International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

Adopting Government Cyber Security Initiatives - A study of SMEs in Saudi Arabia

Mohammed Abdulwahab Alghamdi, Salem Awad Salem Alomari*, Mohammed Alkatheri

Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

*salmalomry@gmail.com

Abstract

The study, which targeted SMEs, aims to determine the risks to cybersecurity in these institutions and implement countermeasures to reduce these risks, such as regulatory, material and technical measures.

The study relied on the method of applied research, through a comprehensive questionnaire consisting of several departments targeting more than 60 institutions. For the purpose of data analysis, we used the Information Security Governance (ISG) assessment tool to measure the extent of conformity of implementation and actual documentation the requirements of the standard specification for SMEs in Saudi Arabia.

The study reached several results, the most important of which is that cybersecurity in SMEs is exposed to many risks and threats, and that there is a weakness in legislation and laws that protect cybersecurity and the lack of written policies of most institutions participating in the questionnaire confirms the extent of this weakness.

We have seen that the role of the national cybersecurity authority in the Kingdom of Saudi Arabia is good but needs to make more practical efforts to enhance cybersecurity inside and outside institutions.

At the end of the study, we presented a framework that contains the most prominent international standards for building safe cyber institutions, which include standards for risk management, risk reduction and response, work environment security, access control, communication security, physical security, external relations, and employee awareness training.

Keywords: Cybersecurity, Security of SMEs, Cyberspace.

Chapter One: Project Outlines

Introduction

This project aims to create a cybersecurity framework based on the outputs of the questionnaire, interviews, etc. that were directed to the SMEs in Saudi Arabia. The questionnaire was divided into a set of sections, with each section containing a set of questions. All these sections are related to the cybersecurity. Special focus was made on the points that didn't have clear answers by these institutions, in order to guide them on the best practices and to deliver the right security guidance, which could be used by the different SMEs to enhance their security posture and protect them from different security threats. The framework was based with reference to standard procedures that are accepted by the cybersecurity community worldwide.

This project pays special attention to assist SMEs in Saudi Arabia to assess their cybersecurity situation; and review possible ways to enhance their security and to provide a coherent roadmap and mechanisms for implementing and achieving the national vision on cybersecurity in these institutions. So that they become safe, vibrant, resilient, and reliable institutions that protect their assets and interests and promote participation in cyberspace for economic prosperity.

Problem Statement

The I (TS) [2] Company, the first managed security services provider in Saudi Arabia in 15 years. Indicated that 49% of cyber phishing attacks are primarily directed at small institutions, followed by medium [1].

Ponemon Institute, which specializes in information security, revealed that 64% [2] of the medium and small institution in the Saudi Arabia do not have security policies that make them able to confront breaches and phishing. So, there is a big gap separating institutions from following security standards and procedures, and not all institutions have solid cybersecurity framework to follow in their work. This will negatively affect the institutions' business and the performance of its employees. Additionally, there is lack of auditing on the state of security and the performance of employees, and the absence of deterrent actions that stops the employees from breaking the security procedures, and also the lack of awareness of the employees and stakeholders regarding the recommended security procedures must to follow within the institutions.

Through our research that targeted 64 SMEs, we found that 76.6 % of the institutions did not deal with government agencies regarding cybersecurity, and that 46.9% had absolutely no written strategy for cybersecurity. and that 46.9% do not have any ongoing training program to build skills and competencies for cybersecurity.

So the results are worrying, and we will list the impact of cyber risks on institutions in particular and national security in general:

- The sabotage operations that hit some websites.
- Fraudulent practices.
- Electronic blackmail.
- Exploitation occurs online, especially when employees are not aware.

- Economic sabotage by denying citizens access to governmental and non-governmental electronic services.
- Coordinated electronic espionage.
- Malicious interference with computer systems and other digital devices.
- Electronic hacking.
- Theft of intellectual assets.
- Electronic terrorism.
- Online financial.
- Money laundering.
- Denial of service.

All of these things are inconsistent with the development and advancement policy of any institution and have the economic impact that would be enough to destroy any institution.

Research Questions

Therefore, the aim of the project is to understand the extent to which the small and medium-sized companies in the Kingdom of Saudi Arabia implement the principles of cybersecurity and thus the research questions are:

1. What is the extent of the implementation of SMEs in the Kingdom of Saudi Arabia on the principles of cybersecurity?
2. What is the minimum number of cybersecurity requirements that must be implemented by SMEs in Saudi Arabia?
3. What is the proposed cybersecurity framework for SMEs in the Kingdom of Saudi Arabia?

Objectives

The main objective of this project is to assess the situation of SMEs in the Kingdom of Saudi Arabia, and to assist them in applying best practices to maintain their cybersecurity, based on internationally recognized frameworks such as COBIT, ISO and NIST. The framework addresses security requirements in terms of integrity, confidentiality and availability of information.

Definition of Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from defended against damage, unauthorized use or modification, or exploitation [3].

Types of Cyber Security Threats:

- **Ransomware:** It is a malicious program that restricts access to the computer system that infects it, and demands a ransom payment for the program maker in order to access files.
- **Phishing:** An attempt by hackers to gain critical information about victim such as credit card details by showing themselves as a trusted entity in an electronic connection.
- **Social engineering:** Defined as tricking people into obtaining data, information or money that should be private and safe.
- **Malware:** It is software that is intentionally included in a computer system for malicious purposes, without the owner's consent. It may be used to disrupt computer operation, collect sensitive information, or access private computer systems.

What are the Cyber Risks?

Cyber risks are the possibility of a threat and fragility within an organization's cyberspace, which harms the security, safety, and availability of information systems and basic infrastructure.

The following are definitions of key elements in information security, that we seek to achieve:

Table (1): Key Elements In Information Security

Key	Definition
Confidentiality	The data element that will provide a reliable, consistent and repeatable value for confidentiality would be the asset's data classification rating. This typically reflects the sensitivity of the data stored, processed, or transmitted by the asset and if it has been accurately reported to the assessor [4].
Integrity	Ensure that no unauthorized transformation of information occurs while the information is under the custody of enterprise LANs [5].
Availability	Ensure that the system is reliable and available with uninterrupted access to authorized users.
Non-repudiation	Certainty that someone has done something related to information and its inability to deny that it actually did this work.

Importance of the Project

- Search how to determine the actual security level of a company.
- provide quick, immediate and easy way to make security assessment for SMEs.
- To regulate and empower the cybersecurity practices of the SMEs.
- To increase the overall cybersecurity maturity level of the SMEs.
- To define an overall set of cybersecurity requirements that shall be implemented in SMEs.
- To achieve confidentiality, integrity, and availability in SMEs.
- To encourage the SMEs to apply best practices for cybersecurity measures.

- Cooperating with the National Cybersecurity Authority (NCA) in Saudi Arabia to achieve vision 2030.

Scope:

In this search, we provide a comprehensive set of cybersecurity requirements that must be implemented by the SMEs in Saudi Arabia to fulfill the minimum-security requirements. By establishing a security operation document we will target SMEs in Saudi Arabia; such as ISPs (Intranet Service Providers) and any other organization that at least have a website, a facebook page, or private email that they use to offer services to their clients. Also, the cybersecurity framework will include the following levels: management level, technical level, stakeholders and clients.

Project Plan

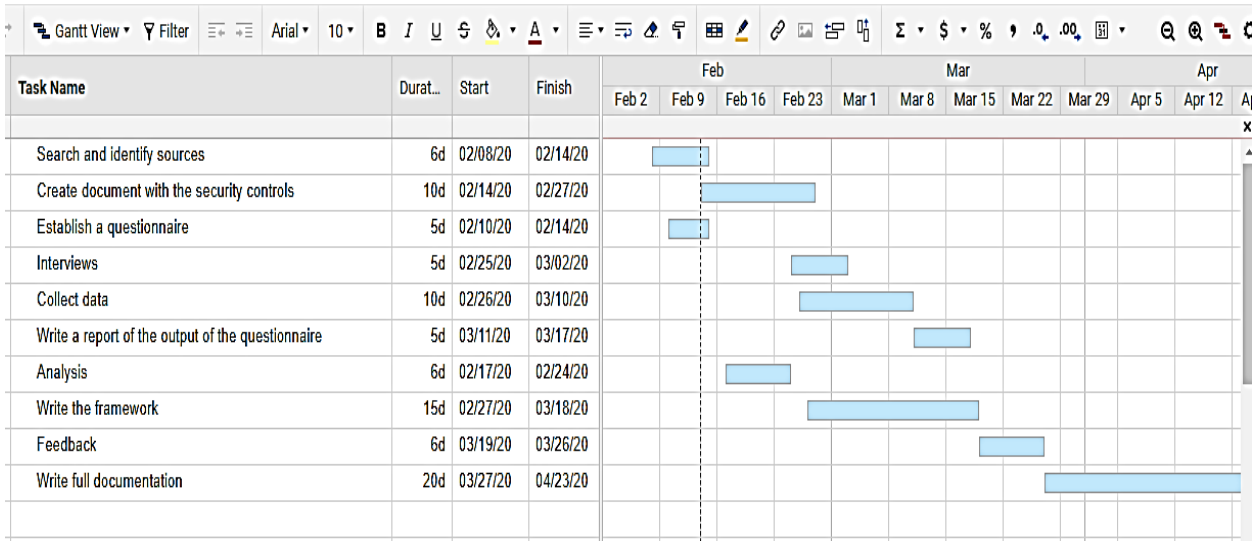

Figure (1): Project Plan

Chapter Two: Literature Review

2.1 Introduction

With the beginning of the era of computers, crime related to computers caused physical damage to devices or infrastructure. In the 1980s, the path changed to target computer software using malware, and with the advent of the Internet and its availability in 1996, e-crime expanded and its spread became wider. Every second, about 25 computers became a victim of cyberattack and about 800 million people were affected by it until 2013 [6]. This number is very conservative because most cases have never been reported.

Cybersecurity frameworks contains a set of technical, guidelines, organizational and administrative means that are used to prevent unauthorized use, misuse of exploitation and restore electronic information and communication and information systems that contain it with the aim of ensuring the availability and continuity of the work of information systems and enhancing the protection, confidentiality and privacy of personal data and taking all necessary measures to protect citizens and consumers from the dangers in cyberspace. So cybersecurity is a strategic weapon in the hands of governments and individuals, especially since cyber warfare has become an integral part of modern tactics of wars between countries.

Cybersecurity has become an essential part of any national security policy, as it has become known that decision makers in the United States of America, the European Union, Russia, China, India and other countries have become categorizing cyber defense/cybersecurity issues as a priority in their national defense policies. In addition to the above, more than 130 countries around the world have announced the allocation of sections and scenarios for cyber war within the national security teams [7]. All these efforts add to the traditional security efforts to combat cyber crime, cyber fraud and other aspects of cyber risks.

We study the current cybersecurity frameworks like ISO IEC 27001, COBIT, NIST and The national cybersecurity authority at saudi arabia to understand the nature of cybersecurity frameworks; to create effective strategies for SMEs used to protect their assets from cybersecurity attacks; to know the challenges that faced; and develop a framework for SMEs in Saudi Arabia.

2.2 ISO IEC 27001

ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then [8].

This framework helps companies maintain the security of their information. The ISO 27001 system is used by thousands of companies around the world and allows them to create an effective and clear system to keep confidential data so that it is safe and at the same time available to authorized users. This standard combines procedures and workforce security requirements, as well as the company's physical and technical aspects.

The International Organization for Standardization (ISO) defines ISO 27001 as follows: The ISO/IEC 27001: 2013 standard defines requirements for the establishment, implementation, maintenance and continuous improvement of a cybersecurity management system. ISO 27001 also includes requirements for assessing and addressing cybersecurity risks according to the needs of the organization. The requirements set forth in ISO/IEC 27001: 2013 are general requirements and aim to apply to all institutions, regardless of their type, size or nature.

Why is ISO 27001 Important?

Security risk management is a vital component of an effective security plan, and there are many options available to companies. Therefore, a reliable standard such

as ISO 27001 provides comprehensive general guidelines for creating a security system and information recovery plan in the event of a security breach.

The ISO 27001 standard includes all requirements necessary to investigate the company's information security risks and considers threats, vulnerabilities and potential breaches of that company. It consists of a guide to select and implement a set of data security controls, measures and procedures to manage the company's most difficult risks. It also highlights the need for continuous follow-up so that security measures are constantly updated, risks are addressed and the organization's individual information security needs are continuously met.

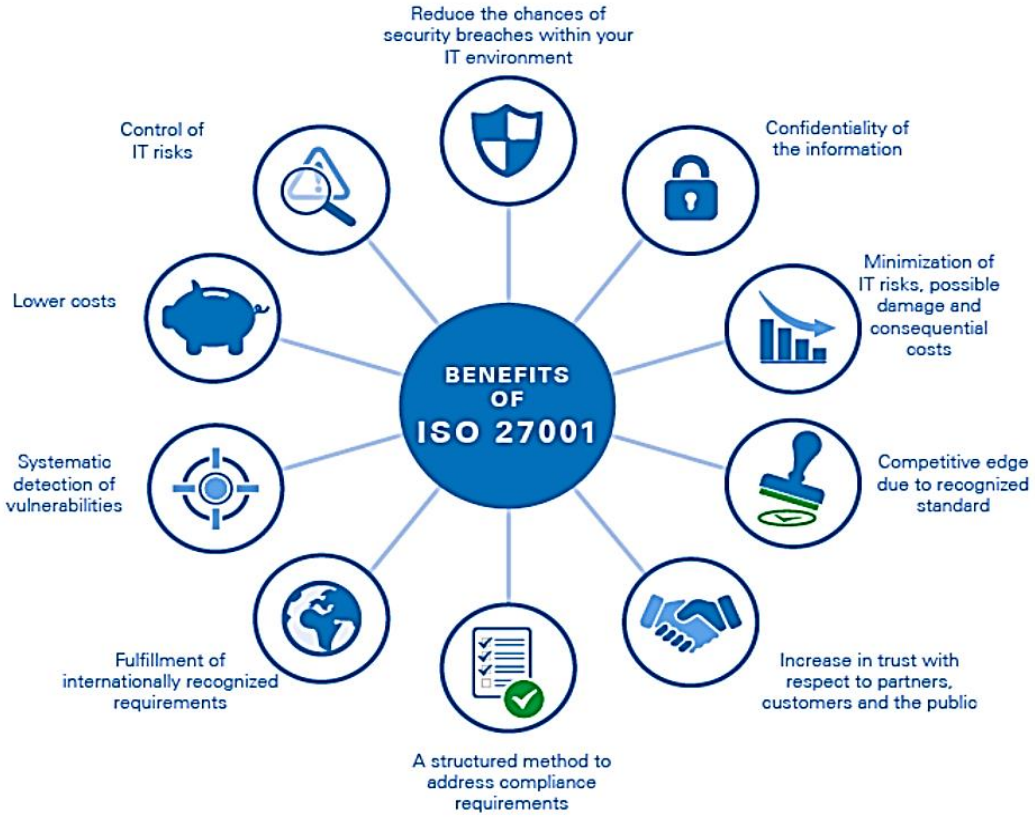

Figure (2): Benefits Of ISO 27001

If you want to implement the ISO 27001 system in order to apply for the ISO 27001 certification for marketing purposes or apply it to make the institution conform to international standards in information security management. Applying the standard returns to you with many benefits, some of which we mention in the following infographic: [9]

2.3 COBIT

COBIT (Control Objectives for Information and Related Technologies) is a cybersecurity framework that integrates a business's best aspects to its IT security, governance, and management. ISACA (Information Systems Audit and Control Association) developed and maintains the framework[10]. COBIT is a standard framework consisting of several tools that help enterprise managers to reduce the gap and reduce risks between information systems and technical needs.

This framework also helps to provide a pre-road map for communication between the activities of the information and communication systems departments with the organization's managers, shareholders and other parties that may have a relationship or interest in information systems governance.

The framework contains a set of monitoring and follow-up systems, the most important of which are:

- A basic system for linking monitoring systems, as each system contains data, inputs and outputs of the system.
- The main activity or activities for each system.
- The goals of the system.
- Performance indicators for each system.
- A general model for measuring the performance of an organization.

The COBIT framework attempts to link the organization's primary goals with business systems and the goals of the IT Department. This is done through the following:

- Standard modeling related to information systems for easy reading and implementation.
- Provide models to measure achievement and performance.
- Connecting the responsibilities and the officials of the organization at all levels up to the level of information technology systems.

The framework contains the following components:

- Planning and organizing
- Ownership and implementation.
- Delivery and assistance.
- Monitoring and evaluation.
- Characterization and maps of systems in line with previous pillars.
- Subsidiary control systems for monitoring systems and measuring performance.
- Guidance for clarifying relationships and responsibilities between work systems.
- Linking to other standard systems related to planning, implementation and follow-up.

The COBIT assist in creating a complete system of governance for work systems at the level of services provided to clients and linking them to the governance of work systems and work systems with information and communications technology.

2.4 NIST Cybersecurity Framework

The national institute of standards and technology offered a cybersecurity framework in 2014 after hold effected meetings with owners of institutions and senior officials

in the field of cybersecurity, conducted opinion polls, and workshops attended by thousands. This framework provides a guide for the different institutions from different fields to protect their systems from cybersecurity attacks includes "review of cybersecurity practices, improvement of existing security, communicating cybersecurity requirements and revising cybersecurity practices." NIST can be applicable to different institutions to keep their online platforms safe.

NIST cybersecurity framework has five core functions; identify, protect, detect, respond and recover.

Table (2): Five Core Functions for NIST Framework

Function	Definetion
Identify	with this function. The existing assets must be determined, and the priority and sensitivity of these assets must be arranged according to the strategic objectives.
Protect	supports maintaining the critical infrastructure and containing the impact of any security event that may occur.
Detect	It detects activities that may be a precursor to an event that violates the safety system.
Respond	Implement appropriate procedures regarding a cyber security event.
Recover	It is based on the existence of flexible and thoughtful recovery plans in an attempt to recover any services that were suspended or weakened due to a cyber security event. With Taking lessons from the attack that happened.

NIST is in the process of continuous development and improvement to manage cybersecurity at all levels and take feedback from audiences and experts to understand the next procedures and developments.

