NCA – CCC-P CYBERSECURITY CONSULTATION PROPOSAL

Version: 1.0

Date: 7-6-2023

Prepared By:

Trusted Vision for Governance and Consultation

Document Control

Item	Description
Document Title	NCA- CCC-P CONSULTATION PROPOSAL
File Name	NCA- CCC-P CONSULTATION PROPOSAL.docx
Author (s)	Hashem Al-Azizi
Classification	Confidential

Document Amendment Record

Version	Date	Remarks
1.0	7-6-2023	First Release

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's requirements

The client requests to have the following services:

Consultation of National Cybersecurity Authority cloud cybersecurity– provider controls (NCA-CCC-P).

The Cloud Cybersecurity Controls (CCC – 1: 2020) is developed as an extension to the ECC; to achieve higher levels of national cybersecurity goals by focusing on cloud computing services from the perspective of Cloud Service Providers (CSPs) and Cloud Service Tenants (CSTs).

The main objective of these controls is to minimize the cybersecurity risks of Cloud Service Providers (CSPs), and Cloud Customers, also known as Cloud Service Tenants (CSTs).

CSPs within the scope of CCC are any CSP which provides cloud computing services to the CSTs within the scope of work.

1- Cybersecurity Governance	1-1	Cybersecurity Roles and Responsibilities	1-2	Cybersecurity Risk Management
	1-3	Compliance with Cybersecurity Standards, Laws and Regulations	1-4	Cybersecurity in Human Resources
	1-5	Cybersecurity in Change Management		
2- Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	Information System and Information Processing Facilities Protection	2-4	Networks Security Management
	2-5	Mobile Devices Security	2-6	Data and Information Protection
	2-7	Cryptography	2-8	Backup and Recovery Management
	2-9	Vulnerabilities Management	2-10	Penetration Testing
	2-11	Cybersecurity Event Logs and Monitoring Management	2-12	Cybersecurity Incident and Threat Management
	2-13	Physical Security	2-14	Web Application Security
	2-15	Key Management	2-16	System Development Security
	2-17	Storage Media Security		
3- Cybersecurity Resilience	3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)		
4- Third party Cybersecurity	4-1	Supply Chain and Third-Party Cybersecurity		

Figure 1: Main Domains and Subdomains of Cloud Cybersecurity Controls

CSP's controls in the CCC are an extension and complement to the controls in the ECC; therefore, the CSPs – within or outside the scope of the ECC- must ensure continuous compliance with the controls in both ECC and CCC.

The cloud cybersecurity controls for providers contains:

- 37 Main Controls

- 96 Sub controls

We believe that our expertise in conducting similar data management projects positions us among the elite consulting firms in addition to our:

1. Long and in-depth expertise in designing and implementing similar projects.
2. A balanced mix of international and regional expertise in data consulting-related issues
3. Effective project implementation approach to address project requirements in a timely, professional and quality manner
4. Extensive knowledge and expertise in implementing and designing solutions based on international standards and best practices.
5. Best-of-breed data management consulting expertise
6. Proven project management and implementation methodologies and approach

We hope our proposed services and approach meet your satisfaction, and we look forward to a mutual business relationship.

2. Project Benefits and Values

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

1 Alignment with national and international standards

2 Achieving compliance with NCA

3 Improved decision-making by monitoring the overall cybersecurity governance, risk and compliance.

4 Increased competitiveness through improved customer satisfaction

5 Increased public trust through securing customer's data.

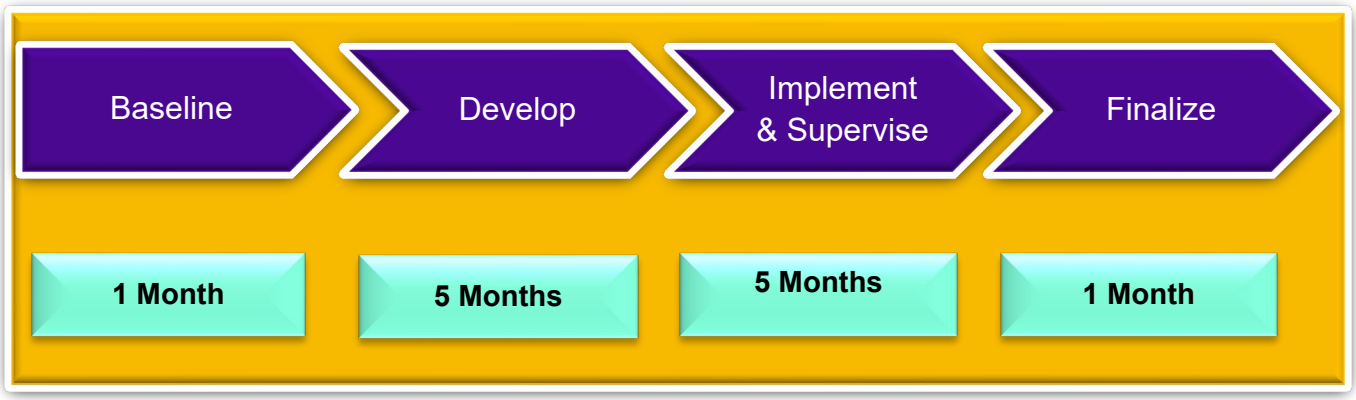
6 Manages the assurance, integrity, security, value, and availability of data.

7 Increased customer and interested party satisfaction.

8 Reduced costs because of data breaches

3. Project Implement Methodology and Approach

To address the Client's requirements, we have structured the project approach into phases as follows:



3.1 Baseline Phase

This is the first phase of the project, during which the following activities will take place.

Trusted Vision Activities		CLIENT Activities	
No	**Activity**	**No**	**Activity**
1	Mobilization of the project team	1	Nomination of the project coordinator and project steering committee
2	Information Gathering which includes. 1 Policies, Procedures, Forms 2 Asset register 3 Technologies 4 Any related Doc's	2	Send all required documents to the consultants
3	Develop project charter that elaborate the project scope, objectives, and project management processes	3	Review and approve project charter
4	Perform Kick-off meeting with all project stakeholders	4	Coordinate Project Kick-off meeting and ensure all stakeholders attendance
5	Conduct interviews with the project stakeholders to understand their needs and expectations, stakeholders are including -but not limited to-: 1 Head of Company 2 Risk Management Committee 3 Manufacturing Department 4 Head of IT Department	5	Coordinate the interviews with all project stakeholders that are nominated by the consultant

	5 Head of Cybersecurity Department 6 Head of Human Resources 7 Head of Legal		
6	Develop a solution matrix sheet that includes the required solutions and tools to be brought to implement the NCA ECC Controls	6	Review and approve the proposed solution matrix sheet that includes the required solutions and tools to be brought by the client to implement the cybersecurity controls
7	Understand company processes, business environment and its context	7	Engaging with vendors and third parties that provides the required cybersecurity solutions and conduct POCs with them and purchase the tools
		8	Acquire and implement all needed cybersecurity solutions and tools
		9	Obtain Top management commitment and buy-in with securing the budget towards implementing NCA cybersecurity controls
		10	Prepare an asset register and send it to the consultant
		11	Dedicate one (1) staff to work with the consultant to achieve the implementation of the project
8	Perform unlimited Interview Saudi cybersecurity cloud specialist (During the project period)	12	Coordinate and Hire at least 3 qualified Saudi cybersecurity cloud specialist
		13	Perform annual screening of personnel working inside KSA who have access to Cloud Technology Stack

9	Provide consultation for the best multi factor authentication tool
10	Provide consultation for the best Web Application Firewall
11	Develop use cases for SIEM
12	Provide consultation for the best EDR Solution
13	Provide consultation on how to implement Anti DDOS Solution
14	Perform Inventory of all information and technology assets
15	Develop Inventory of all end user and mobile devices
16	Provide consultation on the best data storage technologies
17	Provide consultation on the best Backup solutions
18	Provide consultation on the best vulnerability management solutions

14	Acquire multi-factor authentication for privileged users, and candidates of personnel with access to Cloud Technology Stack.
15	Acquire and implement Web Application Firewall
16	Acquire and implement SIEM
17	Acquire and implement EDR Solution
18	Acquire and implement Anti DDOS Solution
19	Acquire and implement asset management tool with labeling and configuration management tool.
20	Acquire and implement mobile device management tool
21	Perform Screen locking for end user devices.
22	Acquire and implement data storage technologies
23	Acquire and implement Backup solutions
24	Acquire and implement vulnerability management solutions

19	Provide consultation on the best SIEM solution	25	1 Acquire and Implement SIEM solutions with continuous monitoring service including: 2 Activating and collecting of login attempts history 3 Activating and protecting all event logs of activities and operations performed by the CSP at the tenant level in order to support forensic analysis. 4 Protecting cybersecurity event logs from alteration, disclosure, destruction and unauthorized access and unauthorized release, in accordance with regulatory, or law requirements 5 Continuous cybersecurity events monitoring using SIEM technique covering the full Cloud Technology Stack 6 Reviewing cybersecurity event logs and audit trails periodically, covering 7 CSP events in the Cloud Technology Stack. 8 Automated monitoring and logging of remote access sessions event logs 9 Secure handling of user-related data found in the audit trails and the cybersecurity event logs

3.2 Develop Phase

This is the second phase of the project, during which the following activities will take place.

