The Role of Cybersecurity KPIs in Enhancing the Quality of Cybersecurity and Information System Audit in Kuwait Oil and Gas Sector

Author/ Fatima Nabeel Jaafar
Senior Auditor

ARABOSAI 14th Scientific Research Competition in the Field of Financial Auditing

June 2024

*This award-winning research paper was originally written in **Arabic** and has been translated into **English** for broader accessibility. In case of any discrepancies between the translated and original versions, the original Arabic version shall prevail.*

Translation Section – The State Audit Bureau of Kuwait

March 2025 ©

Table of Contents

List of Figures

List of Tables

Abstract

This research paper is intended to explore the vital role of cybersecurity key performance indicators (KPIs) in elevating the quality of cybersecurity and information system auditing in Kuwait's oil and gas sector. The research emphasizes the importance of these indicators in enhancing cybersecurity audits as well as the audits of information systems, thereby improving the quality of audit findings as a whole and ensuring a robust cybersecurity infrastructure in Kuwait's oil and gas sector. For purposes of this research, the researcher prepared a web-based survey as part of a field study conducted on a sample of professionals from Kuwait Petroleum Corporation (KPC) and its subsidiaries along with a sample of auditors from the State Audit Bureau (SAB) who are in charge of auditing the oil and gas sector in Kuwait. The study yielded several findings, the most important of which would be that KPC and its subsidiaries will not be able to effectively monitor cybersecurity risks or achieve high-quality audit findings without implementing the measurement of cybersecurity KPIs. Upon analyzing the survey results, it was found that measuring cybersecurity KPIs contributes to improving the quality of audit findings. The field study also revealed a critical need to provide enhanced cybersecurity training within KPC and its subsidiaries. The results indicated that further awareness and training on cybersecurity is essential for boosting the ability of professionals to keep pace with relevant developments and ensure the protection of sensitive data in the oil and gas sector. The present study concludes with several recommendations, the most prominent of which is to measure cybersecurity KPIs within KPC and its subsidiaries. This step would positively reflect on audit planning by ensuring regular review and enhancement of measures to protect this vital sector, the state's primary source of income,

from cyberattacks. Other recommendations of the study also include supporting Kuwaiti cadres working in the field of cybersecurity and information system auditing. Such support is deemed necessary as cybersecurity and information system auditors play a crucial role as the first line of defense in identifying vulnerabilities, providing recommendations to address any potential vulnerabilities in the future, and thereby protecting the national information assets in the oil and gas sector. The study also highlights that investing in human resources within KPC and its subsidiaries in the areas of cybersecurity and information systems is a vital strategic approach to enhancing their capabilities. These efforts would, therefore, contribute to protecting Kuwait's oil and gas sector and achieving its long-term strategic goals.

Research Keywords: Kuwait's oil and gas sector – cybersecurity risks – cybersecurity KPIs – cybersecurity and information system audit – audit quality – cybersecurity – KPIs – the State of Kuwait.

Introduction

Introduction

Nowadays, the audit profession in Kuwait's oil and gas sector is undergoing numerous positive and negative changes caused by the pressures and challenges facing this sector in particular. These pressures stem from the increasing reliance on information technology (IT) within the sector to accomplish tasks across all stages of production and processing. Such a reliance creates an urgent need for utilizing IT tools in performing audits, particularly given the vast amount of data and information to be audited. Due to the confidentiality and sensitivity of these massive data, ensuring data protection has become a mandatory, not an optional, task, which can be achieved by adopting cybersecurity and information systems audits.

Given the advancements in digital technology and the increasing reliance on IT, the significance of cybersecurity audits and cybersecurity KPIs continues to grow in Kuwait's oil and gas sector. This research explores the importance of measuring these indicators to enhance the quality of cybersecurity and information system audits. It evaluates how these indicators contribute to improving the efficiency and effectiveness of audit processes along with ensuring robust responses to cybersecurity threats in this vital sector.

The introduction of cybersecurity over the last few years has brought radical transformations to audit practices in Kuwait's oil and gas sector. The complexity of financial and business transactions in the oil and gas industry has posed challenges to cybersecurity audits. It has also made it difficult to assess the status quo of cybersecurity in state-owned oil companies in Kuwait. In addition, conducting timely cybersecurity and information system audits and protecting

public properties from cyber threats has become increasingly challenging in this vital sector, which represents the primary source of income for the country.

In response to these challenges, considerable efforts have been made within the sector. Several strategies, work systems, standards, and guidelines have been developed in the domain of cybersecurity and information system audits. These efforts aim to facilitate the measurement of cybersecurity KPIs and correct the course of cybersecurity and information system audits within Kuwait's oil and gas sector.

It is worth mentioning that keeping abreast with the relevant developments in the domain of information technology and cybersecurity contributes to the advancement of the oil and gas sector. The adoption of information technologies and the integration of cybersecurity practices would enhance the protection of public funds, secure a company's operations from cyberattacks, and improve the quality of work performed. Although it helps create a paperless environment, which aligns with global trends, the use of modern technologies has also introduced more significant cybersecurity risks. Collecting and uploading sensitive data on a company's internal network and storing such data on the cloud could generate further cybersecurity risks to the oil and gas industry. While many studies have examined the relationship between IT and improved audit quality in the past years, few have specifically addressed the role of cybersecurity KPIs in improving the quality of cybersecurity and information system audits in Kuwait's oil and gas sector. This study, therefore, fills a significant research gap and provides added value to the cybersecurity and industrial sectors.

In recent years, Kuwait has witnessed serious attempts to establish a professional cybersecurity framework. These efforts include the development of a well-defined strategy and fundamental principles on the concept of cybersecurity and the audits of cybersecurity and

information systems. This research explores approaches for measuring cybersecurity KPIs in Kuwait's oil and gas sector, aiming to enhance the quality of cybersecurity and information system audits performed in the sector. The study also explores the importance of improving audit quality through the measurement of KPIs and their impact on enhancing audit outcomes.

In addition to discussing the role of cybersecurity KPIs in elevating the quality of cybersecurity and information systems auditing in Kuwait's oil and gas sector, this research examines how measuring these indicators would positively reflect on the audit reports issued by the state-owned oil and gas companies in Kuwait, as well as SAB audits reports. The study also seeks to develop the skills of auditors by proposing mechanisms for auditing cybersecurity and information systems in the oil companies subject to SAB's audit. The research paper comprises five chapters, as follows:

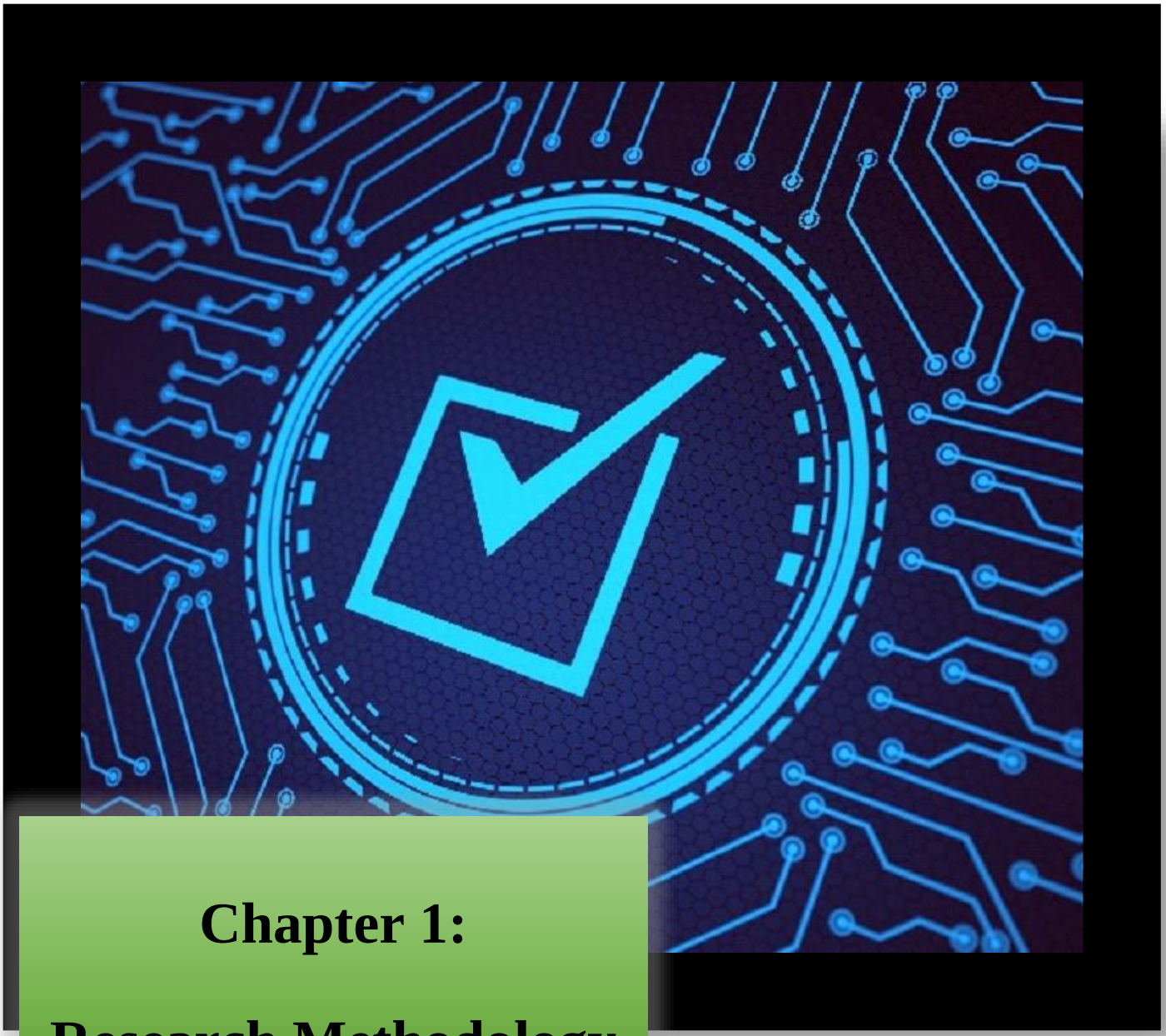
- **Chapter 1** outlines the research methodology. This chapter includes the following sections: Introduction, Research Problem, Research Hypotheses, Importance of the Study, Research Objectives, and finally the Research Scope.
- **Chapter 2** focuses on the research review, encompassing key topics presented in the following sections:
  - **Section 1:** The Evolution of Cybersecurity and Definitions Related to Cybersecurity and Information Systems
  - **Section 2:** The Oil and Gas Industry in Kuwait
  - **Section 3:** Cybersecurity and Information Systems in the Global Oil and Gas Sector and Kuwait's Oil and Gas Sector
  - **Section 4:** The Investment in Cybersecurity and Information Systems in Kuwait's Oil and Gas Sector

- **Section 5:** Case Studies of Cyberattacks on the Oil and Gas Sector
- **Section 6:** Cybersecurity Frameworks
- **Section 7:** The Benefits of Cybersecurity and Information Systems Audits in Performing and Documenting Audit Work, Protecting Public Funds, and Ensuring National Security
- **Section 8:** The Importance of Cybersecurity KPIs and Their Positive Impact on Audit Quality
- **Section 9:** Auditing Cybersecurity and Information Systems in Selected SAIs
- **Section 10:** A Look into the Future of Cybersecurity in Kuwait's Oil and Gas Sector

➢ **Chapter 3** discusses the scientific framework of the research and the field study. This chapter includes the methodology, the research population and sample, and the study tool, i.e., web-based survey, which was specifically designed for the field study.

➢ **Chapter 4** presents an analysis of the field study using the SPSS statistical software.

➢ **Chapter 5** comprises the key findings and recommendations that should be taken into consideration to enhance and develop the audit role of Kuwait's oil and gas sector, as well as the State Audit Bureau, in the domain of cybersecurity and information systems auditing. These findings and recommendations emphasize the importance of keeping pace with the latest advancements in information technology while ensuring national security by safeguarding the state's sole source of income against cyberattacks. In addition, the presented recommendations highlight the necessity of supporting and fostering auditors' skills to improve the quality of audit outcomes within the oil and gas sector through the measurement of cybersecurity KPIs. The implementation of such measurement practices is deemed critical, based on the principle that "what cannot be measured cannot be improved".



Chapter 1:

Research Methodology

Chapter 1

Research Methodology

Introduction

Business in the oil and gas sector has faced many functional changes and challenges in the last two decades of the twentieth century. The complete automation of all works in the sector, as well as the shift to the total reliance on electronic systems at all stages of the oil and gas extraction, including exploration, refining, production, manufacturing, and the marketing of oil and gas products, were the most prominent of these changes and challenges. Accordingly, many systems and applications have been established that have contributed to raising the quality of audit outcomes and promoting the use of cybersecurity in the sector in order to protect sensitive data from cyberattacks and ensure business continuity. Furthermore, several features and elements were introduced in the audit environment due to the concern of cyber risks and threats, in addition to the audit of cybersecurity and information systems.

Supreme Audit Institutions (SAIs) in various countries are embracing an approach towards Cybersecurity Audit (CSA), information systems audit, and digital transformation. Such an approach requires the automation of all works and tasks in the oil and gas sector to improve and develop the audit work, and that is done by facing the challenges and obstacles found in the evolving environment of the oil and gas sector. Human investment through continuing professional education (CPE) in cybersecurity, information technology, and artificial intelligence is an effective tool that positively affects auditors' performance in all stages of cybersecurity and information systems audits. Such an investment would also contribute to enhancing the quality of audit outcomes in the oil and gas sector.

Based on the above, this research will demonstrate the importance of implementing the measurement of cybersecurity key performance indicators (cybersecurity KPIs) in the oil and gas sector in the State of Kuwait. Furthermore, the paper will address the advantages of using cybersecurity KPIs in cybersecurity and information systems audits in relation to the performance of audit tasks and their documentation. In addition, the paper will examine the mechanism employed in Kuwait's oil sector for the audit of cybersecurity and information systems in State-owned oil companies, as well as the use of cybersecurity KPIs in elevating the quality of cybersecurity and information systems audits. Finally, we will examine the ensuing impact of using these KPIs on the reports issued by the Kuwait Petroleum Corporation (KPC), its subsidiaries, and the State Audit Bureau (SAB).

In view of the continuous development of the oil and gas sector in Kuwait, along with the increase in cyber risks and threats and the increasing technical intricacies in the sector, the use of cybersecurity KPIs to enhance the quality of cybersecurity and information system audits has become mandatory. Using KPIs would contribute to providing accurate insight into the state of digital security and the effectiveness of the preventive and corrective measures in place.

The importance of cybersecurity KPIs is reflected in enhancing the quality of cybersecurity and information system audits, as they provide standardized and accurate benchmarks for cybersecurity performance in the sector. These indicators also contribute to identifying and directing efforts toward the areas of weakness detected in State-owned oil entities where cybersecurity requires enhancement. Furthermore, cybersecurity KPIs promote transparency and accountability, thus facilitating the assessment and review of the effectiveness of the cybersecurity strategy implemented in the sector.

This research aims to contribute to clarifying the importance of measuring cybersecurity KPIs for the enhancement of audit quality in Kuwait's oil and gas sector and how to effectively apply them in order to enhance the security of information and systems against increasing cyber threats in that vital sector. Hence, this paper addresses the topic of the role of cybersecurity KPIs in enhancing the quality of audit work, in addition to examining the oil and gas sector's mechanism for overseeing cybersecurity and information systems in oil companies in the public sector in Kuwait. The paper also discusses the need to develop auditors' skills in using information technology at all stages of auditing in order to enhance the quality of cybersecurity and information system audits.

Research Problem

What cannot be measured cannot be improved, and here lies the "research problem", which is specifically focused on the oil and gas sector in Kuwait. The failure of Kuwait's oil and gas sector to measure cybersecurity KPIs in KPC and its subsidiaries may reflect negatively on the results of cybersecurity and information system audits, as well as SAB's audit results. Such a failure would make it challenging to provide the requirements for the integration of information technologies in performing audit tasks on cybersecurity and information systems matters, in addition to compromising the protection of the sector's infrastructure. The sector represents the State's sole source of income, and the lack of measurement could adversely affect the development and improvement of its audit results.

It is worth mentioning that the existence of obstacles in measuring cybersecurity KPIs in Kuwait's oil and gas sector does not necessarily impede the development and improvement of the performance of audit tasks and their documentation. The research problem lies in revealing the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information systems

audits in the sector. The research problem also lies in how to use KPIs results to elevate the quality of audits and their impact on the audit reports issued by Kuwait's oil and gas sector as well as SAB reports.

Thus, the research problem can be conveyed through the following major research question:

Is there a role for cybersecurity KPIs in elevating the quality of cybersecurity and information systems audits and enhancing the audit results in the oil and gas sector in Kuwait?

The major question branches out to the following sub-research questions:

1. *Is there a role for cybersecurity KPIs in improving the quality of information in the oil and gas sector in Kuwait?*
2. *Does improving the quality of information lead to higher-quality cybersecurity and information system audits in the oil and gas sector in Kuwait?*

Research Objectives

The main objective of this research paper is to identify the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information system audits within the oil and gas sector in Kuwait. This objective may be achieved through the following sub-objectives:

- Presenting an accurate and scientific foundation for the concepts of cybersecurity, information systems, and KPIs to demonstrate their effectiveness in enhancing the quality of cybersecurity and information system audits.
- Developing proposals and recommendations that would enhance the role of the oil and gas sector in auditing cybersecurity and information systems, as well as the role of SAB in auditing cybersecurity within the oil entities in order to raise the quality of audits using

cybersecurity KPIs in Kuwait's oil and gas sector. This is in addition to enhancing SAB's reports and remarks related to the field of cybersecurity and information systems.

- Analyzing the relationship between cybersecurity KPIs and the audits of cybersecurity and information systems.
- Educating the reader about the importance of cybersecurity and information systems in the oil and gas sector in Kuwait for sustaining national security.
- Identifying the requirements for performing cybersecurity and information system audits in the public oil and gas sector in Kuwait.
- Identifying the importance of using cybersecurity KPIs to raise the quality of audits in the public oil and gas sector in Kuwait and its impact on the performance of auditors and the audit outcomes.

Research Signification

Consistent development in performance at all levels in Kuwait's oil and gas sector requires the use of IT and its maximum utilization in executing all daily tasks in this vital sector. The oil and gas sector in Kuwait is one of the most distinguished sectors, as it is marked for its outstanding performance and the fulfillment of its duties with the highest degrees of professionalism. The sector achieves that by keeping up-to-date with the latest technology in the field and keeping pace with the developments in modern IT. Furthermore, the work mechanism in the sector is regularly updated to keep up with the latest state-of-the-art technology.

The use of modern technologies and the storage of massive data of a distinct nature and sensitive national information render the measurement of cybersecurity indicators in the oil and

gas sector very vital and mandatory for facilitating the process of auditing cybersecurity and information systems. Meanwhile, the availability of cybersecurity KPIs can reflect positively on the results of cybersecurity and information systems audits and contribute to enhancing the results of the audits performed by SAB in the oil and gas sector.

With that said, this research is deemed significant for the following reasons:

1. Recognizing the role of KPC and its subsidiaries in protecting the State's sensitive information against cyber-attacks through the system in place and the information systems infrastructure. This is in addition to identifying potential future improvements.
2. Recognizing the role of cybersecurity KPIs in improving the quality of cybersecurity and information systems audit outcomes, which in turn improves decision-making within oil and gas companies.
3. Demonstrating the importance of measuring cybersecurity KPIs in the public oil and gas sector in Kuwait to enhance the results of cybersecurity and information systems audits by raising audit quality and its impact on the audit reports issued by State-owned oil companies as well as SAB reports.
4. Assisting public oil and gas companies in Kuwait in facilitating the use of cybersecurity KPIs in order to achieve the objectives of the National Cybersecurity Strategy and the strategy of KPC and its subsidiaries.
5. Raising awareness of cybersecurity in public oil and gas companies in Kuwait by defining cybersecurity KPIs and linking them to the quality of cybersecurity and information systems audits.

6. Formulating conclusions, recommendations, and proposals that support cybersecurity and information systems audits by using KPIs to prevent cyber-attacks in Kuwait's most vital sector, which represents the State's primary source of income.

Research Hypotheses

The research is based on a main hypothesis followed by several sub-hypotheses, which are as follows:

Main Hypothesis: Cybersecurity KPIs contribute to enhancing the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.

The main hypothesis branches out to the following sub-hypotheses:

Hypothesis 1: Kuwait's oil and gas sector is marked for adopting a well-defined strategy for the measurement of cybersecurity KPIs.

Hypothesis 2: The measurement of cybersecurity KPIs contributes to elevating the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.

Hypothesis 3: There are defined requirements for integrating cybersecurity into audit practices within Kuwait's oil and gas sector.

Hypothesis 4: Kuwait's oil and gas sector keeps pace with the latest advancements in the domain of cybersecurity and the audits of cybersecurity and information systems.

Hypothesis 5: Employees of Kuwait's oil and gas sector are sufficiently trained and qualified in cybersecurity.

Research Scope

The research scope includes the following:

- **Time scope:** This research was prepared in 2024.
- **Time scope for the Web-based Survey**: The field study was carried out in March 2024, targeting a segment of KPC, its subsidiaries, and SAB employees.
- **Geographical scope:** The geographical scope is limited to government-owned oil and gas companies, specifically KPC and its subsidiaries in the State of Kuwait.
- **Human scope:** This study sampled employees from KPC and its subsidiaries, including internal auditors, accountants, computer engineers, financial managers, cybersecurity experts, and information systems managers. Additionally, the sample population encompassed auditors from SAB's Oil Bodies Production and Manufacturing Audit Department, as well as the Oil Bodies Marketing and Investment Audit Department.
- **Literature scope:** Given that cybersecurity is a modern and rapidly evolving field, the literature reviewed for this research was carefully selected to ensure it reflects contemporary developments in the sector. All sources used were published between 2016 and 2024, the year this research paper was prepared.

Chapter 2: Literature Review

Chapter 2

Literature Review

In recent years, there has been a notable increase in the use of Information Technology (IT) in Kuwait's oil and gas sector and a complete reliance on it, which has led to the emergence of cybersecurity. The main factor for this increase is the large amount of data and information processed across all stages of oil and gas production. In addition, this use of technology has also had a significant impact on the audit environment, especially the audit of cybersecurity and information systems. With the advancement of information technologies and the growing reliance of Kuwait's oil and gas sector on them, the protection of sensitive information in the internal and external networks and automated systems has become a necessity. This entails the integration of cybersecurity and the measurement of cyber risks. Hence, auditing cybersecurity and information systems have come into play.

Relevantly, the oil and gas sector in Kuwait has asserted through its 2040 Strategy that it is necessary not only to embrace the concept of cybersecurity within the sector but also to invest in it. Furthermore, it has been established that employees across all departments should possess a clear understanding of cybersecurity and the IT environment. It is worth mentioning that human investment in this field can yield positive returns for the oil and gas sector. Such investment can assist auditors in defining the nature and scope of audits focused on cybersecurity and information systems. Accordingly, auditors would be better equipped with a strong foundation and extensive knowledge in this domain, supported by the presence of well-defined cybersecurity KPIs, a comprehensive cybersecurity strategy, and a set of guidelines for cybersecurity and information system audits.

It must be noted that Kuwait's growing interest in the field of cybersecurity, alongside the reliance of all state sectors on technology- particularly the oil and gas sector, which serves as the primary source of income for the state- has enabled the achievement of high levels of accuracy and performance. Nevertheless, this reliance also introduces significant risks and the potential for cyberattacks. The oil sector has actively participated in numerous cybersecurity working groups and conferences, aiming to invest in the field and enhance protection for companies against cyberattacks. Moreover, these participations were also aimed at providing assistance for the accomplishment of a range of tasks related to cybersecurity and cybersecurity KPIs.

Accordingly, this research will examine "the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information systems audit in the oil and gas sector in the State of Kuwait", which will be demonstrated under the following main sections:

Section 1: The Evolution of Cybersecurity and Definitions Related to Cybersecurity and Information Systems

This section explores the concepts of cybersecurity and information systems in a broad sense, focusing on their definitions, key objectives, and essential elements. Additionally, it examines the concepts of cybersecurity and information systems within the field of control and auditing. However, after extensive research and examination, it has been determined that there is no specific definition for the terms "cybersecurity" and "information systems", as their meanings vary from one source to another at global and local scales. This section also addresses the fundamental elements of cybersecurity and the various types of cybercrime.

Information Technology (IT) plays a pivotal role in supporting human efforts. This technology has evolved over many years and significantly contributed to advancements in various industries, particularly in the energy and industrial sectors. However, the extensive reliance on IT

for all tasks has led to the emergence of a new field known as “Cybersecurity”. Given that cybersecurity is a modern field, certain related terms need to be precisely clarified in order for the reader to understand the importance of this research, along with its sections, findings, and recommendations. To that end, this section will focus on the emergence of Cybersecurity, highlighting the most important terms in this field.

Many sources have provided definitions for Cybersecurity. However, this paper will focus on the major definitions provided by specialized authorities in the field. The National Cyber Security Center (NCSC) of Bahrain defines Cybersecurity as "*the practice of protecting any internet-connected systems, networks, software, and different types of data from cyberattacks."* The NCSC also defines Cyberattacks as "*any unauthorized attempt to expose, alter, disable, or destroy information systems*" (National Cyber Security Center of Bahrain, 2022).