NIST's Cybersecurity Core Program [11]

- Research, Development, and Specification:
  - Security Mechanisms (e.g. protocols, cryptographic, access control, auditing/logging).
  - Security Mechanism Applications: confidentiality, integrity, availability, authentication and non-repudiation.

- Secure System and Component configuration.
- Assessment and assurance of security properties of products and systems.

2.5 The National Cybersecurity Authority

The National Cybersecurity Authority (NCA) is the government entity in charge of cybersecurity in the country, and it serves as the national authority on its affairs. The NCA was established in 2017. The NCA has both regulatory and operational functions related to cybersecurity, and it works closely with public and private entities to improve the cybersecurity posture of the country in order to safeguard its vital interests, national security, critical infrastructures, high-priority sectors, and government services and activities [12].

The NCA established the National Cyber Security Center (NCSC) to build a secure and flexible e-space sphere to protect the priorities of the country and its citizens. The NCSC will also be boosting the economy through enhancing cooperation with government agencies and vital installations that are sensitive to cyber-threats, responding to cyber-incidents and activating security knowledge of the situation [13].

The Most of NCA'S Prominent Achievements:

- Issuance of the national manifesto, which is known as "Strengthening Cybersecurity" with its binding rules for all parties to protect their security especially their data security [14].
- Develop policies, governance mechanisms, frameworks, standards, controls and guidelines related to cybersecurity, circulate them to the relevant authorities, follow up on their commitment to them, and update them [15].

- Licensing individuals and non-governmental organizations to engage in activities and operations related to cybersecurity determined by the authority [16].
- The launch of programs aimed at building national capacities in the field of cybersecurity. Like Cybersecurity Training Program (CyberPro) which aims at raising the competency of public-sector employees working in the cybersecurity field and recent university graduates in majors related to cybersecurity [17].
- Organization of many partnership workshops in cooperation with government agencies to raise awareness, readiness, maturity and sharing of information in the field of protection against cyber-threats at the national level [18].
- Developing performance indicators for cybersecurity, and preparing periodic reports on the state of cybersecurity in the Kingdom at the national and sectoral levels [19].

How is SMEs Responding to NCA in Saudi Arabia?

The NAC considers each entity, public or private, an essential partner in achieving the goals for which it was established. The authority has confirmed that it is the competent authority which specialized with cybersecurity in the Kingdom, and that does not absolve any public or private party or any other of its responsibility towards cybersecurity in a manner that does not contradict the authority tasks.

2.6 Comparison between ISO IEC 27001, COBIT and NIST SP 800-53 [21]

Table (3): Comparison Between ISO IEC 27001, COBIT And NIST SP 800-53

Requirement	COBIT	ISO	NIST
Comprehensive coverage	Yes	Yes	Yes
Harmonizes relevant business and compliance requirements	No	No	No
Prescriptive controls	Yes	Partial	Yes
Practical and scalable controls	Yes	No	No
Risk-based rather than compliance-based	Yes	Yes	Yes
Supported and maintained by a third party	Yes	Yes	Yes
Vetted by healthcare and industry experts	No	Yes	Yes
Open and transparent update process	No	Yes	Yes
Detailed audit or assessment guidance	Yes	Yes	Yes
Consistency and accuracy in evaluation	Partial	Partial	Yes
Certifiable for implementing organizations	Yes	Yes	Partial
Assess once and report many	No	Partial	Partial
Support for third-party assurance	Yes	Yes	Partial

Therefore, all relevant institutions shall be committed to the following: [20]

1. Enabling the authority to carry out its functions and implement its tasks fully.
2. Immediately notify the authority of any danger, threat, or breach of its cybersecurity, real or potential.
3. Implementing policies, governance mechanisms and frameworks and applying the criteria and controls approved by the authority.
4. Full cooperation with the authority.
5. Providing the authority with the documents, information, data and reports necessary to carry out its functions and tasks and enabling it to examine the devices, networks, systems and software of these entities.

2.7 Frameworks Scope, Advantages and Drawbacks: [22]

Table (4): Frameworks Scope, Advantages and Drawbacks

Framework	Scope	Advantages	Drawbacks
COBIT 5.0, Risk IT, Val IT (2012)	IT governance (COBIT) combines a business perspective and IT control model approach. Risk IT focuses on IT-enabled risk management and Val IT covers financial IT governance	• Emphasizes relationships between business and IT processes • Includes aspects of control, risk, cost efficiency and maturity • Compatible with audit procedures • Uses RACI (Responsible-Accountable-Consulted-Informed) charts presenting a detailed allocation of responsibilities	• Lack of technical details and low level practices • No description of methods to transition
SABSA (2009)	Framework for the development of a security architecture in an enterprise	• Intuitive and understandable distribution of layers • Well planned and described risk management processes and their succession, interfaces and attributes	• Lack of coverage of all aspects of IT cybersecurity at an equal detail level • The concepts covered without the required explanation, which makes it difficult to properly implement
ITIL 3.0, M_o_R (2011)	A set of practices for IT service management, combining IT services with a business perspective	• Popular and widely used description language • Recommendations based on best practices • IT service management considered in a systematic and consistent manner	• Expensive to implement • Long time to implement correctly • Neither generic nor self-sufficient, should be combined with another risk management framework
CC-ISO 15408 ver. 3.1 (2009)	International technical standard for IT cybersecurity certification of products related to IT	• Facilitates risk assessment in relation to particular assets (systems, applications, devices) • Defines different levels of cybersecurity and quality requirements	• Expensive to implement • Used mainly at the development stage • Does not support a holistic approach to the organization, but focuses only on the evaluation of a particular resource or product

Chapter Three: Methodology

This study requires an assessment of cybersecurity at the level of SMEs in the Kingdom in order to identify weaknesses in information systems, websites, networks, and data processing operations, as well as weaknesses in the infrastructure of vital information in institutions. The assessment of institutional weakness helps to assess the level of their lack of preparedness and the need to protect information infrastructure. The aim of the study is to build mechanisms for taking countermeasures that will facilitate the ability of institutions to address vulnerabilities between information systems, vital information infrastructure, and protect their future existence in cyberspace.

3.1 Curriculum and Research Method

The two researchers, using the applied research method, through field coexistence, interviews, and a comprehensive questionnaire consisting of several sections are shown in the appendix (1) were determining the degree to which of SMEs in Saudi Arabia have implemented an Information Security Governance (ISG) framework at the strategic level within their institution, and for the purpose of data analysis, we used the Information Security Governance (ISG) assessment tool to measure the extent of conformity of implementation and actual documentation the requirements of the standard specification for SMEs in Saudi Arabia. Based on this tool, a score was determined for each question of the questionnaire shown in Table No (1). The number (4) represents the highest score (fully implemented) and the number (0) represents the lowest score (not implemented).

Table (5): Scoring for questionnaire questions

Item	Score
Not Implemented	0
Planning Stages	1
Partially Implemented	2
Close to Completion	3
Fully Implemented	4

3.2 The Research Sample

After we had prepared the questionnaire, we presented it to the competent supervisor so that he ruled it. We took the notes from him and made the necessary adjustments, then we decided that the way of distributing the electronic questionnaire via Google forms in Arabic to a sample of people who have or work in small or medium companies in the Kingdom of Saudi Arabia; the selected persons have knowledge of the cybersecurity situation in their institutions so that the results are accurate and transparent. 64 institutions participated in filling this questionnaire. This task took three weeks.

3.3 Questionnaire Details

We have a questionnaire with five sections (institution information, risk management, people, processes and technology); each section has a set of related questions. Each department has a specific set of points to measure whether or not the organization adheres to cybersecurity standards and also to determine its compliance.

We made sure that the questions were appropriate for the intended institutions of the study, as we moved away from the complex details in cybersecurity, so that the questionnaire would be realistic and in hands to SMEs. We also provided the questionnaire in Arabic language so that it is understandable and appropriate to the target group as the Arabic language is the mother tongue in Saudi Arabia. See Table (3) explaining the sections and the questions of each section.

Table (6): questionnaire sections

	Section	#Questions
1	Institution Information	8
2	Risk Management	8
3	People	7
4	Processes	33
5	Technology	10

Table (7): Questionnaire

	Section I: Institution Information	
1.1	Institution name and field of work	
1.2	Contact name and job qualifications	
1.3	E-mail	
1.4	Mobile Number	
1.5	Number of Employees	
1.6	Did you deal with the National Authority for cybersecurity in Saudi Arabia?	
1.7	Your comments if you deal with the National Authority for cybersecurity in Saudi Arabia.	
1.8	Have you interacted with government agencies regarding cybersecurity?	
	Section II: Risk Management	
Score	Scoring: Not Implemented = 0, Planning Stages = 1, Partially Implemented = 2, Close to Completion = 3 and Fully Implemented = 4.	
	هل لدى مؤسستك برنامج موثق للأمن السيبراني؟	2.1
	هل أجرت مؤسستك تقييمًا للمخاطر لتحديد الأهداف الرئيسية التي يجب دعمها بواسطة برنامج الأمن السيبراني الخاص بك؟	2.2
	هل حددت مؤسستك الأصول الهامة والوظائف التي تعتمد عليها؟	2.3

2.4	هل تم تحديد تهديدات أمن المعلومات ومواطن الضعف المرتبطة بكل من الأصول والوظائف الحرجة؟	
2.5	هل تم تخصيص تكلفة لفقدان كل أصل أو وظيفة مهمة؟	
2.6	هل لديك استراتيجية مكتوبة للأمن السيبراني؟	
2.7	هل تتضمن استراتيجية الأمن السيبراني المكتوبة الخاصة بك خططًا تسعى إلى تقليل المخاطر إلى مستوى مقبول بشكل فعال، مع الحد الأدنى من الاضطرابات في العمليات؟	
2.8	هل يتم مراجعة الاستراتيجية وتحديثها على الأقل سنويًا أو أكثر عندما تتطلب التغييرات المهمة ذلك؟	
	Section III: People	
3.1	هل هناك شخص أو مجموعة مسؤولة عن الحفاظ على برنامج الأمان وضمان الامتثال؟	
3.2	هل يمتلك مديرو وموظفو الأمن السيبراني للمؤسستك الخبرة والمؤهلات اللازمة؟	
3.3	هل المسؤولية محددة بوضوح لجميع مجالات بنية الأمن السيبراني والامتثال والعمليات ومراجعات الحسابات؟	
3.4	هل تم تعيين مسؤولية محددة لتنفيذ خطط استمرارية العمل واستعادة القدرة على العمل بعد الكوارث (سواء داخل أو خارج وظيفة الأمن السيبراني)؟	
3.5	هل لديك برنامج تدريبي مستمر لبناء المهارات والكفاءات من أجل الأمن السيبراني؟	
3.6	هل يعمل موظف الأمن السيبراني بنشاط مع الوحدات الأخرى (الموارد البشرية، شؤون الموظفين، الادارة) لتطوير وتطبيق الامتثال لسياسات وممارسات الأمن السيبراني؟	
3.7	هل قمت بتنفيذ برنامج للتثقيف والتوعية في مجال الأمن السيبراني بحيث يعرف جميع المسؤولين والموظفين والمزودين الخارجيين والضيوف وغيرهم سياسات الأمن السيبراني التي تنطبق عليهم وتوضح مسؤولياتهم؟	
	Section IV: Processes	
	Security Technology Strategy	
4.1	هل لدى مؤسستك بنية أمنية رسمية للمعلومات، بناءً على تحليل إدارة المخاطر واستراتيجية الأمن السيبراني؟	
4.2	هل يتم تحديث بنية الأمان بشكل دوري لمراعاة الاحتياجات والاستراتيجيات الجديدة وتغير التهديدات الأمنية؟	
4.3	هل وضعت إجراءات لإشراك موظفي الأمن في تقييم ومعالجة أي آثار أمنية قبل شراء أو إدخال أنظمة جديدة؟	
4.4	إذا تبين أن النظام المنشور لا يتوافق مع بنيانك الرسمي، فهل هناك عملية وإطار زمني محدد لجعله متوافقًا أو لإزالته من الخدمة أو التطبيقات أو العمليات التجارية؟	
4.5	هل هناك إعدادات تكوين محددة وموثقة متعلقة بالأمان لجميع الأنظمة والتطبيقات؟	
	Policy Development and Enforcement	
4.6	هل سياسات الأمن السيبراني المكتوبة متسقة وسهلة الفهم ومتاحة بسهولة للمسؤولين والموظفين والشركاء؟	
4.7	هل هناك طريقة لإيصال السياسات الأمنية للمسؤولين والموظفين والشركاء؟	
4.8	هل النتائج المترتبة على عدم الامتثال لسياسات الشركة يتم توصيلها وتطبيقها بوضوح؟	
4.9	عند تحديث السياسات أو تطوير سياسات جديدة، هل يتم إجراء تحليل لتحديد الآثار المالية والمتعلقة بالموارد المترتبة على تنفيذ السياسة الجديدة؟	
4.10	هل تعالج سياسات الأمان الخاصة بك بشكل فعال المخاطر المحددة في تحليل المخاطر/ تقييمات المخاطر الخاصة بك؟	
4.11	هل يتم النظر في قضايا الأمن السيبراني في جميع القرارات المهمة داخل المؤسسة؟	
	Information Security Policies and Procedure	
	بناءً على استراتيجية إدارة مخاطر أمن المعلومات لديكم؛ هل لديكم سياسات أو إجراءات أمنية مكتوبة رسمية تتناول كل مجال من المجالات التالية؟	
4.12	المسؤوليات الفردية للموظفين عن ممارسات أمن المعلومات	
4.13	الاستخدام المقبول لأجهزة الكمبيوتر والبريد الإلكتروني والإنترنت	
4.14	حماية الأصول التنظيمية، بما في ذلك الملكية الفكرية	
4.15	إدارة مشكلات الخصوصية، بما في ذلك انتهاكات المعلومات الشخصية	
4.16	ممارسات ومتطلبات التحكم في الوصول والتوثيق والترخيص	
4.17	تصنيف البيانات والاحتفاظ بها وتدميرها	
4.18	تبادل المعلومات، بما في ذلك تخزين ونقل البيانات المؤسسية عن الموارد الخارجية	

	إدارة الثغرات الأمنية	4.19
	التخطيط للطوارئ التعافي من الكوارث	4.20
	توثيق الحوادث والاستجابة لها	4.21
	مراقبة الامتثال الأمني وتطبيقه	4.22
	الأمن المادي وتصاريح الموظفين	4.23
	الإبلاغ عن الأحداث الأمنية للأطراف المتأثرة، بما في ذلك الأفراد والجمهور والشركاء	4.24
	التحقيق الفوري وتصحيح أسباب الفشل الأمني	4.25
	النسخ الاحتياطي للبيانات وتأمين التخزين خارج الموقع	4.26
	نقوم بالتخلص الآمن من البيانات أو الوسائط القديمة أو المواد المطبوعة التي تحتوي على معلومات حساسة	4.27
	Physical Security	
	بالنسبة إلى مراكز البيانات الهامة وغرف البرمجة ومراكز عمليات الشبكة والمرافق أو المواقع الحساسة الأخرى:	
	هل توجد تدابير أمنية مادية متعددة لتقييد الدخول القسري أو غير المصرح به؟	4.28
	هل هناك عملية لإصدار المفاتيح و / أو الرموز و / أو البطاقات التي تتطلب ترخيصًا مناسبًا والتحقق من الخلفية للوصول إلى هذه المنشآت الحساسة؟	4.29
	هل الأجهزة الأساسية والأسلاك الخاصة بك محمية من فقدان الطاقة والعبث والفشل والتهديدات البيئية؟	4.30
	Security Program Administration	
	هل تقوم مؤسستك باختبار وتقييم أو تدقيق برنامج الأمان السيبراني والممارسات والضوابط والتقنيات بشكل دوري لضمان تنفيذها بفعالية؟	4.31
	هل تجري تقييماً مستقلاً دوريًا أو تدقيقًا لبرنامج وممارسات الأمن السيبراني لكل وحدة أعمال؟	4.32
	هل يقوم كل تقييم أو تدقيق دوري بتقييم مدى امتثال كل وحدة عمل لمتطلبات إطار عمل قياسي للأمن السيبراني وسياسات ومعايير وإجراءات وإرشادات الأمان السيبراني ذات الصلة؟	4.33
	Section V: Technology	
	هل الخوادم القابلة للوصول إلى الإنترنت محمية بواسطة أكثر من طبقة أمان واحدة؟	5.1
	هل يتم فحص الشبكات والأنظمة والتطبيقات الخاصة بك بشكل دوري للتحقق من عدم وجود ثغرات أمنية وكذلك تكامل التكوينات؟	5.2
	هل تراقب باستمرار شبكاتك وأنظمتك وتطبيقاتك في الوقت الفعلي للوصول غير المصرّح به والسلوكيات الشاذة مثل الفيروسات أو إدخال الكود الضار أو محاولات الاختراق؟	5.3
	هل البيانات الحساسة مشفرة ومفاتيح التشفير المرتبطة محمية بشكل صحيح؟	5.4
	هل توجد آليات فعالة وموثوقة لإدارة الهويات الرقمية (الحسابات، المفاتيح، الرموز) طوال دورة حياتها، من التسجيل إلى الإنهاء؟	5.5
	هل تدعم جميع الأنظمة والتطبيقات الخاصة بك إدارة تغيير كلمة المرور التلقائية أو تنفذها تلقائيًا أو انتهاء صلاحية كلمات المرور، فضلاً عن تعقيد كلمة المرور وقواعد إعادة الاستخدام؟	5.6
	هل لديك نظام تخويل يفرض حدود زمنية وتقصير عن الحد الأدنى للامتيازات؟	5.7
	؛ وقفل شاشة سطح المكتب؟(session) هل تطبق أنظمتك وتطبيقاتك ممارسات إدارة جلسة العمل	5.8
	هل كل حاسوب والخادم محمي ببرنامج مكافحة الفيروسات؟	5.9
	مع مراعاة الخطورة والإلحاح، هل توجد آليات للإبلاغ عن مجموعة متنوعة من الحالات الشاذة والأحداث الأمنية والرد عليها؟	5.10

3.4 Scoring Tool

After the institution completes the questionnaire, the examination is as follows:

First: The institution determines total reliance on IT score as shown in the table (8).

