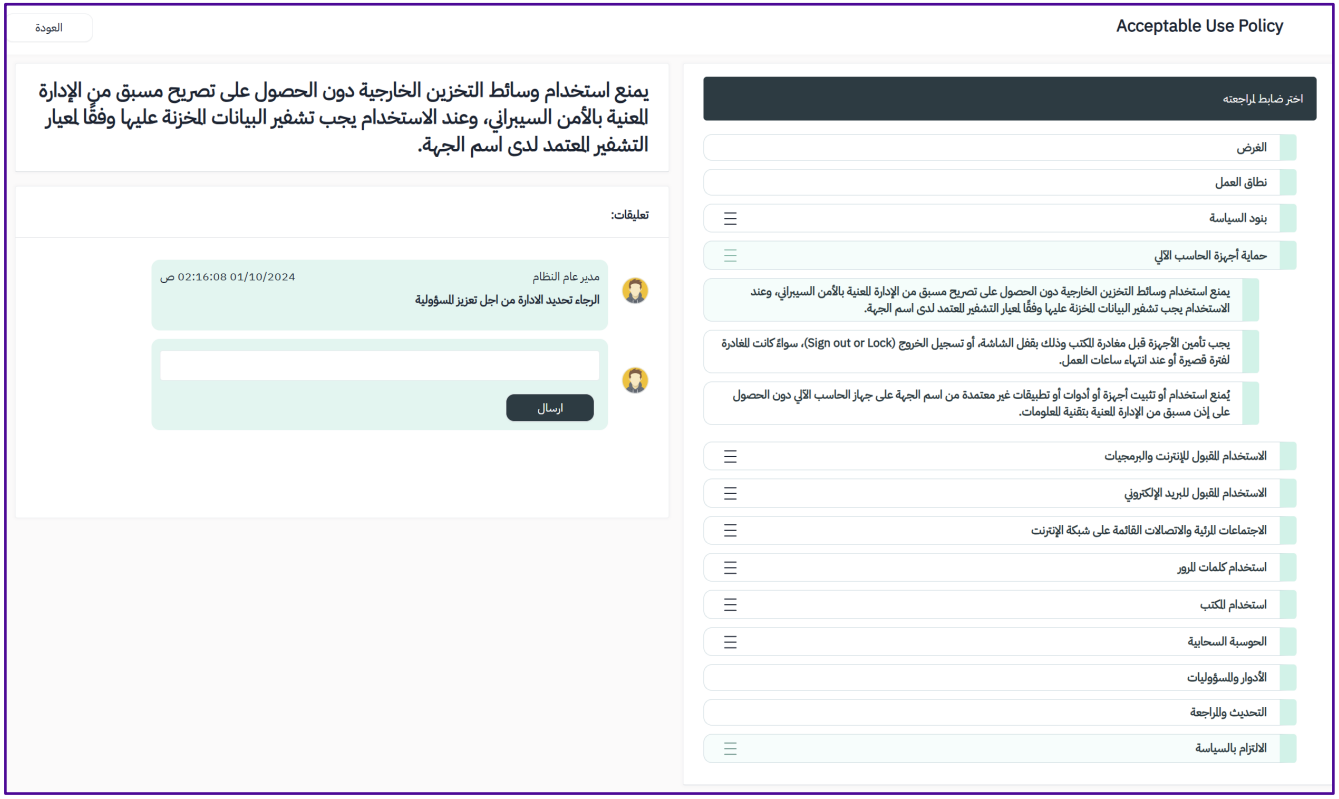


Fig 5 Policy Review Examples

6.2 Strategy Module:

Identifying Strategic Objectives

The system supports setting a strategic plan for cybersecurity, defining and clarifying strategic objectives, and linking them to initiatives and projects.

Managing Strategy Projects and Initiatives

The module allows users to manage a wide range of cybersecurity projects and initiatives within the strategic framework. It helps plan projects, identify necessary resources, and track progress continuously to ensure effective completion according to specified timelines.

Performance Measurement Indicators (KPIs)

The system supports linking the strategy to performance indicators and measuring them throughout the strategy implementation period.

Approval Workflow

The system supports adopting an approval workflow that includes several stages, requiring the approval of relevant parties before starting the implementation of strategies and projects.

System Images

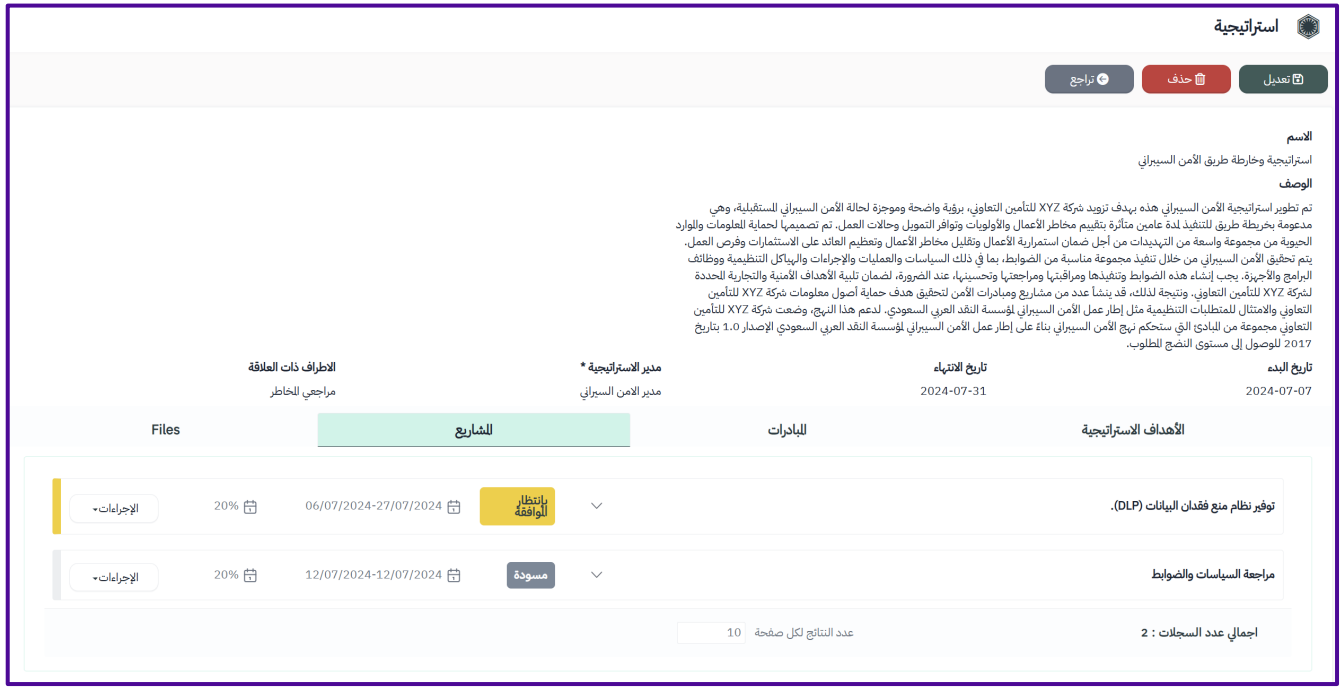


Fig 6 Example of a strategy with affiliate projects

6.4 Risk Management Unit

- Providing a Risk Framework

  To help organizations adopt a risk management methodology, a ready-made template for an information security risk management framework has been designed based on the ISO 27005-2022 methodology.
- Comprehensive Documentation of Risks in All Their Details