Moreover, the Information Systems Audit and Control Association (ISACA) defines Cybersecurity as "*the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems."* Meanwhile, the National Institute of Standards and Technology (NIST) defines Cyberspace as "*a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers."*(National Cyber Security Center of Bahrain, 2022)

It must be noted that many sources did not differentiate between Information Security and Cybersecurity. Yet, while being interconnected, it is important to distinguish between the two terms as they still differ in meaning. Information Security focuses on the protection against external attacks and the ways to detect and respond to them. Cybersecurity, on the other hand, includes the strategy, policies, and standards relevant to the security of Cyberspace defined above,

in addition to its flexibility, recovery, and safeguarding of information. Both Information Security and Cybersecurity contribute to maintaining information confidentiality and integrity. (IDI Handbook on IT Audit for SAIs, 2022)

After addressing the definitions of Cybersecurity and Cyberspace, it is necessary to examine the term Information Systems. This term is defined as "*a set of interconnected resources and elements that interact through a process within a specific framework and operate as a single unit in a specific environment in order to achieve the organization's objectives."* (Westmark, 2004)

Information Systems include four main elements. The first is Input, which refers to information that comes from external sources and is fed into the system. The second is Processing, which involves converting input data into outputs. The third is Output, which is the tangible or intangible results produced as a consequence of processing the input data. The last element is Feedback, which contributes to taking corrective measures in order to achieve the organization's objectives. (Westmark, 2004)

Building on the above, this section will address the topic of the emergence of cybersecurity, which is contingent on the reliance on IT across various fields and sectors. The progress that occurred in the use of digital technology and the Internet has contributed to the emergence of the field of Cybersecurity. In other words, it is evident that the increased use of technology and networks has led to security threats that pose risks to local and global economies, as well as to personal data worldwide. Furthermore, the heavy reliance on digital infrastructure has rendered it vulnerable to more significant threats. As these cyber risks continue to escalate, an urgent need has arisen to develop solutions to protect states and their citizens. Such solutions mainly involved adopting strategies and tools to protect states, their economies, digital data, and infrastructures.

Hence, cybersecurity emerged as an independent discipline within IT, encompassing several elements, as demonstrated in Figure 1 below. (National Cyber Security Center of Bahrain, 2022; Benetis, 2018)

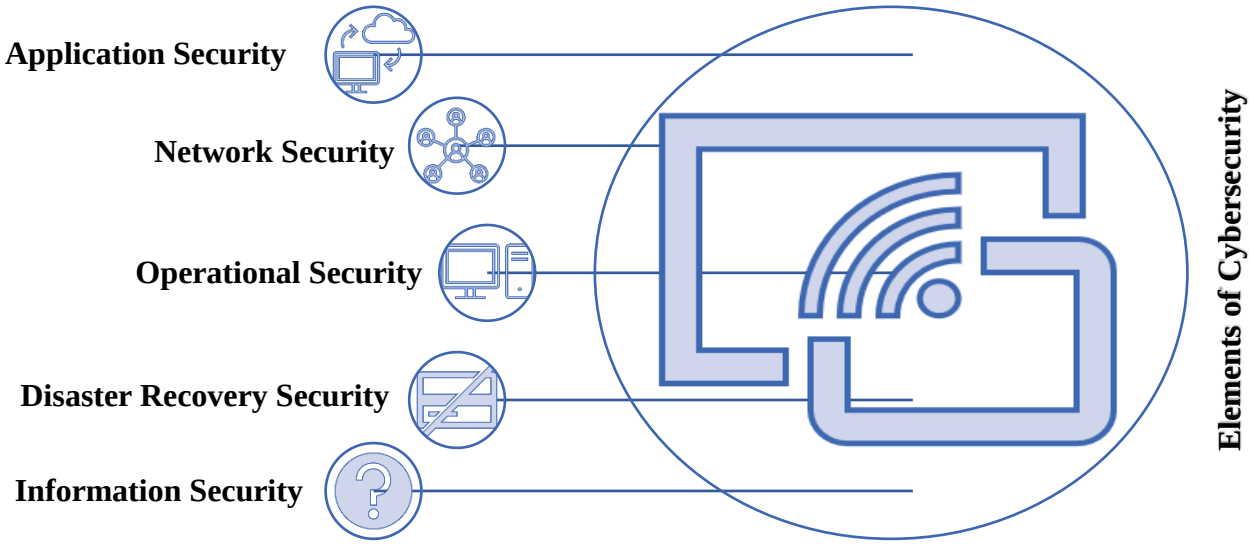


Figure 1: Elements of Cybersecurity

Source: Adapted from Benetis (2018)

After exploring the concepts of Cybersecurity and Information Systems in terms of their broad meaning and elements, the focus will now shift to examining their implications within the field of control and auditing in accordance with the definitions provided by several professional organizations. In line with the shift toward heavy reliance on IT and its developments, along with the emergence of Cybersecurity as an independent field, Cybersecurity Audit (CSA) has evolved. CSA refers to "the independent review and examination of records and activities aimed at assessing the effectiveness of cybersecurity controls and ensuring compliance with policies, operational procedures, standards, and relevant legislative and regulatory requirements." (Communications, Space & Technology Commission (CST) of Saudi Arabia, 2020)

Kuwait's National Cybersecurity Strategy 2017-2020, issued by the Communication and Information Technology Regulatory Authority (CITRA), defined CSA as "a systematic analysis of all security components including people, policies, solutions and tools used by any institution to secure its environment. Furthermore, a security audit aims to monitor compliance with security policies, assess the level of risk, and the balance between resources including organizational, technical, and human resources." (CITRA, 2016)

As for the audit of information systems, it was defined by the General Audit Manual issued by SAB as a process of testing and examining information systems through which evidence is collected and evaluated with the aim of determining whether the information system of the audited entity is designed to keep the data complete, accurate, and reliable, protects assets, and allows the achievement of the entity's objectives and the effective use of resources, in addition to emphasizing confidentiality. Cybersecurity, on the other hand, was not addressed in the manual. (General Audit Manual, 2020)

Information Technology has significantly enhanced the efficiency and quality of business operations. However, its misuse and security gaps have contributed to the rise of cyberattacks. Digital crimes have soon become a growing phenomenon, with the associated risks extending beyond local boundaries to affect global economies. (Al-Samhan, 2020)

Cybersecurity represents the future, driven by the fact that infrastructures worldwide have become prime targets. As a result, the importance of both Cybersecurity and Cybersecurity Audits has become evident. Cybersecurity aims to maintain the confidentiality, integrity, and availability of information (Mahrous & Saleh, 2022). Moreover, Cybersecurity is built on four main components, as illustrated in Figure 2.

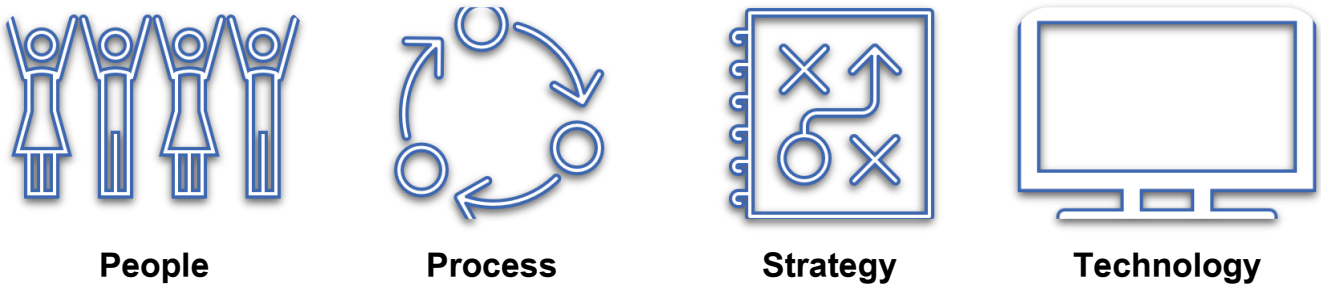


Figure 2: Main Components of Cybersecurity

Source: Adapted from Mahrous & Saleh (2022)

The implementation of cybersecurity components, mainly the strategy, would assist in achieving cybersecurity goals. It would also contribute to preventing cyberattacks and crimes that target the economy, exploit and trade personal information, and pose threats to national security. The main types of cybercrime are depicted in Figure 3 below (Mahrous & Saleh, 2022).

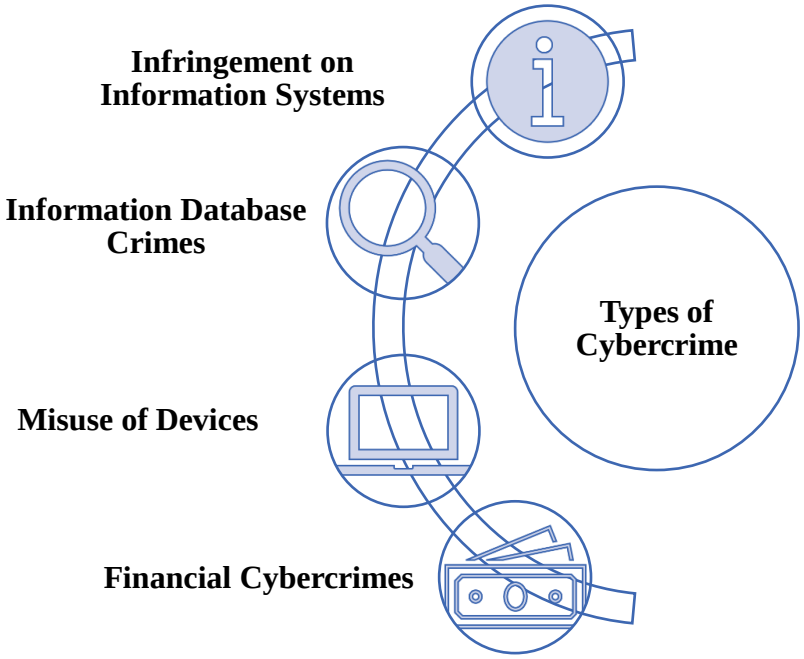


Figure 3: Main Types of Cybercrime

Source: Adapted from Mahrous & Saleh (2022)

In order to prevent future cyberattacks and crimes, states must develop a clear vision and a strategy for cybersecurity that prioritizes safeguarding national security and the economy. This national strategy should also encompass the goals of comprehensive digital transformation and infrastructure development, paving the way for the application of artificial intelligence and thereby protecting the state's vital interests across all sectors. (Al-Samhan, 2020)

Moreover, it is evident that no matter how the definitions of cybersecurity and information systems may vary, they still share the same essence. All definitions highlight that cybersecurity and information systems audits involve the collection and evaluation of evidence to ensure that the existing strategy, systems, standards, and evidence found in cyberspace are sufficient and well-designed to safeguard digital data and protect information assets, ultimately enabling the achievement of organizational goals. These audits also help identify whether resources are being used effectively and contribute to preventing cyberattacks across all sectors of the state. Furthermore, the variety of methods available for cybersecurity and information systems audits allows auditors the flexibility to choose and use the most suitable method based on the nature of the audit and the specific audit objectives to be achieved. In conclusion, it can be said that the importance of cybersecurity lies in maintaining the security and safety of the state and its citizens. (Al-Samhan, 2020)

Section 2: Oil and Gas Industry in the State of Kuwait

This section addresses the history and development of the oil and gas industry in Kuwait, along with the increasing reliance on IT to manage the massive volume of data. Since this research primarily focuses on the oil and gas sector in Kuwait, this section is a critical component, as it explores the emergence and significance of this particular sector. The role of cybersecurity in protecting this vital sector will be further discussed in the subsequent sections of the paper.

Kuwait is among the first states to produce oil and gas, with oil production serving as the primary source of income and energy. Kuwait also relies on oil as the sole source of state income, and it occupies a prominent position in the world's oil reserves, with estimates suggesting that the country can continue producing oil for the next 150 years. The first oil field in Kuwait, known as the “Burgan” field, was discovered on 22 February 1938. Prior to the year 1938, oil- referred to as ‘the black wealth’- was still undiscovered, and the black liquid found in the desert was still unidentified. Recognizing the commencement of oil production in neighboring GCC countries such as Bahrain and Saudi Arabia, the then ruler of Kuwait, Sheikh Ahmed Al-Jaber Al-Sabah, decided to sign an oil concession agreement in 1934. (Britannica, 2021)

The signing of the agreement was a sound decision. This decision shaped the future of Kuwait and its future generations, as it was the key to the country’s wealth. However, the agreement alone, without implementation and effort, did not yield immediate benefits for the state. It was the subsequent efforts made to implement its provisions that ultimately led to the discovery of oil in Kuwait. (Britannica, 2021)

Immediately after signing the agreement, the Kuwait Oil Company (KOC) conducted a field study and issued multiple technical reports and recommendations that led to the discovery of oil. During that period, the country gained experience in drilling, exploration, and oil production.

The next step was the beginning of the export of oil, which took place on 30 June 1946 with the exportation of the first shipment of crude oil. Ultimately, that pushed Kuwait to join the ranks of the world's major oil producers. By 1975, Kuwait was able to gain complete control over its oil resources and establish the Kuwait Petroleum Corporation (KPC), which now encompasses all state-owned oil companies. (Britannica, 2021)

Oil, often referred to as ‘black gold’, has become a target for many system hackers seeking access to sensitive data in Kuwait's oil and gas sector, potentially threatening the state’s economy. Mega projects in Kuwait rely on IT and massive production networks aimed at increasing production capacity, and that constitutes Kuwait’s vision for the oil and gas sector. KPC subsidiaries are working on achieving mega projects to boost the state’s economy and national income. (Britannica, 2021)

That being said, it is evident that Kuwait's oil and gas sector is vital and all companies within are closely interconnected. This heightens the risk of cyberattacks, which could have significant repercussions on both the local and global economies. Additionally, the successful implementation of mega projects in the oil and gas sector necessitates a robust infrastructure for data protection. Such an effort would ultimately facilitate the effective implementation and control of cybersecurity, as well as the development of relevant audit methods.

Section 3: Cybersecurity and Information Systems in the Global Oil and Gas Sector and Kuwait's Oil and Gas Sector

This section presents an overview of cybersecurity in the oil and gas sector worldwide and in the State of Kuwait. Furthermore, it addresses the importance of cybersecurity and information systems audits and their impact on achieving objectives related to state control, national security, and the protection of public funds and sensitive data. The section also explores the most significant cyberattacks on the oil sector, cyber risks, and cyber resilience, in addition to regional and global indicators.

The advancement of Kuwait's oil and gas sector and the use of the latest technology are factors for an increased potential for cyberattacks. This sector is considered the primary source of national income, as it is a revenue generator sector that accounts for 90% of Kuwait's national income and 40% of GDP. Consequently, protecting the oil and gas sector against cyberattacks is critical to safeguarding both the national income of the state and its GDP (RSA Conference, 2020). Additionally, the sector is marked for the distinct nature and confidentiality of its data and information, as digital assets in the oil and gas sector are classified as confidential data. Such data must be securely protected, and a strategy must be implemented for that purpose. (Technologies, 2023)

The oil and gas sector is an active source of income for the majority of states worldwide and serves as a primary source of income in a few, including Kuwait. This critical role has rendered the sector highly vulnerable and an attractive target for cyberattacks. In 2023, Sangfor Technologies classified the oil, gas, and energy sector as high-risk and among the most susceptible to cyberattacks worldwide (Technologies, 2023). In addition, an analytical study conducted in the

first half of 2023 ranked three sectors as the most vulnerable to cyberattacks, placing the energy, oil, and gas sector in second place, as illustrated in Figure 4 below. (O 'Flaherty, 2023)

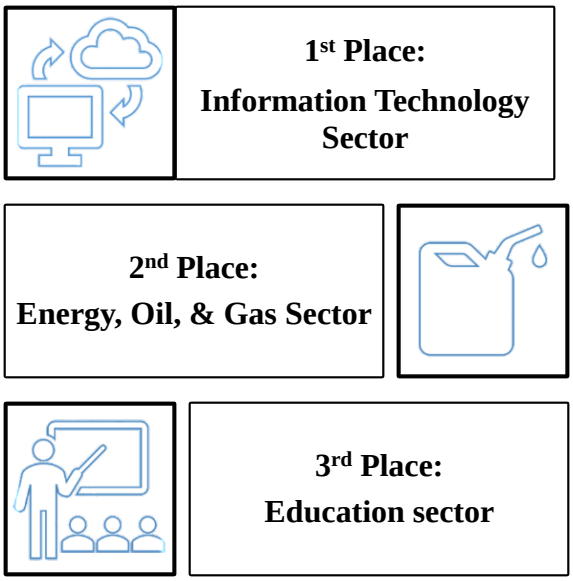


Figure 4: Sectors Most Vulnerable to Cyberattacks

Source: Adapted from O'Flaherty (2023)

The same study also indicated that companies operating in vital sectors with sensitive infrastructure and holding sensitive information assets, such as the energy and water sector, the health sector, and the transport sector, are among the most targeted sectors. This mainly owes to the data in these sectors being classified as sensitive data with an impact on national security, while the information assets in the oil and gas sector have a direct impact on the local and global economies. (O 'Flaherty, 2023)

Due to the importance of this vital sector and the associated risks, this section is also dedicated to examining the oil and gas sector as well as cybersecurity and information systems audits from several other aspects, as follows:

1) Cyberattacks on Oil Companies

The oil and gas sector has faced several cyberattacks that were documented as the biggest in the history of cyberattacks. While some oil companies have chosen to disclose these attacks, others opted to remain silent to preserve their reputation and client base. However, news has rapidly spread, and disclosure has become compulsory, as per the reports issued by several reliable sources. Figure 5 below presents six globally recognized companies in the oil and gas sector that have been targeted by cyberattacks. (Technologies, 2023)

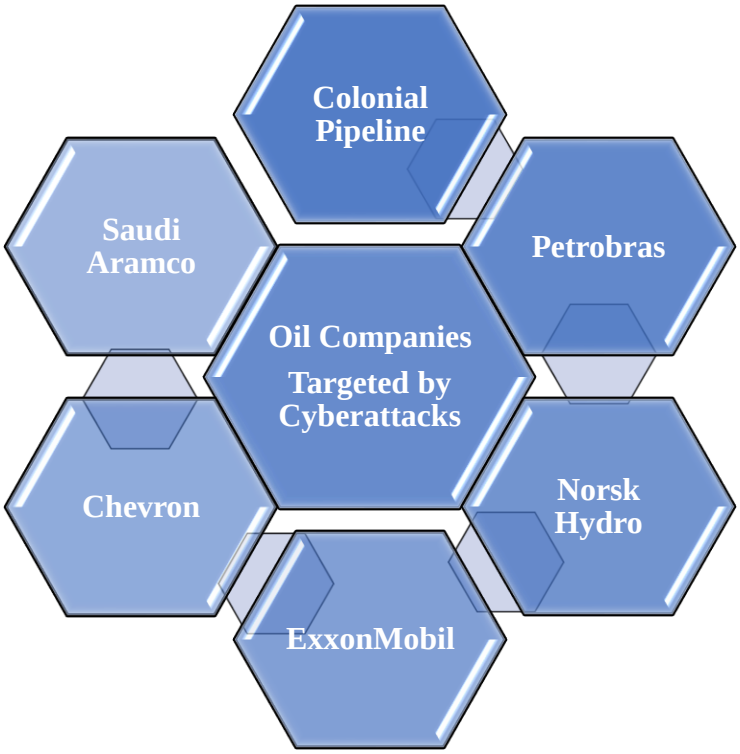


Figure 5: Oil Companies Targeted by Cyberattacks

Source: Adapted from Technologies (2023)

As depicted in the previous diagram (Figure 5), one of these companies is an international company from the GCC region, which is Saudi Aramco. However, since this research paper is intended to shed light on the oil sector in Kuwait, the cyberattack on Saudi Aramco, which is

located in the same geographical area, will be discussed in detail in a separate section. However, the occurrence of a cyberattack on an oil company within the region signals a warning for Kuwait, as its oil sector may be susceptible to similar attacks. Furthermore, examining this cyberattack incident reinforces the importance of the objective of this research paper, which is to prevent similar attacks in Kuwait's oil sector by measuring the role of cybersecurity KPIs in auditing. KPIs measurement would also contribute to identifying consequential losses. Nevertheless, the magnitude of Aramco's losses caused by the cyberattack remains undetermined as the company decided to withhold disclosure. (Technologies, 2023)

The oil and gas sector in Kuwait and other countries relies heavily on IT, making it more vulnerable to cyberattacks. As a result, auditing cybersecurity and information systems in the sector has become a necessity and a priority to address vulnerabilities, prevent future cyberattacks, and safeguard digital assets (RSA Conference, 2020). In 2022, a study recorded a number of 21 cyberattacks on the oil sector in the form of ransomware. The same study indicated that the oil and gas sector is among the most vulnerable sectors to cyberattacks due to several factors, including the nature of its data and the security gaps present in digital and information systems used across the production, extraction, and exploration stages of the industry. The existence of such gaps weakens systems and exposes companies to significant future risks. (Technologies, 2023)

2) Cyber Risks and the Audit of Cybersecurity and Information Systems in the Oil and Gas Sector

The US Accountability Office (GAO) publishes several cybersecurity reports, including the Cybersecurity Risk Report issued in 2022, which addresses cybersecurity risks in the oil and gas sector. The report highlighted that the primary factor making this sector highly vulnerable to cyber risks is the nature of its infrastructure, which relies entirely on IT. Additionally, the report pointed out that in several countries, the infrastructure of the oil and gas sector is considered outdated and fragile, particularly in monitoring and other systems. Such systems require regular updates to keep pace with rapid technological advancements. (Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure, 2022)

Auditing cybersecurity and information systems in the oil and gas sector is essential for identifying vulnerabilities. The report explains that these vulnerabilities were mainly caused by deficiencies in operational technology (OT) systems responsible for monitoring and controlling equipment, rendering it highly susceptible to cyberattacks. (Technologies, 2023)

The oil and gas sector is a primary target for hackers due to its local and global economic significance. Therefore, cyberattacks on this sector may not have an immediate impact but a future one as their consequences may extend to the economies of other countries, triggering a “ripple effect.” That means that the impact of a cyberattack may extend to more than a company in more than one location and country, impacting multiple economies worldwide. This factor makes preventing and dealing with future attacks considerably intricate and challenging. Furthermore, the ripple effect can also affect several other elements in the event of a cyberattack on the oil and gas sector, the most important of which is the fluctuation of global oil prices, oil and gas production lines, and the impact on production and exportation. (Technologies, 2023)

The role and importance of auditing cybersecurity and information systems is placed upon the auditor, and that is mainly because of its significant role in preventing cybersecurity attacks. Moreover, in case of the occurrence of cyberattacks, auditing would also assist in mitigating their effects and the chance of their recurrence. A threat analysis report issued in 2022 has ranked the oil and gas industry as "high risk" and presented several recommendations that were focused on the mitigation of cyber risks, including auditing and control. Those recommendations are summarized in Figure 6. (Cyber Risk to the Oil and Gas Industry Threat Analysis Report, 2022)

Figure 6: Key Recommendations for Cyber Risk Mitigation

Source: Adapted from Cyber Risk to the Oil and Gas Industry Threat-Analysis-Report (2022)

A study conducted by KPMG revealed significant risks in the oil and gas sector, identified through an analysis of cybersecurity threats. The key risks include: (KPMG, 2021)

i. technical and non-technical external and internal attacks;

ii. unauthorized access;

iii. disruptions to oil and gas production operations; and

iv. disruptions to security and safety systems in oil companies.