Trusted Vision Activities		CLIENT Activities	
No	**Activity**	**No**	**Activity**
1	Develop Cybersecurity roles and RACI assignment for all stakeholders of the cloud services including Authorizing Official's roles and responsibilities.	1	Review and approve Cybersecurity roles and RACI assignment for all stakeholders of the cloud services including Authorizing Official's roles and responsibilities.
2	Revise the cybersecurity risk management framework and: • Define acceptable risk levels for cloud services. • Consider data and information classification in cybersecurity risk management methodology	2	Review and approve the revised cybersecurity risk management framework
3	Developing cybersecurity risk register for cloud services	3	Monitoring periodically the cybersecurity risk register for cloud services
4	Ensure a cybersecurity policies and procedures that are required by NCA-ECC is approved and implemented	4	Implement NCA-ECC related cybersecurity policies and procedures
5	Integrate cybersecurity requirements in the HR process	5	Approve and implement cybersecurity requirements in the HR process
6	Develop change management methodology	6	Review, approve and implement change management methodology

7	Identify all generic accounts for accountability and revise the access management process	7	Review and approve access management process
8	Provide consultation on how to perform secure session management, including session authenticity, session lockout, and session timeout termination	8	Perform Secure session management, including session authenticity, session lockout, and session timeout termination
9	Develop configuration standards for all technologies	9	Review, approve and implement all configuration standards for all technologies.
10	Develop Data storage policy, standard and procedures	10	Provision to CSTs of securely data storage processes, procedures, and technologies to comply with related legal and regulatory requirements
11	Develop Backup policy, procedure and standards	11	Securing access, storage and transfer of Cloud Technology Stack and CST's backups and its mediums, and protecting it against damage, amendment or unauthorized access
12	Develop vulnerability management policy, procedure and standards	12	Review, approve and implement vulnerability management policy, procedure and standards
13	Develop incident response plan	13	Review, approve and implement incident response plan
14	Develop Key management policy and procedure	14	Review, approve and implement Key management policy and procedure
15	Develop System Development Security policy and procedure	15	Review, approve and implement System Development Security policy and procedure

16	**Develop Disaster Recovery and business continuity procedure**

16	**Review, approve and implement Disaster Recovery and business continuity procedure**

3.3 Implement and Supervise Phase

This is the third phase of the project, during which the following activities will take place.

Trusted Vision Activities		CLIENT Activities	
No	**Activity**	**No**	**Activity**
1	Provide consultation on how to clarify cybersecurity acceptable risk levels for the cloud services to the clients (if applicable)	1	Clarifying cybersecurity acceptable risk levels for the cloud services to the clients (if applicable)
2	Assurance of separation and isolation of data, environments, and information systems across CSTs, to prevent data commingling	2	Perform separation and isolation of data, environments, and information systems across CSTs, to prevent data commingling
3	Provide consultation on how to monitor traffic	3	Perform Monitoring of traffic across the external and internal networks to detect anomalies (Using existing SOC Team)
4	Provide consultation on how to isolate and protect Cloud Technology Stack network from other internal and external networks	4	Perform Network isolation and protection of Cloud Technology Stack network from other internal and external networks.
5	Provide consultation on how to Protect data that is being transmitted through the network; from and to the Cloud Technology Stack network using cryptography primitives; for management and administrative access	5	Perform Protection of data transmitted through the network; from and to the Cloud Technology Stack network using cryptography primitives; for management and administrative access.

6	Provide consultation on how to perform access control between different network segments	6	Perform Access control between different network segments
7	Provide consultation on how to Isolation between cloud service delivery network, cloud management network and enterprise network	7	Perform Isolation between cloud service delivery network, cloud management network and enterprise network
8	Provide consultation on using Cloud Technology Stack's data in environments other than production environment, after applying strict controls for protecting that data, such as: data masking or data scrambling techniques	8	Perform data masking or data scrambling techniques Cloud Technology Stack's data in environments other than production environment
9	Revise existing contracts and ensure that CST's data is disposed in a secure manner on termination or expiry of the contract with the CSP	9	Perform Disposal of CST's data in a secure manner on termination or expiry of the contract with the CSP
10	Revise existing contracts and ensure that Commitment to maintain the confidentiality of the CST's data and information, according to related legal and regulatory requirements is exists	10	Demonstrate Commitment to maintain the confidentiality of the CST's data and information, according to related legal and regulatory requirements
11	Provide consultation on how to provide CSTs with secure means to export and transfer data and virtual infrastructure	11	Providing CSTs with secure means to export and transfer data and virtual infrastructure
12	Provide consultation on how to implement technical mechanisms and cryptographic primitives for strong encryption, in according to the advanced level in the	12	Implement Technical mechanisms and cryptographic primitives for strong encryption, in according to the advanced level

	National Cryptographic Standards (NCS-1:2020).
13	Provide consultation on how to issue certification in a secure manner, or usage of certificates from a trusted certification authority
14	Provide consultation on how to Send Notification to CSTs of identified vulnerabilities that may affecting them, and safeguards in place.
15	Perform training for employees and third-party personnel to respond to cybersecurity incidents, in line with their roles and responsibilities
16	Provide consultation on the authorized and specialized organizations and groups that need to be subscribed to
17	Provide consultation on the best contractor who provide forensic investigation
18	Provide consultation on how to request from third parties the following: • security documentation for any equipment or services • Risk management and security governance

	in the National Cryptographic Standards (NCS-1:2020).
13	Certification authority and issuance capability in a secure manner, or usage of certificates from a trusted certification authority
14	Send Notification to CSTs of identified vulnerabilities that may affecting them, and safeguards in place.
15	Subscribing in authorized and specialized organizations and groups to stay up to date on cybersecurity threats, common practices and key know-how
16	Subscribing in authorized and specialized organizations and groups
17	Contract with company to perform forensic investigation (if needed)
18	Request from third parties to provide: • security documentation for any equipment or services • Risk management and security governance

3.4 Finalize Phase

This is the last phase of the project, during which the following activities will take place

Trusted Vision Activities	
No	**Activity**
1	Conduct 3 cybersecurity awareness workshops for cybersecurity roles and RACI assignment
2	Perform cybersecurity audit against NCA-CCC-P
3	Ensure Data sanitation and secure disposal for end-user devices, especially for those with exposure to the Cloud Technology Stack
4	Perform two penetration test for Cloud Technology Stack
5	Perform testing the incident response capability
	Perform training for company employees and third-party personnel to respond to cybersecurity incidents, in line with their roles and responsibilities

CLIENT Activities	
No	**Activity**
1	Coordinate the 3 cybersecurity awareness workshops
2	Review and implement all required actions to comply with NCA-CCC-P
3	Perform Data sanitation and secure disposal for end-user devices, especially for those with exposure to the Cloud Technology Stack
4	Review and approve penetration testing report
5	Coordinate incident response testing
6	Coordinate training

4. Project Scope and Assumptions

4.1 Out of Scope

1. Implementing technology proof of concept
2. Any other service that has not been clearly mentioned in the previous section(s) shall be considered out of scope.
3. Developing RFP for any solution or tool

4.2 Scope Assumptions

1. All deliverables will be in English Language
2. All activities will be conducted during the project timeline which is six (6) months.
3. Trusted Vision is not responsible if a delay has occurred from the client side.
4. The client will be committed to the Project Timeframe and will take responsibility if any delay has occurred on their side.
5. Cooperation from executives, departments heads and all Client staff shall be demonstrated and be committed to the timeline of this project.
6. Each task will be performed during the project time, Trusted Vision is not responsible if the client has delayed any of the tasks or has any circumstances.
7. The proposal includes only one review of the submitted documents.
8. An AI bot will be added to record and summarize conversations, aiming to assist consultants in improving and developing meeting minutes.
9. 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.

5.1 GRC Orbit Technical Proposal

5.1.1.1 Introduction

Trusted Vision Company is pleased to present its technical and financial proposal related to the Governance, Risk Management and Compliance System "GRC Orbit". This system was designed to meet the needs of the Saudi market and to enable in the Cybersecurity staff - and other departments staff - to set the necessary controls for cyber security governance, management, cyber security risk management, compliance with legislative, contractual and internal requirements.