Table (8): Total reliance on IT score

Low	High	Dependency
0	8	Very Low
9	16	Low
17	32	Medium
33	48	High

Table (8): Total security assessment score

Total risk management score	
Total people score	
Total processes score	
Total technology score	
Total security assessment score (risk management, people, process and processes)	

Second: calculate the total score in each section, and after that calculate the total of all sections (total security assessment score) as shown in the table (9).

Third: Overall security evaluation rating.

Table (10): Overall Security Evaluation Rating

Reliance on IT	Program Rating Ranges		Overall Assessment
Very High	0	199	Poor
	200	274	Needs Improvement
	275	336	Good
High	0	174	Poor
	175	249	Needs Improvement
	250	336	Good
Medium	0	149	Poor
	150	224	Needs Improvement
	225	336	Good
Low	0	124	Poor
	125	199	Needs Improvement
	200	336	Good
Very Low	0	99	Poor
	100	174	Needs Improvement
	175	336	Good

Example: If we had a software company, the number of employees was about 20 employees, and its reliance on information technology with score 47 points and the results of the questionnaire appeared as follows:

Total risk management score	40
Total people score	25
Total processes score	70
Total technology score	55

First: Reliance on information technology 47 points, meaning that it relies with **high** level on information technology according to table (4).

Second: Total security assessment score = 190.

Total risk management score	40
Total people score	25
Total processes score	70
Total technology score	55
Total security assessment score (risk management, people, process and processes)	190

Third: High reliance on IT with total security assessment score = 190 so the overall security evaluation rating = **needs improvement** according to table (6).

Chapter Four: Results

4.1 Study Hypotheses

The study questions arise from: (What is the reality of cybersecurity in SMEs in Saudi Arabia? And what are the ways to develop them?) The following hypotheses:

- **The First Hypothesis:** Infrastructure protection positively affects the cyber security of the institutions. From this hypothesis, the following sub-hypotheses are derived:

  1. The availability of physical protection affects the institutions positively.
  2. The availability of software protection affects institutions positively.
  3. The availability of individual protection has a positive impact on institutions.

- **The Second Hypothesis:** the existence of written policies is very important in SMEs.
- **The Third Hypothesis:** Control of access to information systems affects institutions positively.
- **The Fourth Hypothesis:** The availability of regulatory measures to control information systems affects the management of cybersecurity positively.

4.2 Results of Statistical Testing

We depend on "information security governance assessment tool for higher education" to create our questionnaire. 64 SMEs institutions in Saudi Arabia shared in this questionnaire and based on their response, we received the following results:

- **First Section (Institution Information):**

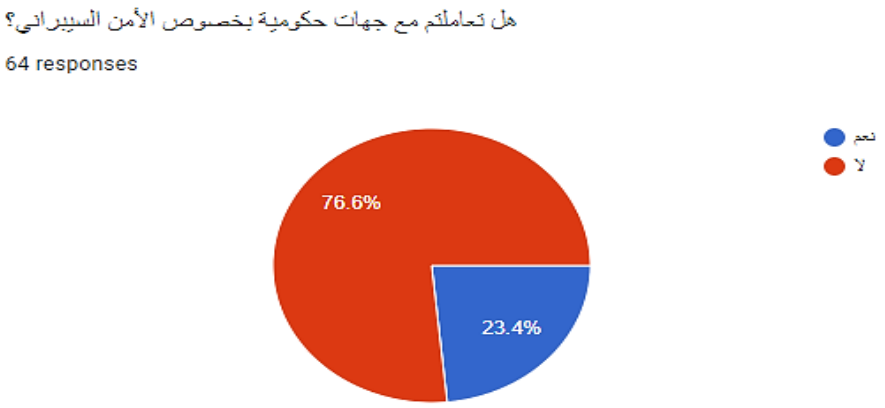

Figure (3): Questionnaire questions, enterprise information section, Q#1

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

Figure (4): Questionnaire questions, enterprise information section, Q#2

Approximately 19% of the institutions deal with the National Cybersecurity Authority and 23% of the deal with a government agency concerned with cyber security, and most of them commend them and the Kingdom's efforts to maintain institutional security.

- **Second Section (Risk Management):**

This section assesses the risk management process as it relates to create an information security strategy and program.

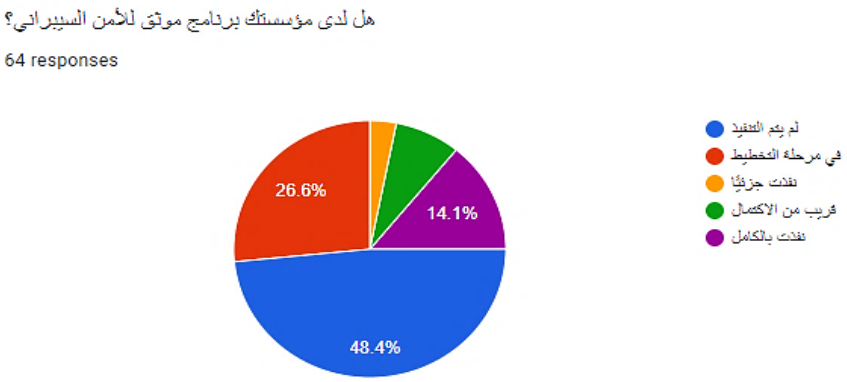

Figure (5): Questionnaire questions, risk management section, Q#1

That the organizations that have a documented program for cybersecurity and fully Implemented 14.1% and close to completion 7.5%, Partially Implemented 3.4% and 26.6% the planning stage and 48.4 do not have any documented cybersecurity program.

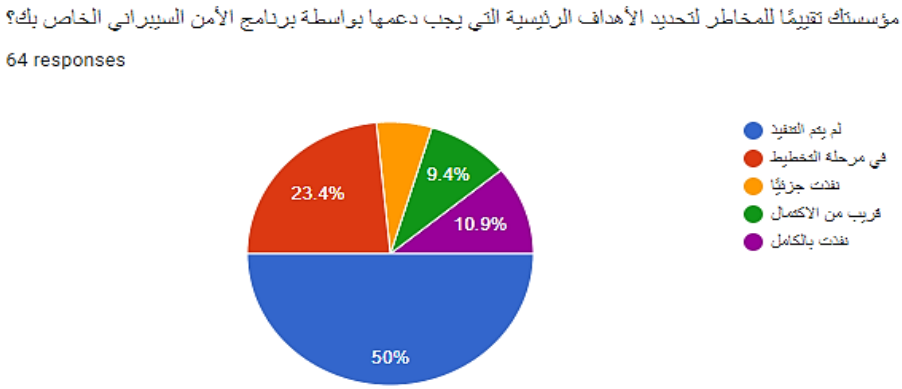

Figure (6): Questionnaire questions, risk management section, Q#2

That the Organizations that have conducted a risk assessment to identify the main objectives to be supported by their cybersecurity program and fully Implemented 10.9% and close to completion 9.4%, Partially Implemented 6.3% and 23.4% the planning stage and 50% not Implemented.

Figure (7): Questionnaire questions, risk management section, Q#3

The organizations that have identified important assets and the functions that depend on them and fully Implemented 14.1% and close to completion 10.9%, Partially Implemented 10.9% and 21.9% the planning stage and 42.2% not Implemented.

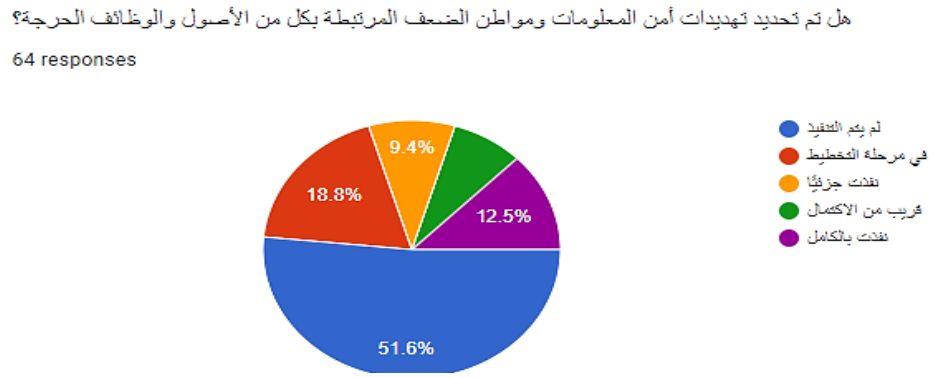

Figure (8): Questionnaire questions, risk management section, Q#4

The Organizations that have identified information security threats and vulnerabilities associated with both assets and important functions and fully Implemented 12.5% and close to completion 7.7%, Partially Implemented 9.4% and 18.8% the planning stage and 51.6% not Implemented.

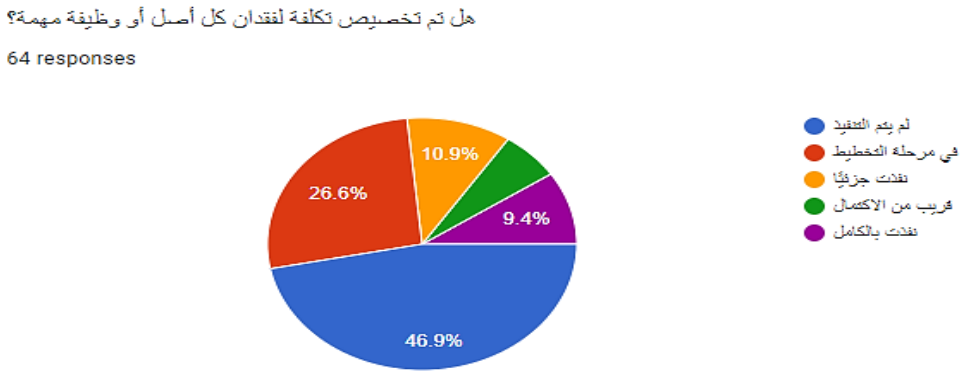

Figure (9): Questionnaire questions, risk management section, Q#5

The Organizations that have assigned a cost to lose an important asset or functions and fully Implemented 9.4% and close to completion 6.2%, Partially Implemented 10.9% and 26.6% the planning stage and 46.9% not Implemented.

Figure (10): Questionnaire questions, risk management section, Q#6

The Organizations with a written cybersecurity strategyand fully Implemented 12.5% and close to completion 3.2%, Partially Implemented 7.7% and 29.7% the planning stage and 46.9% not Implemented.

Figure (11): Questionnaire questions, risk management section, Q#7

The Organizations that have sought to include their written cybersecurity strategy plans to reduce risk to an acceptable level effectively, with minimal operational

disruptions and fully Implemented 7.8% and close to completion 10.9%, Partially Implemented 6.3% and 32.8% the planning stage and 42.2% not Implemented.

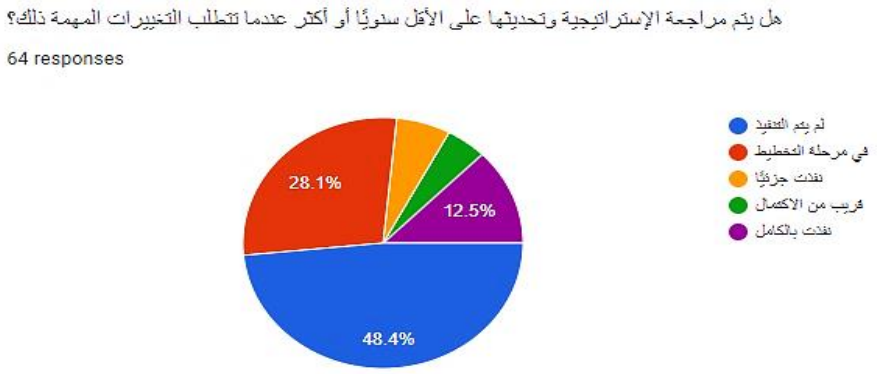

Figure (12): Questionnaire questions, risk management section, Q#8

The Organizations that review and update the strategy at least annually or more when significant changes require it and fully Implemented 12.5% and close to completion 3.3%, Partially Implemented 7.7% and 28.1% the planning stage and 48.4% not Implemented.

- **Third Section (People):**

This section assesses the organizational aspects of your information security program.

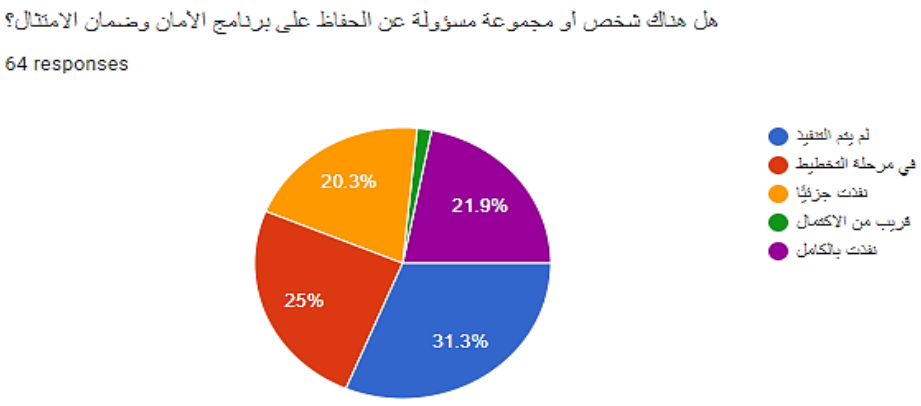

Figure (12): Questionnaire questions, people section, Q#1

The Organizations that have a person or group responsible for maintaining the safety program and ensuring compliance and fully Implemented 21.9% and close to completion 1.5%, Partially Implemented 20.3% and 25% the planning stage and 31.3% not Implemented.

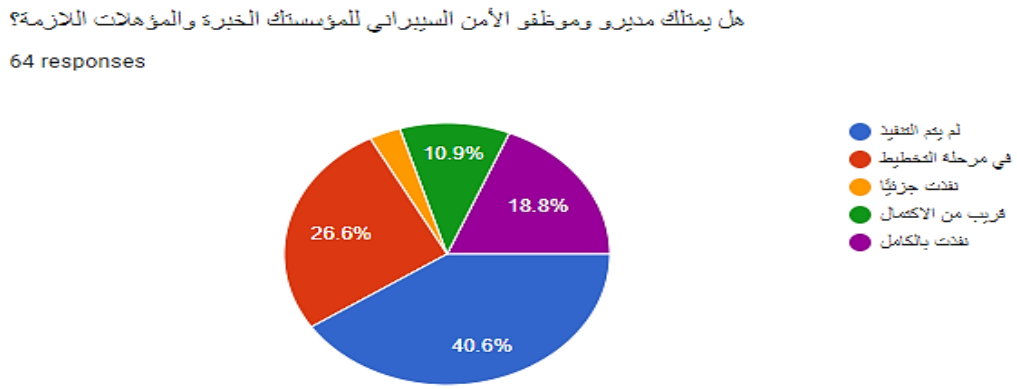

Figure (14): Questionnaire questions, people section, Q#2

The Organizations in which cybersecurity managers and staff possess the necessary expertise and qualifications and fully Implemented 18.8% and close to completion 10.9%, Partially Implemented 3.1% and 26.6% the planning stage and 40.6% not Implemented.

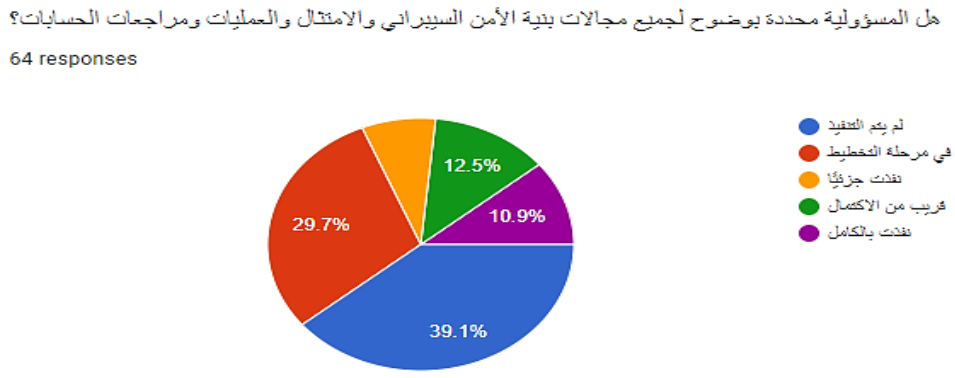

Figure (13): Questionnaire questions, people section, Q#3

The Organizations that clearly define responsibilities for all areas of cybersecurity infrastructure, compliance, operations, and audits and fully Implemented 10.9% and close to completion 12.5%, Partially Implemented 78% and 29.7% the planning stage and 39.1% not Implemented.

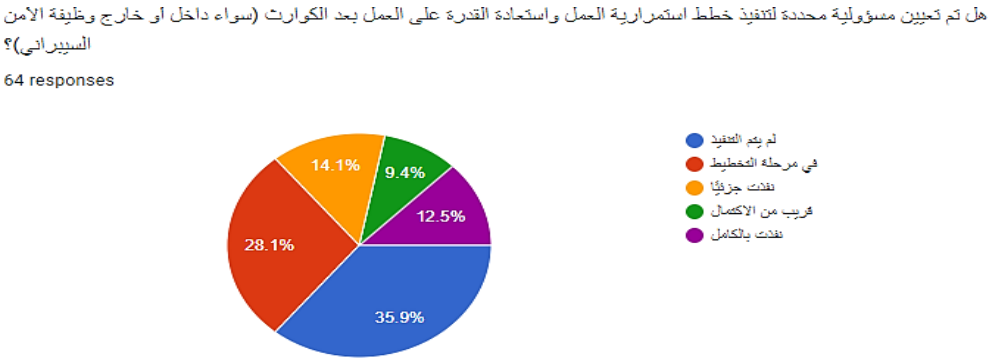

Figure (14): Questionnaire questions, people section, Q#4

The Organizations assigning specific responsibility for implementing business continuity plans and restoring the ability to work after disasters (both inside and outside the cybersecurity function) and fully Implemented 12.5% and close to completion 9.4%, Partially Implemented 14.1% and 28.1% the planning stage and 35.9% not Implemented.