Furthermore, multiple studies have identified gaps in internal audits across most organizations. Notably, the effectiveness of internal auditing entails attracting skilled cybersecurity professionals to manage IT-related risks. If a defect or a vulnerability is detected while conducting internal audit work, cybersecurity risks cannot be accurately identified across all sectors. Therefore, it becomes evident that internal auditing plays an essential role in identifying cybersecurity-related risks. (Ameerhum, 2022; Cybersecurity risk, 2018)

3) Cyber Resilience in the Oil and Gas Sector

Cyber resilience is considered a key solution to mitigating cyberattacks. Research and studies have found that enhancing cyber resilience in the oil and gas sector- and the state in general- plays a crucial role in protecting against cyber threats. One of the most important requirements for cyber resilience is the development and implementation of a clear cybersecurity strategy to secure information systems in the oil and gas sector. Additionally, cyber resilience contributes to the long-term sustainability of companies and the preservation of their reputation. Many companies have been targeted by cyberattacks but have attempted to withhold disclosure in order to protect their

reputation. However, in today's digital era, controlling the spread of news remains a significant challenge. (Technologies, 2023; Mohammed et al., 2022)

Cyber resilience in the oil and gas sector differs significantly from other sectors. It requires the adoption of six distinct principles that are specific to the oil and gas industry, the most important of which include governance, risk assessment, and resilience, as illustrated in Figure 7 below. (Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers, 2023)

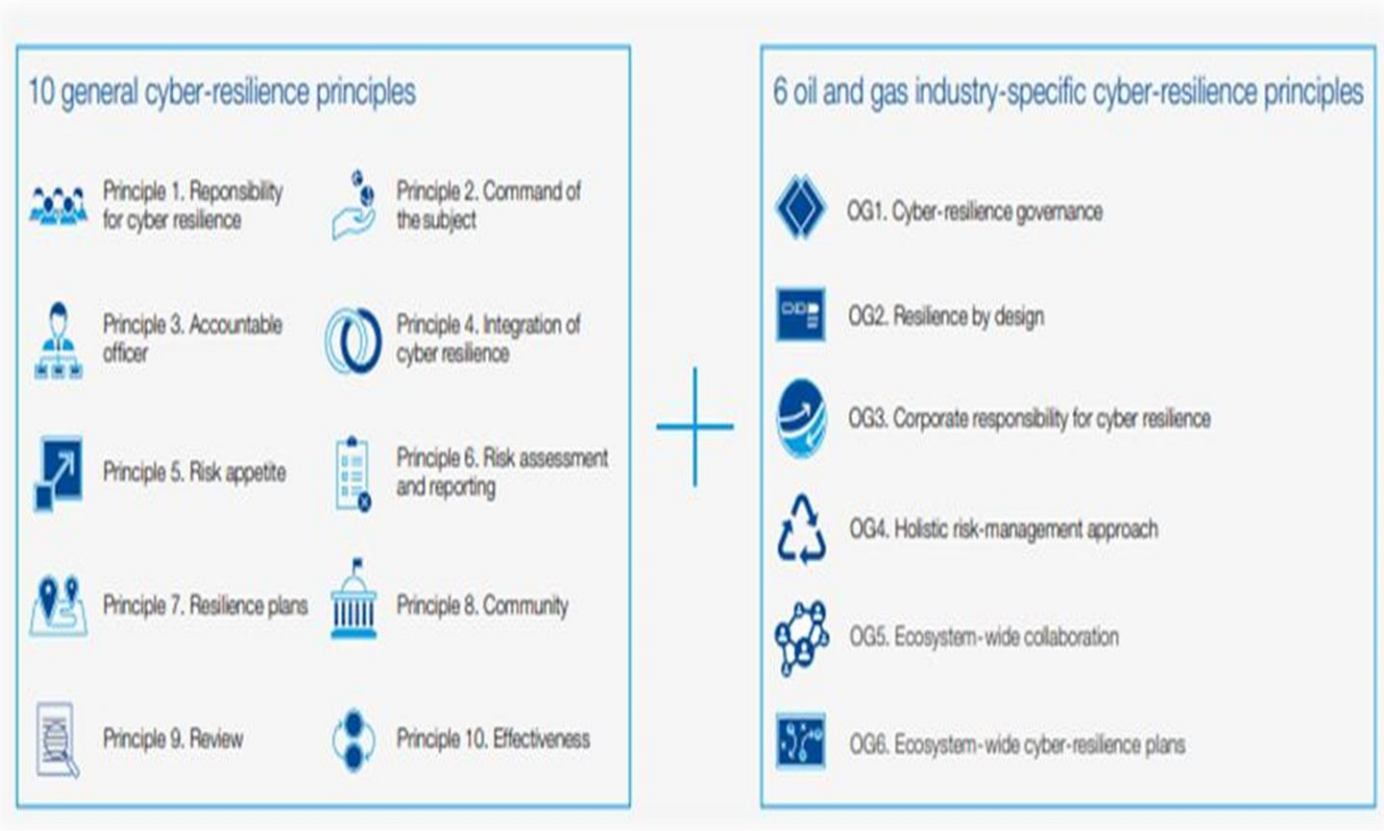


Figure 7: Cyber Resilience Principles in the Oil and Gas Sector Compared to Other Sectors

Source: Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers (2023)

4) Regional and Global Cybersecurity and Information Systems Indicators in the Oil and Gas Sector

The MENA region is a primary target for cybersecurity threat groups seeking to gain political advantages and disrupt local and global economies. This is particularly evident given that most cyberattacks in the region primarily target government entities. However, a number of cyberattacks were detected in the region targeting both the public and private sectors across all industries. Among those attacks were cyber espionage operations targeting government entities, which were detected in many countries, including Saudi Arabia, the United Arab Emirates, Qatar, and Jordan. (NCSC, 2023)

Therefore, it is evident that there are high risks to cybersecurity and information systems in the oil and gas sector, both locally and globally. Additionally, auditors in this sector encounter various challenges and impediments, including the integration of IT into auditing processes and their documentation, along with the reliance on modern IT for oil and gas production operations. Addressing these challenges requires continuous training on the latest IT programs and applications, fostering a strong cybersecurity culture, and staying informed about emerging threats for the purpose of protecting national security.

Section 4: Investment in Cybersecurity and Information Systems in Kuwait's Oil and Gas Sector

The oil and gas sector in Kuwait comprises KPC, as the parent company, and seven subsidiaries. The parent company has invested in the field of cybersecurity by developing a vision and a path to establish a clear plan that includes a strategy, standards, and decisions specific to cybersecurity. The plan is illustrated in Figure 8 below. (RSA Conference, 2020)

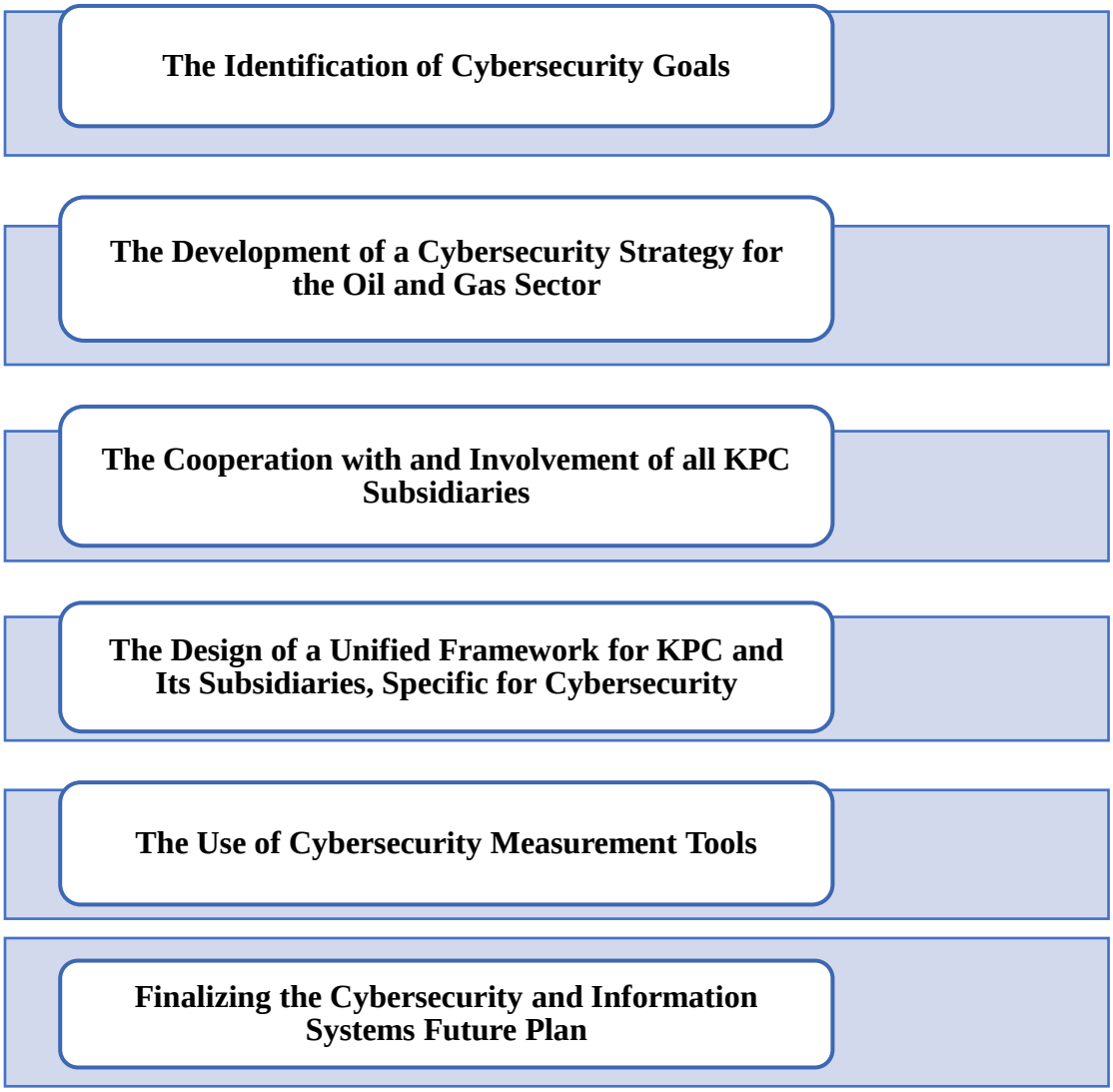


Figure 8: KPC Cybersecurity Investment Plan

Source: Adapted from RSA Conference (2020)

The activities of Kuwait's oil and gas sector are similar to those of the global oil and gas sector, starting with exploration and ending with the exportation of oil and gas products. These activities rely heavily on IT, modern systems, and human resources. Investing in the human element is considered the most important investment compared to others. In line with this mindset and direction, the oil and gas sector in Kuwait has been keen to invest in its human capital. It has made efforts to enhance cybersecurity awareness, particularly after recognizing that investment in the human element for cybersecurity within the sector is considered insufficient. One of the proposed solutions is the **involvement of all** employees in cybersecurity, rather than targeting a specific department or company. Such involvement is critical, as cybersecurity has become a necessity for everyone. (RSA Conference, 2020)

Moreover, with the aim of protecting the state from cyberattacks in the oil and gas and other sectors, the State of Kuwait has issued Decree 37/2022 on the establishment of the National Cyber Security Center (NCSC). The Center's objectives include establishing an effective national cybersecurity system to protect Kuwait from cyberattacks, mitigate their impact, and promote a culture of cybersecurity. As a result, the establishment of the NCSC has helped to set a strategy and standards specific to cybersecurity in Kuwait. (RSA Conference, 2020)

Similarly, Kuwait's oil and gas sector has developed a cybersecurity framework and strategy aligned with the National Cybersecurity Strategy. The objectives of this framework include protecting the State of Kuwait from cyber threats, enhancing cybersecurity awareness, and fostering a strong cybersecurity culture across all state sectors, particularly in the oil sector, due to its significance and impact on the local economy. That, in addition to protecting and monitoring national assets, and providing opportunities for and means of cooperation and coordination

between all State sectors and entities in the field of cybersecurity and information systems. (RSA Conference, 2020)

However, Kuwait's oil and gas sector faced several challenges during the development of the cybersecurity vision and strategy, mainly the following: (RSA Conference, 2020)

1. Lack of a national cybersecurity strategy at the time when a cybersecurity plan has already been developed for the oil and gas sector in Kuwait.
2. Lack of a unified budget allocated to cybersecurity and information systems that includes all subsidiaries, as each individual company examined and estimated the required budget separately.
3. "Cascading Attacks" are considered one of the most difficult challenges facing the sector, owing to the fact that the parent company and its subsidiaries are attached through data, systems, and infrastructure. Therefore, any cyberattack on one company would impact the rest of the companies, as well as the local economy in general.

Kuwait's oil and gas sector is marked for its achievements, particularly those related to cybersecurity. The major achievements of the sector in this field are summarized in Figure 9. (RSA Conference, 2020)

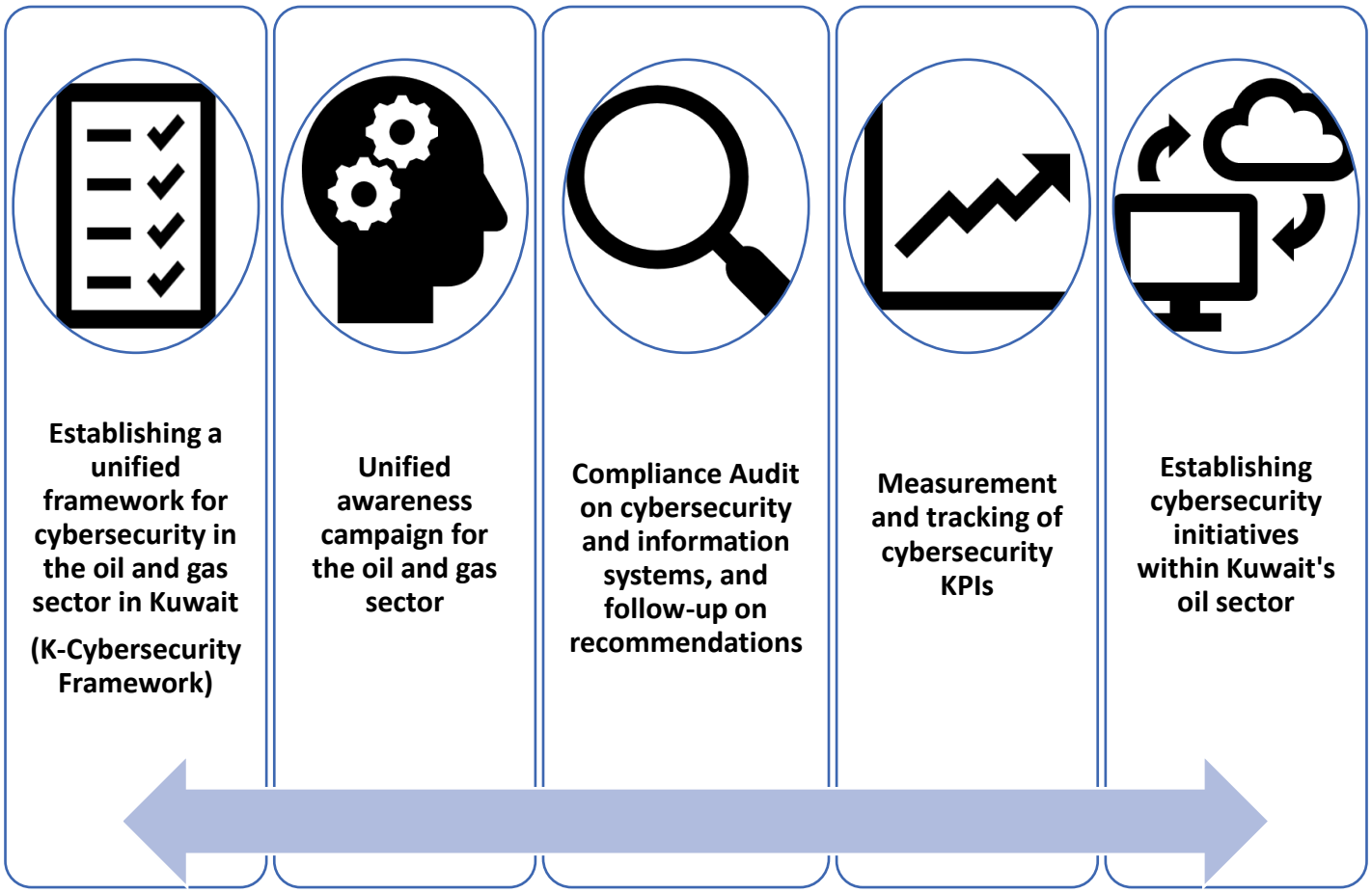


Figure 9: Key Achievements of Kuwait Petroleum Corporation (KPC) and its Subsidiaries in Cybersecurity

The researcher believes that the study of cybersecurity risks in Kuwait's oil and gas sector has become mandatory and that investing in human resources and their capacity in cybersecurity is considered the most important investment. The researcher also believes that it is necessary to apply the cybersecurity framework and strategy and ensure their effectiveness. The latter entails measuring cybersecurity KPIs periodically to ensure constant adjustments and further improvements. Implementing all of the above will contribute to achieving the national strategic goals and vision of cybersecurity, which is to protect the State of Kuwait from cyberattacks and protect the country's only source of income.

Section 5: Case Studies of Cyberattacks on the Oil and Gas Sector

This section presents a case study pertaining to the largest cyberattack targeting the oil and gas sector in the Arabian Gulf region, in addition to other global case studies. Cybersecurity KPIs were not used before these attacks.

A. Saudi Aramco: A Case Study from the GCC Region

In 2012, Saudi Aramco was targeted by a cyberattack that caused great damage to public funds and the oil and gas sector in Saudi Arabia. The cyberattack disrupted the company's activity for a month, and the losses were not disclosed. Since the oil and gas sector is one of the primary sources of income in the Kingdom of Saudi Arabia, the breakdown caused material losses that impacted the national economy. The research also showed that the damage was not only immediate but also extended into 2016 and 2017 through malware linked to the initial cyberattacks in 2012. This cyberattack was the largest in history against an oil company in the Gulf Cooperation Council (GCC) region. Due to concerns about the company's reputation, extreme confidentiality was maintained regarding the incident. However, some reports have revealed part of the attack's consequences, which included replacing 50,000 computer hard drives. For security reasons, the company was unable to use its internal and global network for about five months. (Al-Samhan, 2020)

The effects of cyberattacks on the oil sector may extend for several years. Therefore, Aramco has taken preventive measures to mitigate the risk of similar future attacks. A study on the Saudi Aramco- Riyadh branch- found that the company has implemented effective measures to protect its cyberspace. For example, an automated system lock is activated if the system remains inactive for a specific period set by the company. Additionally, biometric authentication methods,

such as eye print recognition and other security features, are enforced to enhance protection. (Al-Samhan, 2020)

Another study on GCC countries revealed deficiencies in network security, highlighting the need for an increased focus on IT security, network security, and cybersecurity to address vulnerabilities and prevent cyberattacks. The study also identified malicious cyberattacks linked to email spam as the most common type of attack. This type of cyberattack requires enhanced governance and operational improvements in this region, along with accelerating the adoption of modern technology. (Al-Samhan, 2020)

Implementing cybersecurity in the oil and gas sector enhances system and data protection. It also contributes to countering cyberattacks and incidents related to companies' information security and protection in both the public and private sectors. Therefore, establishing a robust cybersecurity infrastructure is crucial for protecting national information related to the national economy. Such a measure also contributes to identifying strengths, weaknesses, and gaps and helps address them.

B. Global Case Studies

In May 2021, an undisclosed American company in the oil and gas sector was subjected to one of the largest cyberattacks in the industry. The cyberattack seized control of a fuel pipeline in the United States, causing significant financial losses. The attack forced the shutdown of production lines and successfully infiltrated the system through a ransomware attack. A $5 million ransom was demanded to restart production, highlighting critical vulnerabilities in the infrastructure of the US oil and gas sector. (KPMG, 2021)

In the same year, an international energy company also fell victim to a cyberattack, during which hackers managed to seize control of the company's data and leak sensitive information through one of its contractors. This incident was also a ransomware attack, in which blackmailers seized a massive amount of data- approximately 1 terabyte- until the company paid a ransom to retrieve the data. (KPMG, 2021)

After reviewing case studies on cyberattacks in the oil and gas sector, the researcher believes that industrial automation in this sector provides significant advantages in facilitating production processes. However, it requires the establishment of specialized cybersecurity protocols and core functions that are in line with the developments in the sector to safeguard public security and the national economy from cyber threats. Additionally, by examining the case studies, it was found that there is no link between cybersecurity KPIs and the attacks against the companies, neither before nor during these incidents.

Section 6: Cybersecurity Frameworks

This section will discuss global and local cybersecurity frameworks in the oil and gas sector and explain the importance of establishing a regulatory framework for cybersecurity.

The best way to protect the oil and gas sector against cyberattacks is to develop risk-based plans assessed according to global frameworks, such as the cybersecurity framework issued by the National Institute of Standards and Technology (NIST). These frameworks enhance the sector's resilience to cyberattacks and serve as effective tools for auditing cybersecurity risks and measuring cybersecurity KPIs. They also contribute to improving IT infrastructure in the oil and gas sector. (Cybersecurity Frameworks 101- The Complete Guide, Prey Blog, 2022; Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry, 2017)

In general, cybersecurity frameworks must include standards, foundations, and best practices for cyber risk management, which would, in turn, contribute to measuring cybersecurity KPIs. There are several special cybersecurity frameworks, the most important of which are shown in Figure 10 below.

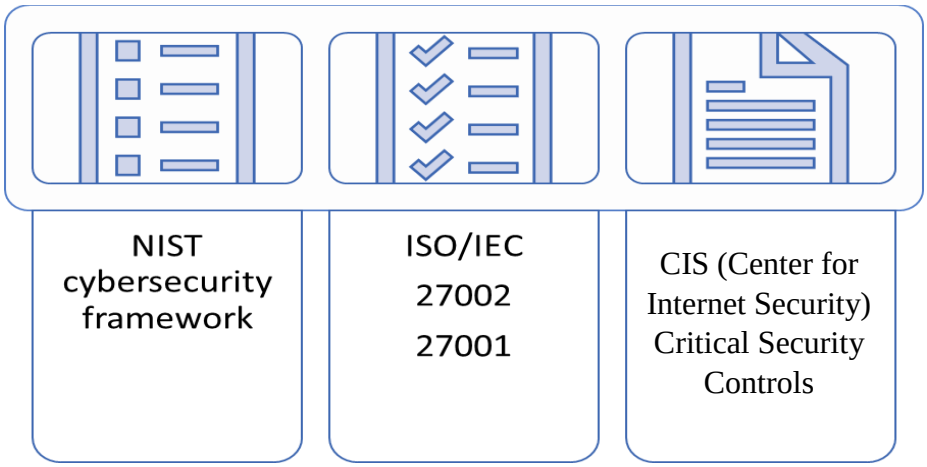


Figure 10: Key Cybersecurity Frameworks

Source: Adapted from Cybersecurity Frameworks 101- The Complete Guide, Prey Blog (2022)

Implementing any of the above frameworks would be beneficial for the oil and gas sector. However, it is more effective when the framework is specifically designed for the sector, ensuring better accuracy and suitability for the specific needs of the end users. From this perspective, the oil and gas sector in the State of Kuwait has designed its own cybersecurity framework, which will be addressed in detail next.

- **Cybersecurity and Information Systems Framework in Kuwait's Oil and Gas Sector**

The 2040 Strategy for the oil sector in Kuwait addresses several aspects, including information systems and cybersecurity. This strategy was referred to during the development of the sector's cybersecurity framework. Undoubtedly, the establishment of a cybersecurity framework within the sector is fundamental. While there are different frameworks across various sectors worldwide, including the oil and gas sector, each country must develop its own framework in proportion to the nature and size of business in the sector. (RSA Conference, 2020)

The oil and gas sector in Kuwait stood out by developing a clear cybersecurity framework, known as the K-Cybersecurity Framework. This framework encompasses four main components, as outlined in Figure 11 below, and 34 sub-components. (RSA Conference, 2020)

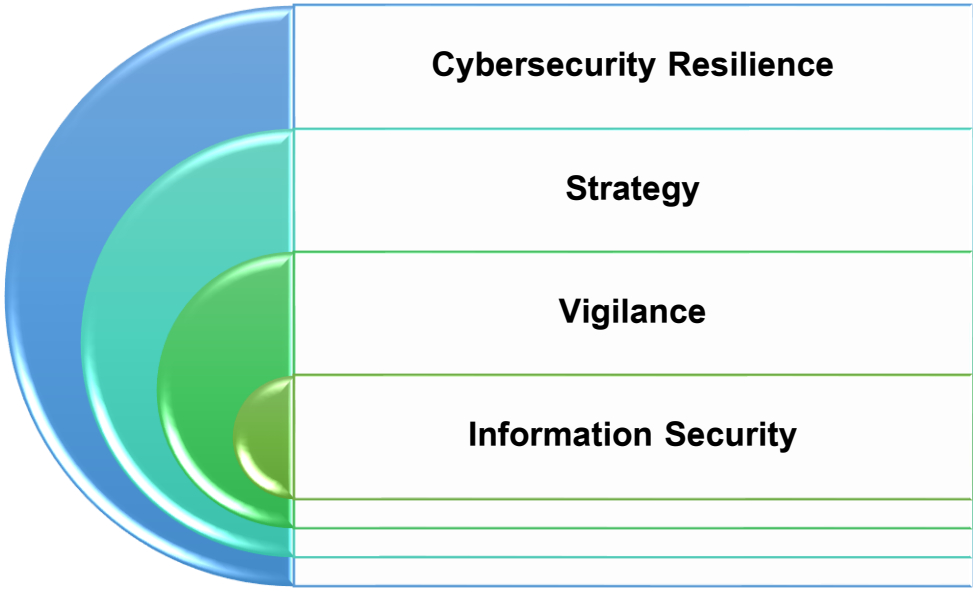


Figure 11: Key Components of the K-Cybersecurity Framework of KPC and its Subsidiaries

Source: Adapted from RSA Conference (2020)

Cybersecurity resilience reflects the ability of oil companies to respond to and recover swiftly from cyberattacks. The Strategy helps establish a clear vision and a future direction for cybersecurity practices. Vigilance plays a critical role in continuous monitoring, proactively detecting internal and external cybersecurity threats, and responding swiftly to safeguard systems against cyber risks. As for information security, this component involves anticipating cyberattacks and implementing periodic security measures. (RSA Conference, 2020; 7 Cybersecurity Frameworks That Help Reduce Cyber Risk (List & Resources), 2024)

Designing a regulatory framework for cybersecurity enhances the management of cybersecurity risks and is considered a fundamental requirement for securing digital assets. Such a framework must incorporate a well-defined mechanism that aligns with global best practices, building on effective cybersecurity frameworks to protect national security and digital infrastructures. Furthermore, a cybersecurity regulatory framework must include a distinct methodology for managing cyber risks, applying best cybersecurity practices, and increasing the level of cybersecurity maturity. The key components that should be included when designing a cybersecurity regulatory framework are illustrated in Figure 12. (Communications, Space and Technology Commission [CST], 2020)

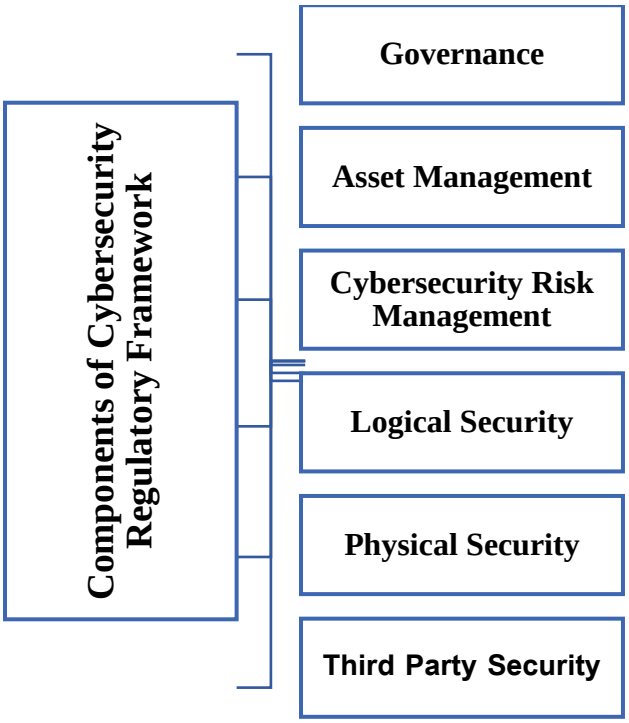


Figure 12: Key Components of the Cybersecurity Regulatory Framework

Source: Adapted from Communications, Space and Technology Commission (2020)

A study conducted on internal cybersecurity audits revealed a deficiency, negatively impacting cybersecurity risk management. This deficiency can be attributed to several factors, including the lack of a cybersecurity framework and the failure to update audit methodologies pertaining to cybersecurity and information systems to keep pace with rapid technological advancements. Additionally, adherence to traditional audit methodologies, the inflexibility of audit plans, and poor communication between relevant parties further exacerbate the issue. (Mahrous & Saleh, 2022; Al-Matari et al., 2020; Al-Burzangi & Al-Saqqa, 2023)

The researcher believes that designing a cybersecurity framework is a necessity. Furthermore, it is important to measure the framework's effectiveness on a periodical basis with the aim of continuous improvement so that it can be used to protect the oil and gas sector from cyberattacks.