  The system enables the recording and documentation of all potential risks that may affect information security or disrupt the organization's basic operations. With accurate documentation that includes the risk name, description, source, and potential impact, the system provides a clear and comprehensive picture of potential risks. This allows for scientific and organized risk management, helping teams identify and address threats proactively, reducing exposure to risks, and enhancing business sustainability.
- Accurately Classify Risks into Specific Categories

  The system is characterized by its ability to classify and distribute risks into different categories, such as technical, operational, and strategic risks. These classifications help specialized teams understand the types of risks and how to deal with them according to priorities. This enhances risk management and allows for a more focused allocation of resources. This classification provides the organization with a clear vision of the nature of potential risks and enables them to be managed more effectively.
- Advanced Analytical Tools to Assess the Likelihood and Impact of Risks

  The system provides effective and thoughtful assessment tools based on global analytical methodologies, such as scenario analysis and SWOT. These tools help assess the likelihood of a risk occurring and determine the size of its impact. Through this assessment, the organization can gain a deeper understanding of the risks and plan ways to address them in advance. This accurate analysis aids in developing proactive strategies aimed at protecting the organization's interests and ensuring sustainable security.
- Arranging Risks According to the Degree of Severity to Determine Priorities

  The system is equipped with the ability to rank risks based on their severity, enabling the organization's management to focus on the risks that pose the greatest threat and require an immediate response. This capability helps make informed strategic decisions that ensure the protection of vital assets and support the organization's stability in the face of potential threats.
- Objective Calculation of the Risk Score According to International Standards

The system relies on internationally recognized standards, such as ISO 31000, for calculating the risk score, ensuring high accuracy and reliability in risk assessment. These standards add a professional dimension and provide reliable assessment tools that enhance confidence among management and decision-makers, leading to improved overall risk management performance.

- Measuring the Effectiveness of Controls Before and After Implementing Risk Treatment Plans
  The system allows for measuring the effectiveness of security controls before and after implementing the risk treatment plan. This helps evaluate the improvements achieved from modifications or actions taken. Through this analysis, the organization can ensure that new or improved controls effectively reduce risks and enhance security, providing valuable insights for data-driven decision-making and the development of more effective security strategies.
- Multiple and Flexible Treatment Options to Meet the Organization's Needs
  The system offers several options for treating risks, such as acceptance, transfer, mitigation, and avoidance. This variety of options enables the organization to choose the optimal solution for each type of risk, increasing flexibility and allowing the adaptation of procedures based on the specific needs of each case. This flexibility in managing risks makes the system suitable for organizations of all types and helps reduce the negative impact of risks on operations.
- Detailed Treatment Plans and Clear Implementation Procedures
  The system allows for the preparation of clear and specific treatment plans, detailing all the actions to be taken. This ensures that responsible teams can implement necessary actions on time. With accurately defined timelines and responsibilities, the system guarantees commitment and effective implementation, contributing to the achievement of the organization's security and strategic objectives efficiently.
- Periodic and Regular Follow-Up of the Implementation of Treatment Plans
  The system continuously monitors the progress of risk treatment plan implementation, providing periodic updates on the extent to which the set goals are being achieved. This ongoing follow-up ensures that the organization can adapt quickly to any new developments or changes in risks, enhancing its flexibility and ability to respond immediately.
- Effective Monitoring of Residual Risks After Implementing Treatment Plans
  After implementing treatment plans, the system continues to monitor residual risks to ensure their ongoing impact is minimized. This process ensures that all threats have been effectively dealt with and that there are no uncontrolled risks, creating a safer, more secure environment.
- Real-Time Monitoring System to Ensure Integrated Protection

The system enables continuous, real-time monitoring of risks, allowing for the immediate detection of any changes in the security situation or the emergence of new risks. This feature provides comprehensive and integrated protection by detecting new threats directly, giving security teams enough time to respond and neutralize threats before they affect operations. The risk management module manages all organizational risks, including cybersecurity risks, based on the organization's approved risk management methodology.

System Images

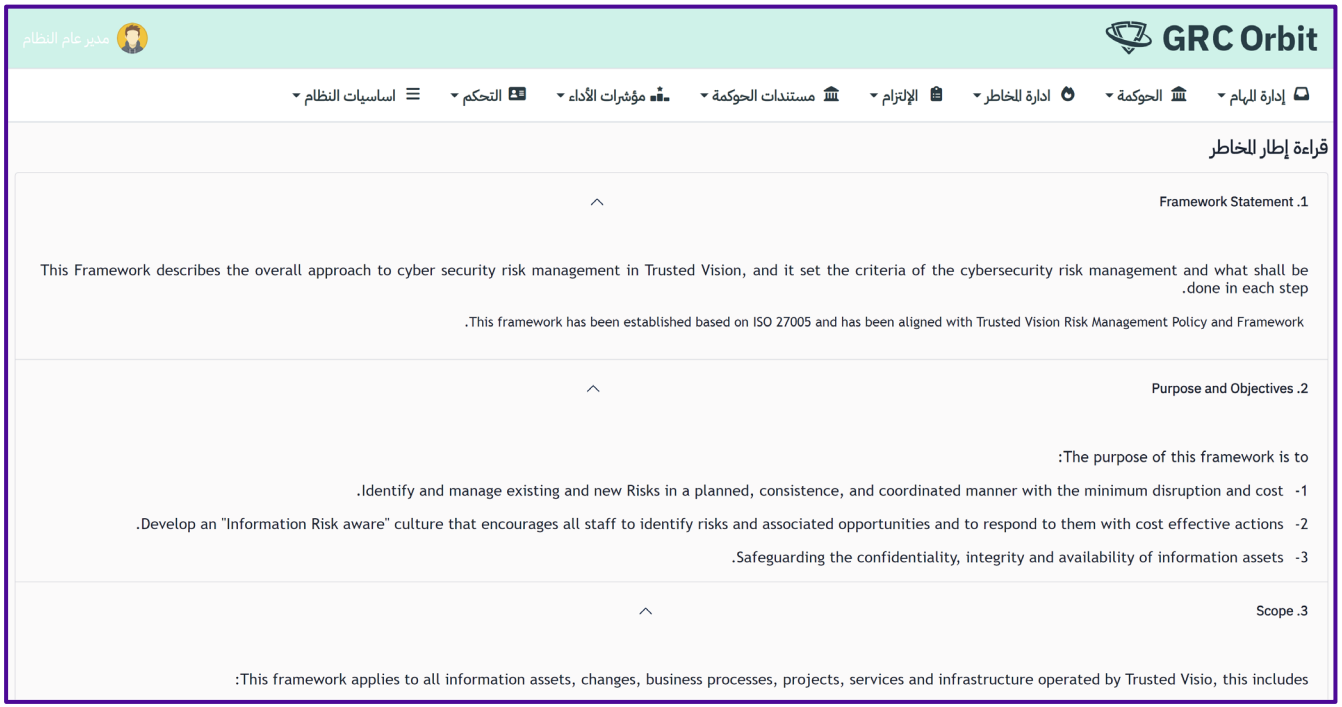


Fig 7 Risk Management Framework Based on ISO 27005-2022 Methodology

Integrity Level

Title	value	Description
Critical	5	Any loss of integrity of the information asset will result in extremely high, serious, immediate, and/or Long-term losses of: • Confidence / Reputation and Public Confidence. • Operational (Technology). • Financial or Property. • Legal and Regulatory. • Business Services.
Significant	4	Loss of integrity of the information asset will result in high and immediate losses of: • Confidence / Reputation and Public Confidence. • Operational (Technology). • Financial or Property. • Legal and Regulatory. • Business Services.
Marginal	3	Loss of integrity of the information asset will result in moderate losses of: • Confidence / Reputation and Public Confidence. • Operational (Technology). • Financial or Property. • Legal and Regulatory. • Business Services.
Minimal	2	Loss of integrity of the information asset will result in low losses of: • Confidence / Reputation and Public Confidence. • Operational (Technology). • Financial or Property. • Legal and Regulatory. • Business Services.
Negligible	1	Loss of integrity of the information asset results in very low losses of: • Confidence / Reputation and Public Confidence. • Operational (Technology). • Financial or Property.