5.1.1.2 Objectives

By developing the GRC Orbit system, we aim to improve the processes related to governance, risk management and compliance through:

1- Automation of governance, risk management and compliance processes
2- Getting rid of complex work files that exhaust the entity's employees by placing everything related to governance, risk management and compliance matters (external standards and frameworks, policies, procedures, risks, audits, compliance rates, follow-ups) on the GRC Orbit system
3- Transferring the expertise of the consultants in the field of governance, risk management and compliance, and placing it in the GRC Orbit system
4- Providing content related to cybersecurity, such as local and international standards and legislation, and elements of information security risks

5.1.1.3 Benefits obtained from the GRC Orbit system.

The GRC Orbit system has been developed to meet business needs related to governance, risk management and compliance within organizations. The following are the most important benefits and advantages obtained when acquiring this system:

1 Manage all risks of the organization (risks related to cybersecurity and risks of other departments as well) according to the risk management methodology approved within the organization
2 Dealing with all risks of the organization and following them up in real time
3 Promoting the culture of governance and risk management within organizations
4 Promoting the principle of accountability by assigning responsibilities to the relevant parties and monitoring them on an ongoing basis
5 Take decisions based on accurate information
6 Monitoring compliance with the policies and legislation that the organizations comply with
7 Managing cyber security incidents and monitoring them until they are closed

8 Auditing internal policies or external standards, following up problems with relevant parties and involving them in the audit process

5.1.1.4 The main features of the GRC Orbit system

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

1. Supports both Arabic and English languages
2. Comprehensive Dashboards in Governance, Risk Management and Compliance
3. Measurements of performance indicators
4. The possibility of integration with Active Directory system
5. The possibility of integration with multi factor authentication tool
6. The possibility of integration with the organization's file management system File Management System
7. The possibility of integration with the organization's e-mail system, Email Gateway
8. The possibility of installing the system on the company's internal servers or on a Saudi cloud service provider

5.1.1.5 Major Components of the GRC Orbit System

The GRC Orbit system consists of six main modules as shown in the figure below.

5.1.1.6 Governance Module

The Governance module consists of international and local standards and frameworks, which are continuously updated by our technical team. Focus has been placed on local standards and frameworks related to the Kingdom of Saudi Arabia, such as:

1. National Cybersecurity Authority (NCA) which includes ECC, TCC, DCC, OSMACC, OTCC and CCC
2. Saudi Central Bank – CSF, BCM and ITG
3. Capital Market Authority Cybersecurity Guidelines
4. Communication, Space and Technology Commission cybersecurity standards
5. Saudi Aramco Cybersecurity Standards
6. ISO 27001 – Information Security Management System
7. National Institute of Standards and Technology – Cybersecurity Framework

Work is underway to add other local and international standards so that organizations can measure compliance, follow up on the status of controls, and take the necessary actions to ensure that the requirements of these standards are met.

Figure (1) below shows the local and international standards that have been added to the tool

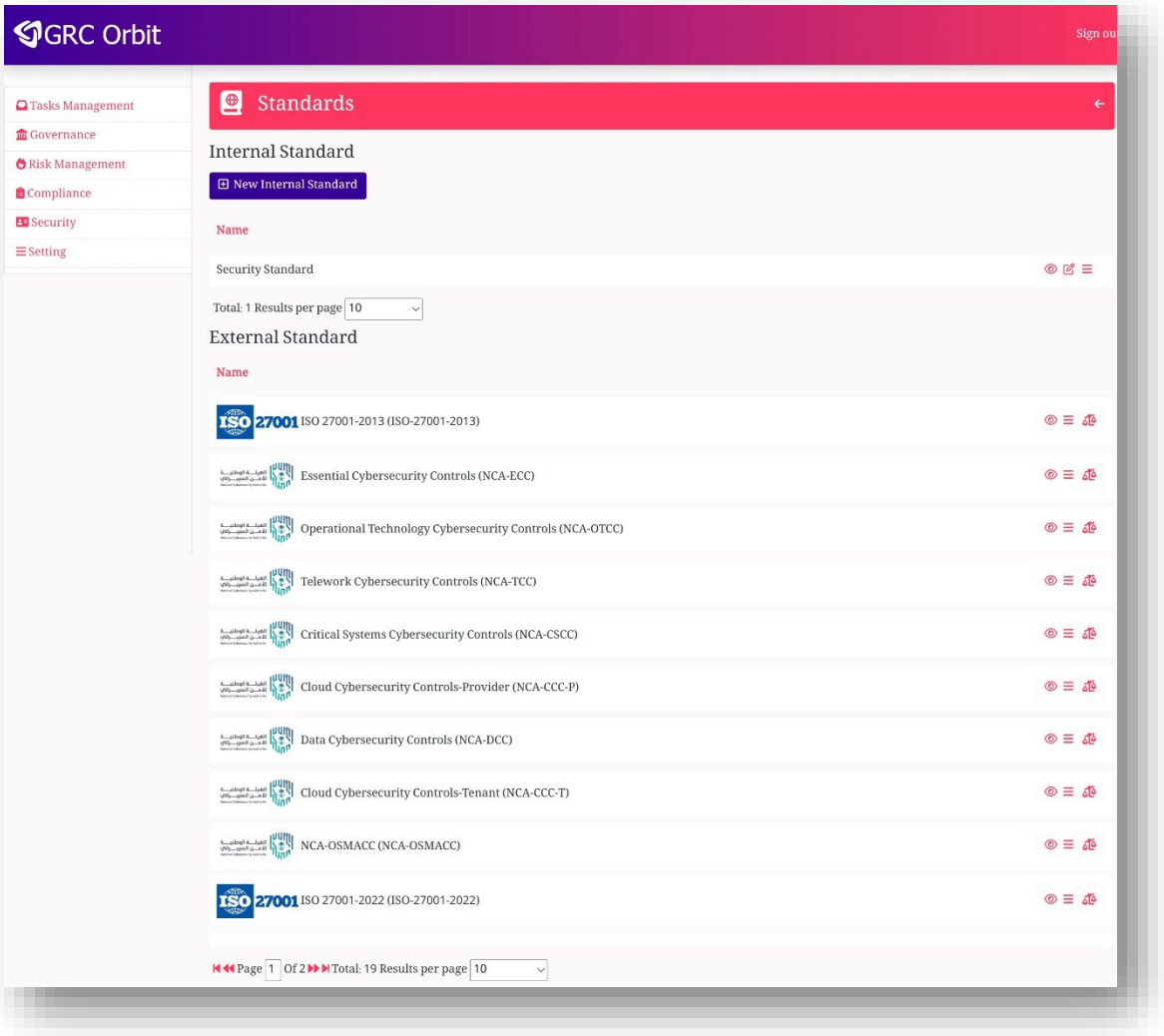


Figure (1) Examples of local (National Cybersecurity Authority) and international standards (ISO 27001) added in the system.

The system also contains the internal policies and procedures followed by the organization, which can be added as in Figure (2).

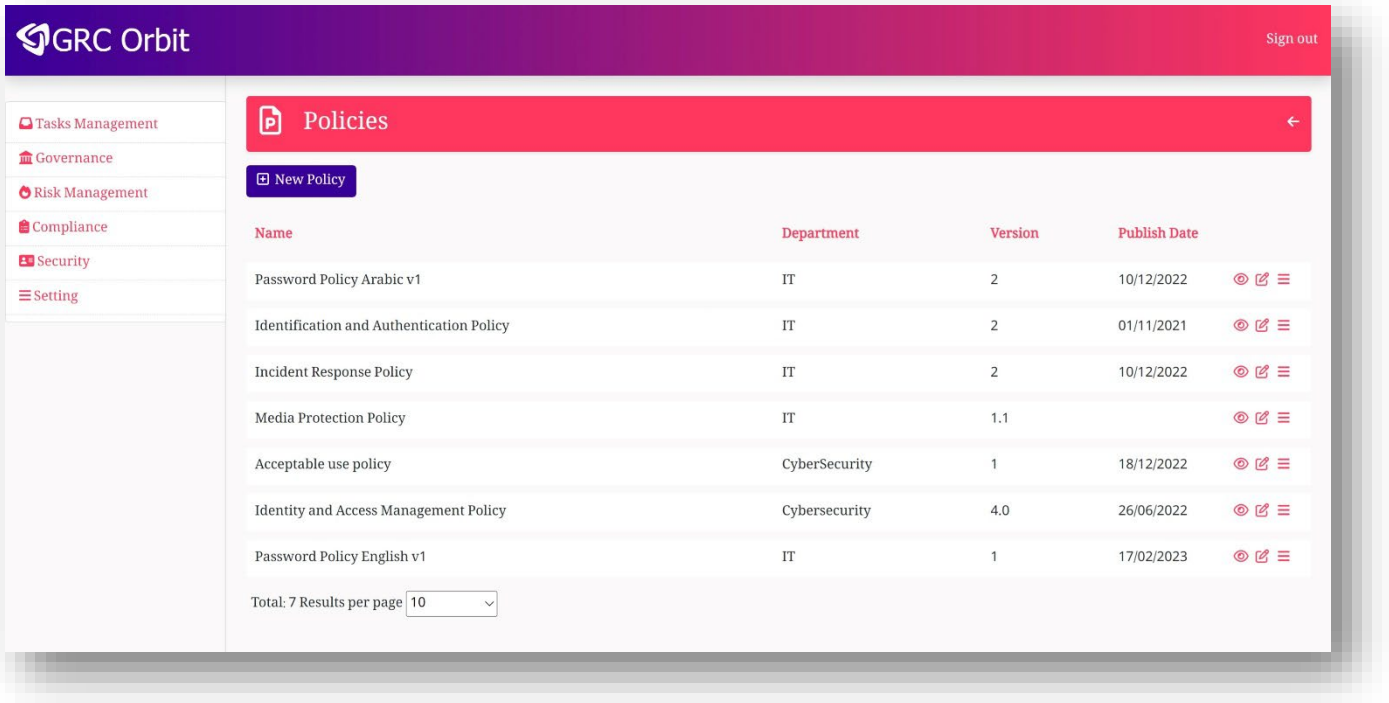


Figure (2) Examples of internal policies added in the system.