Section 7: The Benefits of Cybersecurity and Information Systems Audits in Performing and Documenting Audit Work, Protecting Public Funds, and Ensuring National Security

This section discusses the audit methodologies adopted in the oil and gas sector for auditing cybersecurity and information systems in oil companies in accordance with global audit guidelines. It will also address the audit results reached by several Supreme Audit Institutions (SAIs).

Information security and its importance are not new topics. However, the increasing reliance on information technology has made cybersecurity and information security a necessity. In 1997, information security was classified in the United States as a high-risk area, and since then, cyberattacks and associated risks have continued to arise. Therefore, there is an urgent and critical need to audit cybersecurity and information systems to direct the state to the underlying weaknesses and gaps based on audit results and to adopt effective solutions and proposals for corrective measures. Recognizing the importance of cybersecurity auditing, some countries have developed guidelines and standards for auditing cybersecurity and information systems, including the United States. Several cybersecurity audit guidelines have been issued by SAIs worldwide, including the U.S. Government Accountability Office (GAO), which issued an audit guide in September 2023, as well as the European Union (EU). This section will discuss the most important findings related to cybersecurity audits. *(Cybersecurity Program Audit Guide, 2023)*

The U.S. Government Accountability Office (GAO) has extensive experience in auditing cybersecurity and information systems and has already issued thousands of proposals after examining, auditing, and reviewing cybersecurity. This highlights the importance of cybersecurity auditing and the crucial role of auditors in protecting public funds. Due to the increase in cyberattacks, auditing has become mandatory across the state's vital sectors. The existence of a cybersecurity audit guide would assist cybersecurity analysts and auditors in the performance of

audit tasks by providing a distinct methodology and identifying tools for analysis and evaluation. Moreover, the guide issued by GAO is flexible and can be used by any other entity. *(Cybersecurity Program Audit Guide, 2023)*

The Cybersecurity Program Audit Guide (CPAG) issued by the U.S. GAO addresses sensitive and confidential data in various sectors across the country, including the energy sector. The energy sector comprises the oil and gas industry, which relies entirely on information technology. Protecting this sector and its data is considered a key factor in safeguarding national security. The risks faced by this sector may be internal, such as employees, or external, such as targeted cyberattacks by external parties. However, with emerging technologies, detecting cyberattacks before they occur is becoming increasingly challenging and complex for auditors. One example of this is the use of artificial intelligence (AI) in cyberattacks, which makes the detection of cyber threats even more challenging and obstructs rapid responses to potential cyberattacks. Here lies the national challenge of protecting state security by keeping pace with the latest advancements in this field. *(Cybersecurity Program Audit Guide, 2023)*

All data in critical sectors are targets for cyber threats. However, cybersecurity and information systems audits have found that sensitive personal data is particularly more vulnerable to cyberattacks and hacking, posing a significant threat to governments. The breach of such data would render them easy to delete, modify, or erase. This threatens national security and the stability of local and global economies in major sectors such as energy, health, and education. The audit results issued by the U.S. GAO in 2021 found that there were 32,000 cyberattacks on sensitive personal data, which makes it classified as high-risk. (Cybersecurity Program Audit Guide, 2023)

Auditing cybersecurity and information systems is essential for protecting public funds and national security from cyberattacks that may negatively affect the economy. Here, we emphasize the importance of auditors in detecting such attacks. Cybersecurity audits contribute to improving performance and operations across all entities, reducing costs and risks, and facilitating decision-making. There are three main phases of a cybersecurity audit, as outlined in Figure 13 below. (Cybersecurity Program Audit Guide, 2023; Sabillón, 2022)

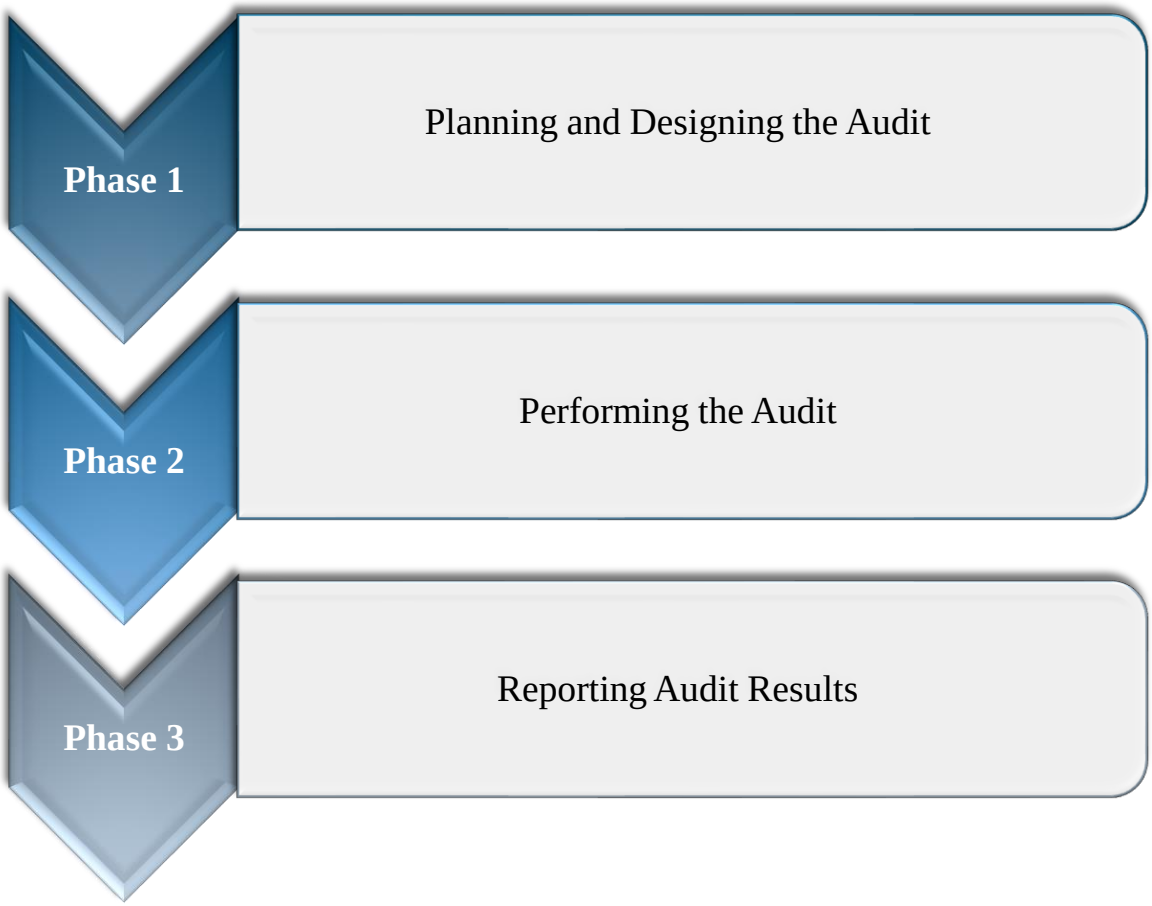


Figure 13: Phases of Cybersecurity and Information Systems Audit

Source: Adapted from Cybersecurity Program Audit Guide (2023)

Phase 1 (Planning and Designing the Audit): This phase serves as the foundation of the cybersecurity audit process and is the key to the success of an audit task if prepared accurately and meticulously. Auditors must possess a comprehensive understanding of cybersecurity and information systems, as this phase involves a thorough assessment of cybersecurity controls. Measurement is a fundamental cybersecurity indicator in this context, highlighting the importance of systematic evaluation. Additionally, this stage involves supplementing cybersecurity performance audits by assessing the effectiveness of cybersecurity within the systems. Auditors are responsible for ensuring data confidentiality through periodic and continuous assessments of system resilience.

Upon comprehending and studying all aspects of cybersecurity, auditors delineate the scope and boundaries of the audit. This requires expertise, familiarity, and an in-depth knowledge of information technology and cybersecurity. The scope of a cybersecurity audit includes the systems, networks, and data that form an integral part of the cybersecurity program. Additionally, auditors may leverage established cybersecurity frameworks such as NIST and FISMA, which mandate annual evaluations. These evaluations facilitate the identification of an organization's current cybersecurity posture. (Cybersecurity Program Audit Guide, 2023)

Phase 2 (Performing the Audit): The successful implementation of the audit plan and the seamless progression of this phase rely heavily on the mastery of the first phase. At this phase, auditors collect evidence and other documentation to substantiate the audit process, ensuring that these materials align with both the plan and scope of the audit. Key sources of documentary evidence include previous audit reports, interviews, inquiries, and other credible primary sources. A meticulous review of these documents is essential before proceeding with the implementation phase in order to verify their integrity and authenticity and to ensure the accuracy and reliability

of data. If auditors deem the data unreliable, it becomes imperative to revise the audit plan and adjust objectives accordingly to reflect the current landscape. In such cases, auditors will not be able to rely on these data to formulate the final report on the audit conclusions and recommendations. (Cybersecurity Program Audit Guide, 2023)

Phase 3 (Reporting Audit Results): This phase begins following the first and second phases and upon completion of the audit work in accordance with the approved standards and frameworks. This phase focuses mainly on formulating key findings and recommendations reached by auditors that would ultimately lead to protecting national security and public funds. Accordingly, a draft report is prepared for review and comment, and the received feedback is carefully considered when compiling the final report for submission to the organization's management. (Cybersecurity Program Audit Guide, 2023)

Awareness in the field of cybersecurity is expanding, and there is a growing recognition of the importance of cybersecurity and information systems audits. Furthermore, there has been increased appreciation for the role of both internal and external auditors in this field. However, these auditors still face formidable challenges in performing their duties effectively. Such challenges may include a lack of adequate support from senior management, even though auditors are considered the first line of defense in safeguarding an organization's assets as well as public funds. Additionally, auditors play a crucial role in mitigating potential cyber risks, as cybersecurity and information systems audits contribute to strengthening organizational objectives. This is achieved by adopting appropriate methodologies for cybersecurity and information systems auditing, in addition to enhancing governance and cyber risk management practices. (Internal Control Challenges, 2020; Auditing Cybersecurity, 2016)

Governments are not immune to cyberattacks, regardless of how aware they may be. There will always be emerging technologies that pose a threat to governments, as well as to both local and global economies, such as artificial intelligence. Therefore, the role of auditors has become critical in various fields, particularly cybersecurity and information systems. The continuous training of auditors in information technology is not limited to a specific category; rather, it is essential for all professionals to enhance their knowledge and skills in this domain. Additionally, the ability of employees to periodically assess cybersecurity effectiveness by measuring cybersecurity KPIs contributes significantly to enhancing the audit process. (Internal Control Challenges, 2020; Auditing Cybersecurity, 2016)

Raising awareness in the field of cybersecurity is the responsibility of both governments and institutions. It is crucial to prepare and qualify national cadres in the fields of information technology, systems, networks, and data analysis to ensure their proficiency in auditing cybersecurity and information systems. Studies have found a strong correlation between the various dimensions and requirements of cybersecurity, including strategy, operations, procedures, confidentiality protection, privacy, logical security, and cyber risks. Additionally, this research emphasizes the importance of adopting effective methods for the continuous evaluation of internal controls. Such evaluations would help mitigate cybersecurity risks, maintain information security, and adopt special measures to preserve information assets. (Mansour, 2021; Mahrous & Saleh, 2022; Al-Matari et al., 2020)

Cyberattacks are increasing, and cybersecurity risks have been ranked among the top five risks by the Institute of Internal Auditors. Given the total reliance on information technology and the shift to remote work during the COVID-19 pandemic, cybersecurity risks are expected to

escalate further. Post-pandemic lifestyle changes have also contributed to the surge in cyberattacks, particularly amid the widespread reliance on IT nowadays. (Slapničar et al., 2022)

The European Union (EU) issued a detailed report on cybersecurity and information systems audits, presenting relevant findings of audits conducted by the Supreme Audit Institutions (SAIs) in the EU. The report revealed that in 2018, a survey of the SAIs in the EU indicated that approximately half had not conducted cybersecurity audits across all sectors, including the oil industry. However, the findings of the study were promptly addressed, and a cybersecurity audit plan was developed to protect systems in the EU, particularly given the increasing reliance on information technology in certain sectors. Some EU member states have predicted that the upcoming pandemic may manifest in the form of "cyberattacks." Consequently, enhanced preparedness and the establishment of a robust infrastructure are critical to preventing cyber threats. The rising risk and likelihood of cyberattacks necessitate increased national preparedness, particularly for attacks targeting personal information- and here lies the strategic challenge for the state. The following are the key findings and recommendations provided by the European Union on cybersecurity and information systems auditing across various sectors for the period 2014-2020. (Cybersecurity in the EU and Its Member States, 2020)

1. The number and seriousness of cyberattacks, as well as their financial costs and accompanying losses, are escalating. In 2021, costs reached $6 trillion. These costs included stolen money, damage and destruction of data, and lost productivity. The EU also forecasts a 72% increase in cyberattacks in the coming years.

2. A lack of awareness regarding cybersecurity risks poses a significant challenge. A 2018 study on cybersecurity found that organizations would rather pay the hacker's ransom than invest in information security and cybersecurity infrastructure.

3. Having a national cybersecurity strategy is crucial.
4. Annual injection of EUR 970 million during the period 2021-2027 to enhance cybersecurity, national data protection, and public security.

The results of cybersecurity and information systems audits concluded that there was an increase in maintenance costs associated with server rooms and digital infrastructure upkeep. However, periodic maintenance would help mitigate cyberattacks and minimize the losses resulting from such incidents. Accordingly, governments are urged to mandate institutions to create backup copies of state data and invest in an effective mechanism for securely storing these valuable digital assets.

Cybersecurity and information systems auditing is a broad and versatile field that allows for the development of an audit methodology that is in line with national strategies. The EU report on the results of cybersecurity and information systems audits found that audit methodologies varied across SAIs, depending on national strategies and policies. Some SAIs have employed ethical hackers to test the effectiveness of systems and networks in defending against hacking attempts. (Cybersecurity in the EU and Its Member States, 2020)

According to the Information Systems Audit and Control Association (ISACA), a typical cybersecurity audit process undergoes three key phases, as outlined in Figure 14. The first phase, which is the Planning Phase, comprises five steps, including determining the audit subject, setting the audit scope, and determining procedures. The second phase (Fieldwork and Documentation) includes field examination, which involves steps such as acquiring data and documenting results. The third and final phase is the Reporting Phase, which includes drafting the audit report, issuing the report, and the follow-up. (Benetis, 2018)

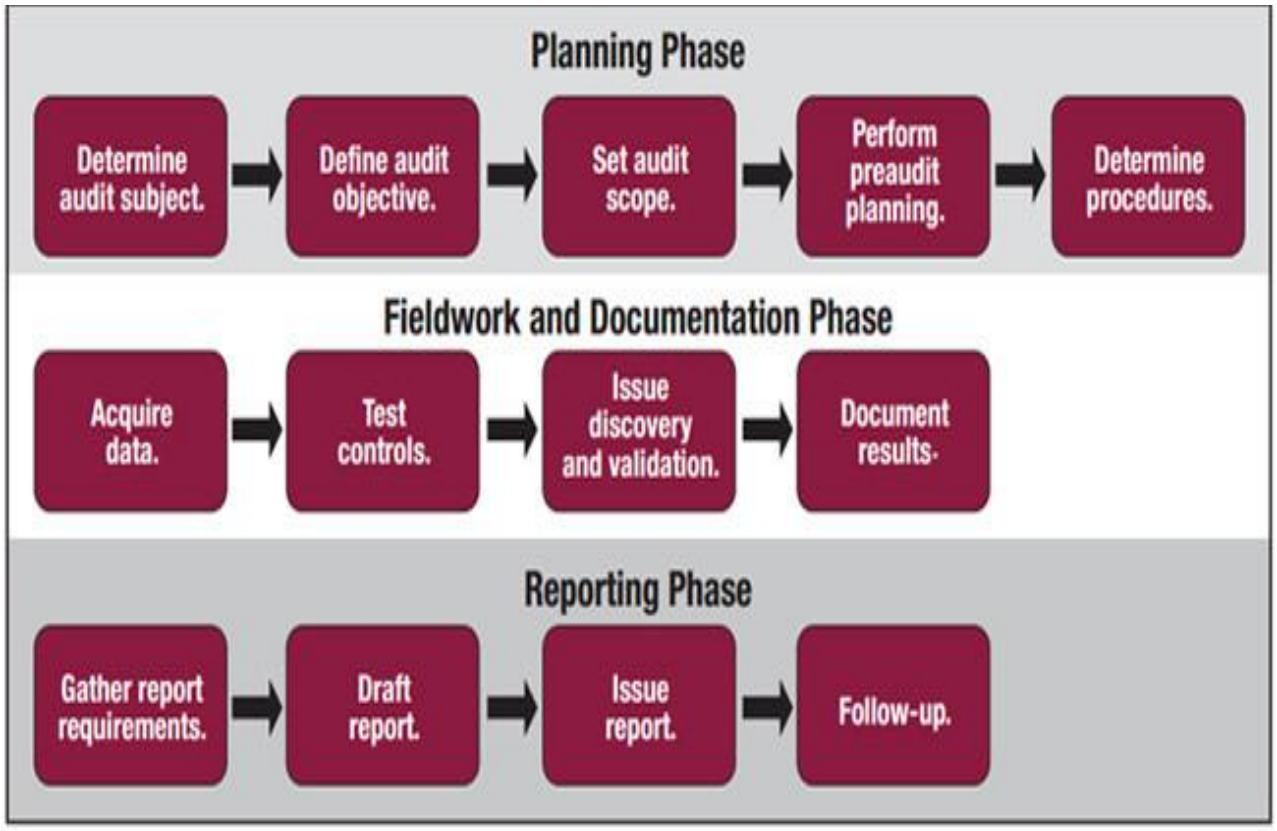


Figure 14: Phases of Cybersecurity Audit Process according to ISACA

Source: Benetis (2018)

The researcher believes that cybersecurity and information systems audits play a significant and effective role in enhancing the quality of audit work and improving outcomes that contribute to achieving the objectives of the National Cybersecurity Strategy. Auditors must keep abreast of developments in this field through continuous learning, awareness, and training. Furthermore, cybersecurity and information systems audits must be integrated into Kuwait's oil and gas sector as well as SAB. It is also essential to use audit programs when conducting audit tasks, as they contribute to enhancing the quality of audit outcomes by reducing the time spent on tasks. These programs would also enable the measurement of cybersecurity KPIs and associated risks, ensure accuracy of sampling, facilitate access to data, and ultimately enhance stakeholders' trust in cybersecurity audit outcomes within the oil and gas sector.

Section 8: The Importance of Cybersecurity KPIs and Their Positive Impact on Audit Quality

This section will address cybersecurity KPIs, their importance, and how they can be utilized in the oil and gas sector to enhance audit quality. It will also highlight the positive impact of KPIs on audit entities' reports and the overall outcomes of oil companies. The ultimate goal of monitoring and auditing cybersecurity and information systems is to ensure effective control over public funds and protect the national security infrastructure.

As the saying goes, "What cannot be measured cannot be improved." Cybersecurity KPIs serve as standards and tools to measure and evaluate the effectiveness of security strategies and measures in protecting systems and data from cyber threats. These KPIs also play a crucial role in decision-making processes, helping institutions identify their weaknesses, strengths, and overall security posture (CyberTalents, 2024). As an effective tool for assessing cybersecurity, KPIs assist auditors in identifying an organization's current cybersecurity status. Kuwait's oil and gas sector uses a maturity assessment tool to measure and assess cybersecurity status. *(RSA Conference, 2020)*

The maturity assessment adopted by Kuwait's oil and gas sector (K-Cybersecurity Maturity Assessment) was used before the preparation of the cybersecurity strategy and frameworks in the sector. It helped identify cybersecurity status by assessing cybersecurity efficiency and practices across KPC subsidiaries. Key areas assessed included risk management, incident response speed, access controls, and general cybersecurity policies. The assessment successfully achieved its primary objective of identifying strengths and weaknesses in cybersecurity while highlighting the areas for improvement. This initiative contributes to enhancing cybersecurity within KPC and its

subsidiaries, positively impacting the overall cybersecurity posture of Kuwait's oil and gas sector. (RSA Conference, 2020)

Cybersecurity measurement tools are of added value as they contribute to enhancing and improving the quality of outcomes and other cybersecurity-related tasks. Their impact becomes evident through correcting the path, addressing vulnerabilities, and preventing cyberattacks as much as possible. (RSA Conference, 2020; Auditing for FISMA and HIPAA: Lessons Learned Performing an In-house Cybersecurity Audit, 2016)

One of the KPIs used in Kuwait's oil sector was the Cyber Resilience Index (CR%). Although it is not a direct cybersecurity indicator, it has been utilized to determine whether subsidiaries are secure against cybersecurity attacks and risks. The Cyber Resilience Index has enabled the sector to identify subsidiaries with poor cybersecurity preparedness. Accordingly, a conceptual and classification framework for KPC subsidiaries was developed, along with a future vision and proposals to enhance the subsidiaries' current cybersecurity posture (RSA Conference, 2020). KPIs have contributed to improving cybersecurity-related outcomes in the oil sector. The KPC subsidiaries have developed proposals to enhance cybersecurity action plans, with a particular focus on high-risk weaknesses and vulnerabilities. These proposals also emphasized the need to develop a structured response plan, which is based on three main pillars: individuals, technology, and systems. (RSA Conference, 2020)

The importance of cybersecurity KPIs is evident in the commitment of various countries to their implementation. There are several successful experiences in neighboring countries, such as Saudi Arabia, which has utilized the Assessment and Compliance Tool to evaluate and measure compliance with fundamental cybersecurity controls. The use of this tool has contributed to enhancing cybersecurity audit tasks. (National Cybersecurity Authority, 2018)

To determine the effectiveness of cybersecurity and information systems audits, some studies have measured indicators such as the Cybersecurity Audit Index, which assesses the impact of internal auditing on cybersecurity risks. A study concluded that there is a correlation between internal audit practices and cybersecurity risk reduction, demonstrating the effectiveness of this indicator. However, the study did not specify the size of companies or the specific sectors analyzed, nor did it address the rationale behind selecting this indicator or its level of accuracy. Overall, there is still a lack of studies on the measurement of cybersecurity KPIs, audits, and governance. (Slapničar et al., 2022)

There is a distinct difference between metrics and KPIs. The difference lies in the method of measurement. A metric represents a quantifiable value and is typically expressed as a numerical figure, such as the number of cyberattacks recorded. A KPI, on the other hand, measures multiple metrics and contributes to decision-making processes. For instance, if an oil company aims to analyze the percentage of systems targeted by ransomware attacks, it may evaluate a set of metrics such as the number of systems, the number of affected devices, and the number of affected systems. Cybersecurity KPIs include the following: (National Cybersecurity Authority, 2018)

1. **Threat Detection Rate:** The speed at which cybersecurity threats are detected and responded to.
2. **Response Time**: The amount of time required to respond and take corrective actions after a threat has been detected.
3. **Response Efficiency**: The effectiveness of the measures taken to respond to and mitigate the impact of cybersecurity threats.
4. **False Detection Ratio**: The reduction of false alarms or false warnings.