Fig 8 ISO 27005 Risk Management Framework – Integrity Impact Analysis

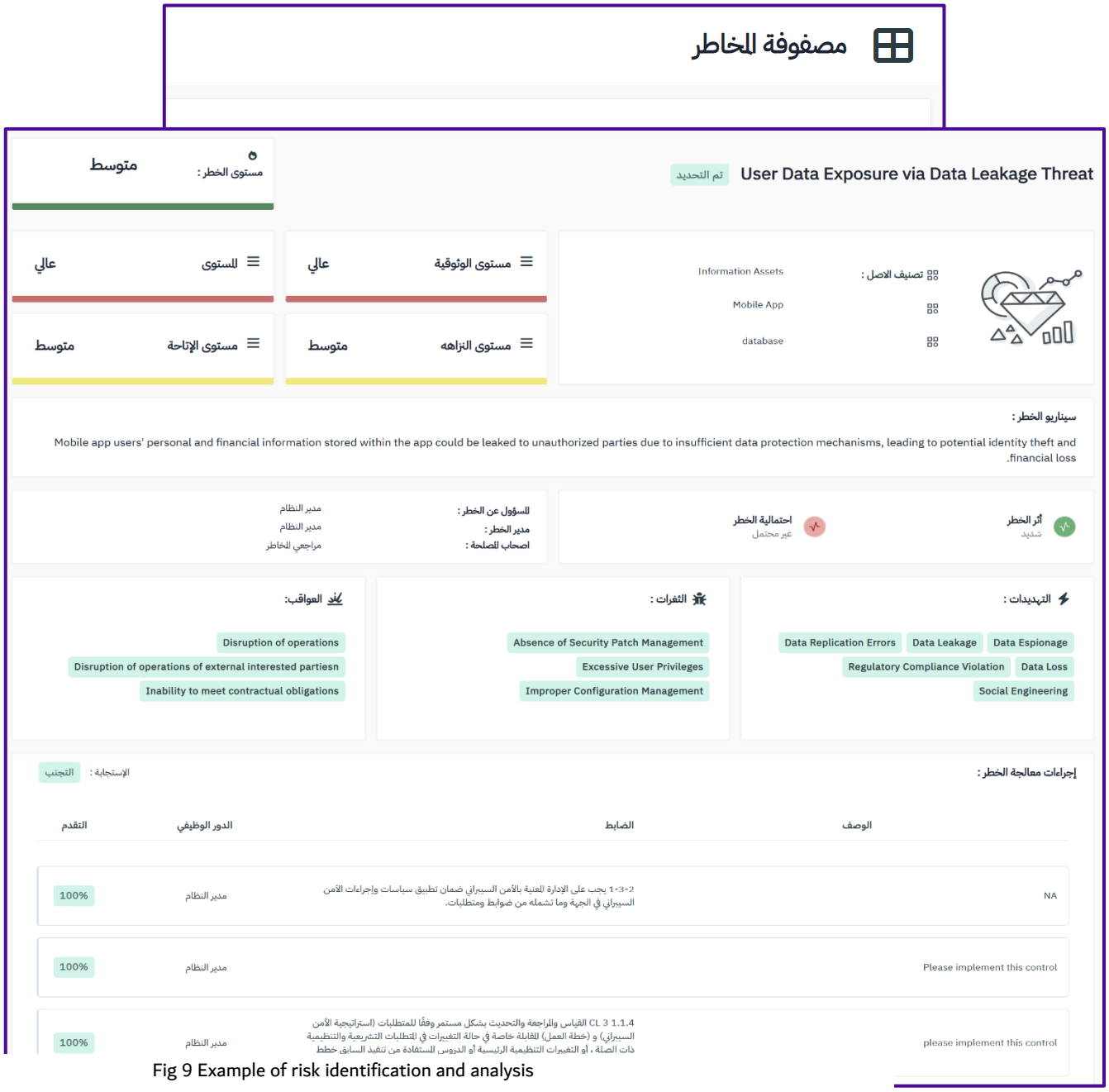


Fig 9 Example of risk identification and analysis

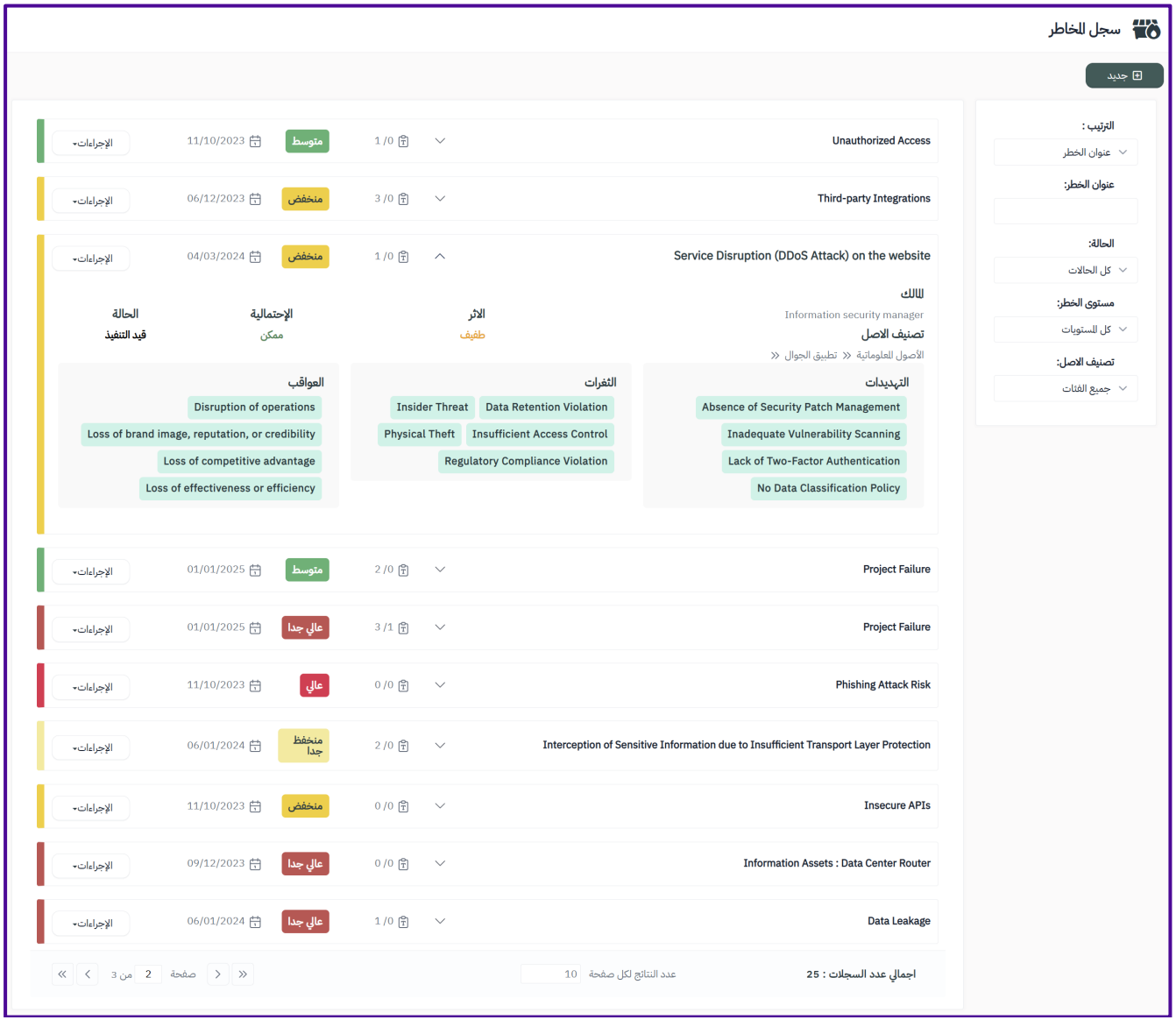
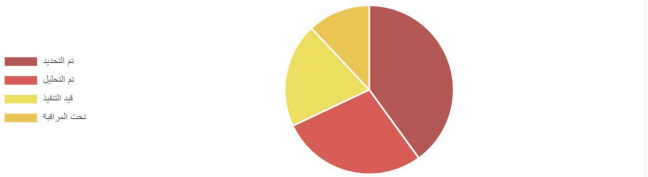