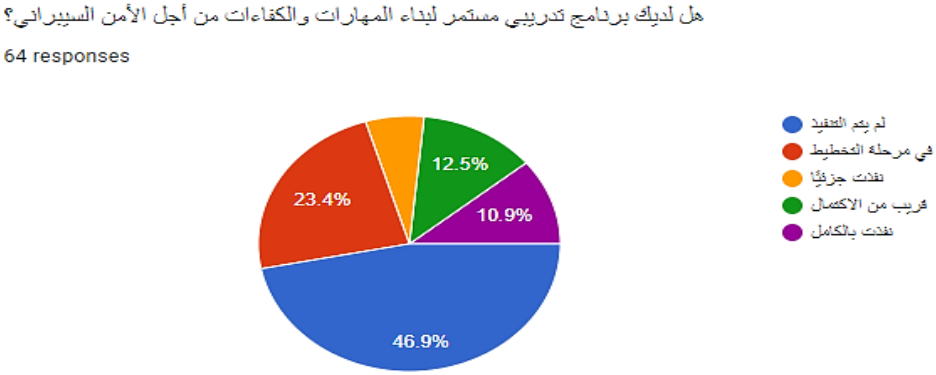

Figure (15): Questionnaire questions, people section, Q#5

The Organizations with an ongoing training program to build skills and competencies in cybersecurity and fully Implemented 10.9% and close to completion 12.5%, Partially Implemented 6.3% and 23.4% the planning stage and 46.9% not Implemented.

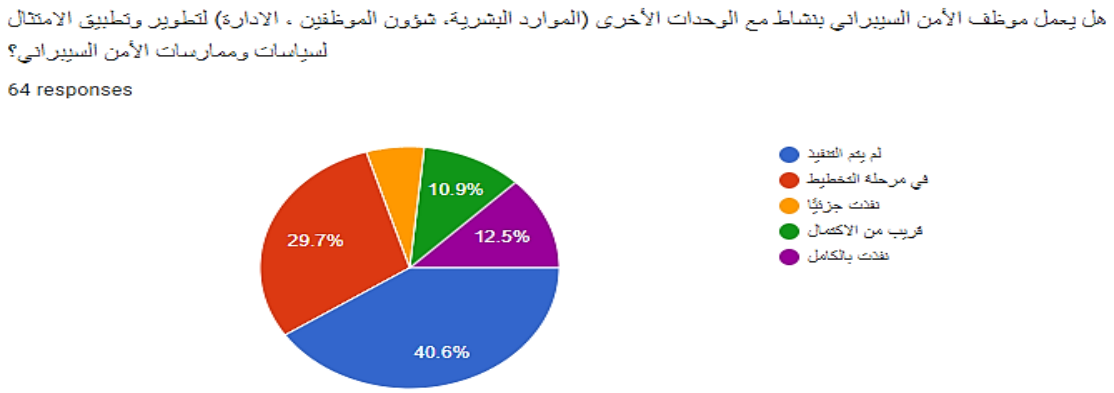

Figure (18): Questionnaire questions, people section, Q#6

The Organizations that the cyber security officer is actively working with other units (human resources, personnel affairs, administration) to develop and implement compliance with cyber security policies and practices and fully Implemented 12.5% and close to completion 10.9%, Partially Implemented 6.3% and 29.7% the planning stage and 40.6% not Implemented.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
IJSR
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

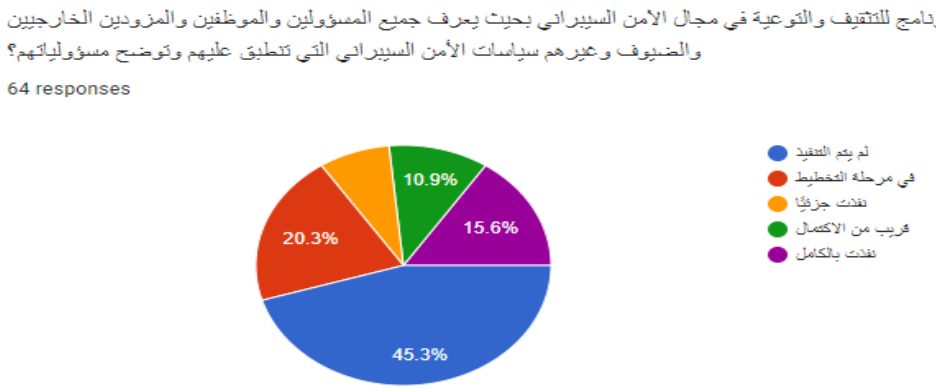

Figure (19): Questionnaire questions, people section, Q#7

The Organizations that have implemented a cybersecurity education and awareness program so that all officials, employees, external suppliers, guests, and others know the cybersecurity policies that apply to them and clarify their responsibilities and fully Implemented 15.6% and close to completion 10.9%, Partially Implemented 7.9% and 20.3% the planning stage and 45.3% not Implemented.

- **Forth Section (Processes):**

1. Security Technology Strategy

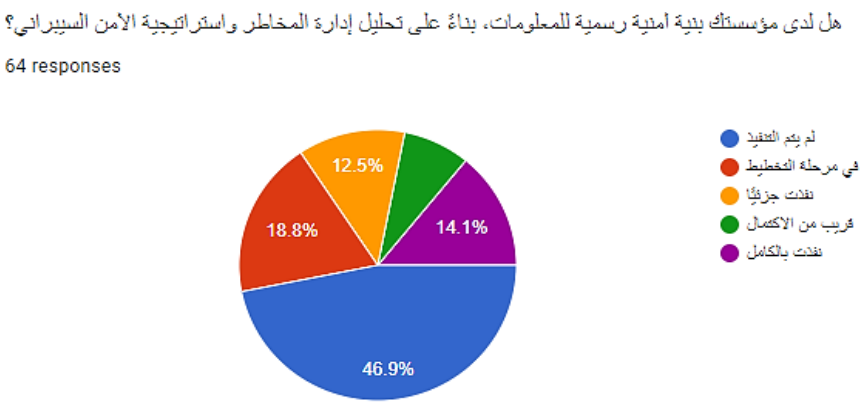

Figure (16): Questionnaire questions, processes section, Q#1

The Organizations with a formal information security architecture, based on risk management analysis and cybersecurity strategy and fully Implemented 14.1% and close to completion 7.7%, Partially Implemented 12.5% and 18.8% the planning stage and 46.9% not Implemented.

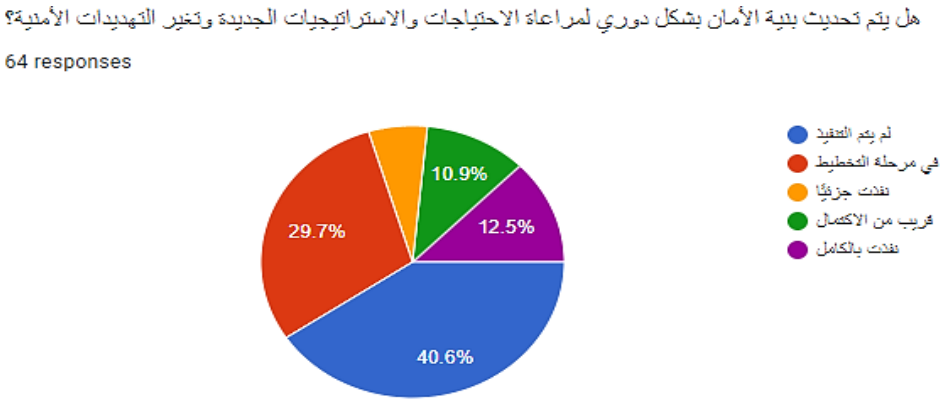

Figure (17): Questionnaire questions, processes section, Q#2

The Organizations that update the security architecture periodically to take into account new needs and strategies and change security threats and fully Implemented 12.5% and close to completion 10.9%, Partially Implemented 6.3% and 29.7% the planning stage and 40.6% not Implemented.

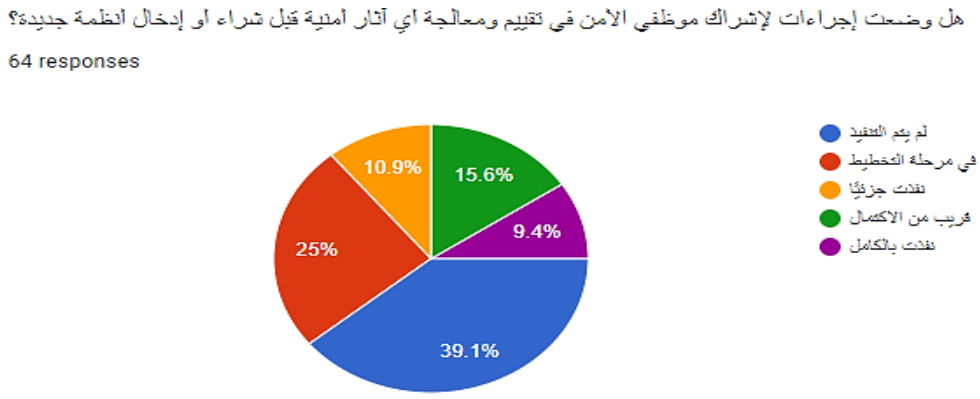

Figure (18): Questionnaire questions, processes section, Q#3

The Organizations that have established procedures to involve security personnel in assessing and addressing any security implications before purchasing or introducing new systems and fully Implemented 9.4% and close to completion 15.6%, Partially Implemented 10.9% and 25% the planning stage and 39.1% not Implemented.

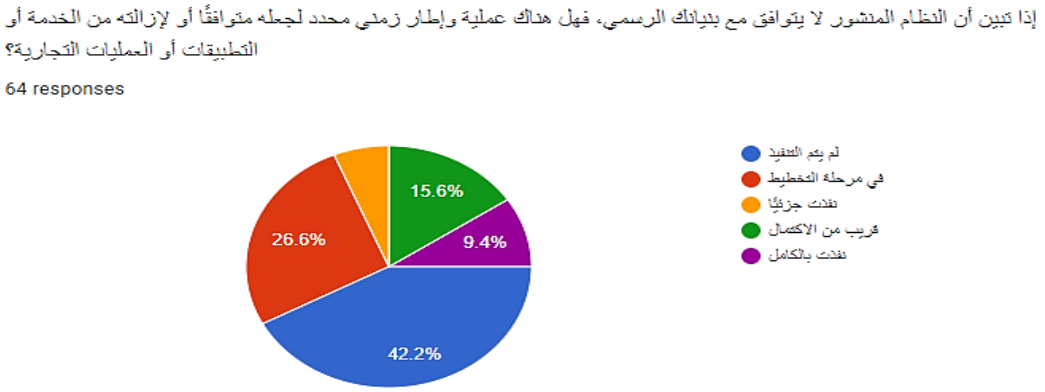

Figure (19): Questionnaire questions, processes section, Q#4

The Organizations that, if it is found that the published system does not comply with its official structure and have a process and time frame to make it compatible or remove it from the service or commercial applications and fully Implemented 9.4% and close to completion 15.6%, Partially Implemented 6.2% and 26.6% the planning stage and 42.2% not Implemented.

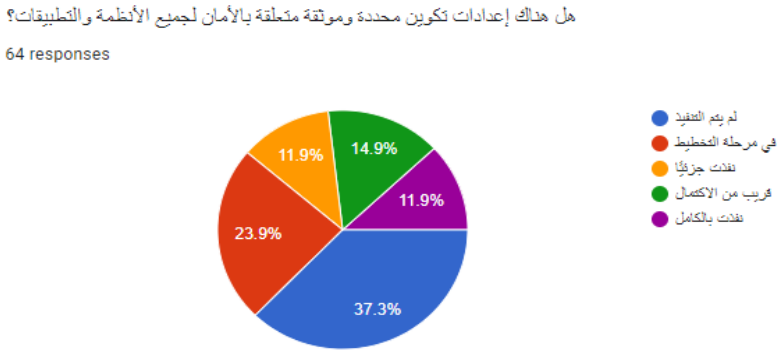

Figure (24): Questionnaire questions, processes section, Q#5

The Organizations that have specific, documented security-related configuration settings for all systems and applications and fully Implemented 11.9% and close to completion 14.9%, Partially Implemented 11.9% and 23.9% the planning stage and 37.3% not Implemented.

2. Policy Development and Enforcement

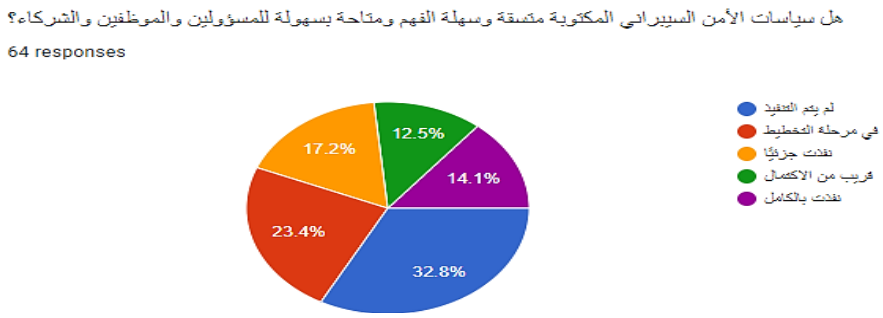

Figure (25): Questionnaire questions, processes section, Q#6

The Organizations with written cybersecurity policies are consistent, easy to understand and readily available to officials, employees, and partners and fully Implemented 14.1% and close to completion 12.5%, Partially Implemented 17.2% and 23.4% the planning stage and 32.8% not Implemented.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

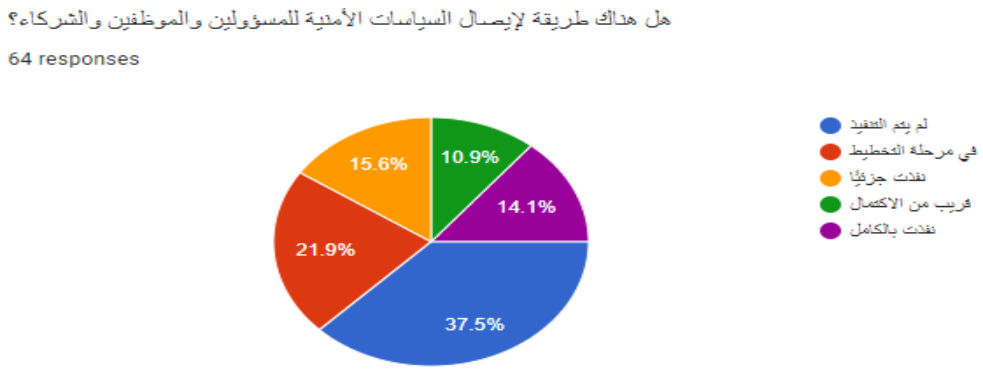

Figure (22): Questionnaire questions, processes section, Q#7

The Organizations that have a way of communicating security policies to officials, employees, and partners and fully Implemented 14.1% and close to completion 10.9%, Partially Implemented 15.6% and 21.9% the planning stage and 37.5% not Implemented.

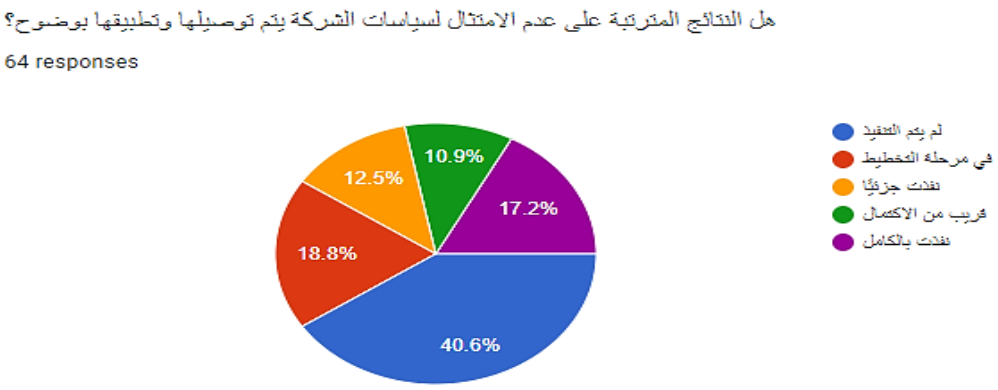

Figure (20): Questionnaire questions, processes section, Q#8

The Organizations that benefit from the consequences of non-compliance with the organization's policies are communicated and applied clearly and fully Implemented 17.2% and close to completion 10.9%, Partially Implemented 12.5% and 18.8% the planning stage and 40.6% not Implemented.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

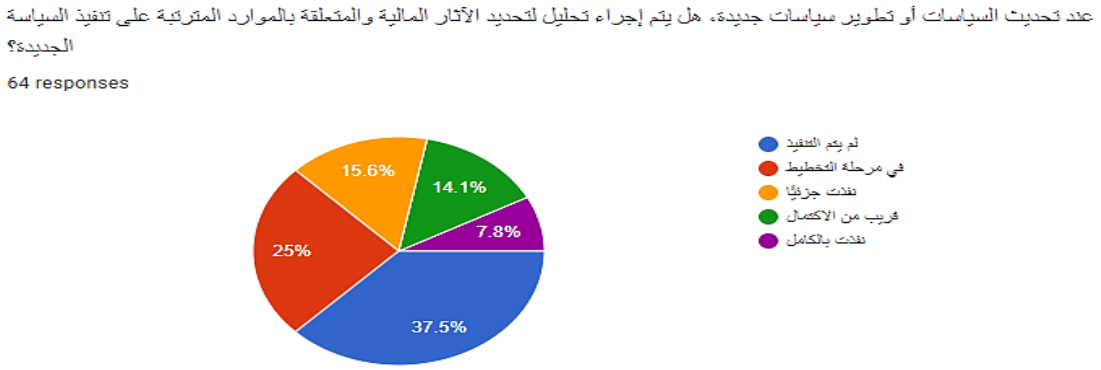

Figure (21): Questionnaire questions, processes section, Q#9

The Organizations that when updating policies or developing new policies conduct an analysis to determine the financial implications related to the resources involved in implementing the new policy and fully Implemented 7.8% and close to completion 14.1%, Partially Implemented 15.6% and 25% the planning stage and 37.5% not Implemented.