5. **Threat Classification**: Assessing the significance and priority of threats and vulnerabilities.
6. **Compliance and Risk Assessment**: Measuring compliance with standards and assessing potential risks.
7. **Staff Training**: Examining the effectiveness of cybersecurity training and awareness programs.
8. **Logs Analysis**: Evaluating activity logs to detect unauthorized activities.
9. **Vulnerability Assessment**: Analyzing areas of weakness in the systems and assessing potential impacts.

Cybersecurity KPIs play a crucial role in determining the strength and effectiveness of security strategies. They ensure continuous improvement of these strategies over time, enabling organizations to effectively respond to emerging cybersecurity challenges. This proactive approach would positively impact government institutions and various sectors. The integration of cybersecurity KPIs provides several benefits, including activating the cybersecurity strategy, enhancing threat analysis, and ensuring a rapid response to threats. The following are the key advantages of using cybersecurity KPIs (Slapničar et al., 2022; Sengupta, 2022):

1. **Enhancing Rapid Response:** KPIs provide accurate information about cybersecurity threats, contributing to faster detection and response.
2. **Improving Effectiveness:** KPIs measure the effectiveness of cybersecurity strategies, ensuring continuous improvement.
3. **Prioritization:** KPIs contribute to better prioritization and allocation of resources to protect systems and data within the oil and gas sector.

4. **Reducing Costs:** KPIs enable the prediction of potential threats and facilitate an effective response, ultimately reducing emergency response costs.
5. **Promoting Awareness:** KPIs promote staff awareness of the importance of cybersecurity and provide a solid ground for improving relevant practices.
6. **Cybersecurity Assessment:** KPIs provide a framework for assessing the performance of cybersecurity systems and identifying gaps and vulnerabilities that need to be improved and addressed.
7. **Meeting Compliance Requirements:** KPIs support compliance with cybersecurity standards and legislation by providing relevant data.
8. **Reporting to Management:** KPIs facilitate the preparation of periodic reports for management that clarify an organization's cybersecurity posture and outline security-related developments.

Cybersecurity KPIs enable professionals to measure the effectiveness of cybersecurity procedures in institutions and assess their readiness to adapt to changes, address vulnerabilities, and respond to cyberattacks. Cybersecurity KPIs are also an effective tool for identifying the level of security in state institutions. A PwC survey highlights that investments continue to pour into cybersecurity, as 69% of respondents predicted a rise in cyber spending in 2022, compared to 55% in 2021. This rise can be attributed to the spread of awareness, the increase in cyberattacks, and the countries' disposition to protect the economy.

Cybersecurity KPIs in the oil and gas sector are of great importance, given that it is one of the most targeted sectors. Technology has become essential in the sector in light of the expansion of the oil projects in size and scope. Accordingly, investing in cybersecurity in the sector has become a necessity to reduce cyber damage, as demonstrated in Figure 15. (Global Cybersecurity Index 2020, 2020)

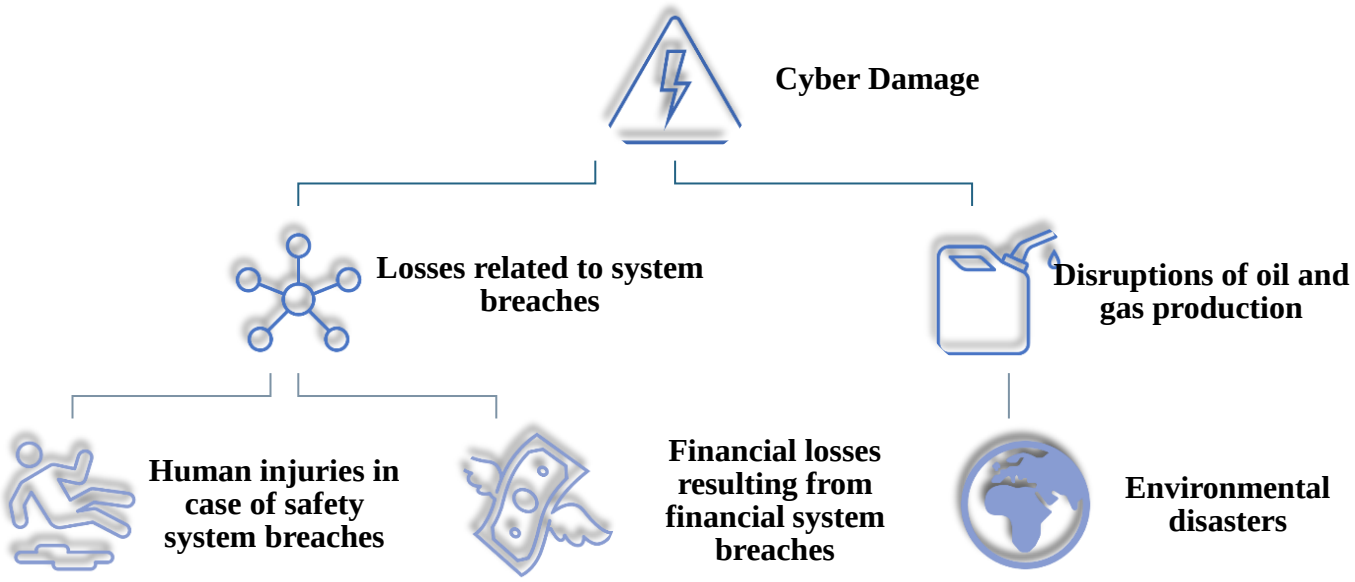


Figure 15: Cyber Damage in the Oil and Gas Sector

Source: Adapted from Global Cybersecurity Index 2020 (2020)

The adoption of cybersecurity measures within the oil and gas sector is, therefore, crucial for the protection of sensitive data, such as digital intellectual property and the data relevant to exploration and refining. Cyberattacks in the oil and gas sector are among the most intricate attacks, as they are led by a network of parties supported by other countries, as well as pirates and criminal groups. Remote work increases reliance on the Internet and other advanced technologies, posing a higher cyber risk to the sector. (The Evolution of Information Systems Audit, 2022)

The Global Cybersecurity Index (GCI) 2020 report, issued by the General Secretariat of the Supreme Council for Planning and Development in the State of Kuwait, indicated an improvement in Kuwait's GCI ranking despite the continued existence of regional cybersecurity vulnerabilities. The effectiveness of cybersecurity was assessed using several indicators, emphasizing the importance of measurement in this field. The evaluation relied on 20 indicators assessed through 82 questions to determine the GCI ranking and, therefore, ensure further cybersecurity improvements in Kuwait. It was concluded that Kuwait had advanced globally by two ranks but fell behind by one rank on the scale of the GCC. The GCI 2020 report has presented key recommendations to enhance cybersecurity in Kuwait, including supporting the digital economy, establishing a sophisticated digital infrastructure, investing in cybersecurity through international partnership contracts, and enacting laws and legislation in the field of cybersecurity. (Global Cybersecurity Index 2020, 2020)

The researcher believes that cybersecurity KPIs are among the most important measurement tools to be integrated into the oil and gas sector. These KPIs guide auditors during the preparation of audit plans and the execution of audit tasks, positively impacting overall audit outcomes in the sector. Additionally, cybersecurity KPIs assist in identifying vulnerabilities to be addressed and mitigated, thereby contributing to the successful achievement of audit objectives. Therefore, the adoption of cybersecurity measurement tools is crucial to ensuring further improvements in the sector.

Section 9: Auditing Cybersecurity and Information Systems in Selected SAIs

This section consists of two subsections. The first outlines the role of the State Audit Bureau of Kuwait (SAB) in cybersecurity auditing and its role in achieving the objectives of Kuwait's National Cybersecurity Strategy (2017-2020). It also examines cybersecurity auditing within the oil entities subject to SAB's control, which are the Kuwait Petroleum Corporation (KPC) and its subsidiaries. On the other hand, the second subsection provides an overview of digital and technological auditing within Dubai's Financial Audit Authority (FAA), recognized as one of the leading SAIs in this field, particularly in the energy and industrial sectors.

First: Cybersecurity Auditing in the State Audit Bureau of Kuwait

Cybersecurity auditing is a newly emerging area of focus for the State Audit Bureau (SAB). Despite its significance in enhancing operational efficiency and safeguarding public funds, SAB does not perform cybersecurity auditing following a standardized framework across all its sectors. Instead, SAB audits the extent to which auditees, including KPC and its subsidiaries, comply with the regulations issued by the National Cyber Security Center (NCSC) and cybersecurity-related contractual agreements.

Cybersecurity auditing is not yet mandatory in SAB; instead, it is performed as part of an auditor's due diligence when auditing entities, as there is no law or regulation mandating SAB to audit cybersecurity. In addition, SAB has not yet issued a cybersecurity audit guide to help establish a standardized methodology and serve as a reference for auditors. Taking this step is essential, following the example of the U.S. GAO, which issued a specialized cybersecurity audit guide in 2023. However, the State Audit Bureau of Kuwait is actively driving digital transformation through the development and implementation of a 'digital transformation plan' to support and facilitate institutional digitalization. The Kuwaiti National Assembly has also tasked

SAB with preparing a report on government actions related to cybersecurity and information technology. (Cybersecurity Program Audit Guide, 2023; Parliament Assigns SAB to Prepare a Report on Government IT and Cybersecurity Measures, 2022)

The audit of cybersecurity in SAB's auditees has become a necessity, as it contributes to achieving the objectives of the National Cybersecurity Strategy. Cybersecurity audits play a crucial role in monitoring critical assets, infrastructure, and sensitive national information, particularly in the oil and gas sector. Audit teams assigned to KPC and its subsidiaries perform cybersecurity auditing by assessing an auditee's compliance with NCSC regulations and the cybersecurity contracts signed by the auditee with private cybersecurity providers. Each year, SAB issues an annual report on the audit results of the entities subject to its control. In its report, *Results of the Examination and Audit of the Budget Implementation and Final Accounts of Independent Entities for FY 2022-2023 (Part III: KPC and its Subsidiaries)*, no observations were made regarding cybersecurity auditing and its implementation, except for a remark on the delay in extending cybersecurity contracts in one of KPC's subsidiaries. Apart from that single remark, the report did not note any further cybersecurity-related findings. (State Audit Bureau, 2022; Results of the Examination and Audit of the Budget Implementation and Final Accounts of Independent Entities for FY 2022-2023. Part III: KPC and its Subsidiaries, 2023)

Second: Digital and Technological Auditing within Dubai's Financial Audit Authority (FAA)

The Financial Audit Authority (FAA) of Dubai plays a pivotal role in auditing the energy and industry sector, with a particular emphasis on digital and technological auditing to assess the effectiveness and efficiency of information systems within FAA's auditees. Since 2018, the FAA has been conducting digital audits in the energy and industry sector to ensure that funds allocated to information systems are appropriately disbursed and utilized for their intended purposes in a

documented and methodologically sound manner. Additionally, the FAA is responsible for ensuring the security of digital assets. (Financial Audit Authority, 2018)

The researcher believes that cybersecurity auditing should be made mandatory in SAIs to protect public funds and facilitate the achievement of their respective national cybersecurity strategies. Additionally, it is essential to raise cybersecurity awareness among SAIs' auditors by issuing a dedicated cybersecurity audit guide that provides a clear methodology for the energy and industry sector. Such an effort is crucial due to the significant financial investments and highly sensitive nature of data in the sector.

Section 10: A Look into the Future of Cybersecurity in Kuwait's Oil and Gas Sector

This section explores the future of cybersecurity and the relevant KPIs in Kuwait's oil and gas sector. It also reviews the findings of significant studies conducted in this domain, including a SAB study on the cybersecurity readiness of oil entities under its control.

Kuwait's oil and gas sector has successfully developed a vision and strategy for the measurement of cybersecurity and information systems indicators, as well as cybersecurity audits. Among the key conclusions and proposals presented was the critical need to establish a minimum baseline for cybersecurity KPIs, ensure a strong commitment to KPI measurement against the defined baseline, and promote knowledge sharing in the field of cybersecurity. Kuwait Petroleum Corporation (KPC) has adopted a unified cybersecurity strategy (K-sector Strategy) that, coupled with the measurement of cybersecurity KPIs, has contributed to assessing the readiness of oil companies to deal with cyberattacks. (RSA Conference, 2020)

The external audit office, KPMG, has prepared a study on cybersecurity in the industrial sector. The study concluded that certain considerations must be prioritized when designing a cybersecurity system for the industrial sector, including the oil and gas industry. Key considerations include the following: (KPMG, 2021)

1. Focusing on business mission and objectives.
2. Focusing on Advanced and Persistent Threat (APT) impact.
3. Assuming that a cyberattack will succeed.
4. Assuming that a cyberattack will maintain a long presence in the system.

Multiple studies have shown that governments and institutions in the industrial sector are not fully prepared for cyberattacks. The percentage of cyberattacks has reached 85% in Saudi Arabia, 74% in Turkey, and 69% in China. Studies have also revealed that ransomware attacks are the most common in the industrial sector and that ensuring cyber resilience and conducting relevant studies to mitigate cybersecurity threats require substantial financial resources. A KPMG study revealed that maintenance costs associated with cybersecurity systems are increasing. However, investing in cybersecurity remains crucial, as it helps strengthen cybersecurity resilience, preventing infrastructure failures and prolonged closures that could last for weeks. Therefore, cybersecurity resilience plays a pivotal role in maintaining economic stability. (KPMG, 2021)

SAIs should play an effective role in enhancing cybersecurity by measuring cybersecurity KPIs and urging their auditees to improve their knowledge of and approach to cybersecurity. As part of an assignment from the Kuwaiti National Assembly, SAB has examined government cybersecurity measures within its auditees and assessed their readiness. In this parliamentary

assignment, SAB utilized cybersecurity KPIs to evaluate the cybersecurity readiness of auditees, including Kuwait's oil companies, in alignment with the latest standards and best practices in this domain. The results of the assessment are presented in Table 1 below. (Al-Khalidi, 2023; The State Audit Bureau is Assigned to Prepare a Report on Government Measures Related to IT and Cyber Security, 2022; The State Audit Bureau: Five Government Entities Excel in Cybersecurity, 2023; State Audit Bureau, 2023)

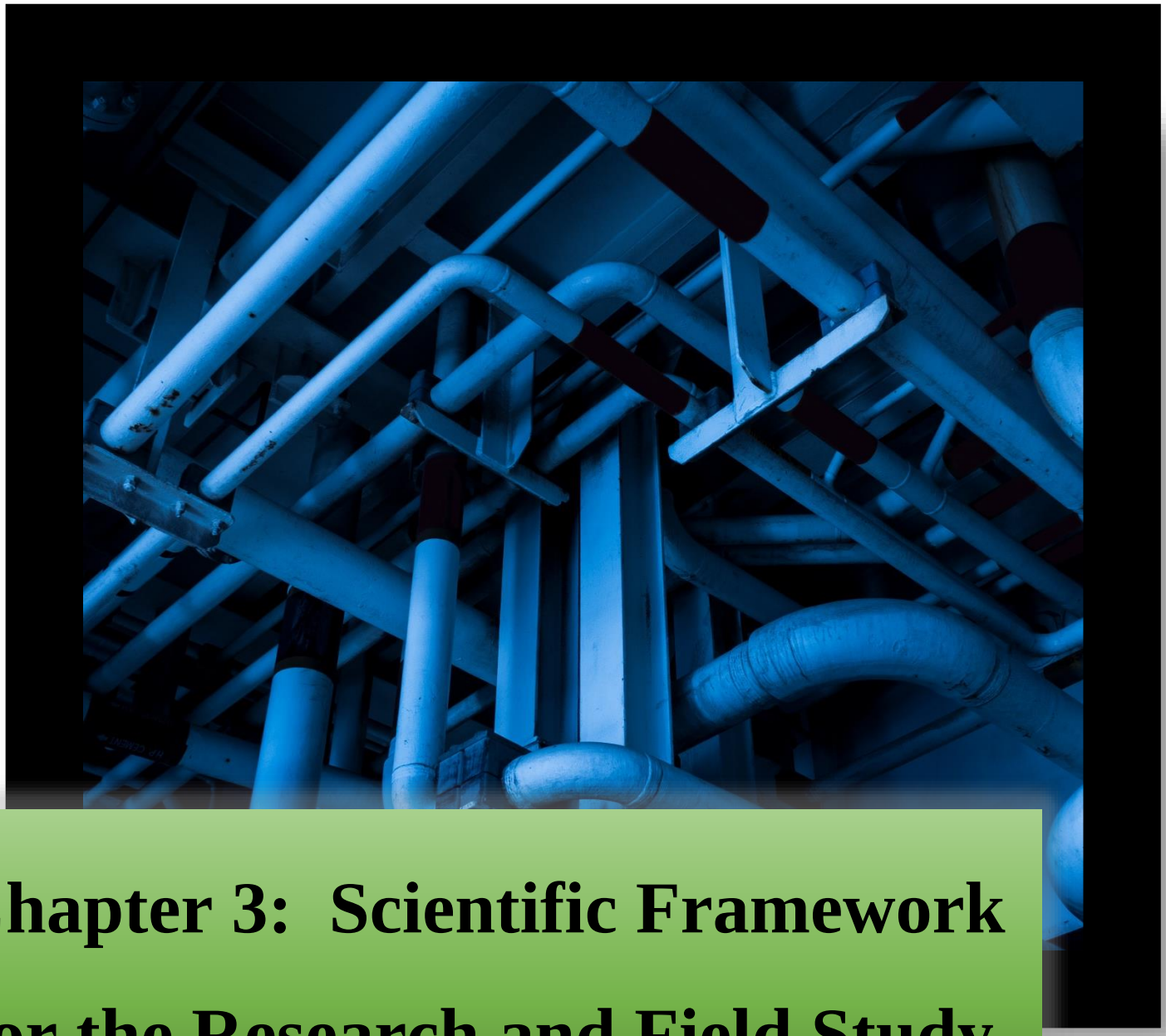
No.	Company	Readiness Ratio	Readiness Rating
1	Kuwait Integrated Petroleum Industries Company (KIPIC)	87 %	High
2	Kuwait Oil Company (KOC)	77%	Good
3	Petrochemical Industries Company (PIC)	74%	
4	Kuwait National Petroleum Company (KNPC)	72 %	
5	Kuwait Oil Tankers Co. (KOTC)	71 %	
6	Kuwait Gulf Oil Company (KGOC)	70 %	
7	Kuwait Petroleum Corporation (KPC)	62%	
8	Kuwait Foreign Petroleum Exploration Company (KUFPEC)	58%	Low
9	Ministry of Oil	8%	Poor

Table 1 – Cybersecurity Readiness of KPC and Its Subsidiaries

Source: Adapted from the State Audit Bureau (2023)

As demonstrated in Table 1, companies in Kuwait's oil and gas sector exhibit varying levels of cybersecurity readiness. While some entities have achieved high ratings, others remain at lower levels. During the COVID-19 pandemic, several companies in the sector implemented new regulations to protect mega projects from cyberattacks, particularly in response to the increased reliance on remote work. Furthermore, cybersecurity has been integrated into contractual agreements, requiring contractors to adhere to cybersecurity policies and state regulations. In the event of a violation of these policies and regulations, the contractor incurs a penalty, which may amount to 2% of the contract value in some oil sector contracts. (Cybersecurity Guidelines for Contractors, 2019; KNPC Increases Cybersecurity Protection with Matrox Extio 3, 2020)

The researcher asserts that cybersecurity is a continuously evolving field that will remain in a state of constant development driven by technological advancements. Therefore, it is essential for oil companies in Kuwait to keep pace with developments in cybersecurity and relevant KPIs to enhance their cybersecurity readiness and ensure the sector's protection against cyber threats. After all, measurement is a fundamental element in assessing the future state of cybersecurity.



Chapter 3: Scientific Framework for the Research and Field Study

Chapter 3

Scientific Framework for the Research and Field Study

I. Methodology

To achieve the objectives of this research and to answer the research question and sub-questions, the researcher relied on the following methods for collecting and analyzing data:

a) **Documentary Method of Data Collection:** In this method, the researcher collects information, facts, figures, and data related to cybersecurity and information systems in Kuwait's oil and gas sector. This involves auditing cybersecurity and information systems by referring to two types of sources:

- **Primary Sources:** A web-based survey tailored to this research. The aim is to achieve specific research objectives and identify cybersecurity KPIs' role in improving the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.
- **Secondary Sources:** These include various materials such as journals, studies, books, websites, laws, decisions, circulars, and articles relevant to the research topic. Given the novelty of the subject matter of the research, all sources used are current, which enhances the research's value and facilitates the implementation of its recommendations. The research utilizes only sources published between 2016 and 2024, ensuring that information is up-to-date. Additionally, most sources are in English due to their abundance, while Arabic sources on auditing cybersecurity and information systems in Kuwait's oil and gas sector are relatively scarce.

b) Descriptive Analytical Method:

This research aims to identify the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information systems audits within Kuwait's oil and gas sector. It will also examine the mechanisms utilized by the oil and gas sector to audit these systems. To achieve this, the researcher will develop and analyze a web-based survey to gather data for the study. The analysis will be conducted using SPSS statistics software.

II. Research Population and Sample

- **Research Population:** The study includes government oil companies within the oil and gas sector in Kuwait, specifically Kuwait Petroleum Corporation (KPC) and its seven subsidiaries, as outlined in the table below.

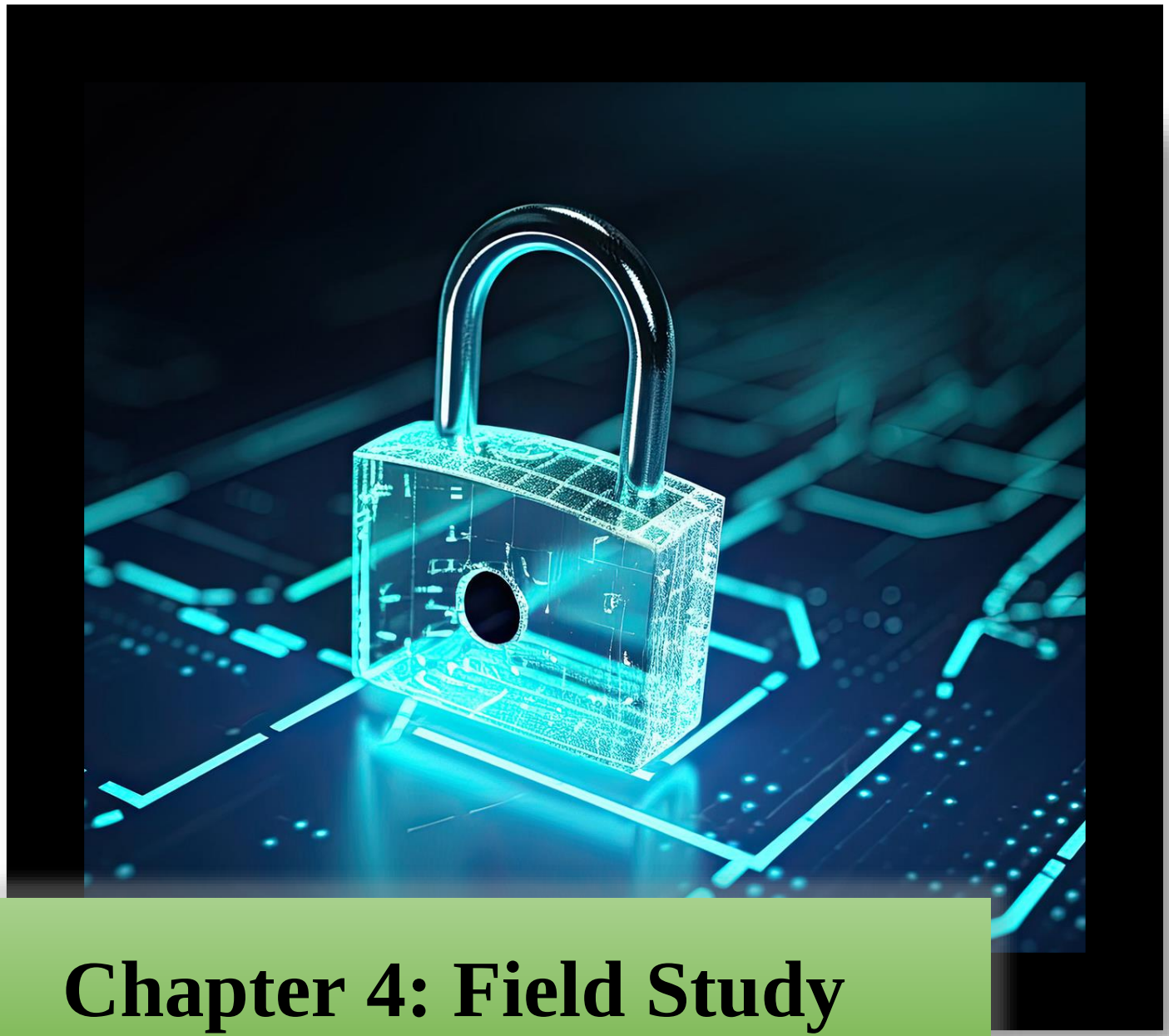
	Company
1	Kuwait Petroleum Corporation (KPC)
2	Kuwait Oil Company (KOC)
3	Petrochemical Industries Company (PIC)
4	Kuwait National Petroleum Company (KNPC)
5	Kuwait Oil Tankers Company (KOTC)
6	Kuwait Gulf Oil Company (KGOC)
7	Kuwait Integrated Petroleum Industries Company (KIPIC)
8	Kuwait Foreign Petroleum Exploration Company (KUFPEC)

Table 2 – List of Study Sample Companies

- **Research Sample:** The sample comprises computer engineers, accountants, internal auditors, cybersecurity experts, and financial managers at KPC and its subsidiaries. Additionally, it includes SABs' auditors in the Oil Entities Production and Manufacturing Audit Department and the Oil Entities Marketing and Investment Audit Department. The sampling was conducted using a stratified sampling method, which included 120 male and female employees.
- **Research Tool:** The web-based survey was created using the "SurveyMonkey" platform and was divided into two sections to encompass all hypotheses:
    - **Section (1):** This section focuses on the respondents' professional information. It includes three profile fields: job title, academic qualification, and years of experience.
    - **Section (2):** This section is divided into six themes: one primary theme addressing the primary hypothesis and five sub-themes corresponding to the five sub-hypotheses of the study:
        - **Primary Theme:** Cybersecurity KPIs contribute to enhancing the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.
        - **Theme 1:** Kuwait's oil and gas sector is marked for adopting a well-defined strategy for the measurement of cybersecurity KPIs.
        - **Theme 2:** The measurement of cybersecurity KPIs contributes to elevating the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.
        - **Theme 3:** There are defined requirements for integrating cybersecurity into audit practices within Kuwait's oil and gas sector.