Fig 11 Information Security Risk Register

Fig 12 List of risk management actions requested from stakeholders

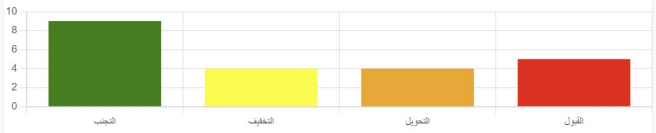
لوحة المعلومات للمخاطر

المخاطر حسب الحالة



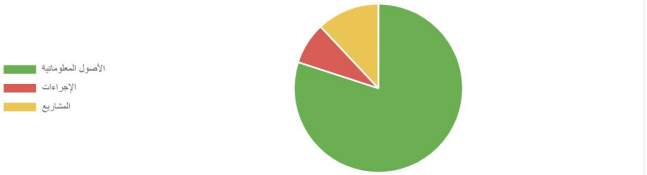
المخاطر حسب الاحتمالية

المخاطر حسب الاستجابة



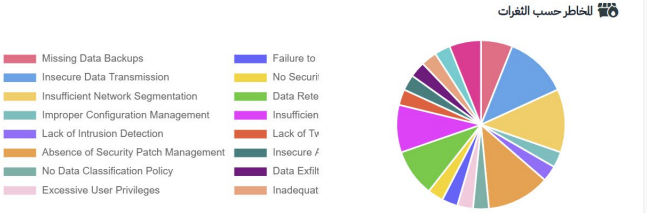
المخاطر حسب الاثر

المخاطر حسب التصنيف

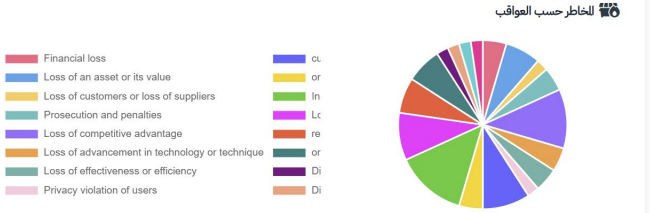


المخاطر حسب التهديدات

المخاطر حسب الثغرات



المخاطر حسب العواقب



المخاطر حسب المستوى

Fig 13 Comprehensive dashboard of information security risks

6.5 Compliance and Audit Management Unit

The Compliance Unit facilitates the auditing of internal policies and procedures, as well as local and international standards and frameworks. The system collects the necessary evidence during the audit process for each officer or item within the policy or standard, then measures the overall compliance rate for these standards and policies.

- Conducting Comprehensive and Accurate Audits

  The system enables thorough audits of internal policies, procedures, and compliance with both local and international standards and frameworks. This advanced audit capability ensures that the organization meets regulatory standards, building confidence in internal operations.

- Collecting and Analyzing Evidence Efficiently and Transparently

  The system collects the required evidence for each item or officer within policies and standards, ensuring an accurate and transparent audit process. This approach helps create a clear picture of the organization's compliance level and identifies areas for improvement.

- Flexibly Assign Tasks and Distribute Evidence

  The system allows tasks to be assigned to relevant departments and evidence to be distributed to the appropriate controls as soon as it becomes available. This streamlines the cooperation process and ensures a smooth flow of information and evidence across the organization.

- Accurate Measurement of the Overall Compliance Rate

  The system provides advanced tools to accurately measure the level of compliance and the overall compliance rate. This gives decision-makers a clear view of the organization’s adherence to policies and standards, helping to identify strengths and areas for improvement in the compliance process.

- Implementing a Comprehensive List of Audits

  The system offers a comprehensive list of audits, requesting evidence from the relevant parties and displaying requirements in a simplified manner for each user. This simplifies the compliance process, ensuring that all parties are committed to providing the required evidence promptly and effectively.

- Displaying Audit Results Clearly and Transparently

  The system presents audit results in a clear and transparent manner, enabling decision-makers to access essential information for informed decision-making. This helps improve compliance levels and determines the necessary corrective actions.

- Periodic Evaluation of Legislative Frameworks and Controls

The system enables the periodic evaluation of legislative frameworks and controls to ensure that policies and procedures align with required standards. This helps the institution stay up to date with legislative changes and maintain compliance with global standards.

- View Similar Controls and Compliance Status in Other Standards

  The system allows easy access to similar controls across different standards, displaying the compliance status for each control. It also enables the easy import of evidence, simplifying audits and saving time and effort.

- Review Previous Assessments to Identify Gaps in Compliance

  The system allows users to review past assessments to identify gaps and weaknesses in compliance. This feature helps provide actionable recommendations that enhance compliance and support the achievement of the institution's goals.

- Developing Clear and Executable Corrective Plans

  The system allows for the development of detailed corrective plans to address any compliance deficiencies, with periodic follow-up on their implementation. This ensures that identified gaps are closed and organizational objectives are met efficiently.

- Collecting Compliance-Related Evidence in a Central System

  The system centralizes the collection and documentation of compliance-related evidence, linking it to relevant controls and standards. This streamlines access and analysis, improving the accuracy and efficiency of the audit process.

- Organizing Documents and Evidence in an Accessible Manner

  The system helps organize documents and evidence in a structured way, making it easier for work teams and auditors to verify compliance, which accelerates both internal and external audit processes.

- Advanced Mechanism for Tracking Evidence Associated with Each Compliance Process

  The system offers a continuous monitoring mechanism for evidence linked to each compliance process, with periodic updates on the evidence's status. This ensures that the organization remains prepared for compliance audits at any time.

- **Continuous Preparation of Evidence for Internal and External Audits**

  The system facilitates the continuous preparation of evidence to ensure full compliance, enabling smooth internal and external audits. This helps enhance the organization's confidence in its ability to meet the required standards.

- **Simple and Organized User Interface**

The system features an intuitive and easy-to-use interface, making it easier to collect, follow up on evidence, and track the status of each officer. This streamlined design improves the user experience and supports better compliance management.