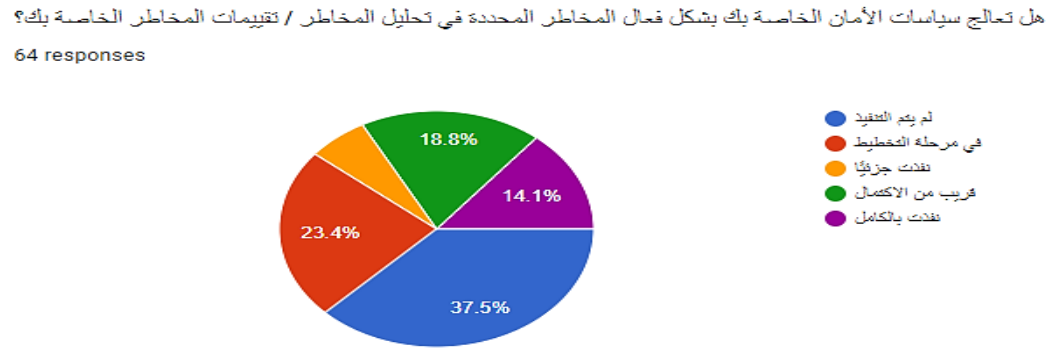

Figure (22): Questionnaire questions, processes section, Q#10

The Organizations whose security policies effectively address the risks identified in their risk analysis / risk assessments and fully Implemented 14.1% and close to

completion 18.8%, Partially Implemented 6.2% and 23.4% the planning stage and 37.5% not Implemented.

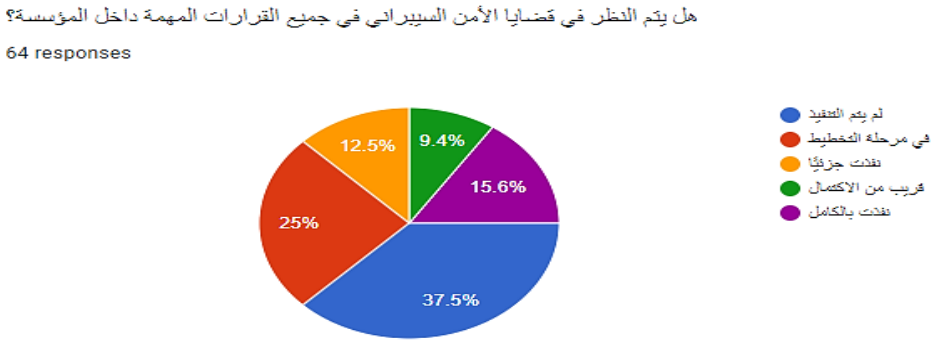

Figure (26): Questionnaire questions, processes section, Q#11

The Organizations that consider cybersecurity issues in all important decisions within the organization and fully Implemented 15.6% and close to completion 94%, Partially Implemented 12.5% and 25% the planning stage and 37.5% not Implemented.

3. Information Security Policies and Procedures

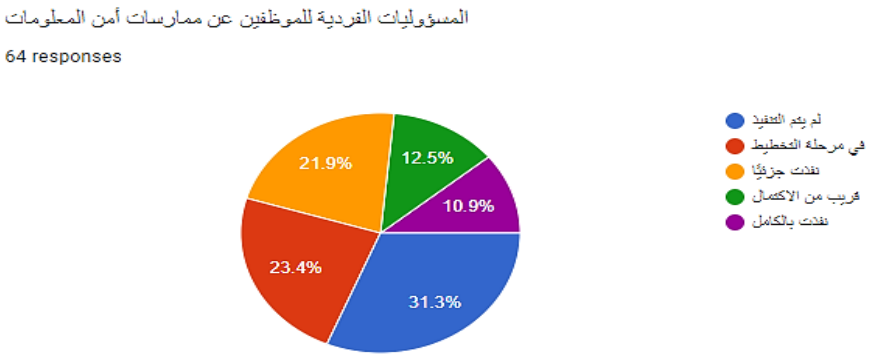

Figure (23): Questionnaire questions, processes section, Q#12

The Organizations that have individual responsibilities of employees for information security practices and fully Implemented 10.9% and close to completion 12.5%,

Partially Implemented 21.9% and 23.4% the planning stage and 31.3% not Implemented.

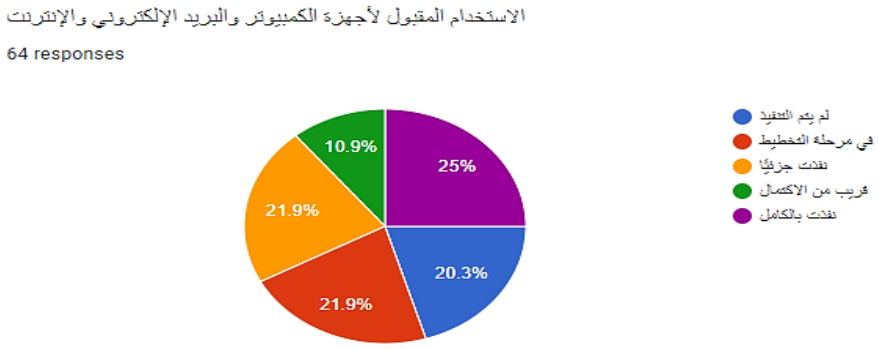

Figure (32): Questionnaire questions, processes section, Q#13

The Organizations with acceptable use of computers, email and the Internet and fully Implemented 25% and close to completion 10.9%, Partially Implemented 21.9% and 21.9% the planning stage and 20.3% not Implemented.

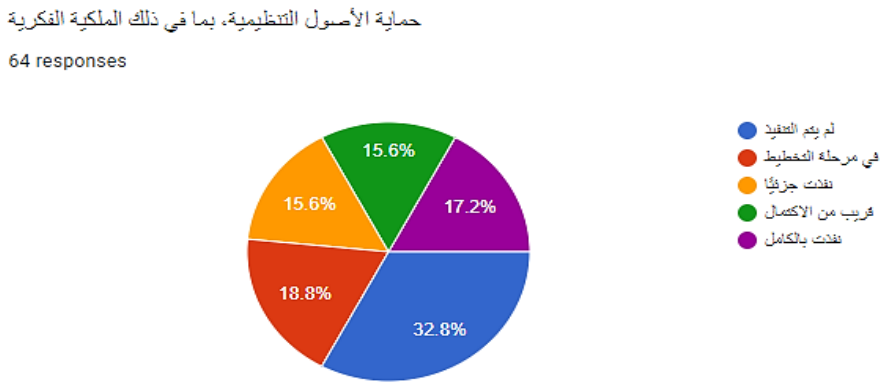

Figure (28): Questionnaire questions, processes section, Q#14

The Organizations that protect regulatory assets, including intellectual property and fully Implemented 17.2% and close to completion 15.6%, Partially Implemented 15.6% and 18.8% the planning stage and 32.8% not Implemented.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

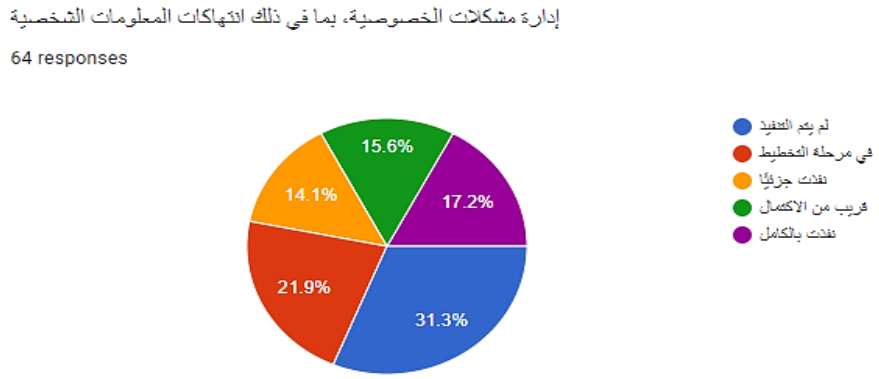

Figure (24): Questionnaire questions, processes section, Q#15

The Organizations that manage privacy issues, including violations of personal information and fully Implemented 17.2% and close to completion 15.6%, Partially Implemented 14.1% and 21.9% the planning stage and 31.3% not Implemented.

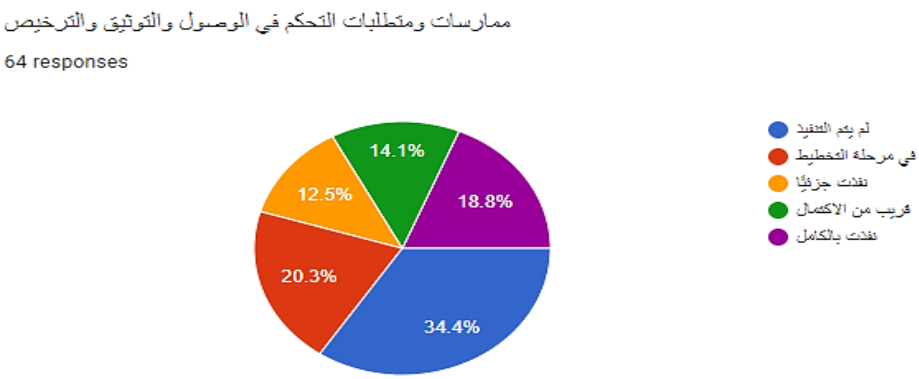

Figure (30): Questionnaire questions, processes section, Q#16

The Organizations that have access control, documentation and authorization practices and requirements and fully Implemented 18.8% and close to completion 14.1%, Partially Implemented 12.5% and 20.3% the planning stage and 34.4% not Implemented.

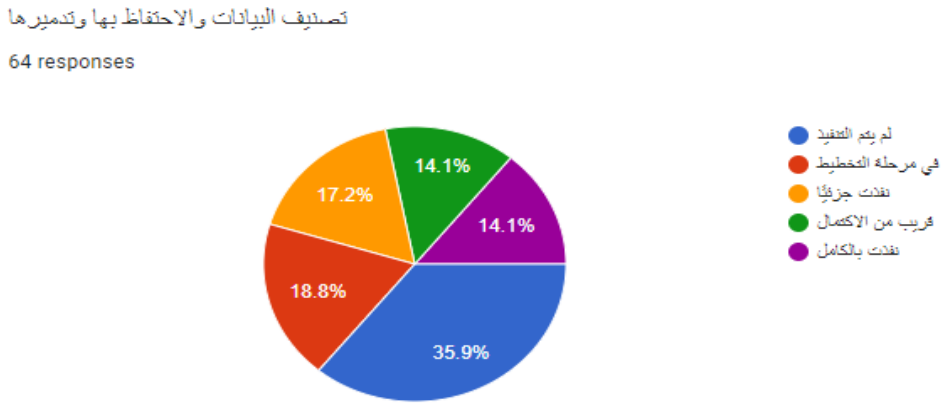

Figure (25): Questionnaire questions, processes section, Q#17

The Organizations that have a classification, retention and destruction of data and fully Implemented 14.1% and close to completion 14.1%, Partially Implemented 17.2% and 18.8% the planning stage and 35.9% not Implemented.

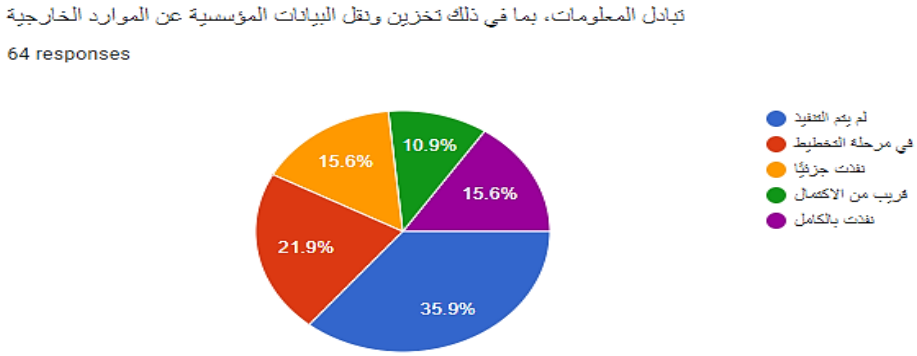

Figure (37): Questionnaire questions, processes section, Q#18

The Organizations with policies and procedures for exchanging information, including storing and transmitting institutional data on external resources and fully Implemented 15.6% and close to completion 10.9%, Partially Implemented 156% and 21.9% the planning stage and 35.9% not Implemented.

International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (3), No. (10) October 2024 الإصدار (3)، العدد (10)

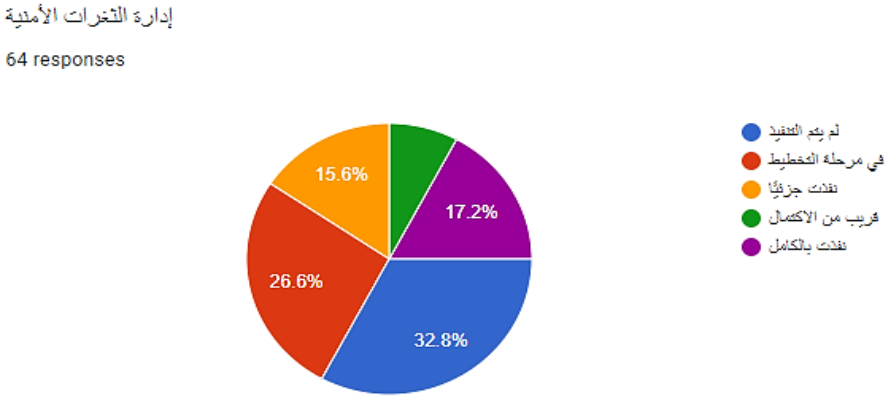

Figure (38): Questionnaire questions, processes section, Q#19

The Organizations with policies and procedures for managing security vulnerabilities and fully Implemented 17.2% and close to completion 7.8%, Partially Implemented 15.6% and 26.6% the planning stage and 32.8% not Implemented.

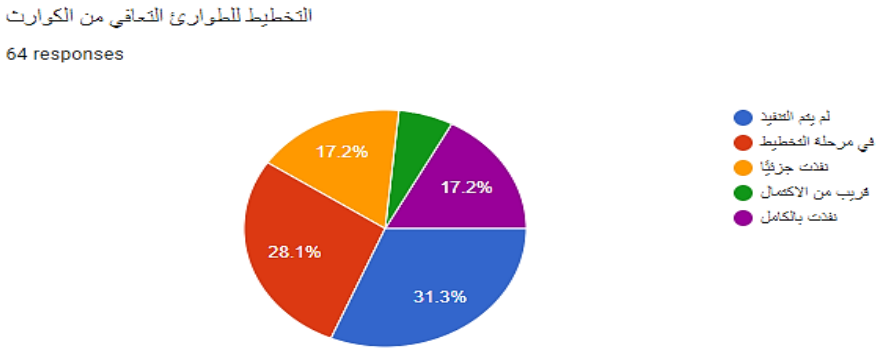

Figure (39): Questionnaire questions, processes section, Q#20

The Organizations with disaster recovery contingency planning and fully Implemented 17.2% and close to completion 6.2%, Partially Implemented 17.2% and 28.1% the planning stage and 31.3% not Implemented.

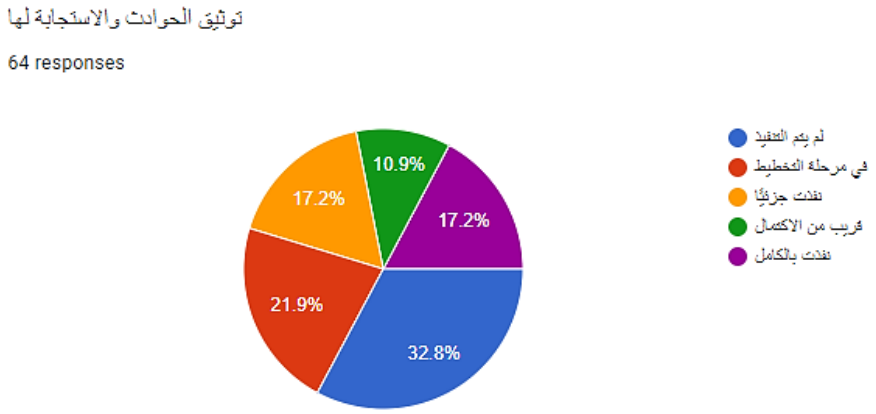

Figure (26): Questionnaire questions, processes section, Q#21

The Organizations documenting and responding to incidents and fully Implemented 17.2% and close to completion 10.9%, Partially Implemented 17.2% and 21.9% the planning stage and 32.8% not Implemented.

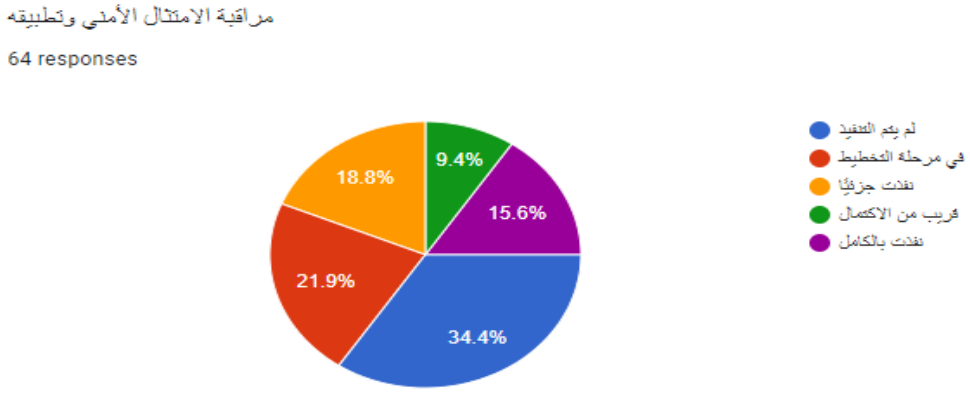

Figure (27): Questionnaire questions, processes section, Q#22

The Organizations that monitor and implement security compliance and fully Implemented 15.6% and close to completion 9.4%, Partially Implemented 18.8% and 21.9% the planning stage and 34.4% not Implemented.