The system owner can also create requests to review internal policies and procedures, take comments and visuals on any modification that occurs, and record these views in a record that is displayed to the owner of the policy or standard, as in Figure 3 and 4.

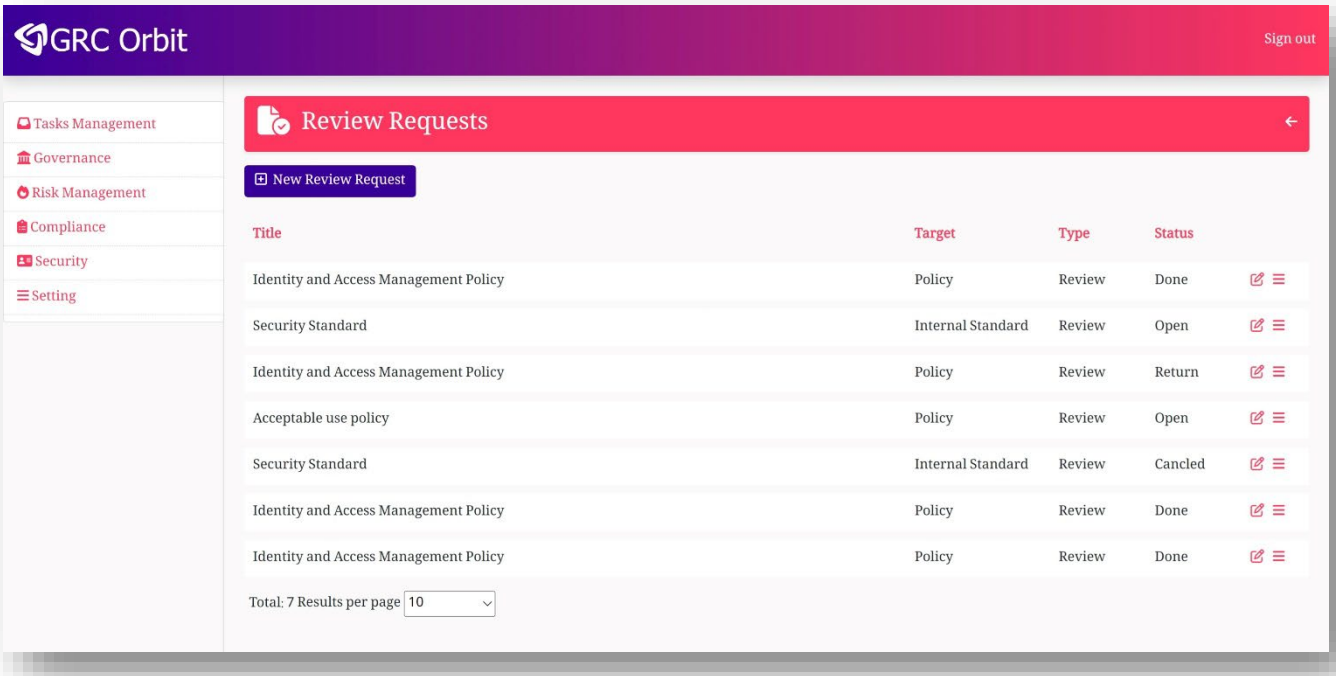


Figure (3) Examples of the status of internal policies and procedures

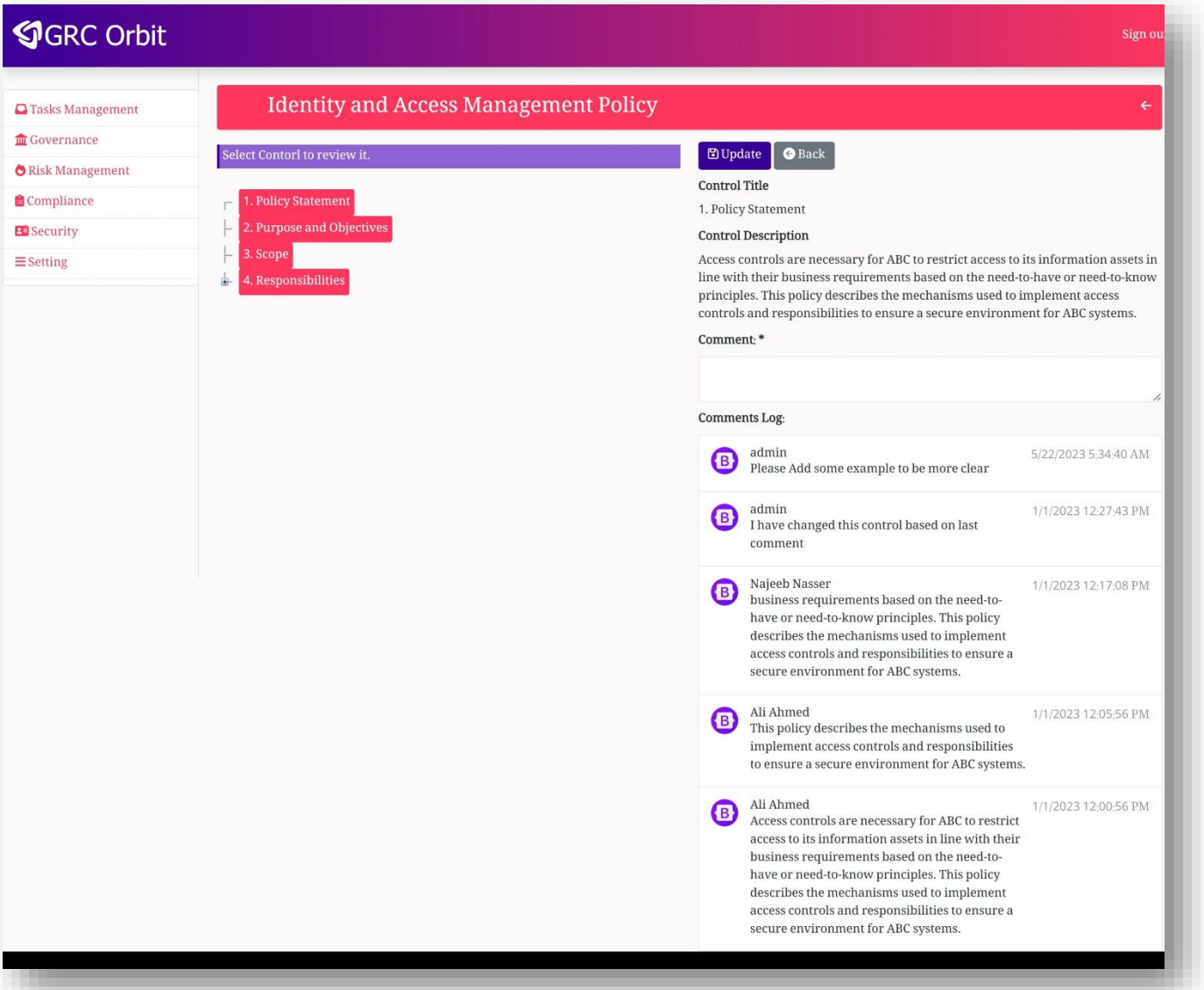


Figure 4 Examples of policy review

5.1.1.7 Risk Management Module

The risk management unit enables the management of all risks of the organization - including cyber security risks - based on the risk management methodology approved by the organization.