System Images

Fig 14 Example of a list of audits

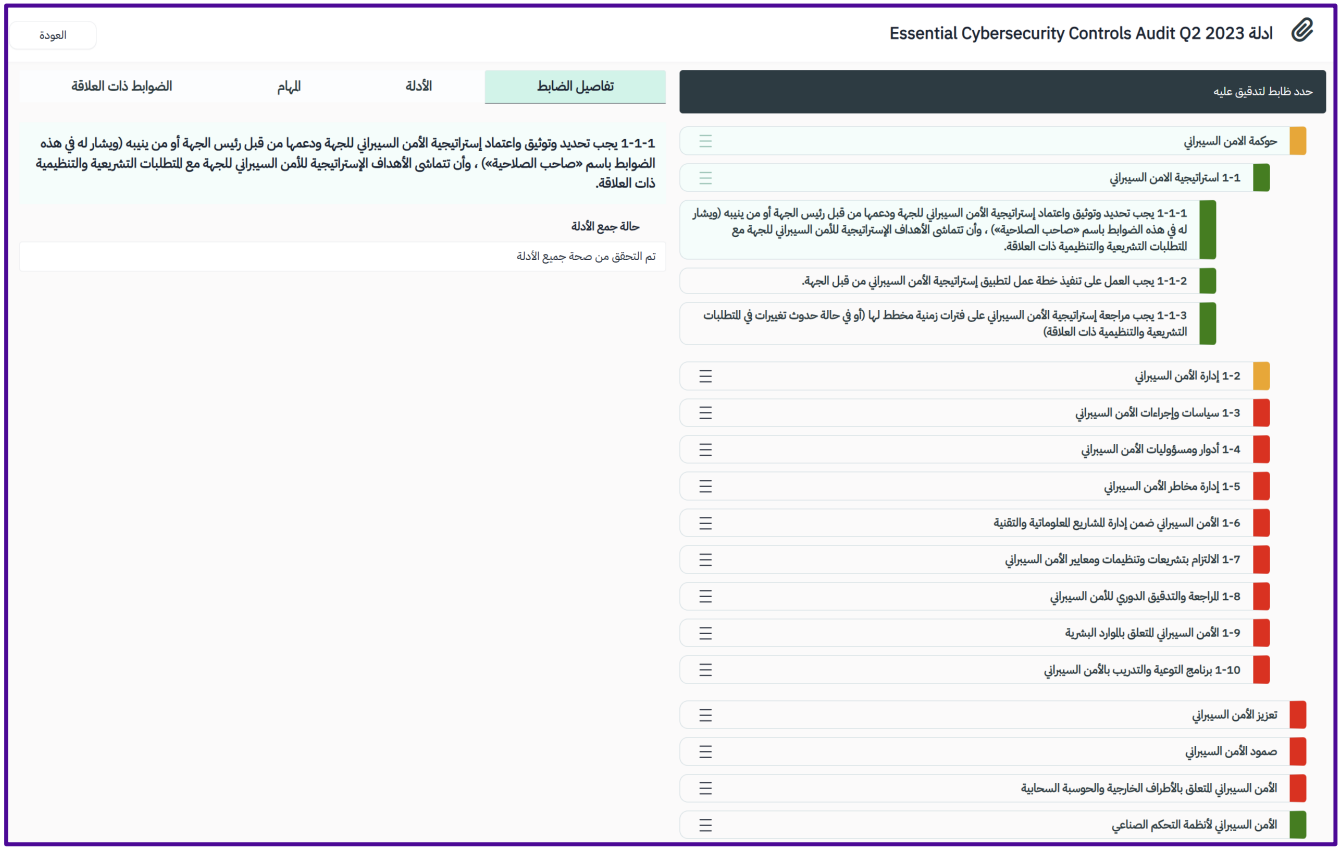


Fig 15 Example of seeing and requesting evidence from stakeholders during the audit process

Fig 16 Example of requirements to be met by a system user during an audit

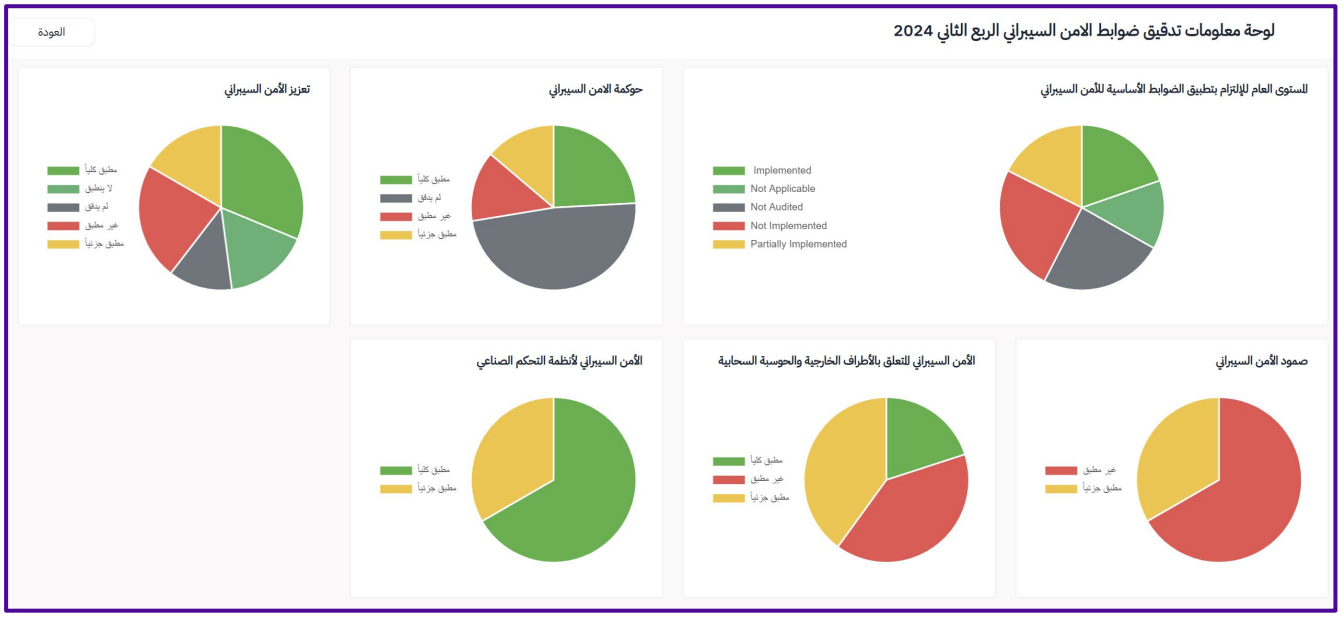


Fig 17 Compliance resulting from the evaluation process with a standard

- Performance Measurement Indicators Uni The Performance Measurement Indicators Unit enables the creation and monitoring of performance indicators to track and achieve organizational goals. These indicators are set within a specific time frame (monthly, quarterly, semi-annually, or annually) and involve identifying all related factors and stakeholders to ensure accurate and effective measurement.