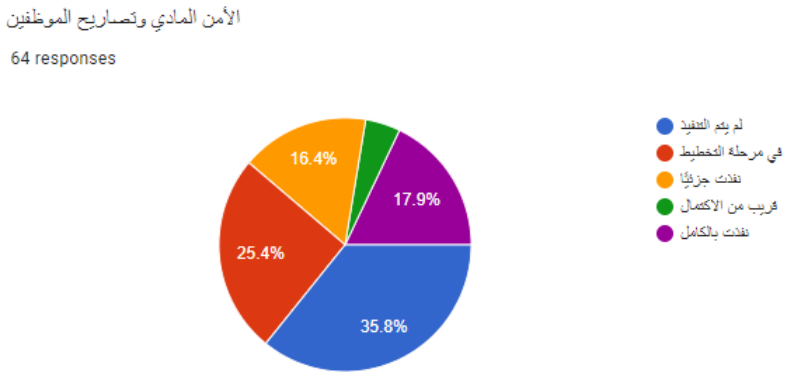

Figure (42): Questionnaire questions, processes section, Q#23

The Organizations that depend on physical security and employee permits and fully Implemented 17.9% and close to completion 4.5%, Partially Implemented 16.4% and 25.4% the planning stage and 35.8% not Implemented.

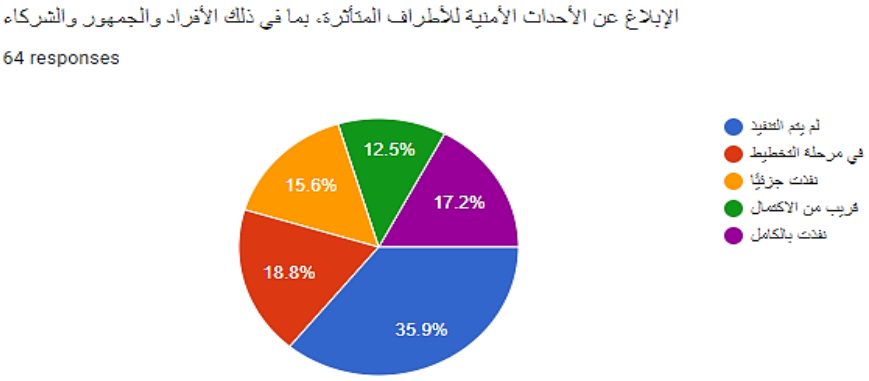

Figure (43): Questionnaire questions, processes section, Q#24

The Organizations that report security events to affected parties, including individuals, the public, and partners and fully Implemented 17.2% and close to completion 12.5%, Partially Implemented 15.6% and 18.8% the planning stage and 35.9% not Implemented.

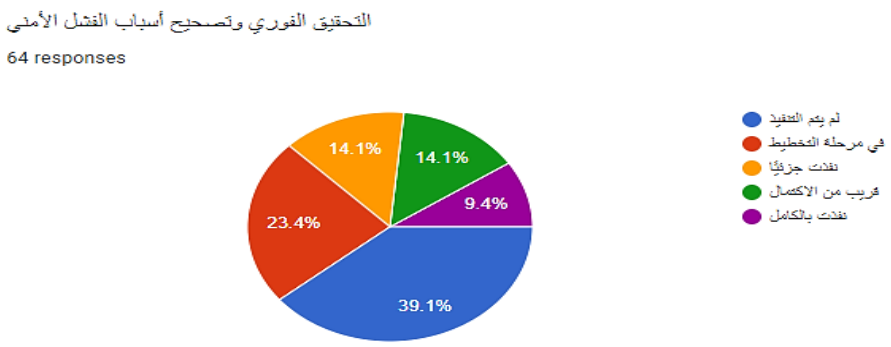

Figure (44): Questionnaire questions, processes section, Q#25

The Organizations that conduct immediate investigations and correct the causes of security failures and fully Implemented 9.4% and close to completion 14.1%, Partially Implemented 14.1% and 23.4% the planning stage and 391% not Implemented.

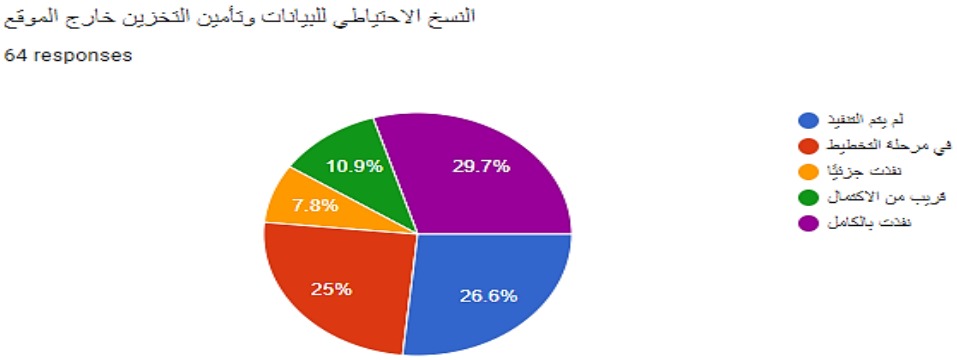

Figure (45): Questionnaire questions, processes section, Q#26

The Organizations that back up data and secure off-site storage and fully Implemented 29.7% and close to completion 10.9%, Partially Implemented 7.8% and 25% the planning stage and 26.6% not Implemented.

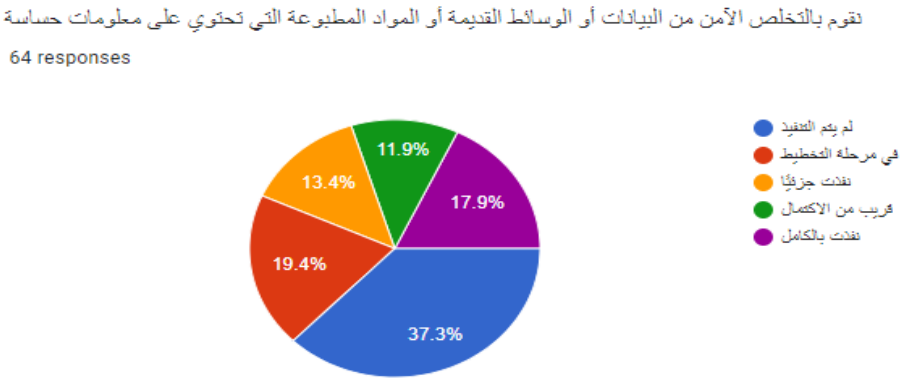

Figure (46): Questionnaire questions, processes section, Q#27

The Organizations that safely dispose of old data, media, or printed materials containing sensitive information and fully Implemented 17.9% and close to completion 11.9%, Partially Implemented 13.4% and 19.4% the planning stage and 37.3% not Implemented.

4. Physical Security

For your critical data centres, programming rooms, network operations centres, and other sensitive facilities or locations:

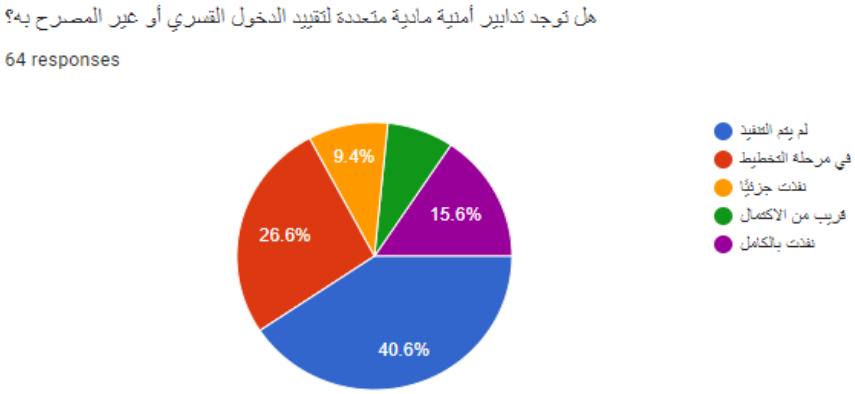

Figure (47): Questionnaire questions, processes section, Q#28

The Organizations that have multiple physical security measures in place to restrict forced or unauthorized entry and fully Implemented 15.6% and close to completion 7.8%, Partially Implemented 9.4% and 26.6% the planning stage and 40.6% not Implemented.

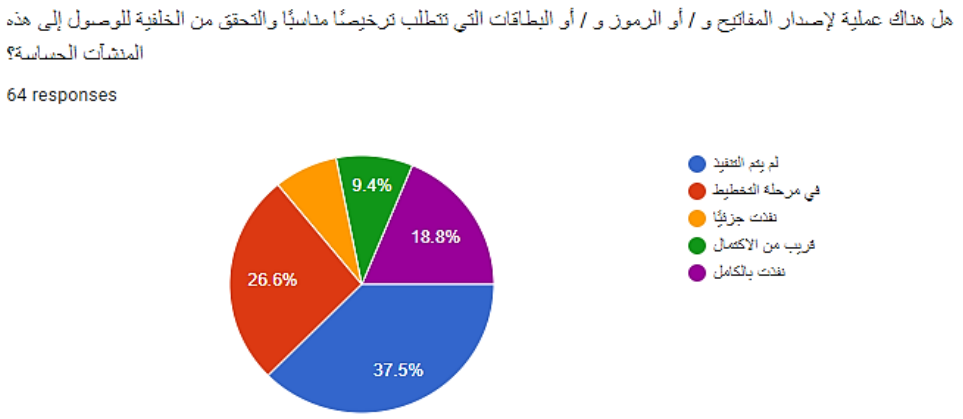

Figure (48): Questionnaire questions, processes section, Q#29

The Organizations with processes for issuing keys, symbols and / or cards that require appropriate licensing and background verification to access these sensitive installations and fully Implemented 18.8% and close to completion 9.4%, Partially Implemented 7.7% and 26.6% the planning stage and 37.5% not Implemented.

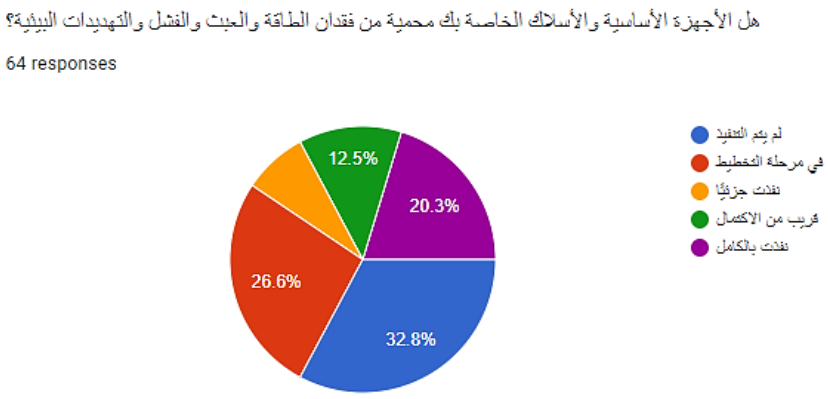

Figure (49): Questionnaire questions, processes section, Q#30

The Organizations whose primary devices and wires are protected from power loss, tampering, failure and environmental threats and fully Implemented 20.3% and close to completion 12.5%, Partially Implemented 7.8% and 26.6% the planning stage and 32.8% not Implemented.

5. Security Program Administration

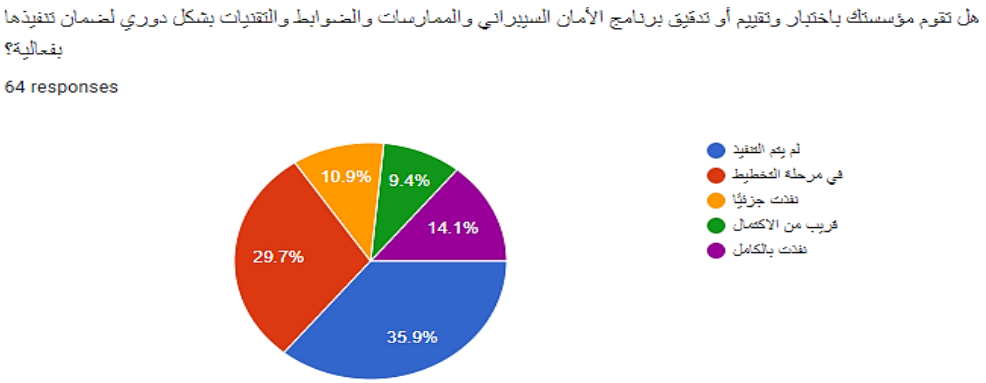

Figure (50): Questionnaire questions, processes section, Q#31

The Organizations that periodically test, evaluate, or audit the cybersecurity program, practices, controls and technologies to ensure their effective implementation and fully Implemented 14.1% and close to completion 9.4%, Partially Implemented 10.9% and 29.7% the planning stage and 35.9% not Implemented.

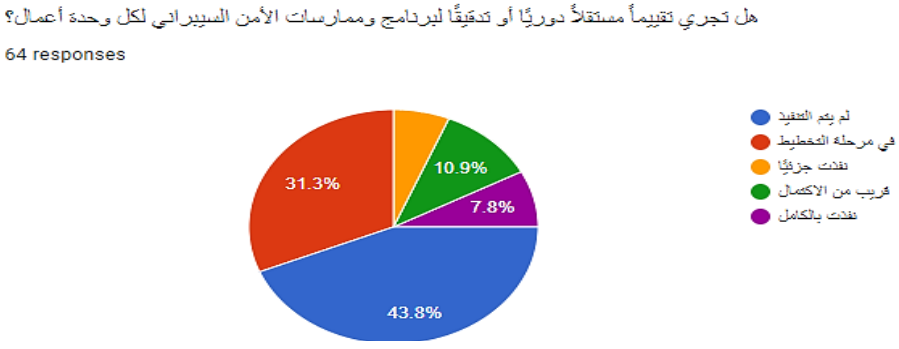

Figure (28): Questionnaire questions, processes section, Q#32

The Organizations conducting periodic, independent evaluation or audit of cybersecurity program and practices for each business unit and fully Implemented 7.8% and close to completion 10.9%, Partially Implemented 6.2% and 31.3% the planning stage and 43.8% not Implemented.

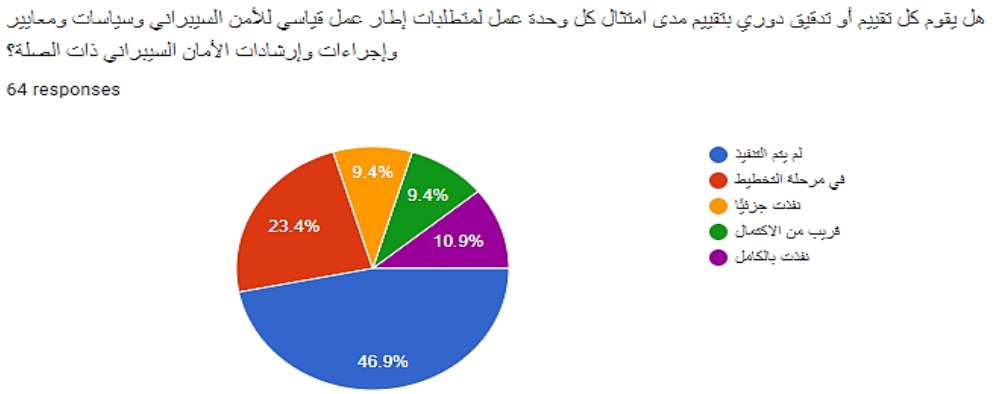

Figure (52): Questionnaire questions, processes section, Q#33

The Organizations in which each periodic assessment or audit assesses the compliance of each business unit with the requirements of a standard cybersecurity framework and relevant cyber security policies, standards, procedures, and guidelines and fully Implemented 10.9% and close to completion 9.4%, Partially Implemented 9.4% and 23.4% the planning stage and 46.9% not Implemented.

- **Fifth Section (Technology):**

In this section, we asked people about Security Technology.

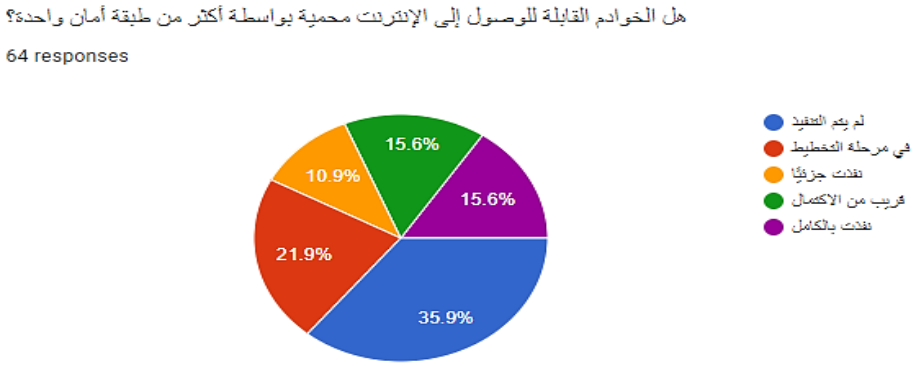

Figure (29): Questionnaire questions, technology section, Q#1

The Organizations with accessible servers are protected by more than one security layer and fully Implemented 15.6% and close to completion 15.6%, Partially Implemented 10.9% and 21.9% the planning stage and 35.9% not Implemented.