To help organizations adopt a risk management methodology, a ready template for information security risk management has been designed based on the ISO 27005 methodology as in Figure 5 to 9

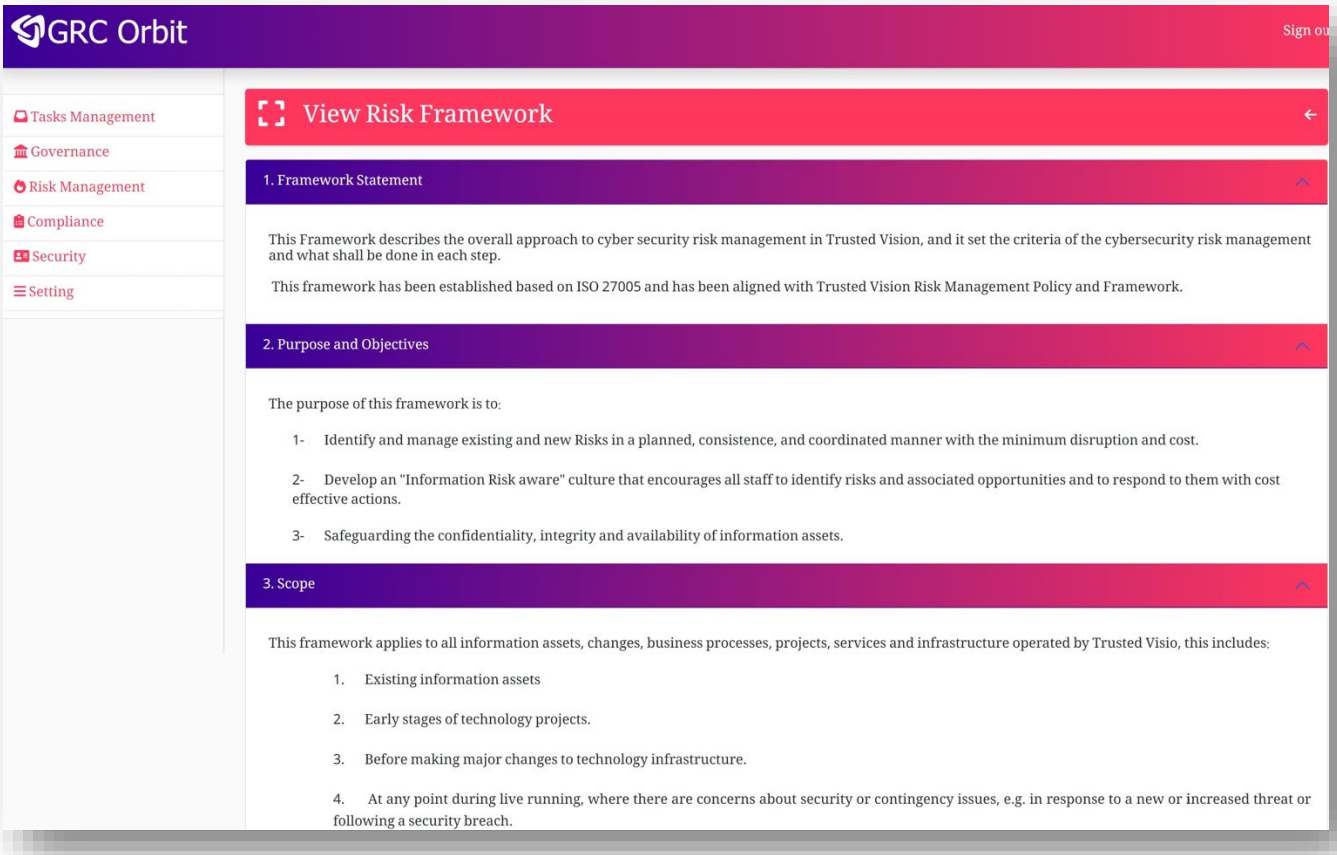


Figure (5) Examples of the status of internal policies and procedures

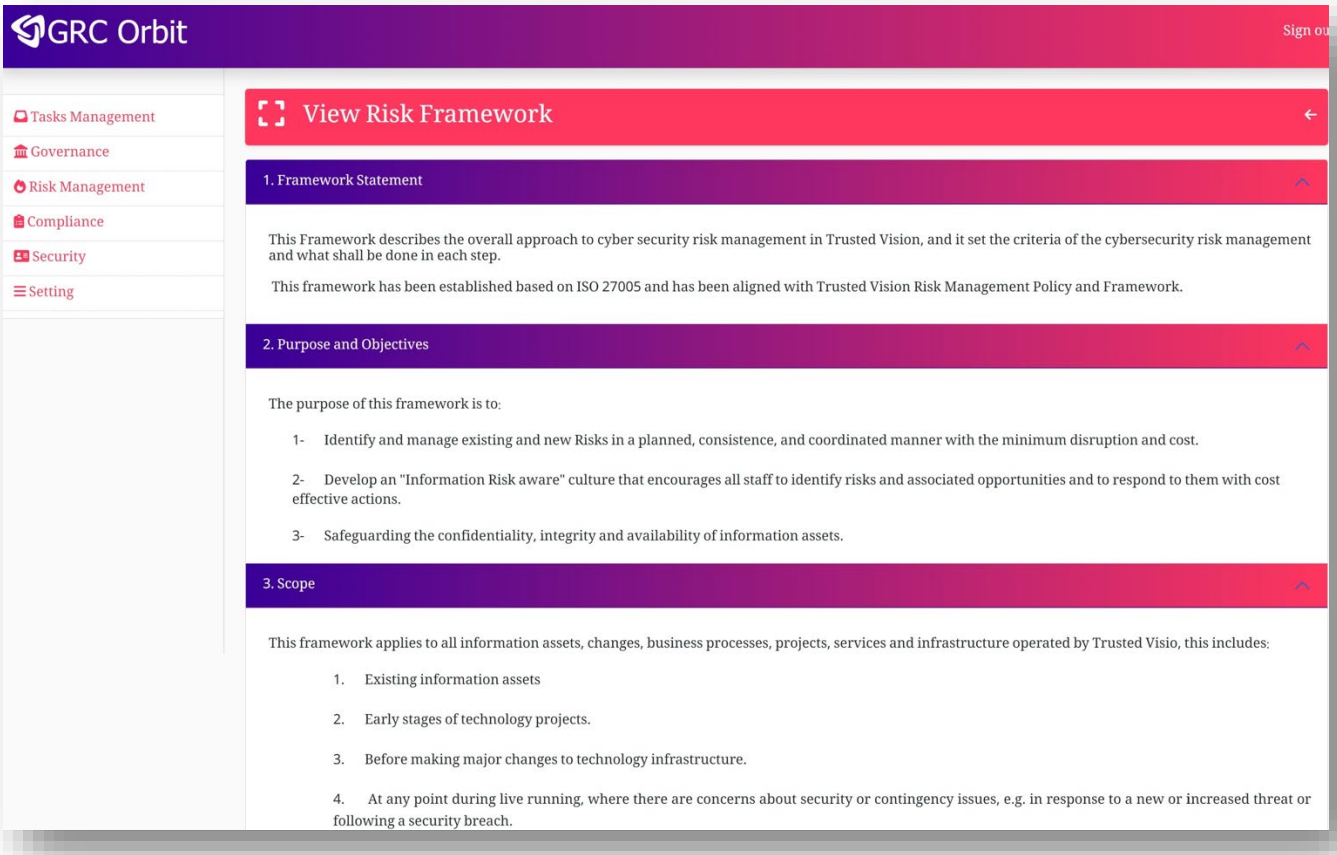
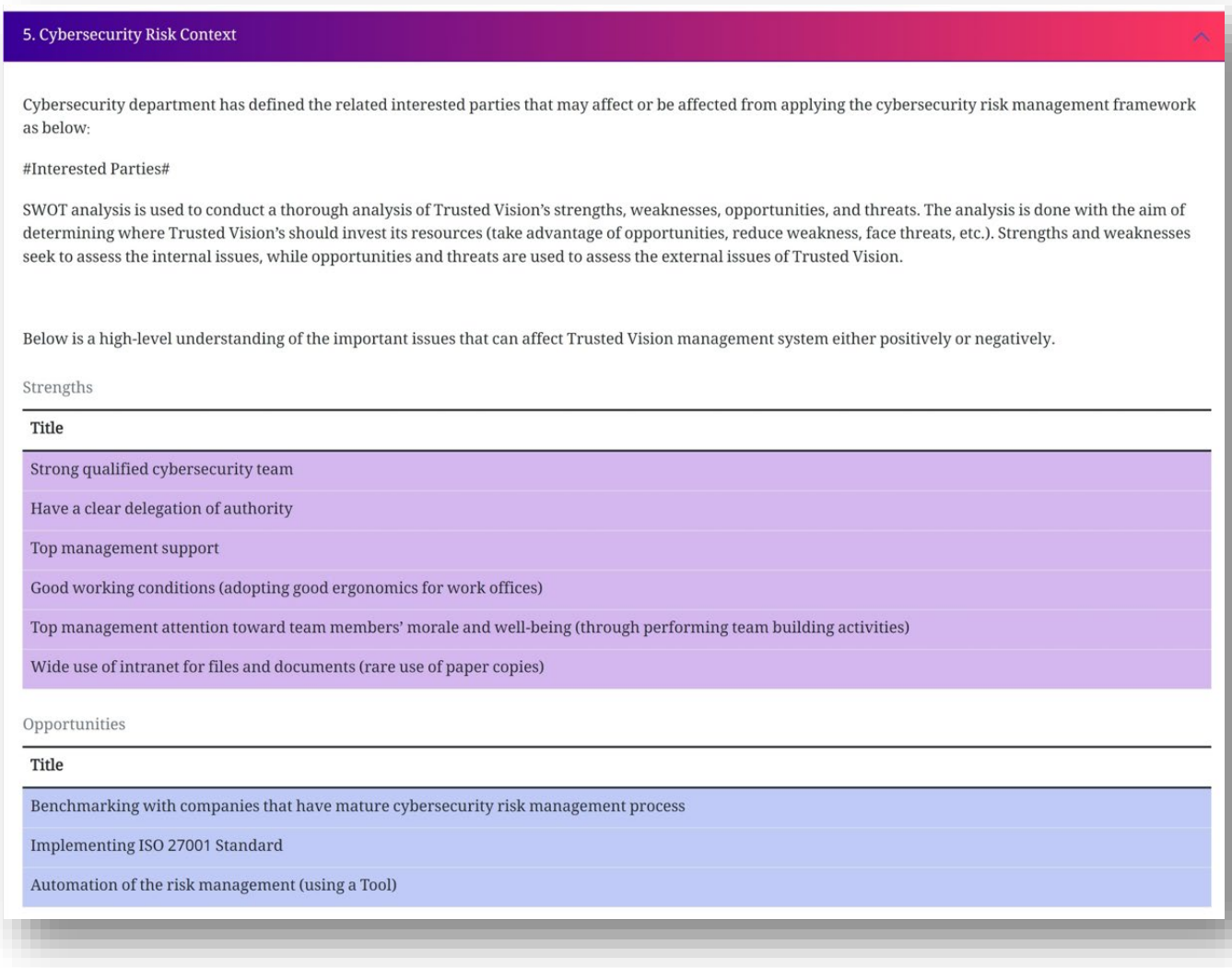