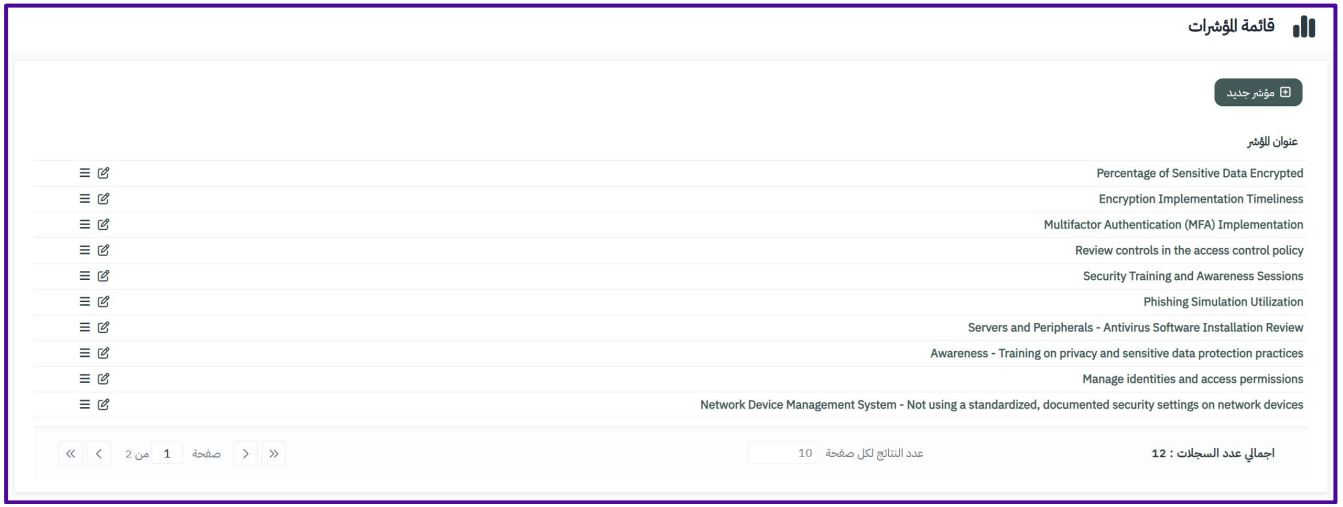


Fig 18 List of KPIs created

Fig 19 Indicator reading

- Task Follow-up Unit

Central Follow-up of Tasks:

The system allows centralized tracking of all tasks across different units (such as evidence collection, risk management, etc.) and assigned to various departments. It provides functionalities for manual escalation (with the option for automatic escalation) and sending manual reminders (with automatic

reminder functionality available). Additionally, the system allows users to filter tasks based on specific criteria, ensuring a streamlined and organized follow-up process.

- One Place for Managing Tasks:

  The system provides a centralized location for managing all tasks related to different units and departments. Users can monitor and manage tasks from this central location, including the ability to close tasks, raise evidence of task completion, and send notes or feedback on tasks to the task creator. This comprehensive tracking ensures that progress is closely monitored, helping to improve efficiency and accountability.

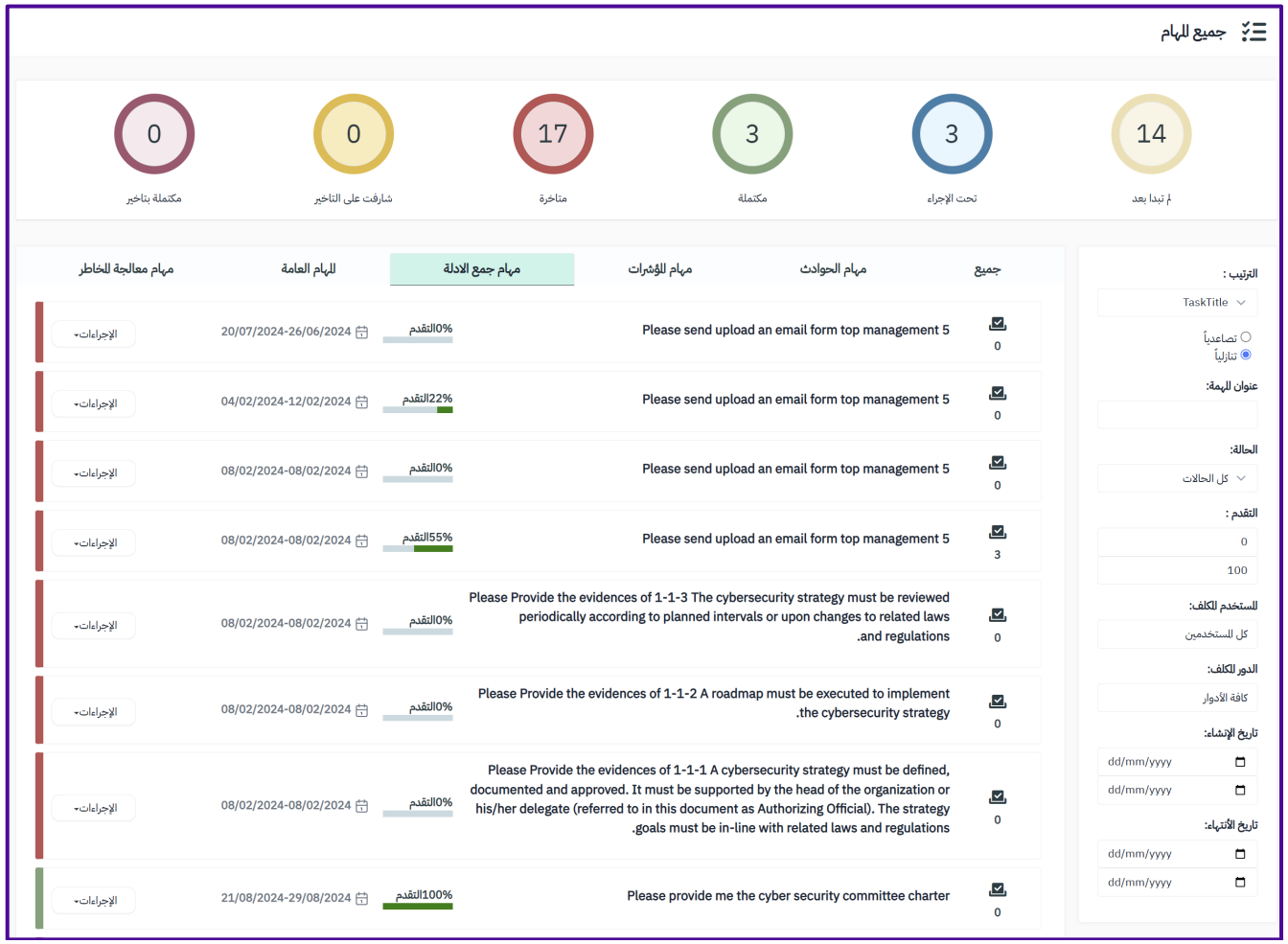


Fig 20 All tasks assigned to departments with filter option

6.6 File Library

- Central library for file management:

  The system provides a central library for all files uploaded to the system, providing file information such as file owner, expiration date, usage locations, and data confidentiality level.

6.7 Vulnerability Management

- Support for Integration with Leading Vulnerability Management Tools:
  The system is designed to integrate seamlessly with popular vulnerability scanning tools like Nessus, enabling automatic import of scanning results. This integration allows for real-time detection of vulnerabilities and provides detailed analysis along with practical remediation recommendations. It enhances response times to security threats and helps streamline the vulnerability management process.