- **Theme 4:** Kuwait's oil and gas sector keeps pace with the latest advancements in the domain of cybersecurity and the audits of cybersecurity and information systems.
- **Theme 5:** Employees of Kuwait's oil and gas sector are sufficiently trained and qualified in cybersecurity.

Survey responses were measured using a five-point Likert scale. In this scale, "1" indicates strongly agree, "2" agree, "3" neutral, "4" disagree, and "5" strongly disagree. To take advantage of the Likert scale, simple yes-or-no questions were avoided. This approach provides a standardized framework for opinion assessment, which promotes objectivity and flexibility in analyzing, preparing results, and formulating recommendations.



Chapter 4: Field Study Analysis

Chapter 4

Field Study Analysis

The researcher's field study will focus on topics related to cybersecurity and information systems audits, as well as cybersecurity KPIs in the oil and gas sector. The analysis of data collected through the survey, using the SPSS statistical software, aims to identify the knowledge, information, and skills of employees affiliated with government oil companies in Kuwait, as well as SAB auditors responsible for auditing KPC and its subsidiaries. This study will evaluate the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information systems auditing in Kuwait's oil and gas sector.

After reviewing the research sections in Chapter 2 and the research scientific framework in Chapter 3, this chapter will discuss the results of the field study conducted to measure the impact of cybersecurity KPIs on enhancing the quality of cybersecurity and information systems auditing in Kuwait's oil and gas sector. Following the data entry in SPSS software, the results of the field study will be analyzed in this chapter.

In this research, a field approach was employed using a web-based survey to gather information on the role of cybersecurity KPIs in enhancing the quality of cybersecurity and information systems auditing within Kuwait's oil and gas sector. The survey targeted employees of KPC and its subsidiaries, as well as auditors from SAB auditing Kuwait's oil and gas sector. The descriptive analysis of the survey encompasses the study population, which was discussed in detail in Chapter 3. The study population consisted of 125 individuals, including employees from KPC and its subsidiaries, along with SAB auditors who audit oil and gas companies in Kuwait. The response rate was 96%, with only 120 completed surveys received electronically.

The following part of the chapter will present an analysis of responses to the statements included under Section 1 and Section 2 of the survey.

Analysis of Section 1 of the Web-based Survey

Professional Information

1. Job Title

A sample of various positions within KPC and its subsidiaries has been collected, focusing on fields such as accounting, cybersecurity, computer engineering, and information systems. The sample also includes titles held by SAB auditors responsible for auditing KPC and its subsidiaries. The participation rates for each role are as follows: accountants had the highest participation rate at 23.3%, internal auditors followed at 20%, and financial managers at 17.5%. Computer engineers accounted for 15% of the participation, while SAB auditors comprised 11.7%. The least represented were cybersecurity experts (9.2%) and information systems managers (3.3%). These statistics are illustrated in Figure 16 and Table 3.

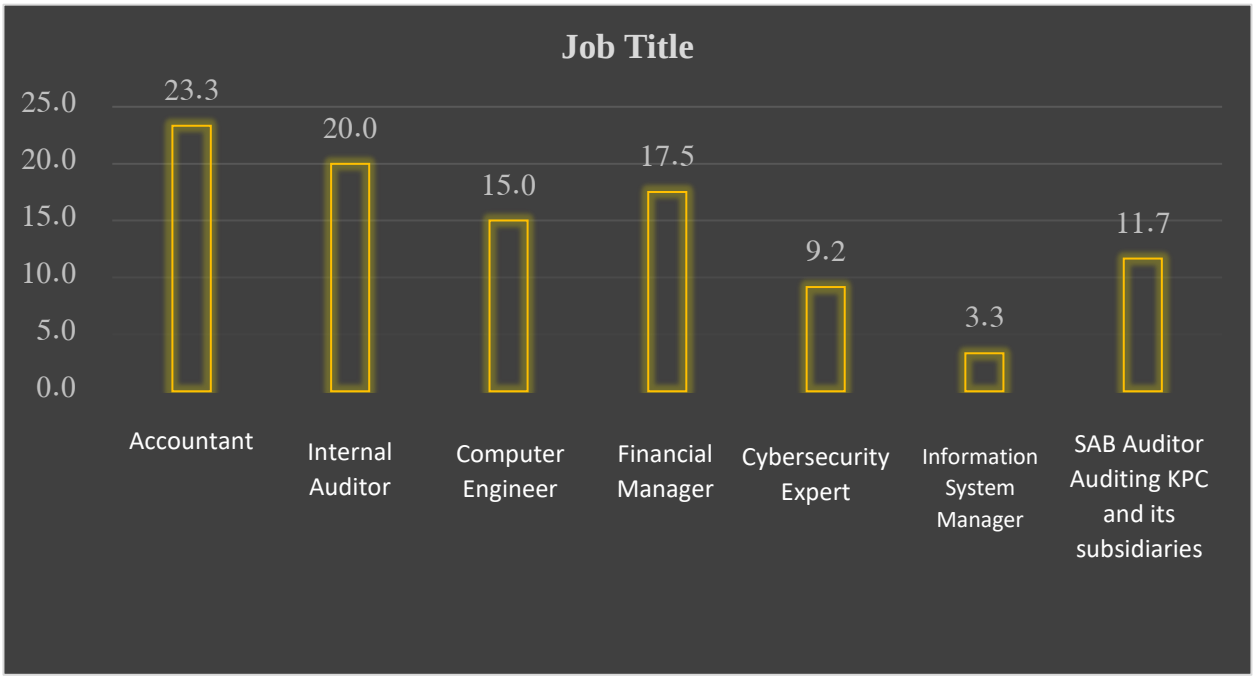


Figure 16: Distribution of Respondents by Job Title

Job Title

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accountant	28	23.3	23.3	23.3
	Internal Auditor	24	20.0	20.0	43.3
	Computer Engineer	18	15.0	15.0	58.3
	Financial Manager	21	17.5	17.5	75.8
	Cybersecurity Expert	11	9.2	9.2	85.0
	Information Systems Manager	4	3.3	3.3	88.3
	SAB Auditor Auditing KPC and its Subsidiaries	14	11.7	11.7	100.0
	Total	120	100.0	100.0	

Table 3 – SPSS Analysis of Respondents' Job Titles

2. Academic Qualification

The study sample consisted of five majors that provide valuable academic qualifications for the research population. Among the respondents' majors, cybersecurity had the highest representation at 29%, followed by business administration at 28% and accounting at 23%. Fewer respondents

specialized in computer engineering, representing 14%, while information systems had the lowest participation rate at only 6%. These findings are illustrated in Table 4 and Figure 17 below.

Academic Qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accounting	28	23.3	23.3	23.3
	Business Administration	33	27.5	27.5	50.8
	Cybersecurity	35	29.2	29.2	80.0
	Computer Engineering	17	14.2	14.2	94.2
	Information Systems	7	5.8	5.8	100.0
	Total	120	100.0	100.0	

Table 4 – SPSS Analysis of Respondents' Academic Qualifications

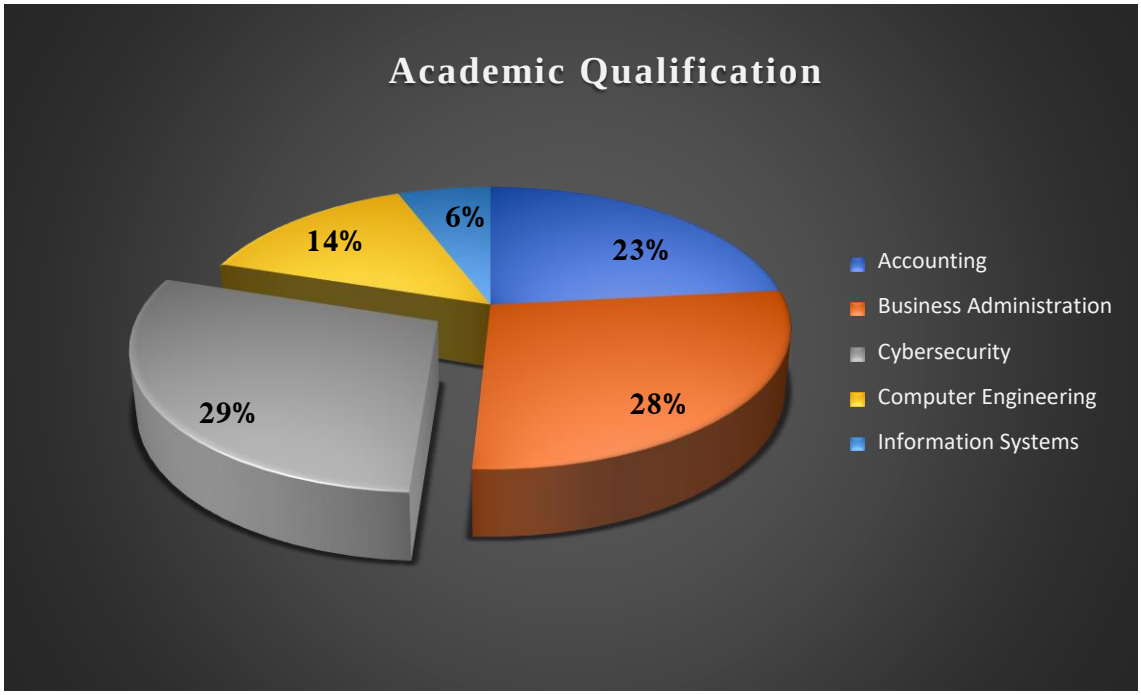


Figure 17: Distribution of Respondents by Academic Qualifications

3. Years of Experience

In terms of professional experience, the survey indicated that the largest segment of respondents, constituting 35%, had between 5 to 10 years of experience. It was closely followed by individuals with 11 to 15 years of experience, who comprised 26.7% of the respondents. Those with less than 5 years of experience represented 22.5%. The smallest group comprised individuals with more than 15 years of experience, accounting for 15.8% of the total respondents. These data are illustrated in Table 5 and Figure 18 as follows:

Years of Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 5 years	27	22.5	22.5	22.5
	5 – 10 years	42	35.0	35.0	57.5
	11 – 15 years	32	26.7	26.7	84.2
	More than 15 years	19	15.8	15.8	100.0
	Total	120	100.0	100.0	

Table 5 – SPSS Analysis of Respondents' Years of Experience

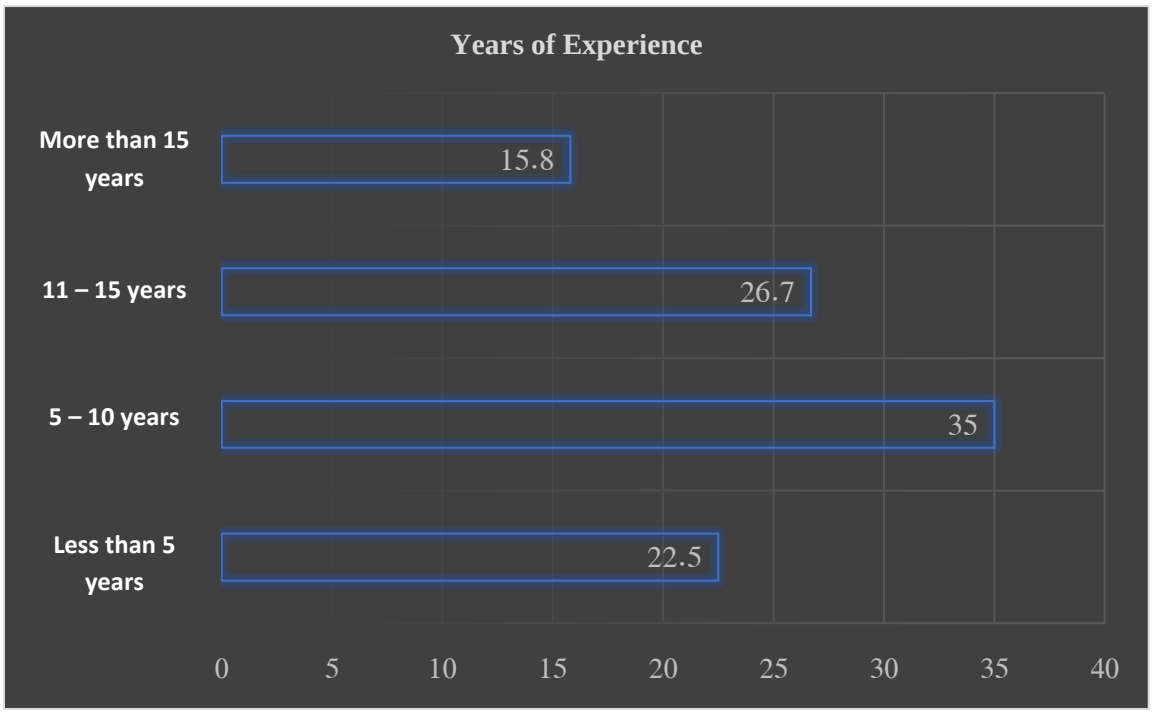


Figure 18: Distribution of Respondents by Years of Experience

Below, the analysis of the second section of the survey will be presented. Section 2 consists of a primary theme and five sub-themes. The primary theme supports the research hypothesis, while the other themes address five sub-hypotheses.

Analysis of Section 2 of the Web-based Survey

I. Primary Theme: Cybersecurity KPIs contribute to enhancing the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.

The first seven survey statements address the research hypothesis, which states that cybersecurity KPIs play a role in improving the quality of cybersecurity and information systems auditing in Kuwait's oil and gas sector. The results of the survey are as follows:

Survey Statement 1: I have sufficient knowledge of the types of cybersecurity KPIs and their measurement mechanisms.

With respect to employees' knowledge of cybersecurity KPIs and their measurement mechanisms, the results of the survey indicated that 24.2% of the respondents strongly disagreed, with an equal percentage (24.2%) remaining neutral or disagreed. Only 19.2% of the respondents agreed that they had knowledge of cybersecurity KPIs. The smallest proportion, at 8.3%, strongly agreed regarding their knowledge of the types of KPIs. These data are illustrated in Table 6 and Figure 19 below.

Q1

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	29	24.2	24.2	24.2
	Disagree	29	24.2	24.2	48.3
	Neutral	29	24.2	24.2	72.5
	Agree	23	19.2	19.2	91.7
	Strongly Agree	10	8.3	8.3	100.0
	Total	120	100.0	100.0	

Table 6 – SPSS Analysis of Statement 1

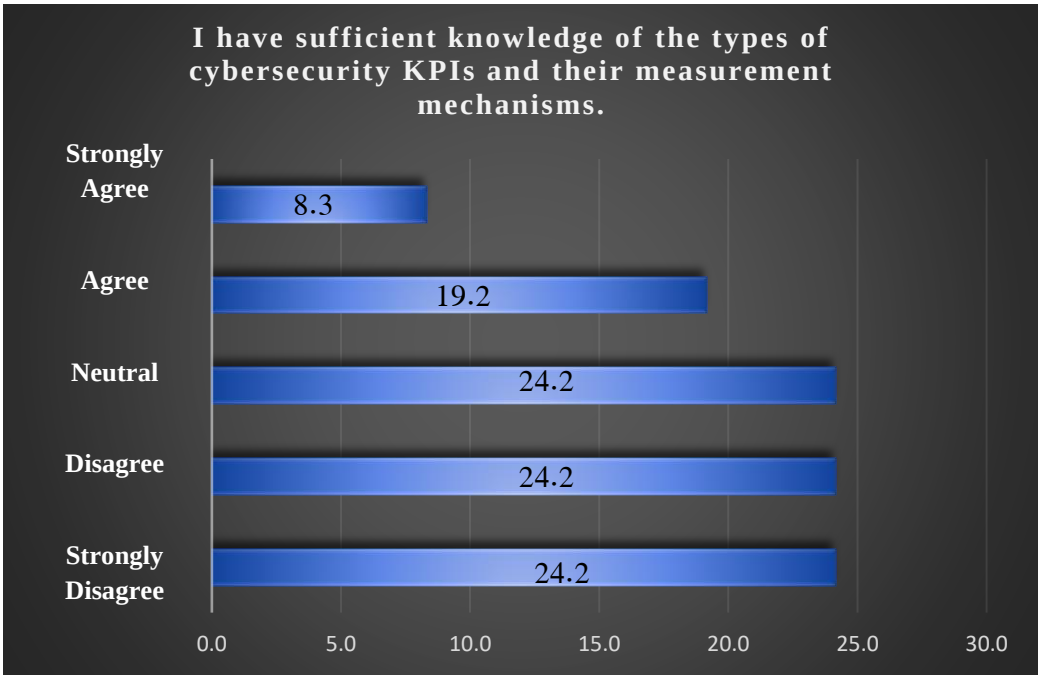


Figure 19: Survey Responses to Statement 1

Survey Statement 2: The company measures cybersecurity KPIs.

Findings revealed that 27.5% of respondents were neutral regarding the statement that KPC and its subsidiaries measure cybersecurity KPIs. Additionally, 23.3% strongly disagreed that the companies measure cybersecurity KPIs, while 20% disagreed. Only 10% strongly agreed, marking the lowest response rate. These data are illustrated in Table 7 and Figure 20 below.

Q2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	28	23.3	23.3	23.3
	Disagree	24	20.0	20.0	43.3
	Neutral	33	27.5	27.5	70.8
	Agree	23	19.2	19.2	90.0
	Strongly agree	12	10.0	10.0	100.0
	Total	120	100.0	100.0	

Table 7 – SPSS Analysis of Statement 2

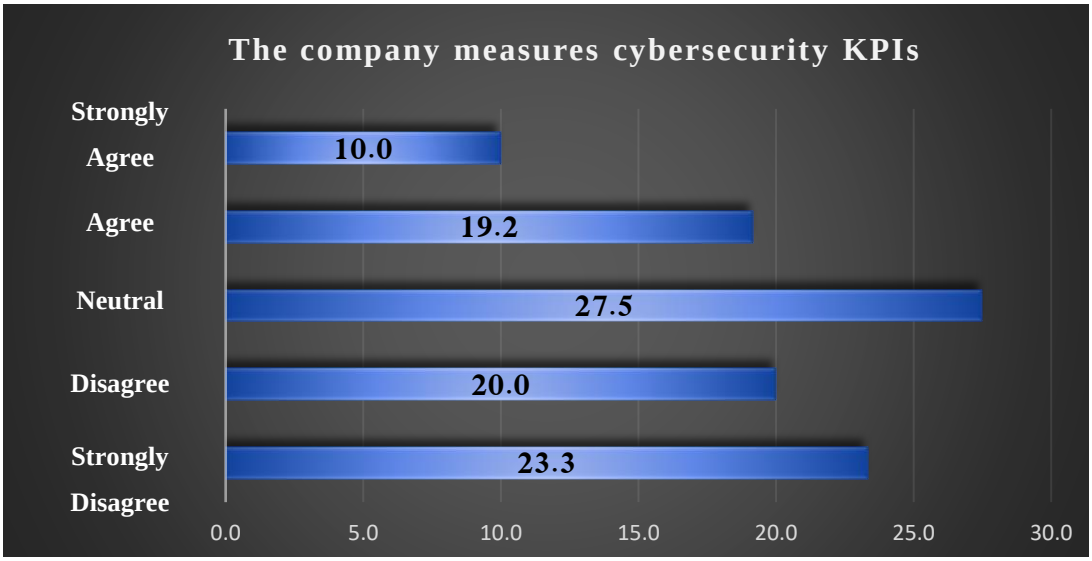


Figure 20: Survey Responses to Statement 2

Survey Statement 3: The company has a defined classification for cybersecurity activities, which makes it easier to measure cybersecurity KPIs and assess cybersecurity risks.

According to the statistical analysis, 26% of respondents agreed that their companies classify cybersecurity activities, making it easier to measure KPIs and assess relevant risks. However, 25% of respondents strongly disagreed with that statement and 24% disagreed. The smallest proportions were observed among 18.3% of neutral respondents and 6.7% who strongly agreed. These data are illustrated in Table 8 and Figure 21 below.

Q3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	30	25.0	25.0	25.0
	Disagree	29	24.2	24.2	49.2
	Neutral	22	18.3	18.3	67.5
	Agree	31	25.8	25.8	93.3
	Strongly Agree	8	6.7	6.7	100.0
	Total	120	100.0	100.0	

Table 8 – SPSS Analysis of Statement 3

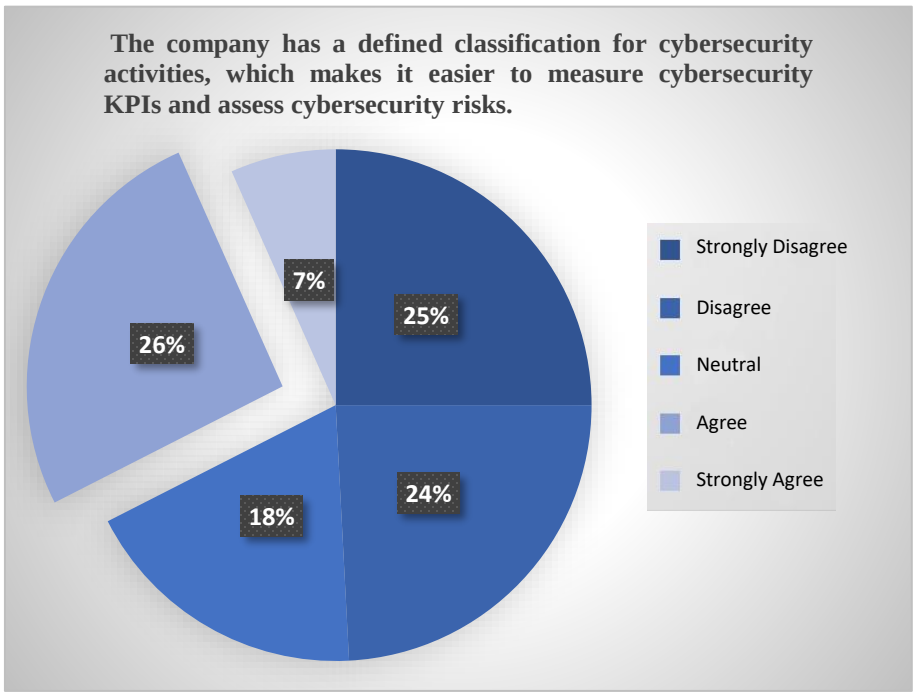


Figure 21: Survey Responses to Statement 3

Survey Statement 4: Measuring cybersecurity KPIs contributes to decision-making within the company.

The statistical analysis revealed that 26.7% of respondents were neutral regarding the contribution of cybersecurity KPI measurement to decision-making. In comparison, 25.8% agreed that measuring KPIs plays a role in making decisions within Kuwait's oil and gas sector. Notably, only 10% of respondents strongly agreed with this statement, as illustrated in Table 9 and Figure 22.