Figure (6) ISO 27005 information security risk management methodology



5. Cybersecurity Risk Context

Cybersecurity department has defined the related interested parties that may affect or be affected from applying the cybersecurity risk management framework as below:

#Interested Parties#

SWOT analysis is used to conduct a thorough analysis of Trusted Vision's strengths, weaknesses, opportunities, and threats. The analysis is done with the aim of determining where Trusted Vision's should invest its resources (take advantage of opportunities, reduce weakness, face threats, etc.). Strengths and weaknesses seek to assess the internal issues, while opportunities and threats are used to assess the external issues of Trusted Vision.

Below is a high-level understanding of the important issues that can affect Trusted Vision management system either positively or negatively.

Strengths

Title
Strong qualified cybersecurity team
Have a clear delegation of authority
Top management support
Good working conditions (adopting good ergonomics for work offices)
Top management attention toward team members' morale and well-being (through performing team building activities)
Wide use of intranet for files and documents (rare use of paper copies)

Opportunities

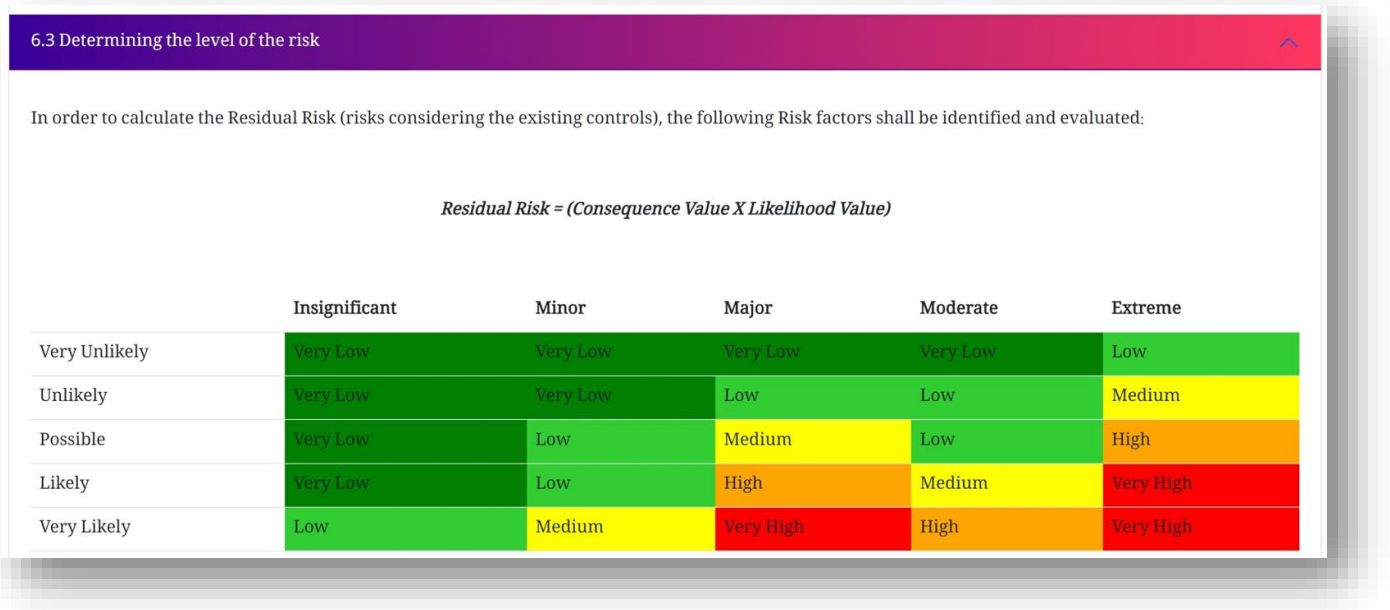
Title
Benchmarking with companies that have mature cybersecurity risk management process
Implementing ISO 27001 Standard
Automation of the risk management (using a Tool)

Figure (7) ISO 27005 Information Security Risk Management Methodology - Analysis of Strengths, Weaknesses, Opportunities and Threats

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.

Figure (8) ISO 27005 Information Security Risk Management Methodology - Integrity Impact Analysis



6.3 Determining the level of the risk

In order to calculate the Residual Risk (risks considering the existing controls), the following Risk factors shall be identified and evaluated:

Residual Risk = (Consequence Value X Likelihood Value)

	Insignificant	Minor	Major	Moderate	Extreme
Very Unlikely	Very Low	Very Low	Very Low	Very Low	Low
Unlikely	Very Low	Very Low	Low	Low	Medium
Possible	Very Low	Low	Medium	Low	High
Likely	Very Low	Low	High	Medium	Very High
Very Likely	Low	Medium	Very High	High	Very High

Figure (9) ISO 27005 Information Security Risk Management Methodology - Risk Heat Map

The system also includes the appropriate procedures for identifying, analyzing, evaluating, dealing with and monitoring the risk, as in Figures 10, 11 and 12.