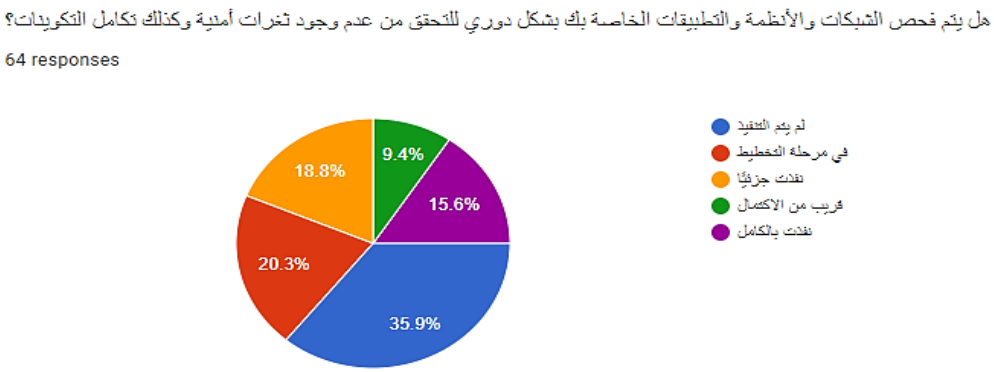

Figure (30): Questionnaire questions, technology section, Q#2

The Organizations that check their networks, systems, and applications periodically to check for security vulnerabilities and configuration integrity and fully Implemented

15.6% and close to completion 9.4%, Partially Implemented 18.8% and 20.3% the planning stage and 35.9% not Implemented.

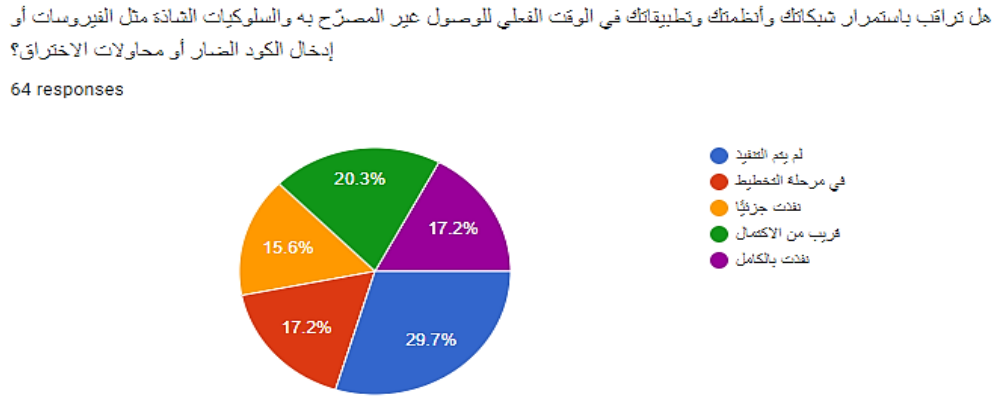

Figure (55): Questionnaire questions, technology section, Q#3

The Organizations that constantly monitor their networks, systems, and applications in real-time for unauthorized access and anomalies such as viruses, malicious code entry, or hacking attempts and fully Implemented 17.2% and close to completion 20.3%, Partially Implemented 15.6% and 17.2% the planning stage and 29.7% not Implemented.

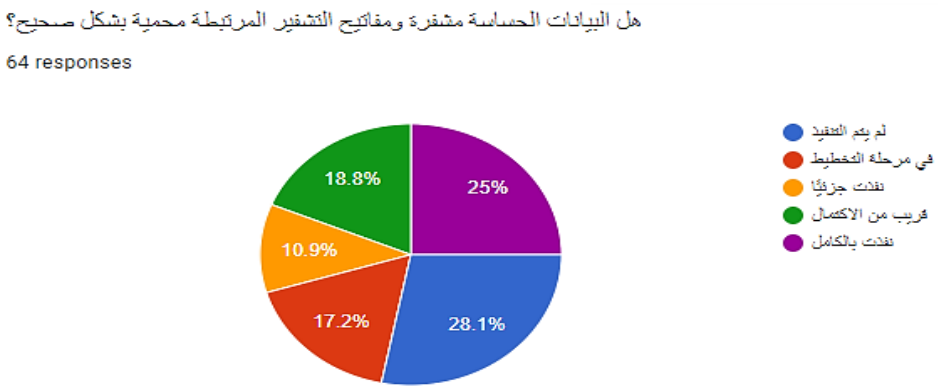

Figure (56): Questionnaire questions, technology section, Q#4

The Organizations that keep sensitive data encrypted and associated cryptographic keys are properly protected and fully Implemented 25% and close to completion 18.8%, Partially Implemented 10.9% and 17.2% the planning stage and 28.1% not Implemented.

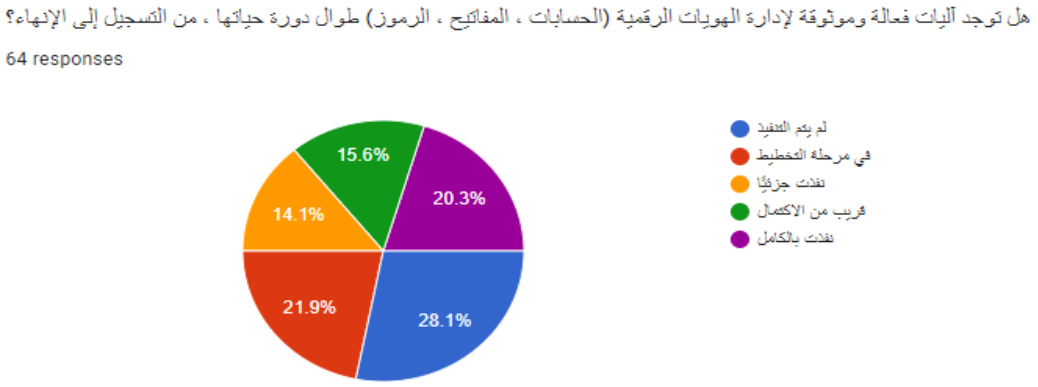

Figure (57): Questionnaire questions, technology section, Q#5

The Organizations that have effective and reliable mechanisms for managing digital identities (accounts, keys, codes) throughout their life cycle, from registration to termination and fully Implemented 20.3% and close to completion 15.6%, Partially Implemented 14.1% and 21.9% the planning stage and 28.1% not Implemented.

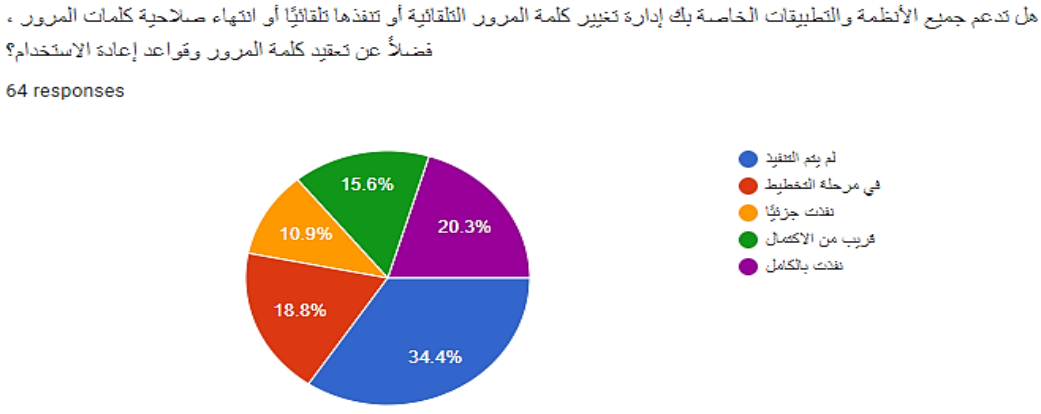

Figure (58): Questionnaire questions, technology section, Q#6

The Organizations that support all of their systems and applications manage or implement automatic password change or password expiration, password complexity and reuse rules and fully Implemented 20.3% and close to completion 15.6%, Partially Implemented 10.9% and 18.8% the planning stage and 34.4% not Implemented.

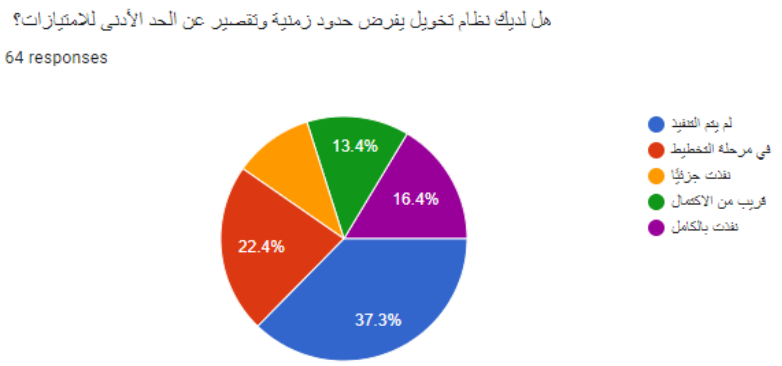

Figure (59): Questionnaire questions, technology section, Q#7

The Organizations with a system of authorization impose time limits and default on minimum privileges and fully Implemented 16.4% and close to completion 13.4%, Partially Implemented 10.5% and 22.4% the planning stage and 37.3% not Implemented.

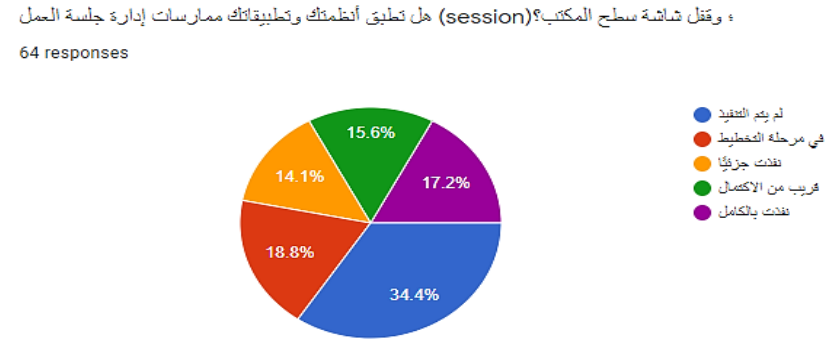

Figure (60): Questionnaire questions, technology section, Q#8

The Organizations whose systems and applications implement session management practices and the desktop lock screen and fully Implemented 17.2% and close to completion 15.6%, Partially Implemented 14.1% and 18.8% the planning stage and 34.4% not Implemented.

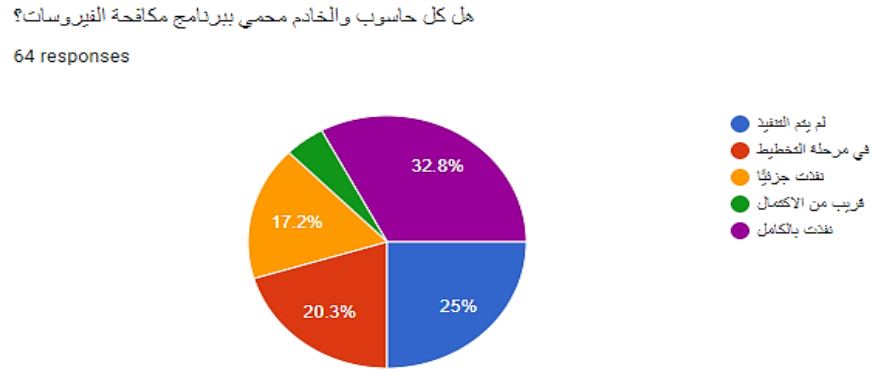

Figure (61): Questionnaire questions, technology section, Q#9

The Organizations that every computer and server are protected with antivirus software and fully Implemented 32.8% and close to completion 4.7%, Partially Implemented 17.2% and 20.3% the planning stage and 25% not Implemented.

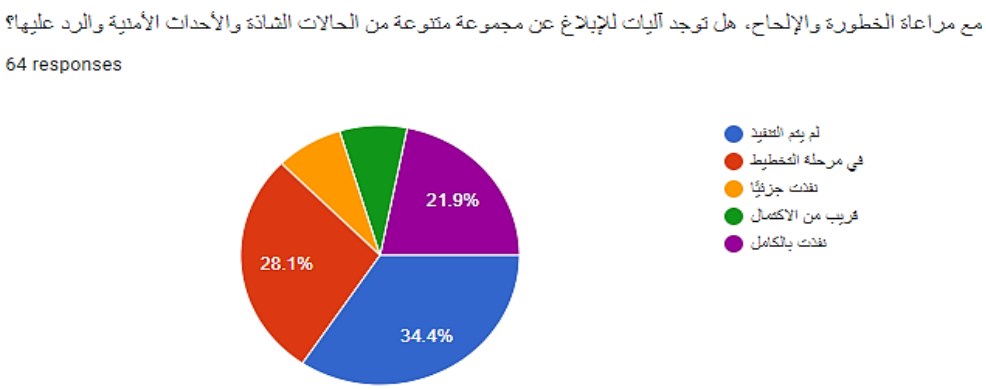

Figure (62): Questionnaire questions, technology section, Q#10

The Organizations that have mechanisms to report and respond to a variety of anomalies and security events and fully Implemented 21.9% and close to completion 7.8%, Partially Implemented 7.8% and 28.1% the planning stage and 34.4% not Implemented.

4.3 Interpretations of Statistical Results

The traditional perception that cybersecurity is only the responsibility of the cybersecurity department, and that protection programs and systems are adequate to fend off cyber-attacks but these are not effective and not sufficient to ensure the protection and privacy of important information assets. For this reason, there is a global and local trend to bridge the knowledge gap among employees in various sectors. There are institutions targeting all workers in government and private institutions at various administrative levels to raise awareness of the importance of cybersecurity and to identify the most serious threats and ways to deal with them. Among the most prominent of these institutions is the national authority for cybersecurity in Saudi Arabia, we found that 81.5% of SMEs in Saudi Arabia did not deal with the authority; and that 76.6 of them did not deal with any government agency to help them with information security; where SMEs believe that cybersecurity It is not that urgent for their systems even that 48.4% of organizations do not have an cybersecurity program and that 14.1% of those have a documented cybersecurity program and the remainder of the ratio is divided between planning or partly executed.

Through the study, it became clear that there is a weakness in the awareness of cybersecurity among many employees who are considered the weakest link in the information system with the erroneous belief that the responsibility for cybersecurity lies with the cybersecurity department alone, as it found 40.6% of the institutions indicated that the cybersecurity officer does not work in compliance with other

company units such as (human resources, personnel affairs, administration). And only 12.5% do the work in concord.

40.6% of the questionnaire participants confirmed that there was a lack of experience and qualifications of cybersecurity officers and managers, and that 18.8% of those found that their skills and capabilities are sufficient and appropriate. This deficiency is the main reason behind the direct and obvious damage suffered by companies, and it turns them into easy targets for attackers.

One of the questionnaire questions was, what do you think of the role of the national cybersecurity authority? The responses were few seven institutions out of sixty-four participated in the questionnaire, because they did not deal with it, but those who dealt with it praised its positive role for protecting cybersecurity in the Kingdom, but the efforts made in their opinion seem to still be within the scope of guidelines, meetings and seminars. We have -touched that companies need practical training to help them build a complete and integrated cybersecurity system in their institutions.

4.4 Case Study (Najm Company)

Established with the aim to develop a convenient, welcoming platform to manage accident related activities in Saudi Arabia, Najm attends the needs of both the general public and insurance companies. Najm has been serving its consumers with the aim to present a vast array of vehicle insurance services [23].

Table (9): Case Study (Najm Company)

	Section I: Institution Information	
1.1	Institution name and field of work	Najm co, for insurance services.
1.2	Contact name and job qualifications	-
1.3	E-mail	f.alghamdi@najm.sa
1.4	Mobile Number	0568694320
1.5	Number of Employees	2000
1.6	Did you deal with the National Authority for cybersecurity in Saudi Arabia?	Yes
1.7	Your comments if you deal with the National Authority for cybersecurity in Saudi Arabia.	Yes
1.8	Have you interacted with government agencies regarding cybersecurity?	-

	Section II: Risk Management	
Score	Scoring: Not Implemented = 0, Planning Stages = 1, Partially Implemented = 2, Close to Completion = 3 and Fully Implemented = 4.	
3	هل لدى مؤسستك برنامج موثق للأمن السيبراني؟	2.1
3	هل أجرت مؤسستك تقييمًا للمخاطر لتحديد الأهداف الرئيسية التي يجب دعمها بواسطة برنامج الأمن السيبراني الخاص بك؟	2.2
3	هل حددت مؤسستك الأصول الهامة والوظائف التي تعتمد عليها؟	2.3
3	هل تم تحديد تهديدات أمن المعلومات ومواطن الضعف المرتبطة بكل من الأصول والوظائف الحرجة؟	2.4
3	هل تم تخصيص تكلفة لفقدان كل أصل أو وظيفة مهمة؟	2.5
4	هل لديك استراتيجية مكتوبة للأمن السيبراني؟	2.6
3	هل تتضمن hاستراتيجية الأمن السيبراني المكتوبة الخاصة بك خططًا تسعى إلى تقليل المخاطر إلى مستوى مقبول بشكل فعال، مع الحد الأدنى من الاضطرابات في العمليات؟	2.7
3	هل يتم مراجعة الاستراتيجية وتحديثها على الأقل سنويًا أو أكثر عندما تتطلب التغييرات المهمة ذلك؟	2.8
25	TOTAL POINTS	

	Section III: People	
2	هل هناك شخص أو مجموعة مسؤولة عن الحفاظ على برنامج الأمان وضمان الامتثال؟	3.1
4	هل يمتلك مديرو وموظفو الأمن السيبراني للمؤسستك الخبرة والمؤهلات اللازمة؟	3.2
3	هل المسؤولية محددة بوضوح لجميع مجالات بنية الأمن السيبراني والامتثال والعمليات ومراجعات الحسابات؟	3.3
3	هل تم تعيين مسؤولية محددة لتنفيذ خطط استمرارية العمل واستعادة القدرة على العمل بعد الكوارث (سواء داخل أو خارج وظيفة الأمن السيبراني)؟	3.4
3	هل لديك برنامج تدريبي مستمر لبناء المهارات والكفاءات من أجل الأمن السيبراني؟	3.5
3	هل يعمل موظف الأمن السيبراني بنشاط مع الوحدات الأخرى (الموارد البشرية، شؤون الموظفين، الإدارة) لتطوير وتطبيق الامتثال لسياسات وممارسات الأمن السيبراني؟	3.6
4	هل قمت بتنفيذ برنامج للتثقيف والتوعية في مجال الأمن السيبراني بحيث يعرف جميع المسؤولين والموظفين والمزودين الخارجيين والضيوف وغيرهم سياسات الأمن السيبراني التي تنطبق عليهم وتوضح مسؤولياتهم؟	3.7
22	TOTAL POINTS	