Q4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	21	17.5	17.5	17.5
	Disagree	24	20.0	20.0	37.5
	Neutral	32	26.7	26.7	64.2
	Agree	31	25.8	25.8	90.0
	Strongly Agree	12	10.0	10.0	100.0
	Total	120	100.0	100.0	

Table 9 – SPSS Analysis of Statement 4

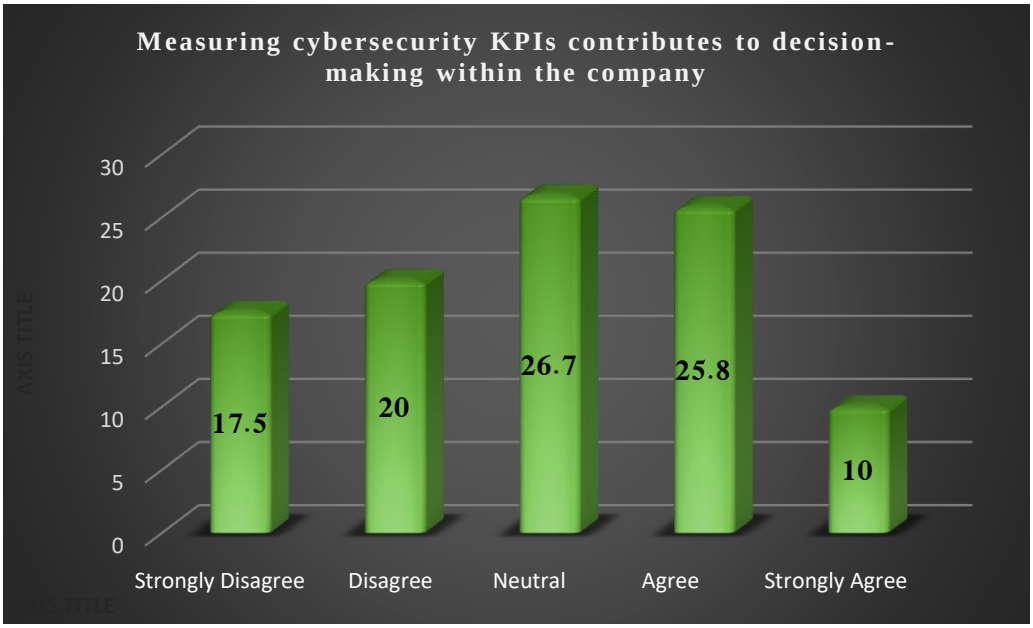


Figure 22: Survey Responses to Statement 4

Survey Statement 5: The cybersecurity-related information and data available at the company are sufficient for the measurement of cybersecurity KPIs.

The responses to this statement on information availability for measuring cybersecurity KPIs were close. Specifically, 28% of the sample chose a neutral stance, while 27% disagreed that the available information was sufficient for measuring KPIs. Moreover, 20% agreed that the available information was adequate, 18% strongly disagreed, and only 7% strongly agreed. These data are illustrated in Table 10 and Figure 23 below.

Q5

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	22	18.3	18.3	18.3
	Disagree	32	26.7	26.7	45.0
	Neutral	33	27.5	27.5	72.5
	Agree	24	20.0	20.0	92.5
	Strongly Agree	9	7.5	7.5	100.0
	Total	120	100.0	100.0	

Table 10 – SPSS Analysis of Statement 5

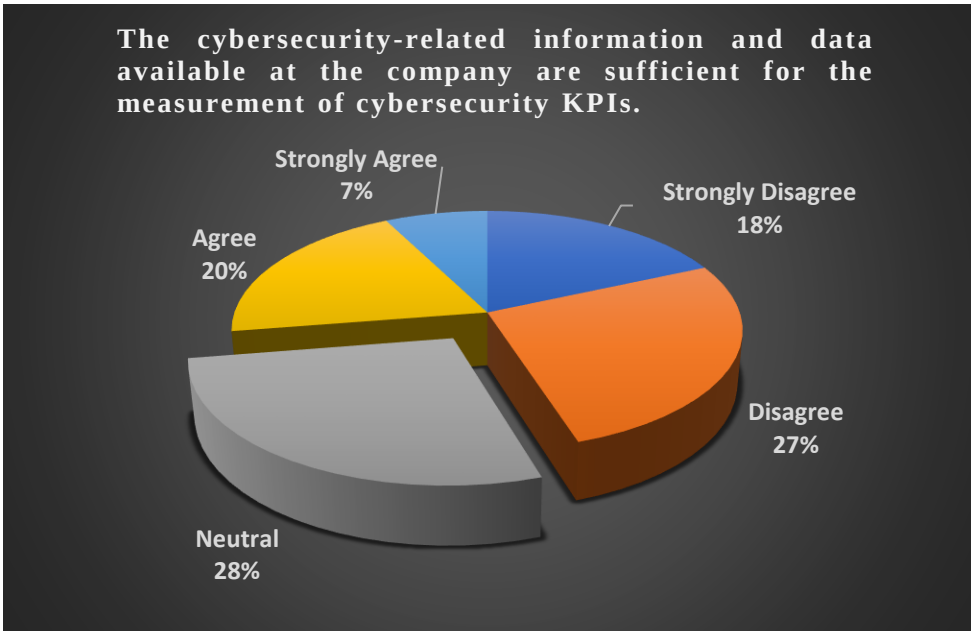


Figure 23: Survey Responses to Statement 5

Survey Statement 6: Measuring cybersecurity KPIs enhances the quality of audit outcomes.

In the survey, 26.7% of respondents agreed that measuring KPIs enhances the quality of audit outcomes, while 19.2% strongly agreed with this statement. The majority of respondents, 31.7%, were neutral on this matter. In contrast, 8.3% of respondents disagreed. These findings are illustrated in Figure 24 and Table 11.

Q6

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	17	14.2	14.2	14.2
	Disagree	10	8.3	8.3	22.5
	Neutral	38	31.7	31.7	54.2
	Agree	32	26.7	26.7	80.8
	Strongly Agree	23	19.2	19.2	100.0
	Total	120	100.0	100.0	

Table 11 – SPSS Analysis of Statement 6

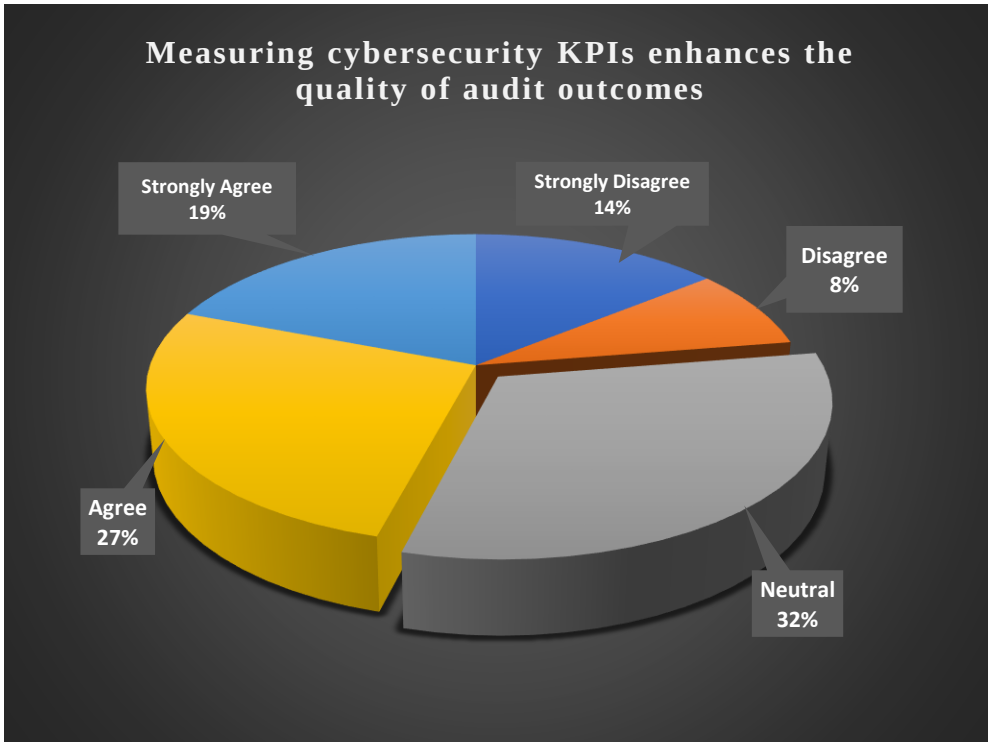


Figure 24: Survey Responses to Statement 6

Survey Statement 7: There is a correlation between cybersecurity KPIs and the quality of audits.

The results showed that 27.5% of respondents agreed that there is a correlation between cybersecurity KPIs and audit quality. 24.2% of respondents were neutral, while 20.8% disagreed. Notably, only 14.2% strongly agreed with the statement, and 13.3% strongly disagreed, marking the lowest rates. These findings are illustrated in Figure 25.

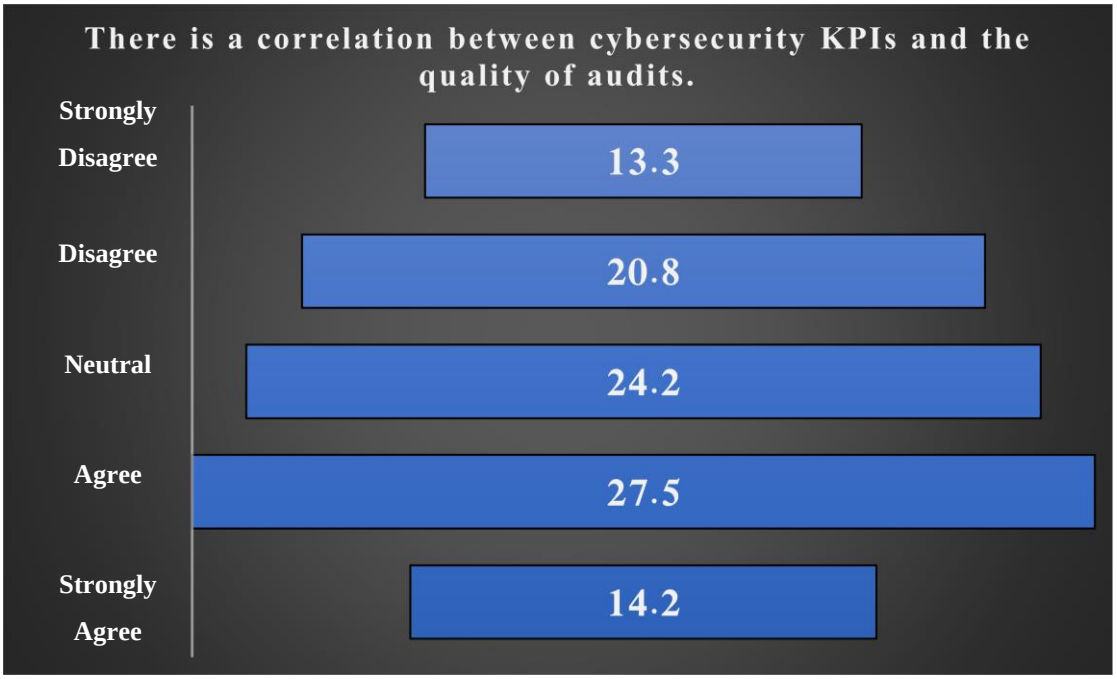


Figure 25: Survey Responses to Statement 7

II. Theme 1: Kuwait's oil and gas sector is marked for adopting a well-defined strategy for the measurement of cybersecurity KPIs.

Survey Statement 8: I have sufficient knowledge of Kuwait's National Cybersecurity Strategy.

Regarding respondents' awareness of the National Cybersecurity Strategy, the question was not framed as a simple yes-or-no question but utilized the Likert scale to assess fluctuations in understanding. The statistical analysis revealed that 30.8% of respondents disagreed that they have knowledge of the National Cybersecurity Strategy. Moreover, 28.3% of respondents were neutral, and 20.8% strongly disagreed with knowing the strategy. Only 15% agreed, while a mere 5% strongly agreed with their knowledge of the National Cybersecurity Strategy. These data are illustrated in Figure 26 below.

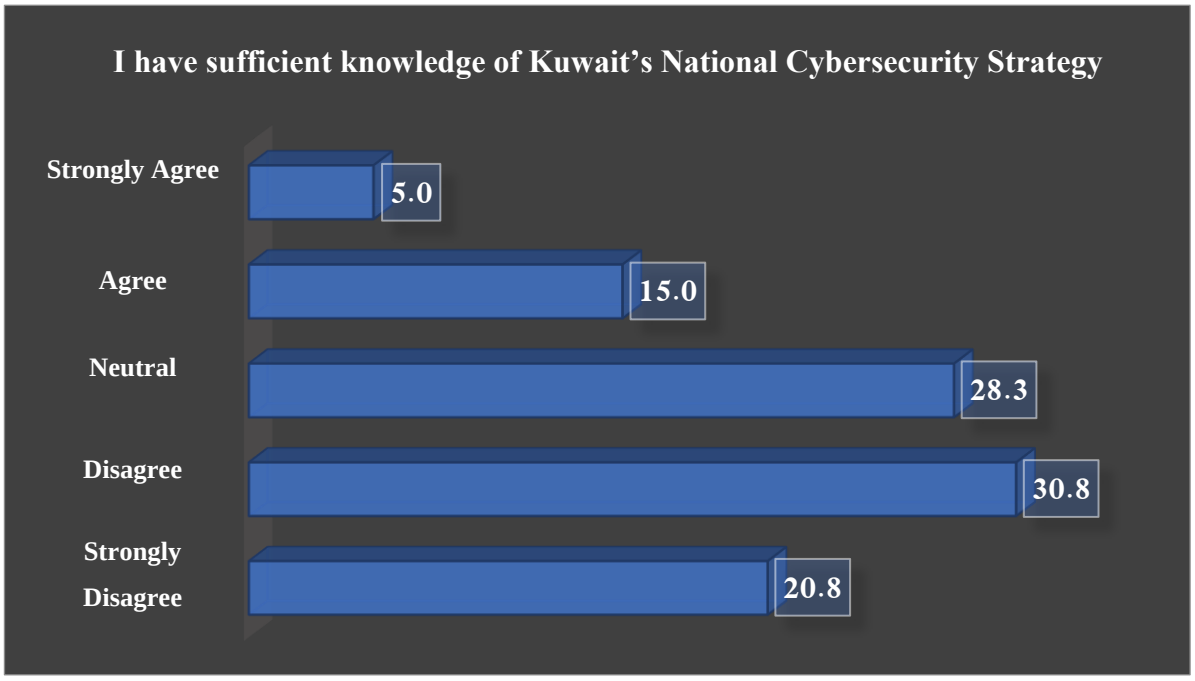


Figure 26: Survey Responses to Statement 8

Survey Statement 9: Kuwait's oil and gas sector has a comprehensive and well-defined strategy for cybersecurity that comprises cybersecurity KPIs.

In terms of opinions regarding the existence of such a strategy in Kuwait's oil and gas sector, 26% of respondents agreed, while an equal percentage (26%) remained neutral on the matter. Conversely, 20% of the sample disagreed, and 17% strongly disagreed. Only 11% of respondents strongly agreed that the sector possesses a comprehensive cybersecurity strategy. These findings are visually summarized in Figure 27.

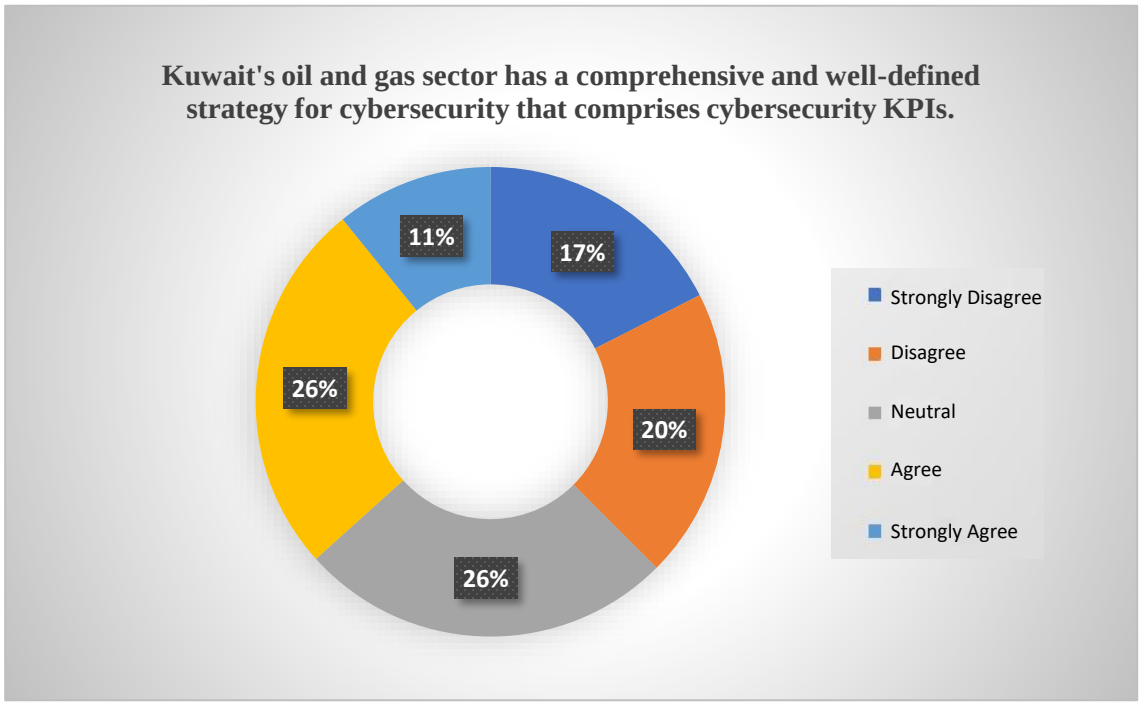


Figure 27: Survey Responses to Statement 9

Survey Statement 10: I have sufficient knowledge of the cybersecurity strategy of Kuwait's oil and gas sector.

The results regarding employees' awareness of the sector's cybersecurity strategy showed notable fluctuations. The highest percentage of respondents, 26.7%, strongly disagreed, while only 8.3% strongly agreed, marking the lowest rate. The remaining respondents exhibited varying degrees of opinion, with 25% remaining neutral and 21.7% disagreeing, as illustrated in Table 12 and Figure 28 below.

Q10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	32	26.7	26.7	26.7
	Disagree	26	21.7	21.7	48.3
	Neutral	30	25.0	25.0	73.3
	Agree	22	18.3	18.3	91.7
	Strongly Agree	10	8.3	8.3	100.0
	Total	120	100.0	100.0	

Table 12 – SPSS Analysis of Statement 10

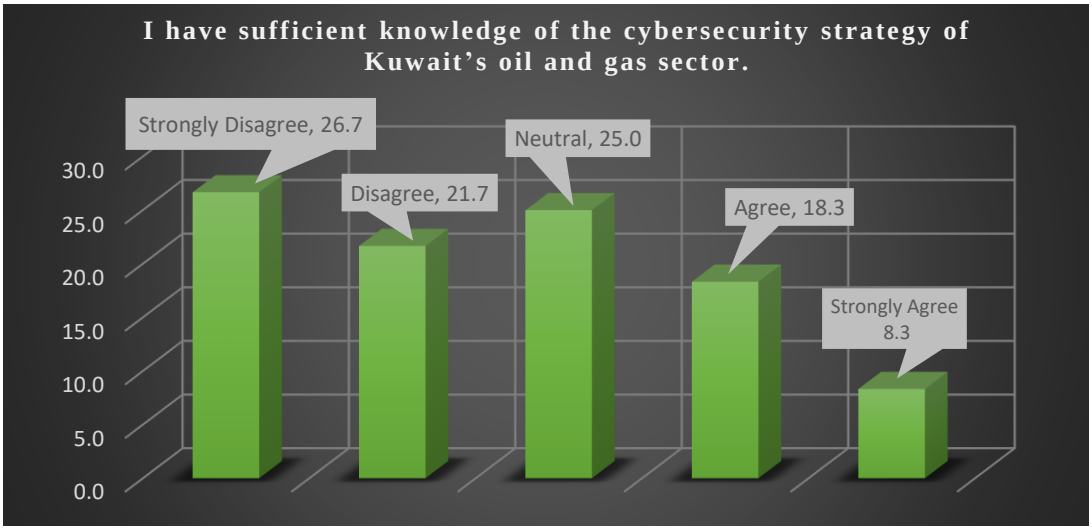


Figure 28: Survey Responses to Statement 10

Survey Statement 11: I have sufficient knowledge of cybersecurity frameworks and their implementation mechanisms for achieving the objectives of the sector's cybersecurity strategy.

In assessing respondents' knowledge of cybersecurity frameworks and their implementation mechanisms, the results revealed that 30% strongly disagreed with knowing these frameworks. In contrast, only 8.3% strongly agreed that they possess complete knowledge. Moreover, 26.7% of respondents remained neutral, 20% disagreed, and 15% agreed with their knowledge of the frameworks, as illustrated in Figure 29 below.

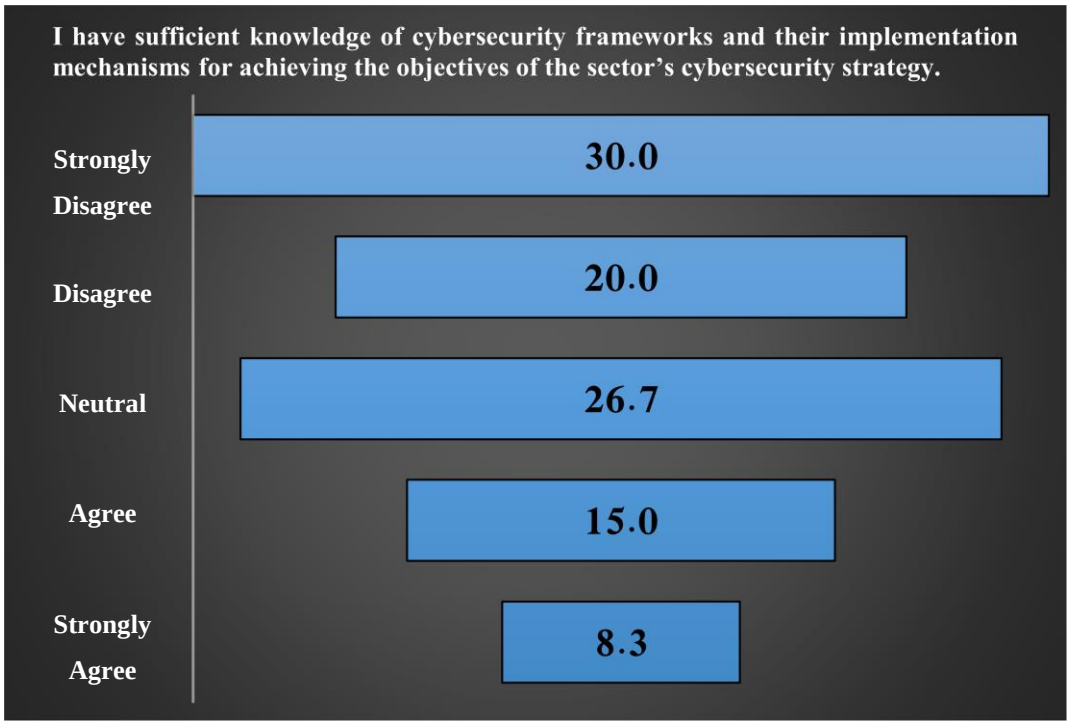


Figure 29: Survey Responses to Statement 11

Survey Statement 12: I have sufficient knowledge of the professional guidelines issued on cybersecurity and information systems audits and a good understanding of how they can be adopted to achieve the objectives of the sector's cybersecurity strategy.

The findings indicated that 34% of respondents disagreed regarding their knowledge of the professional cybersecurity guidelines and their implementation mechanisms to fulfill strategic objectives. Moreover, 26% were neutral regarding this matter, and 23% strongly disagreed. The lowest percentages were for those who agreed, at 12%, and those who strongly agreed, at 5%, as shown in Figure 30 below.

Figure 30: Survey Responses to Statement 12

Survey Statement 13: The company is working on finding suitable strategic solutions to mitigate cybersecurity.

According to the survey results, 28% of respondents agreed that oil companies are actively working on finding strategic solutions to mitigate the risks of cyberattacks. Moreover, 24% of respondents remained neutral on this matter, while 23% disagreed. Only 11% strongly agreed that these companies have strategic solutions to address cyber risks. These findings are illustrated in Table 13 and Figure 31 below.

Q13

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	17	14.2	14.2	14.2
	Disagree	27	22.5	22.5	36.7
	Neutral	29	24.2	24.2	60.8
	Agree	34	28.3	28.3	89.2
	Strongly Agree	13	10.8	10.8	100.0
	Total	120	100.0	100.0	

Table 13 – SPSS Analysis of Statement 13

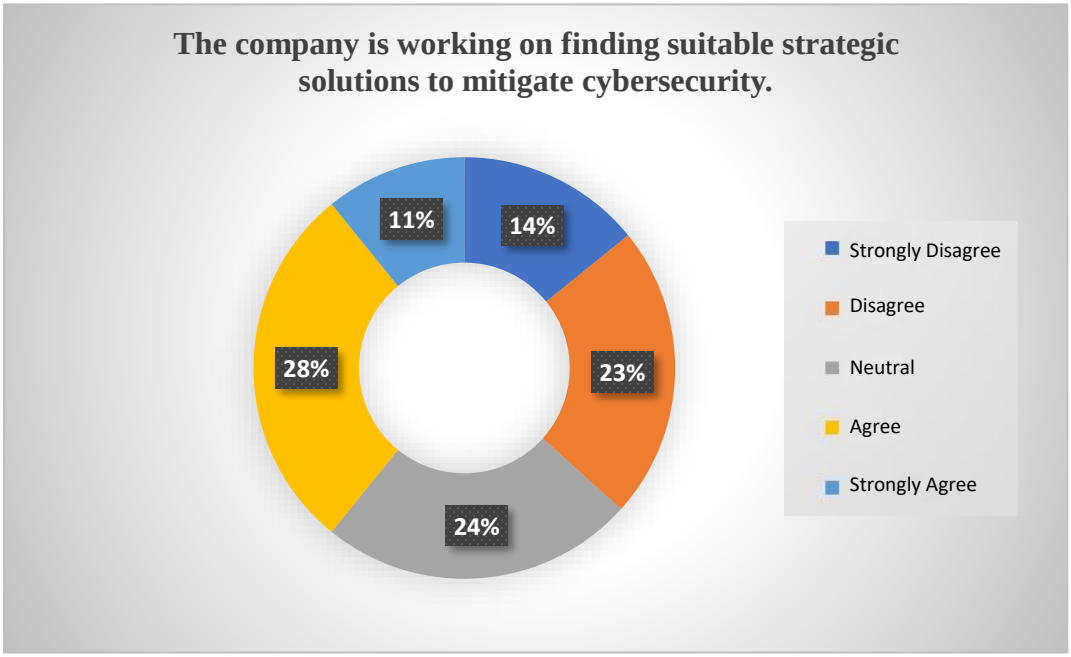


Figure 31: Survey Responses to Statement 13

Survey Statement 14: The cybersecurity strategy contributes to achieving the sector's cybersecurity and information systems objectives.