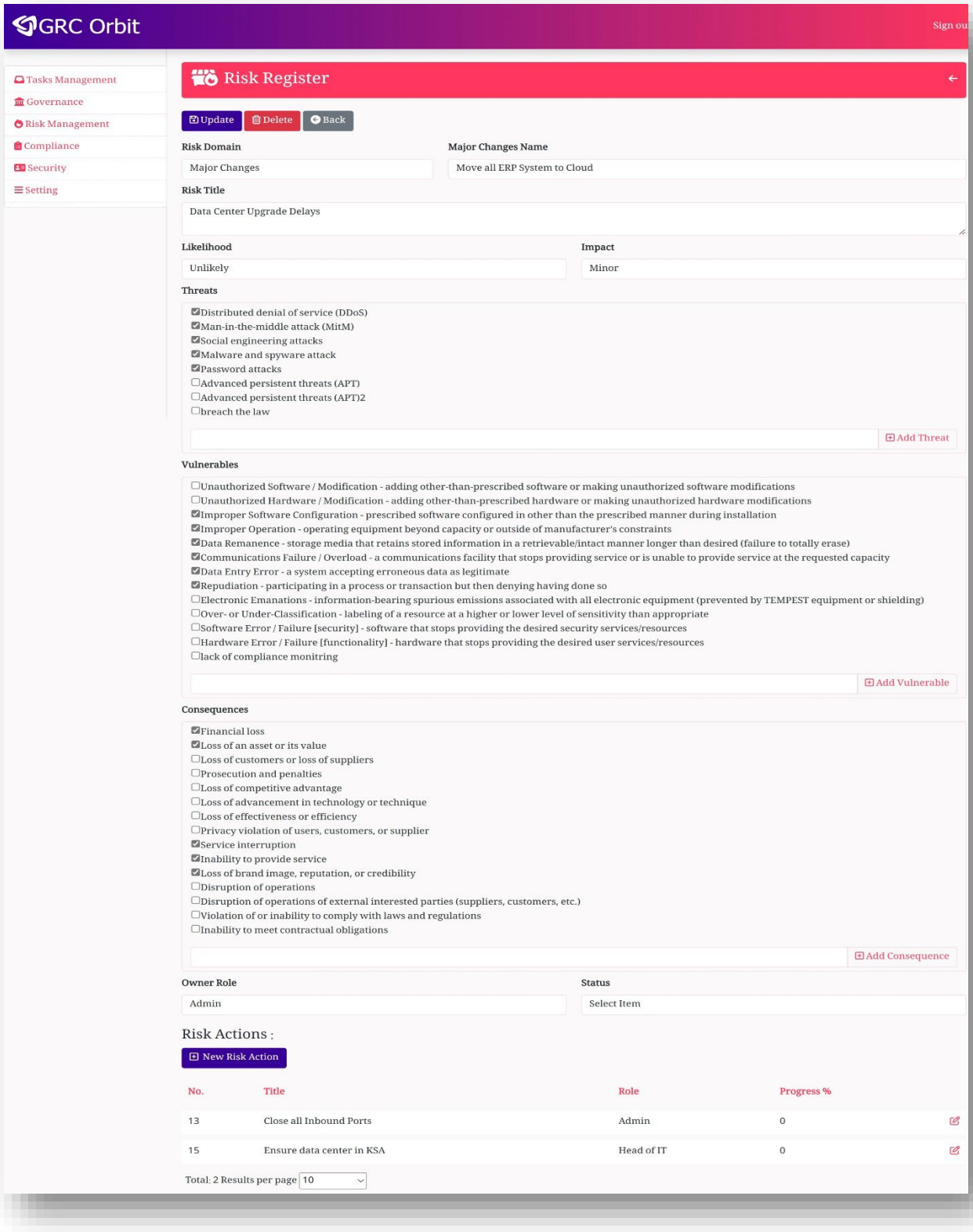


Figure (10) An example of risk identification and analysis

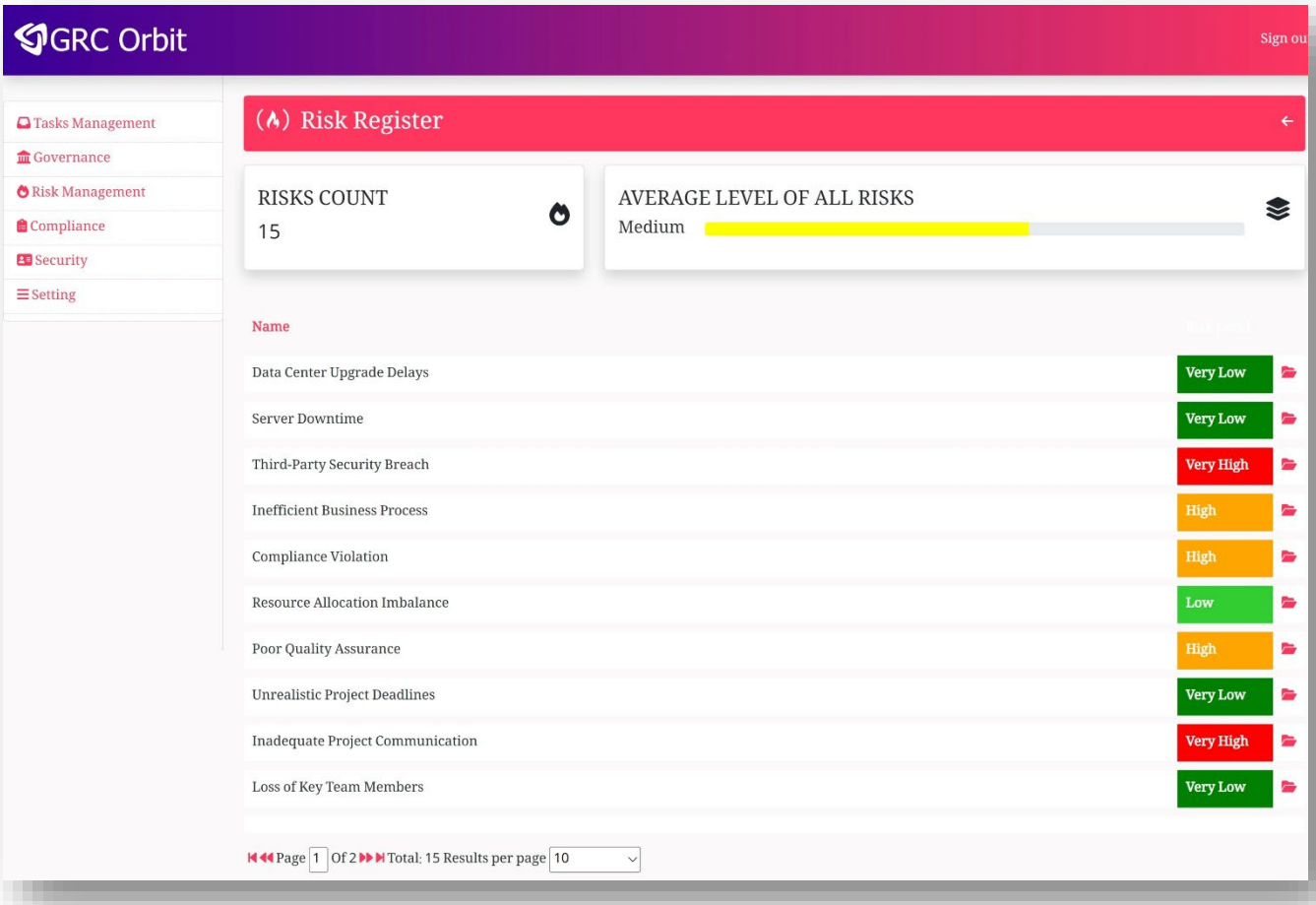
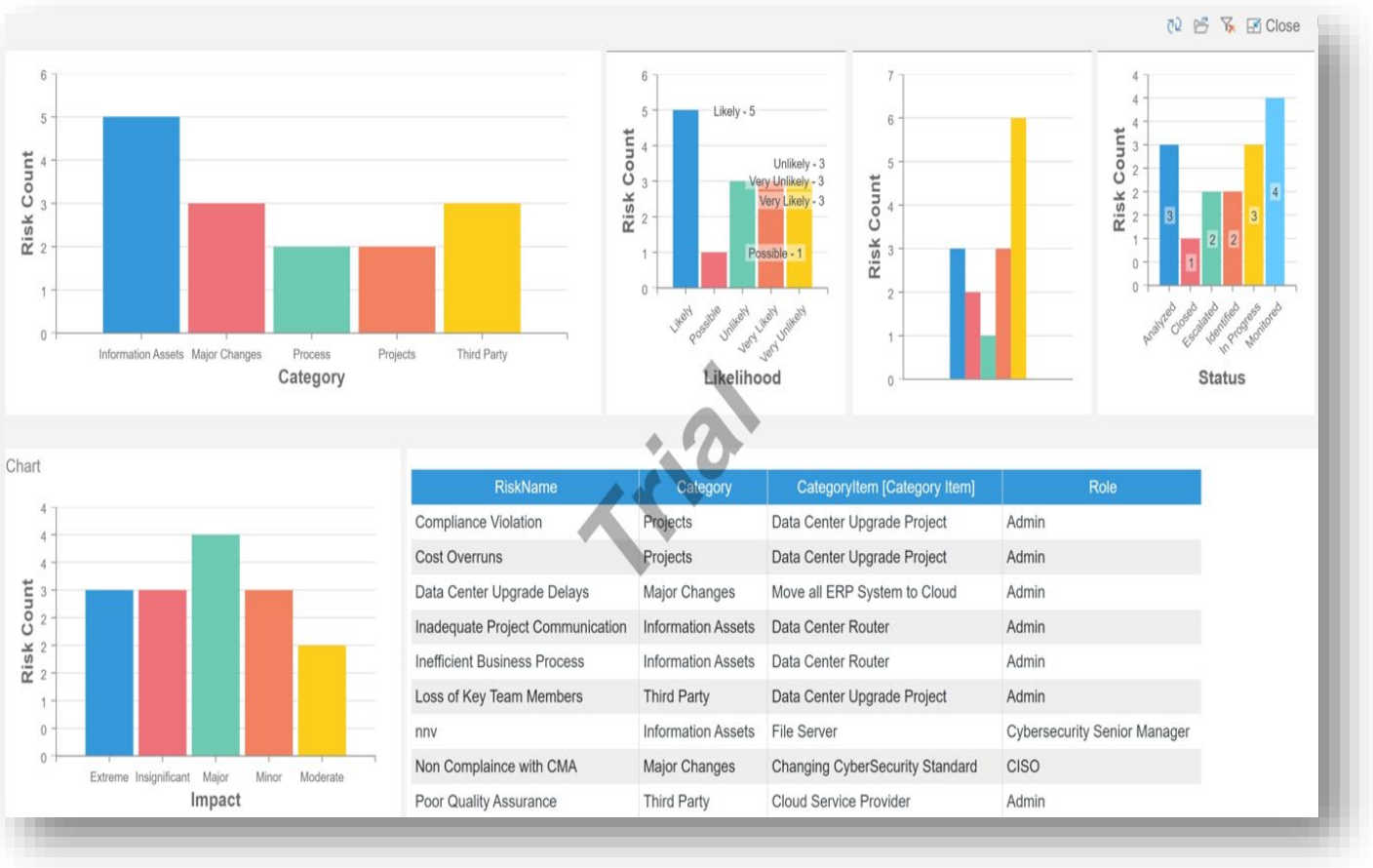