- Centralized Vulnerability Management for Easy Access and Analysis:
  With a unified platform, the system allows security teams to track and manage all vulnerabilities from a central location. This ensures that all relevant information is easily accessible, facilitating quick decision-making. Integration with asset management ensures that vulnerabilities are linked to relevant assets, allowing the teams to prioritize remediation efforts based on the criticality and value of the affected assets. This prioritization helps secure vital organizational resources more effectively.
- Accurate Prioritization of Vulnerabilities Based on Threat Severity:
  The system employs global standards like the Common Vulnerability Scoring System (CVSS) to assess the severity of vulnerabilities. By evaluating the potential impact and likelihood of exploitation, the system provides a clear mechanism for prioritizing vulnerabilities, allowing security teams to focus their efforts on addressing the most critical and high-impact threats first. This ensures resources are allocated efficiently to mitigate risks with the highest potential harm.

- Comprehensive Vulnerability Lifecycle Management for Continuous Remediation:
  The system tracks the entire lifecycle of each vulnerability from detection to resolution. By documenting details such as the vulnerability's type, severity, and potential impact, the system allows for thorough management. Tasks can be assigned to the appropriate teams with defined deadlines for closure. Regular updates on remediation progress ensure that no threat goes unaddressed, helping to maintain continuous protection against emerging security risks.
- Generating Customized Reports for a Comprehensive View of the Status of Vulnerabilities:
  The system allows the generation of detailed, customized reports about vulnerabilities, including their current status. These reports provide decision-makers with insights into the progress of addressing vulnerabilities and support strategic decisions to enhance security.
- Integrated Analysis of Discovered Vulnerabilities and Enhancing the Security Strategy:

The system offers a comprehensive analysis of vulnerabilities, providing recommendations on how to address and mitigate their impact. Additionally, these vulnerabilities can be linked to existing risks within the system, thereby strengthening the risk management strategy and contributing to a more integrated security framework.