	Section IV: Processes	
	Security Technology Strategy	
3	هل لدى مؤسستك بنية أمنية رسمية للمعلومات، بناءً على تحليل إدارة المخاطر واستراتيجية الأمن السيبراني؟	4.1
3	هل يتم تحديث بنية الأمان بشكل دوري لمراعاة الاحتياجات والاستراتيجيات الجديدة وتغير التهديدات الأمنية؟	4.2
3	هل وضعت إجراءات لإشراك موظفي الأمن في تقييم ومعالجة أي آثار أمنية قبل شراء أو إدخال أنظمة جديدة؟	4.3
3	إذا تبين أن النظام المنشور لا يتوافق مع بنيانك الرسمي، فهل هناك عملية وإطار زمني محدد لجعله متوافقًا أو لإزالته من الخدمة أو التطبيقات أو العمليات التجارية؟	4.4
3	هل هناك إعدادات تكوين محددة وموثقة متعلقة بالأمان لجميع الأنظمة والتطبيقات؟	4.5
	Policy Development and Enforcement	
3	هل سياسات الأمن السيبراني المكتوبة متسقة وسهلة الفهم ومتاحة بسهولة للمسؤولين والموظفين والشركاء؟	4.6

2	هل هناك طريقة لإيصال السياسات الأمنية للمسؤولين والموظفين والشركاء؟	4.7
3	هل النتائج المترتبة على عدم الامتثال لسياسات الشركة يتم توصيلها وتطبيقها بوضوح؟	4.8
3	عند تحديث السياسات أو تطوير سياسات جديدة، هل يتم إجراء تحليل لتحديد الآثار المالية والمتعلقة بالموارد المترتبة على تنفيذ السياسة الجديدة؟	4.9
3	هل تعالج سياسات الأمان الخاصة بك بشكل فعال المخاطر المحددة في تحليل المخاطر / تقييمات المخاطر الخاصة بك؟	4.10
3	هل يتم النظر في قضايا الأمن السيبراني في جميع القرارات المهمة داخل المؤسسة؟	4.11
	Information Security Policies and Procedure	
	بناءً على استراتيجية إدارة مخاطر أمن المعلومات لديكم؛ هل لديكم سياسات أو إجراءات أمنية مكتوبة رسمية تتناول كل مجال من المجالات التالية؟	
3	المسؤوليات الفردية للموظفين عن ممارسات أمن المعلومات	4.12
3	الاستخدام المقبول لأجهزة الكمبيوتر والبريد الإلكتروني والإنترنت	4.13
3	حماية الأصول التنظيمية، بما في ذلك الملكية الفكرية	4.14
3	إدارة مشكلات الخصوصية، بما في ذلك انتهاكات المعلومات الشخصية	4.15
3	ممارسات ومتطلبات التحكم في الوصول والتوثيق والترخيص	4.16
3	تصنيف البيانات والاحتفاظ بها وتدميرها	4.17
3	تبادل المعلومات، بما في ذلك تخزين ونقل البيانات المؤسسية عن الموارد الخارجية	4.18
3	إدارة الثغرات الأمنية	4.19
3	التخطيط للطوارئ التعافي من الكوارث	4.20
3	توثيق الحوادث والاستجابة لها	4.21
3	مراقبة الامتثال الأمني وتطبيقه	4.22
2	الأمن المادي وتصاريح الموظفين	4.23
3	الإبلاغ عن الأحداث الأمنية للأطراف المتأثرة، بما في ذلك الأفراد والجمهور والشركاء	4.24
3	التحقيق الفوري وتصحيح أسباب الفشل الأمني	4.25
3	النسخ الاحتياطي للبيانات وتأمين التخزين خارج الموقع	4.26
3	نقوم بالتخلص الآمن من البيانات أو الوسائط القديمة أو المواد المطبوعة التي تحتوي على معلومات حساسة	4.27
	Physical Security	
	بالنسبة إلى مراكز البيانات الهامة وغرف البرمجة ومراكز عمليات الشبكة والمرافق أو المواقع الحساسة الأخرى:	
3	هل توجد تدابير أمنية مادية متعددة لتقييد الدخول القسري أو غير المصرح به؟	4.28
3	هل هناك عملية لإصدار المفاتيح و/ أو الرموز و/ أو البطاقات التي تتطلب ترخيصًا مناسبًا والتحقق من الخلفية للوصول إلى هذه المنشآت الحساسة؟	4.29
3	هل الأجهزة الأساسية والأسلاك الخاصة بك محمية من فقدان الطاقة والعبث والفشل والتهديدات البيئية؟	4.30
	Security Program Administration	
4	هل تقوم مؤسستك باختبار وتقييم أو تدقيق برنامج الأمان السيبراني والممارسات والضوابط والتقنيات بشكل دوري لضمان تنفيذها بفعالية؟	4.31
3	هل تجري تقييماً مستقلاً دوريًا أو تدقيقًا لبرنامج وممارسات الأمن السيبراني لكل وحدة أعمال؟	4.32
3	هل يقوم كل تقييم أو تدقيق دوري بتقييم مدى امتثال كل وحدة عمل لمتطلبات إطار عمل قياسي للأمن السيبراني وسياسات ومعايير وإجراءات وإرشادات الأمان السيبراني ذات الصلة؟	4.33
98	TOTAL POINTS	

	Section V: Technology	
3	هل الخوادم القابلة للوصول إلى الإنترنت محمية بواسطة أكثر من طبقة أمان واحدة؟	5.1
3	هل يتم فحص الشبكات والأنظمة والتطبيقات الخاصة بك بشكل دوري للتحقق من عدم وجود ثغرات أمنية وكذلك تكامل التكوينات؟	5.2
3	هل تراقب باستمرار شبكاتك وأنظمتك وتطبيقاتك في الوقت الفعلي للوصول غير المصرّح به والسلوكيات الشاذة مثل الفيروسات أو إدخال الكود الضار أو محاولات الاختراق؟	5.3
3	هل البيانات الحساسة مشفرة ومفاتيح التشفير المرتبطة محمية بشكل صحيح؟	5.4
3	هل توجد آليات فعالة وموثوقة لإدارة الهويات الرقمية (الحسابات، المفاتيح، الرموز) طوال دورة حياتها، من التسجيل إلى الإنهاء؟	5.5
3	هل تدعم جميع الأنظمة والتطبيقات الخاصة بك إدارة تغيير كلمة المرور التلقائية أو تنفذها تلقائيًا أو انتهاء صلاحية كلمات المرور، فضلاً عن تعقيد كلمة المرور وقواعد إعادة الاستخدام؟	5.6
3	هل لديك نظام تخويل يفرض حدود زمنية وتقصير عن الحد الأدنى للامتيازات؟	5.7
3	هل تطبق أنظمتك وتطبيقاتك ممارسات إدارة جلسة العمل(session) ؛ وقفل شاشة سطح المكتب؟	5.8
4	هل كل حاسوب والخادم محمي ببرنامج مكافحة الفيروسات؟	5.9
4	مع مراعاة الخطورة والإلحاح، هل توجد آليات للإبلاغ عن مجموعة متنوعة من الحالات الشاذة والأحداث الأمنية والرد عليها؟	5.10
32	TOTAL POINTS	

Calculate Najm Scoring:

First: The institution determines total reliance on IT score as shown in the table (4).

Table (12): Total reliance on IT score

		Low	High	Dependency
Total reliance on IT score		**0**	**8**	**Very Low**
		9	**16**	**Low**
		17	**32**	**Medium**
		33	**48**	**High**
		49	**64**	**Very High**

Najm reliance on IT with **High** score.

Second: calculate the total score in each section, and after that calculate the total of all sections (total security assessment score) as shown in the table (5).

Table (10) Total security assessment score

Total risk management score	25
Total people score	22
Total processes score	98
Total technology score	32
Total security assessment score (risk management, people, process and processes)	177

Third: Overall security evaluation rating.

High reliance on IT with total security assessment score = 177***1.448275** = 256.344675 so the overall security evaluation rating = **GOOD** according to table (6).

Table (11): Overall security evaluation rating

NOTE:

Why do you multiply by 1.448275?
The original scoring tool contains 84 score questions, but we have 58 score questions. Therefore, to get accurate results, we must divide the number of original questions 84 by the number of questions we have 58
84/58 = 1,448275
Then we multiply the result by the number of points from the registration questions

Reliance on IT	Program Rating Ranges		Overall Assessment
Very High	0	199	Poor
	200	274	Needs Improvement
	275	336	Good
High	0	174	Poor
	175	249	Needs Improvement
	250	336	Good
Medium	0	149	Poor
	150	224	Needs Improvement
	225	336	Good
Low	0	124	Poor
	125	199	Needs Improvement
	200	336	Good
Very Low	0	99	Poor
	100	174	Needs Improvement
	175	336	Good

Chapter Five: Discussion

5.1 Results

Through research in cybersecurity and tracking the risks faced by SMEs in the Kingdom of Saudi Arabia, the study reached many important results which are as follows:

1. Cybersecurity is exposed to many of the risks and threats that occur in the internet world, while the necessary security measures are not followed to keep pace with developments to combat cyber-crime in SMEs.
2. The weakness of existing legislation on the ground, whether at the state or institutional level.
3. Despite the efforts made by the national cybersecurity authority, it is still not sufficient.
4. Lack of experience of employees in general and cybersecurity personnel in particular within SMEs, which leads to the occurrence of risks from within the institutions themselves, especially the risks of social engineering and fraud.
5. Most institutions (depending on the sample that we targeted) lack a written cybersecurity program.
6. The mistakes and omission among employees is one of the most prominent threats facing cyber security in institutions.
7. Institutions do not attach much importance to classification of their information.
8. There are no ready-made plans to restore the work in emergency situation to most institutions.

5.2 Recommendations

In light of achieving the goals of the study and the results of the analysis, researchers can make a set of recommendations as follows:

1. The results of the questionnaire issued a loud warning that cybersecurity professionals are not present in most of the SMEs in Saudi Arabia, and this calls for the concerned authorities to do more to attract and appoint some specialists in this aspect or at least motivate the existing workers financially. Or morally to be more familiar with the cybersecurity.
2. Institutions should build their own cybersecurity policies, work to publish and implement them, and develop and review them, as these policies have an impact in improving security procedures, clarifying frameworks that guide individuals 'work, and increase their awareness.
3. An invitation to develop the role of the national cybersecurity authority, so that it provides free consultations, extensive practical training for institutions as well as helping institutions build a safe and advanced cybersecurity plans within global standards.
4. The researchers see the necessity for the administration to develop classifications of information in a way that suits its business and the confidentiality of its information, while isolating the data and information whose presentation to the public is harmful to information systems.
5. Improving mechanisms for controlling access to information systems, establishing programs and procedures for roles and powers within information systems and focusing on information security imperatives and its three pillars: (availability, integrity, confidentiality).

5.3 The Proposed Cybersecurity Framework in the Smes in Saudi Arabia

The researchers recommend following the proposed cybersecurity framework in the SMEs in Saudi Arabia that is based on global standards in the field of cybersecurity.

Although there is no set of criteria that can deal with every possible scenario, this framework provides a comprehensive structure that deals with the basic controls in all known areas necessary to provide CIA (confidentiality, integrity, and availability) of the institutions' information assets, and this framework also provides guidance for the officials to make priority decisions.

Risk assessment

Institutions Must Follow the Following:

1. It is very important to assess threats and weaknesses to determine what the institution's security situation is and to develop solutions for the most successful threats to occur and the most influencing the continuity of the institution's performance [24].
2. This is done by constantly checking all that is new about the security threats to the services used in the institution, obtaining and evaluating new information, and taking action on it to identify and treat weaknesses and reduce the rate of exploitation of the threat by the attacker [25].
3. Adequate time, effort, and resources should be devoted to managing and correcting weaknesses.
4. Programs should be updated periodically after ensuring that the update will be compatible with the hardware; also after collecting sufficient information about the new update and its advantages.
5. Cybersecurity bulletins should be published among staff [26].
6. Carefully perform system risk analysis and compare the result with the threat model to ensure that adequate controls exist to prevent attacks.

Mitigate and Respond to Risks:

Institutions must follow the following:

1. Document the requirements of the cybersecurity system so that its components can be designed, implemented and tested to ensure that these requirements are met; and document how to solve problems and close gaps [27].
2. Remove unnecessary user accounts.
3. Remove unnecessary file shares.
4. Remove or disable unsafe operating-system services and ports.

Work Environment:

1. Establishing policies and procedures that address operational, administrative and technical issues.
2. Organizations must establish a specific mechanism to define and review the policy management plan periodically [28].

Asset Management:

1. Track devices such as mobile phones and computers on the wireless network.
2. Know and track programs and services on these devices on the network[29].
3. Track gaps on the network and put protection on the network.

Asset Control:

1. Track employee accounts and establish a specific mechanism for this.
2. Establishing standards to protect sensitive systems in institutions.
3. Establish a mechanism for granting permissions and determining the minimum permissions for each employee, according to what he needs.
4. Grant administrative permissions to a small number of trusted employees.

5. Establish password policies for the organization.

Communication Security:

1. Screen should be locked on systems to restrict access to unattended workstations.
2. Data access should be restricted, permissible internet addresses (IP addresses) restricted and data flow reduced.
3. Web applications should be protected and exposing common web attacks.

Physical Security:

1. It should be ensured that the backup copies are properly protected via physical security or encryption when stored, and when transferred over the network, and make sure that the backup copies are safe and that they are ready to be used when needed.
2. Technical and procedural controls to monitor physical access should be documented and implemented at all access points at all times.

Resource Security and External Relations

1. Standards and requirements must be established when dealing with external companies to negotiate contracts for the purchase of secure configuration systems.
2. It should be ensured that service level agreements and other contractual tools are properly promoted so that sellers and partners fulfil their obligations.
3. Recruitment practices and employee and partner information checks should be reviewed to ensure they comply with policies and evidence request to ensure the level of security in the product and that it is designed correctly.

Security throughout the Asset Life Cycle:

1. To test software internally developed on the Internet and other application software in order to identify potential errors and vulnerabilities [30].

Emergency Planning and Disaster Recovery:

1. Establishing and documenting emergency plans and procedures, based on commercial and security impacts, as it ensures that the institution is able to recover the assets of important information, continue operations after a major interruption, and train staff to deal with accident and emergency plans.
2. Developing and testing business continuity plans and restoring the ability to work after disasters, to ensure that critical information system operations can be restored within an acceptable time frame [31].

Awareness and Training:

1. Educating the technical staff about the threats inside the organization by sending an email and relying on external references [32].
2. Follow a security awareness program that includes detailed objectives and regularly reviews its content [33].
3. Training employees in security awareness, especially those who have access to assets.

References

1. https://www.eyeofriyadh.com/ar/news/details/1536057726- (11/02/2020)
2. https://www.eyeofriyadh.com/ar/news/details/1536057726- (11/02/2020)
3. Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms; Claire Vishik, Mihoko Matsubara, Audrey Plonk; p1
4. Information Security Risk Assessment Toolkit; Mark Ryan M.Talabis Jason L. Martin Evan Wheeler, Technical Editor; 2013 Elsevier, p114.

5. Global Information Assurance Certification Paper; SANS institute, p4.
6. Introduction to Cyber Security; Jeetendra Pande, p15
7. http://www.tra.gov.lb/Cybersecurity-in-few-words-AR (10/3/2020)
8. https://en.wikipedia.org/wiki/ISO/IEC_27001 (10/3/2020)
9. https://www.tuv.com/turkey/en/iso-27001-certification.html (10/3/ 2020)
10. https://cyberexperts.com/cybersecurity-frameworks/ (10/3/2020)
11. National Cybersecurity Challenges and NIST; Donna F. Dodson, p5
12. https://nca.gov.sa/en/pages/about.html (10/3/2020)
13. https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0 (10/3/2020)
14. https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0 (10/3/2020)
15. https://nca.gov.sa/pages/about.html (20/3/2020)
16. https://nca.gov.sa/pages/about.html (20/3/2020)
17. https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0 (22/3/2020)
18. https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0 (22/3/2020)
19. https://nca.gov.sa/pages/about.html (23/3/2020)
20. https://nca.gov.sa/pages/about.html (23/3/2020)
21. https://nca.gov.sa/pages/about.html (23/3/2020)
22. https://www.semanticscholar.org/paper/Enterprise-oriented-cybersecurity-management-Chmielecki-Cho%C5%82da/14d08e6f36314c8a10b69ff0d2e539e63a75dd1e/figure/7 (9/3/2020)
23. https://www.najm.sa/en/about-us (1/4/2020)
24. The CIS Critical Security Controls for Effective Cyber Defense ," Council on Cyber Security CSC 2-2 ", May 2015 , p20.
25. The CIS Critical Security Controls for Effective Cyber Defense ," Council on Cyber Security CSC 2-2 ", May 2015 , p20.
26. How to Implement Security Controls for an Information Security Program at CBRN Facilities , NRECA Cyber Security p20.

27. How to Implement Security Controls for an Information Security Program at CBRN Facilities , NRECA Cyber Security plan 48 p20.
28. The CIS Critical Security Controls for Effective Cyber Defense ," Council on Cyber Security CSC 14-7 ", May 2015 , p30.
29. "Council on Cyber Security CSC 2-5 - Inventory of Authorized and Unauthorized Software", May 2015 , p27.
30. The NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan," NRECA Cyber Security Plan 125", p62.
31. NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan," Unique Security Requirements and Controls For Each Smart Grid Activity Type, Supervisory Control and Data Acquisition (SCADA)",2011, p97.
32. NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan," Addressing Process Risks,
33. Operational Risks",2011, p37.
34. NRECA Guide to Developing a Cyber Security and Risk Mitigation Plan," The NRECA Cyber Security" Plan 21 p32.

Appendix

Appendix (1):

Please visit this link https://docs.google.com/forms/d/e/1FAIpQLSfxouFCR-b9quCjx-N97kTLkE8-KuaTZ4mt-dauvuy_ZQPwZA/viewform?fbzx=1763174177582577764.