Figure (11) Information security risk register



RiskName	Category	CategoryItem [Category Item]	Role
Compliance Violation	Projects	Data Center Upgrade Project	Admin
Cost Overruns	Projects	Data Center Upgrade Project	Admin
Data Center Upgrade Delays	Major Changes	Move all ERP System to Cloud	Admin
Inadequate Project Communication	Information Assets	Data Center Router	Admin
Inefficient Business Process	Information Assets	Data Center Router	Admin
Loss of Key Team Members	Third Party	Data Center Upgrade Project	Admin
nnv	Information Assets	File Server	Cybersecurity Senior Manager
Non Complaince with CMA	Major Changes	Changing CyberSecurity Standard	CISO
Poor Quality Assurance	Third Party	Cloud Service Provider	Admin

Figure (12) A comprehensive dashboard of information security risks

5.1.1.8 Compliance Module

The Compliance module enables audits of internal policies and procedures in addition to local and international standards and frameworks. Where, during the audit process, the necessary evidence is taken based on each control or item within the policy or standard, and then the percentage of total compliance with these standards and policies is measured. Figure 13 below shows a list of audits that have been implemented.

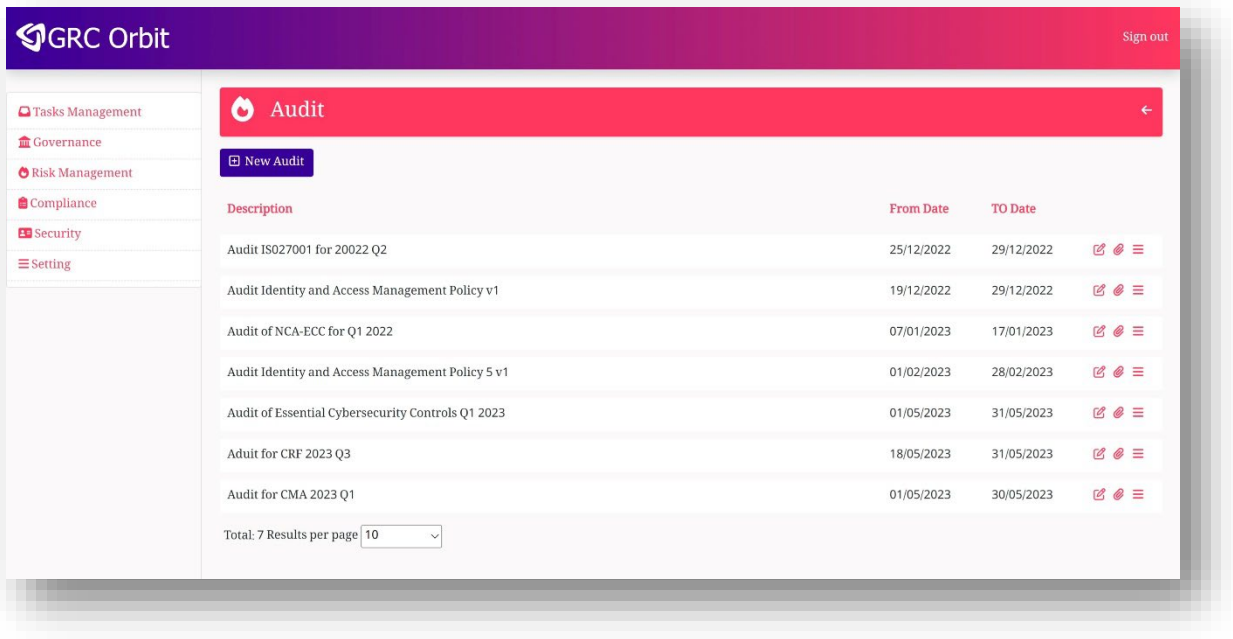


Figure 13 is an example of a list of audits.

The Compliance module also allows for an assessment of local and international standards based on previously identified questions in order to measure the level of compliance and maturity related to this standard, as the assessment includes ISO 27001 standard and the basic controls for cybersecurity NCA-ECC only, as shown in Figure 14 below.

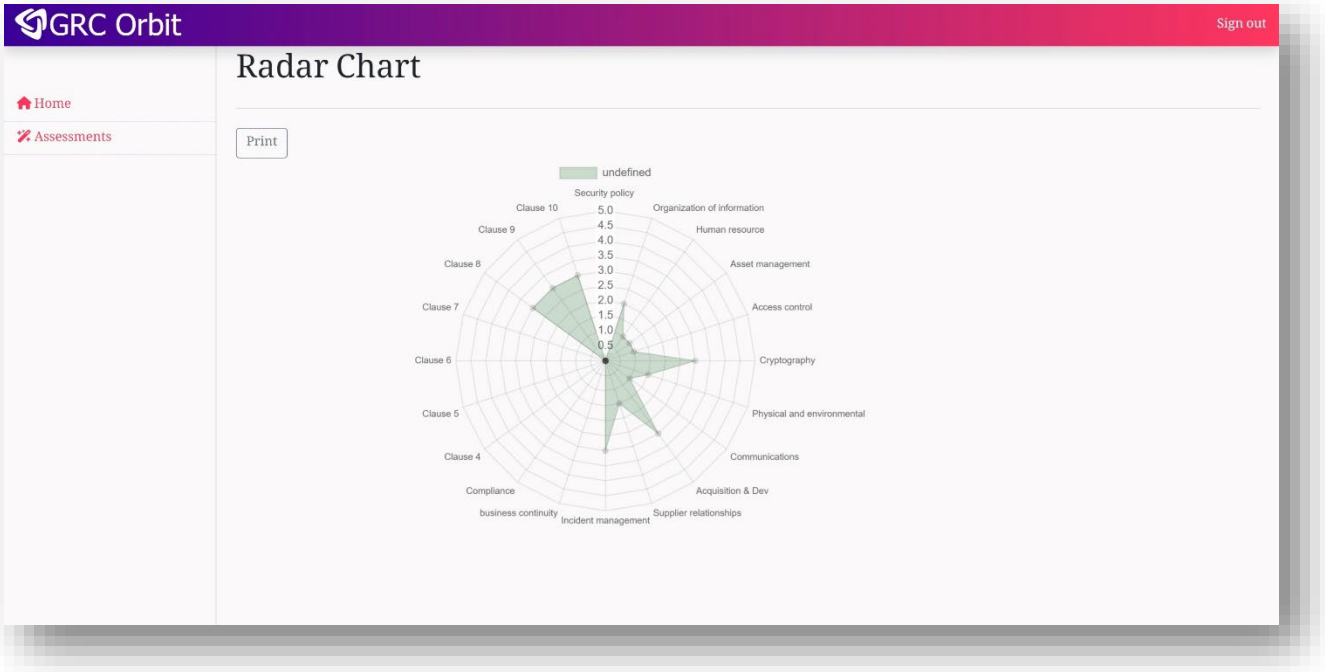


Figure (14) An example of the compliance form resulting from the evaluation process.

5.1.1.9 System installation requirements

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

1. Microsoft SQL Server database system
2. IIS Web Server service
3. Dot Net Framework

5.2 Terms and Conditions

1. This offer is valid for 1 month.
2. The client has the right to stop or exit from the contract at any stage, which and in this case, we have the full right to receive the full payment of the phase whether it is completed or not.
3. All services scope of work as per the technical proposal.
4. For Any delay that is caused by the company, 1000 SAR has to be paid for each day of delay after the end of the agreed end date between both parties.
5. Attending meetings are mandatory for each party and stakeholder in this project.
6. Cooperation with the consultants is mandatory.
7. All deliverables to the client will have 3 days period for their review and approval, if the time is due without any official reply, it is considered as approved deliverable.
8. The proposal includes only one review of the submitted documents.