System Images

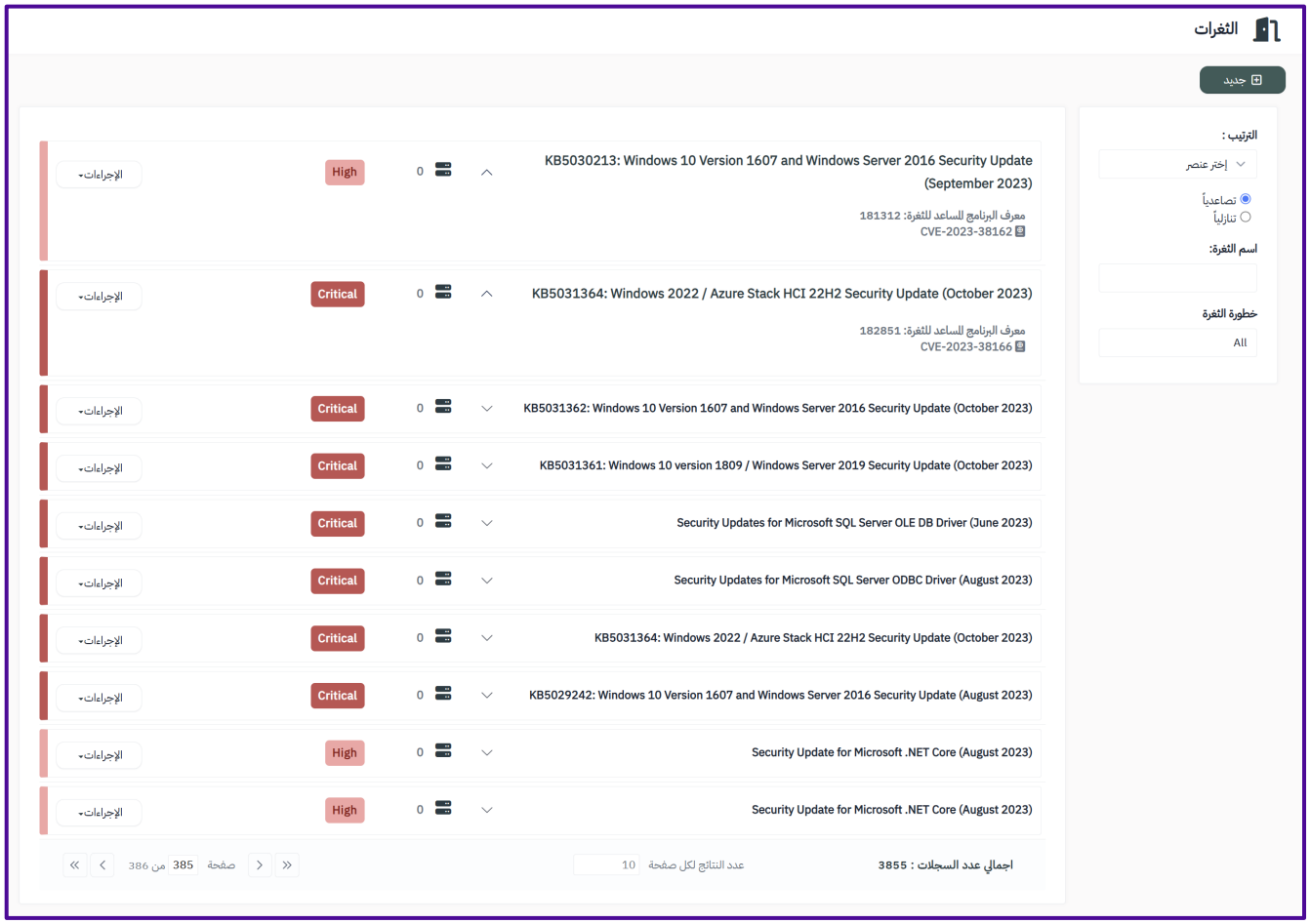


Fig 21 Centralized vulnerability management

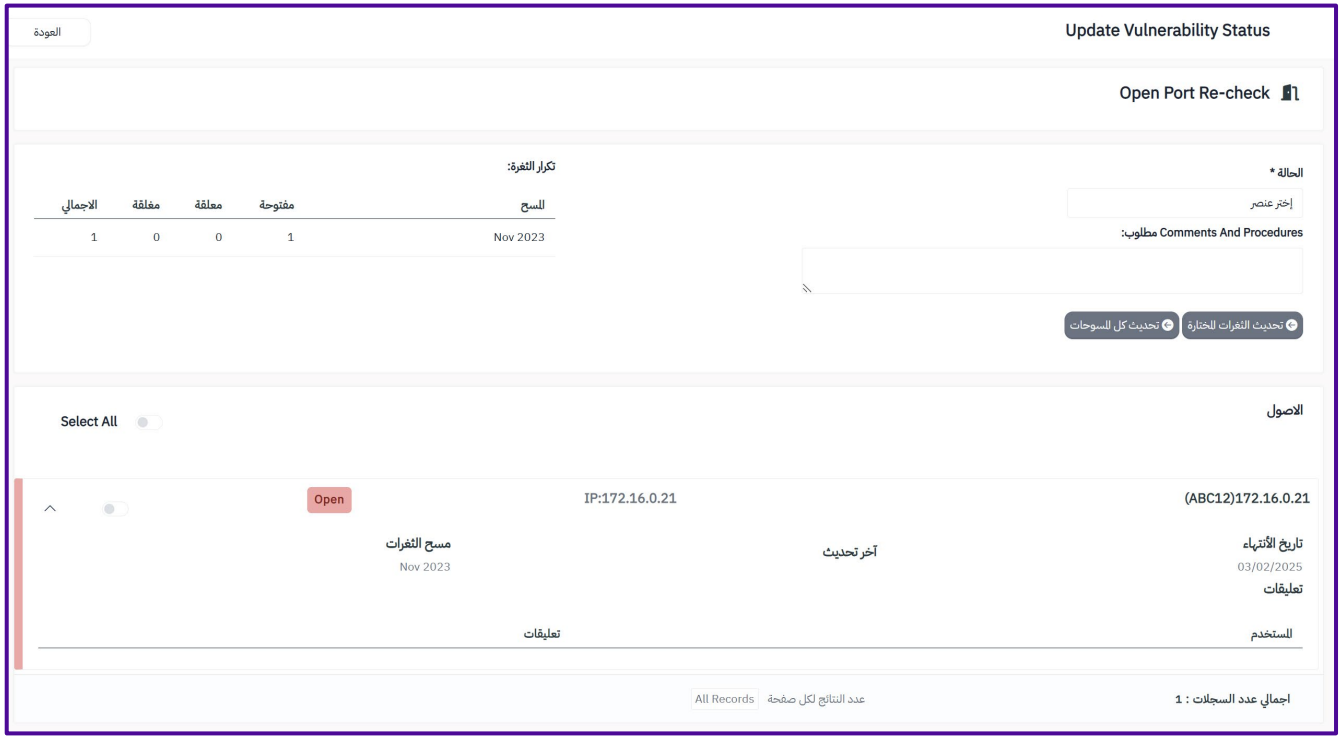


Fig 22 Close the loopholes

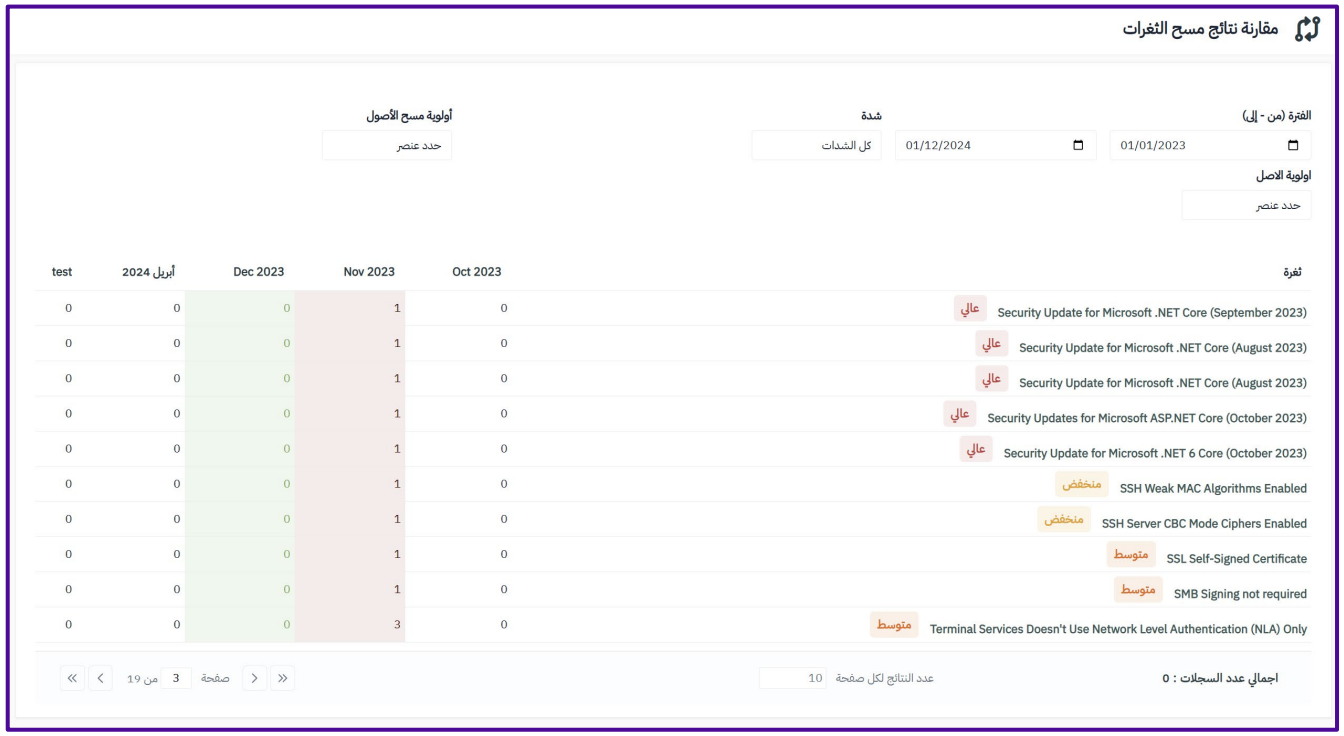


Fig 23 Reports on progress in addressing vulnerabilities

7 System Installation Requirements

To ensure the successful installation of the GRC Orbit system within the entity, the organization must provide the following components:

- IIS Web Server service
- NET Framework
- SQL Server Enterprise (2019 or 2022)
- If you are using any version of SQL Server other than the recommended Enterprise edition or model, please contact the technical team at Trusted Vision Company for advice and to assess the possibility of installing the system on your current version.

8 Why Choose GRC ORBIT

GRC Orbit is the ideal choice for organizations seeking excellence in governance, risk, and compliance management. Here are the top reasons why GRC Orbit is the perfect solution for your organization's needs:

Comprehensive Integration with Existing Systems

- GRC Orbit supports seamless integration with existing systems within the organization, such as identity and access management systems, allowing for centralized control of permissions and roles.
- The platform also integrates with email systems and enterprise file storage to ensure a smooth and efficient flow of information.

Automate and Optimize Processes

With multiple system modules like task management and risk management, GRC Orbit enables the automation of repetitive processes and enhances the efficiency of daily operations by intelligently allocating resources. This helps reduce the time spent on routine tasks and boosts overall productivity.

Advanced Compliance and Audit Support:

The platform provides powerful tools for auditing both internal and external policies and standards. Users can collect and analyze evidence, while monitoring compliance with standards such as ISO 27001 and the National Cybersecurity Authority's standards, which enhances adherence to local and international laws and regulations.

Advanced Risk Analysis:

The risk management module in GRC Orbit is designed to comply with international standards, including ISO 27005. The platform enables comprehensive identification, analysis, and assessment of risks. Users can benefit from conducting SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to understand the impact of risks and take necessary steps to mitigate them.

Comprehensive Dashboards and KPIs:

GRC Orbit provides integrated dashboards that offer a comprehensive view of the organization's performance in governance, risk, and compliance. Users can monitor key performance indicators (KPIs) on a periodic basis (monthly, quarterly, semi-annually, annually), which helps achieve the organization's strategic objectives.

Support for Both Arabic and English Languages:

GRC Orbit supports both Arabic and English languages, making it suitable for organizations in Saudi Arabia and the broader Middle East region.

customizable Solutions:

The platform offers high customization flexibility to meet the needs of different organizations. Whether it is through customizing tasks or modifying compliance settings, GRC Orbit can be adapted to suit your specific requirements.

9 GRC ORBIT Success Story

Through our partnerships with clients across the Levant and Gulf regions, we have achieved significant success in providing specialized consulting services tailored to their diverse needs. For instance, we have developed and implemented innovative management solutions for several leading companies in the region, helping to strengthen their ecosystems and enhance their levels of efficiency and innovation. By focusing on consulting services that are fully aligned with their strategic objectives, we have enabled our clients to excel in their respective fields and stand out in a competitive market. Our successes are a testament to our unwavering commitment to delivering the best possible solutions and driving our clients toward sustainable success.