The survey results demonstrated various responses concerning the effectiveness of cybersecurity strategy in the gas and oil sector and its role in achieving cybersecurity and information systems objectives. About 26.7% of respondents agreed that the strategy effectively supports these objectives. Meanwhile, 25.8% of respondents were neutral and 16.7% disagreed that the strategy effectively aids in achieving these objectives. 15.8% strongly agreed about its contribution, whereas 15% strongly disagreed, indicating a complete lack of faith in the strategy's effectiveness. These data are illustrated in Figure 32 below.

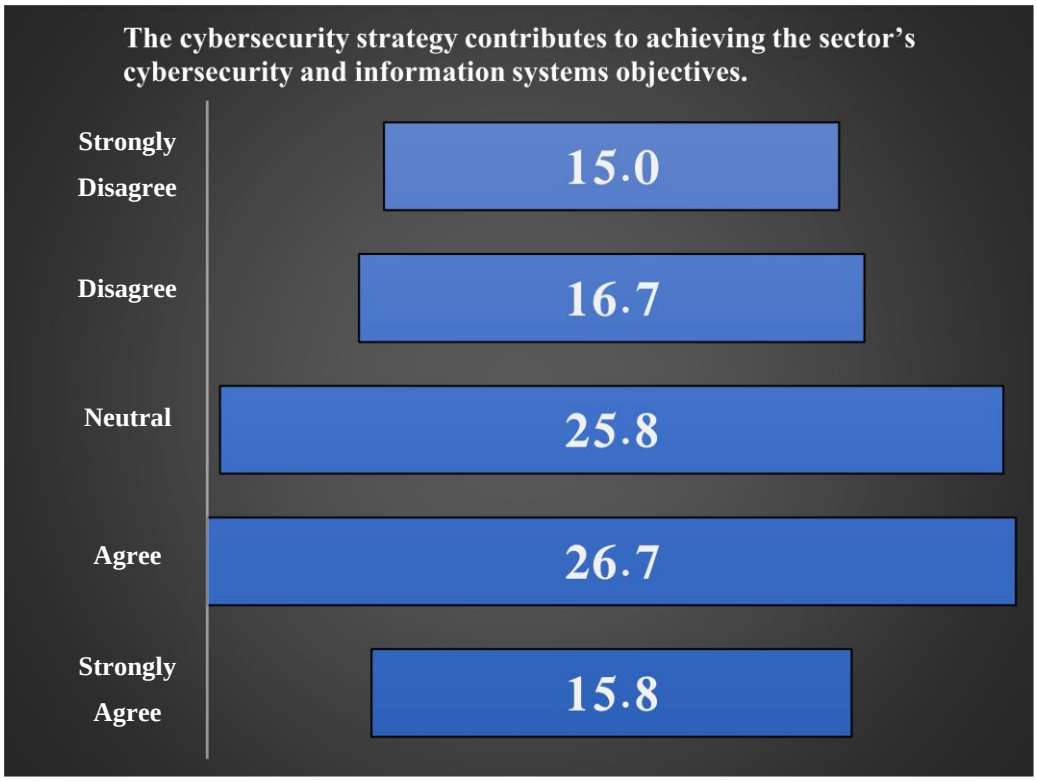


Figure 32: Survey Responses to Statement 14

III. Theme 2: The measurement of cybersecurity KPIs contributes to elevating the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.

Survey Statement 15: Measuring cybersecurity KPIs enhances the quality of audit outcomes within the company.

According to the survey results, 24% of respondents strongly agreed that measuring cybersecurity KPIs enhances the quality of audit outcomes, while 19% agreed. Moreover, 22% remained neutral regarding the matter. In contrast, 21% disagreed, and 14% strongly disagreed. These data are illustrated in Figure 33 below.

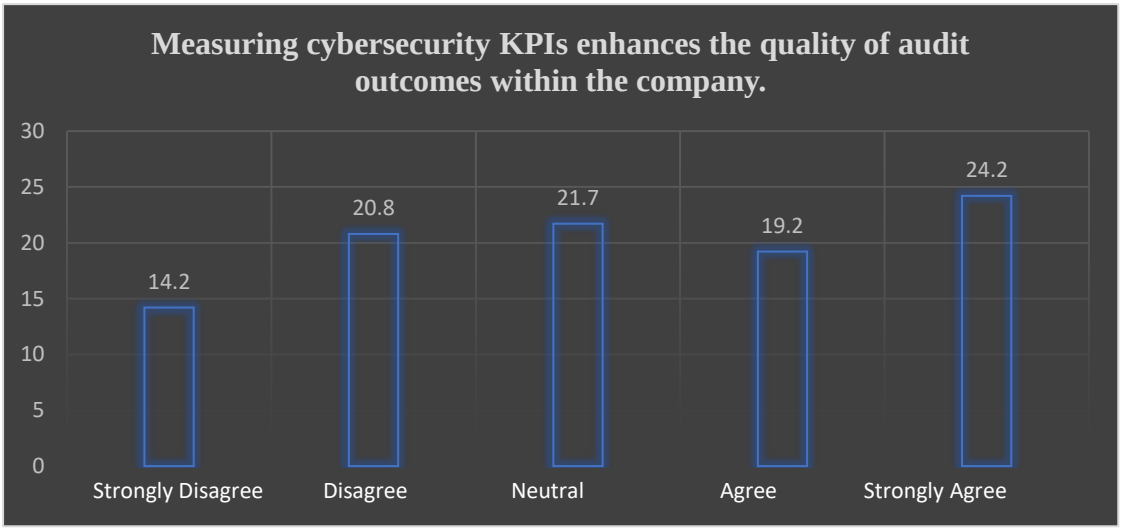


Figure 33: Survey Responses to Statement 15

Survey Statement 16: Measuring cybersecurity KPIs contributes to establishing a well-defined plan for auditing the company's cybersecurity and information systems.

Regarding measuring cybersecurity KPIs and their contribution to establishing a well-defined plan for auditing cybersecurity and information systems, the survey results indicated that 25.8% agreed that the measurement contributes to establishing the plan. In contrast, 22.5% strongly disagreed,

20.8% were neutral on this matter, 16.7% disagreed, and only 14.2% strongly agreed. These data are presented in Table 14 and Figure 34 below.

Q16

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	27	22.5	22.5	22.5
	Disagree	20	16.7	16.7	39.2
	Neutral	25	20.8	20.8	60.0
	Agree	31	25.8	25.8	85.8
	Strongly Agree	17	14.2	14.2	100.0
	Total	120	100.0	100.0	

Table 14 – SPSS Analysis of Statement 16

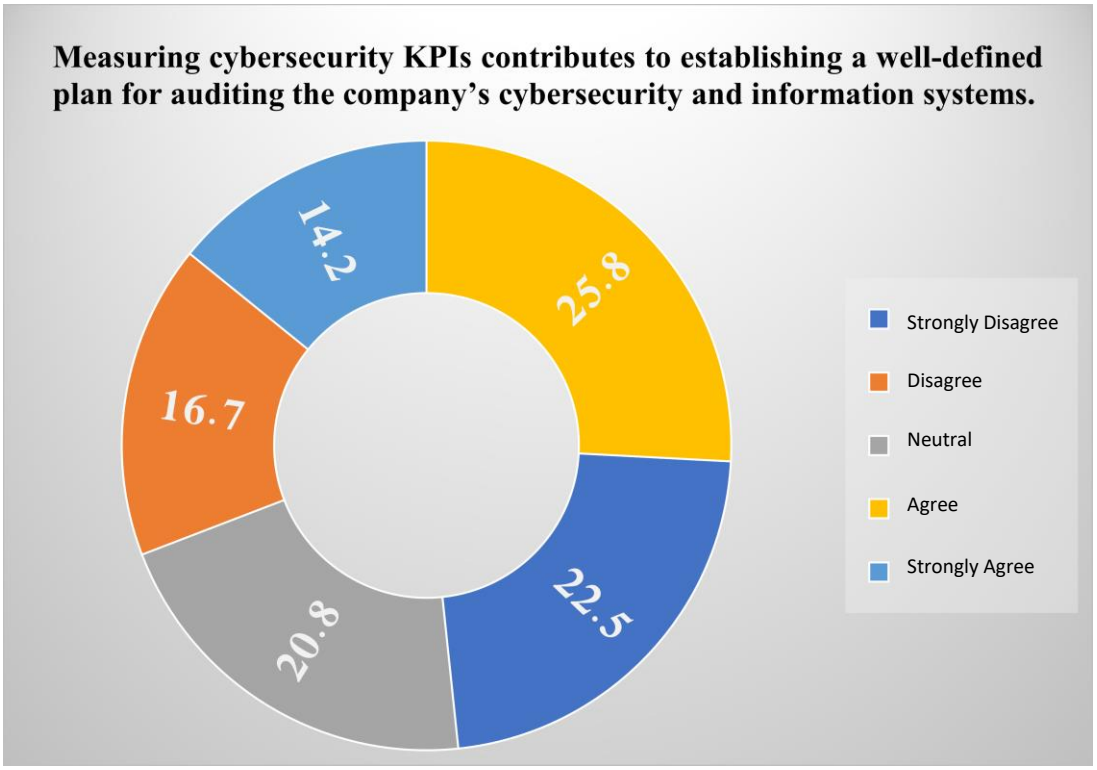


Figure 34: Survey Responses to Statement 16

Survey Statement 17: The definition and measurement of cybersecurity KPIs contribute to improving the quality of cybersecurity and information systems auditing within the company.

In the context of improving the quality of cybersecurity and information systems auditing through measuring KPIs, 26.7% of respondents agreed that defining and measuring cybersecurity KPIs contributes positively to audit quality. Moreover, 20.8% remained neutral on this matter, while 20% disagreed, 16.7% strongly disagreed, and 15.8% strongly agreed. The results are illustrated in Figure 35 below.

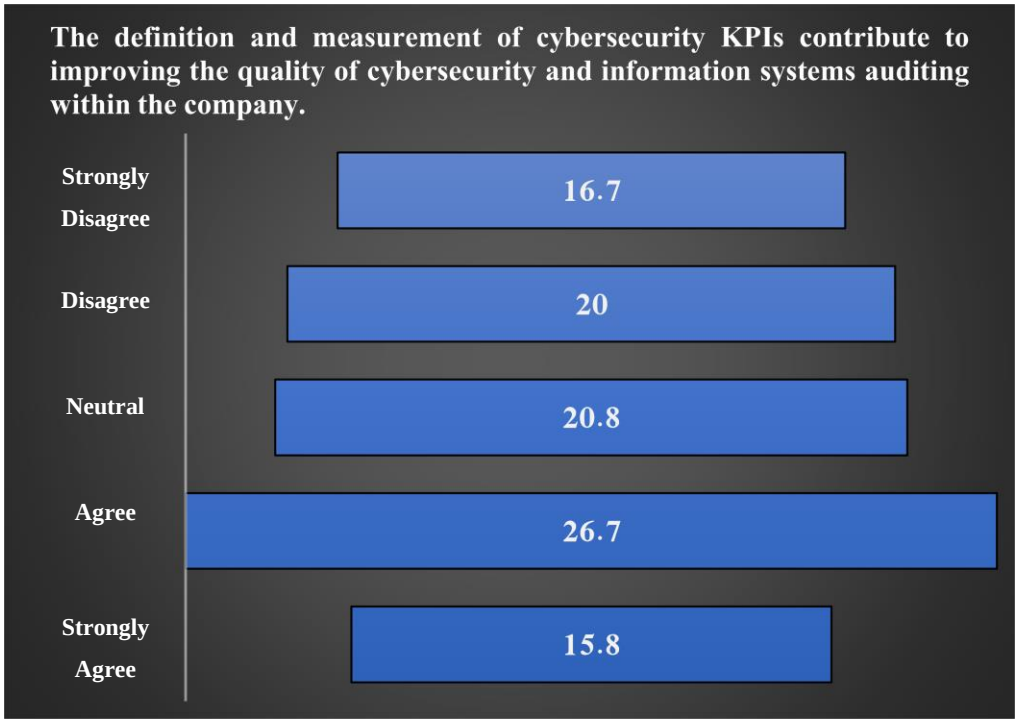


Figure 35: Survey Responses to Statement 17

Survey Statement 18: The measurement of cybersecurity KPIs is considered when making critical decisions in the company.

The survey respondents had varying opinions regarding the oil companies measuring cybersecurity KPIs during critical decision-making. Specifically, 26% of respondents strongly disagreed that cybersecurity KPIs are considered, while 25% remained neutral on this matter, 21% disagreed, 15% strongly agreed, and 13% agreed. These data are illustrated in Figure 36 below.

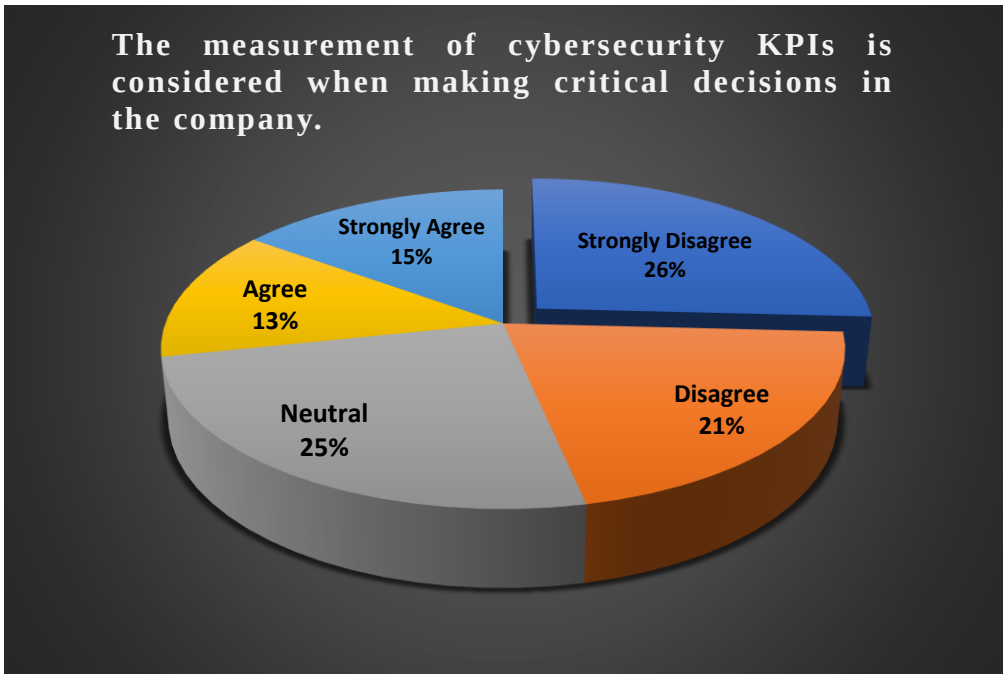


Figure 36: Survey Responses to Statement 18

Survey Statement 19: The company prepares reports on cybersecurity KPIs.

In response to the statement that oil companies prepare reports on cybersecurity KPIs, the survey results indicated the following: 27.5% of respondents strongly disagreed with this statement, 24.2% were neutral, 20.8% disagreed, 19.2% agreed, and only 8.3% strongly agreed. These data are illustrated in Figure 37 below.

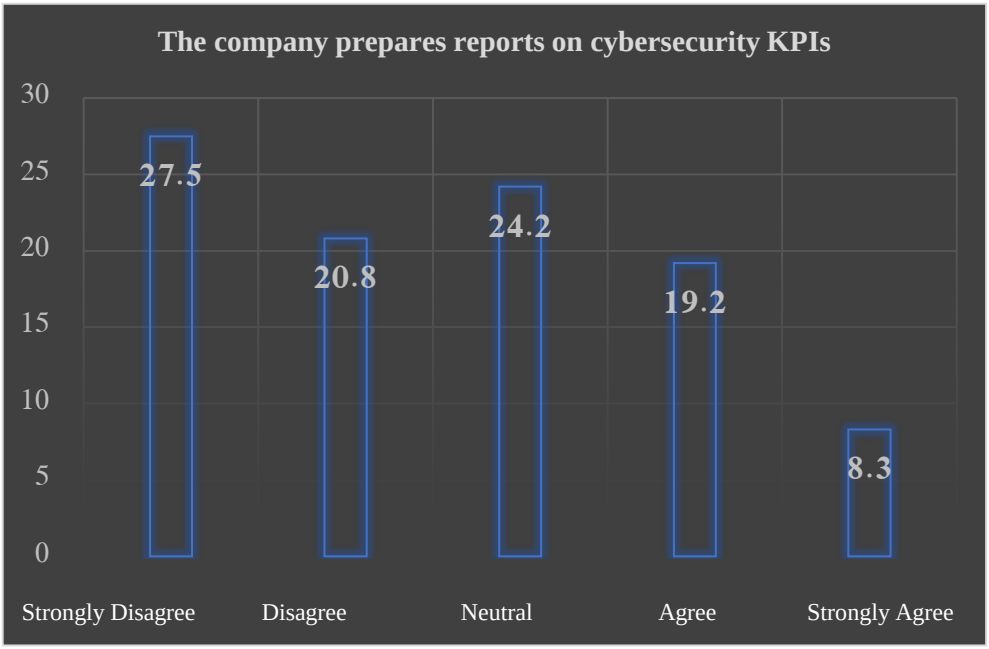


Figure 37: Survey Responses to Statement 19

Survey Statement 20: The company classifies cybersecurity activities and measures the relevant KPIs in order to improve the quality of information as well as the audit outcomes.

In analyzing whether the company classifies activities and measures relevant KPIs to improve information quality and audit outcomes, the survey results indicated that the proportion of respondents who agreed and disagreed was equal, each at 25%. Moreover, 22.5% were neutral on this matter, 16.7% strongly disagreed, and 10.8% strongly agreed. These data are illustrated in Table 15 and Figure 38 below.

Q20

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	20	16.7	16.7	16.7
	Disagree	30	25.0	25.0	41.7
	Neutral	27	22.5	22.5	64.2
	Agree	30	25.0	25.0	89.2
	Strongly Agree	13	10.8	10.8	100.0
	Total	120	100.0	100.0	

Table 15 – SPSS Analysis of Statement 20

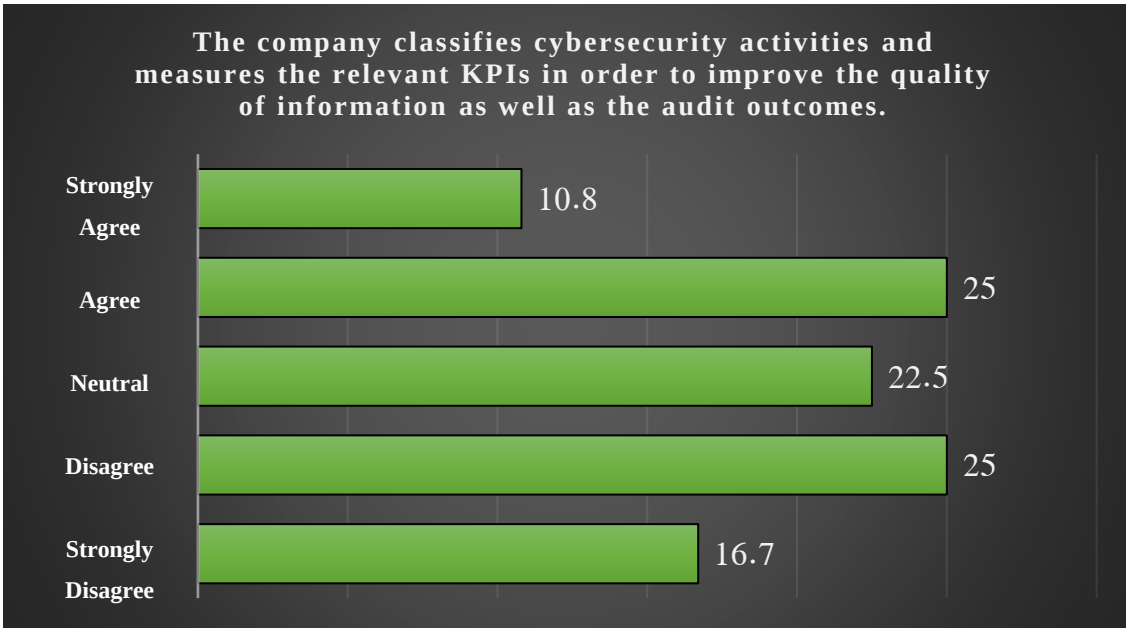


Figure 38: Survey Responses to Statement 20

IV. Theme 3: There are defined requirements for integrating cybersecurity into audit practices within Kuwait's oil and gas sector.

Survey Statement 21: The company has dedicated guidelines for auditing cybersecurity and information systems.

An analysis of having comprehensive guidelines for auditing cybersecurity and information systems within KPC and its subsidiaries revealed varied responses among respondents. Specifically, 36.7% were neutral on this matter, while 26.7% strongly disagreed that such audit guidelines exist. In contrast, 15% of respondents agreed that these guidelines are present. Only 9.2% of respondents strongly agreed, marking the least represented survey sample. These results are illustrated in Figure 39 below.

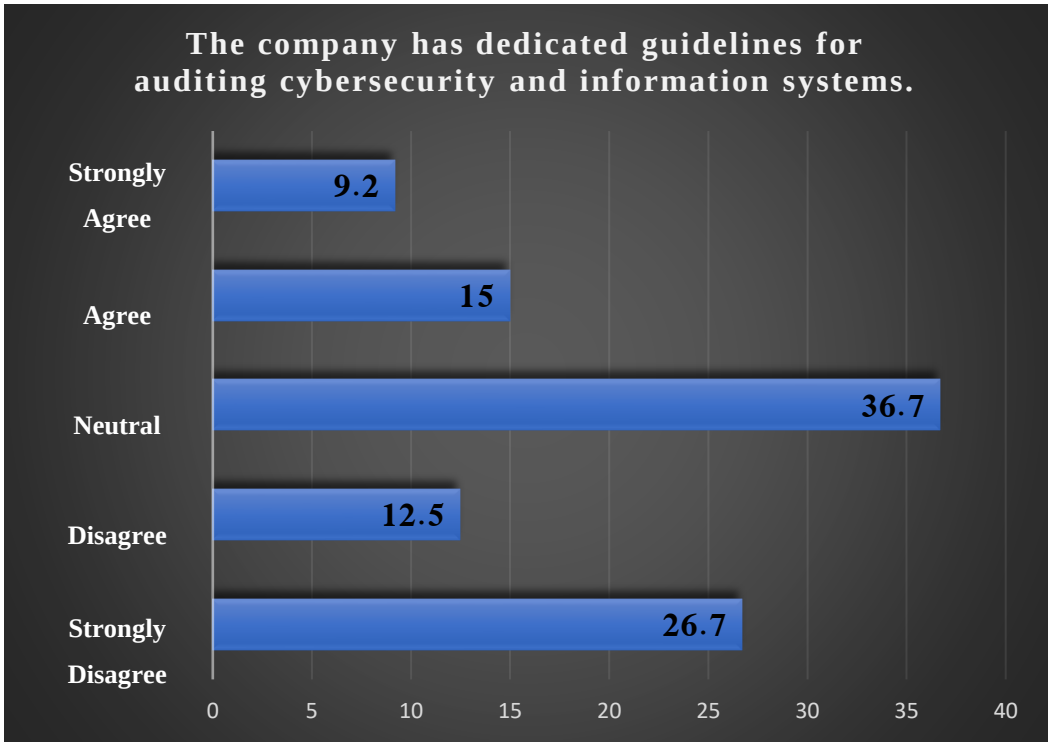


Figure 39: Survey Responses to Statement 21

Survey Statement 22: The company has a defined mechanism for auditing cybersecurity and information systems.

A statistical analysis of KPC and its subsidiaries regarding the existence of a mechanism for auditing cybersecurity and information systems revealed closely aligned responses. Specifically, 25% of respondents were neutral, while 24% agreed that such a mechanism exists in the oil sector. Conversely, 23% strongly disagreed, 19% disagreed, and only 9% strongly agreed. These data are illustrated in Table 16 and Figure 40 below.

Q22

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	27	22.5	22.5	22.5
	Disagree	23	19.2	19.2	41.7
	Neutral	30	25.0	25.0	66.7
	Agree	29	24.2	24.2	90.8
	Strongly Agree	11	9.2	9.2	100.0
	Total	120	100.0	100.0	

Table 16 – SPSS Analysis of Statement 22

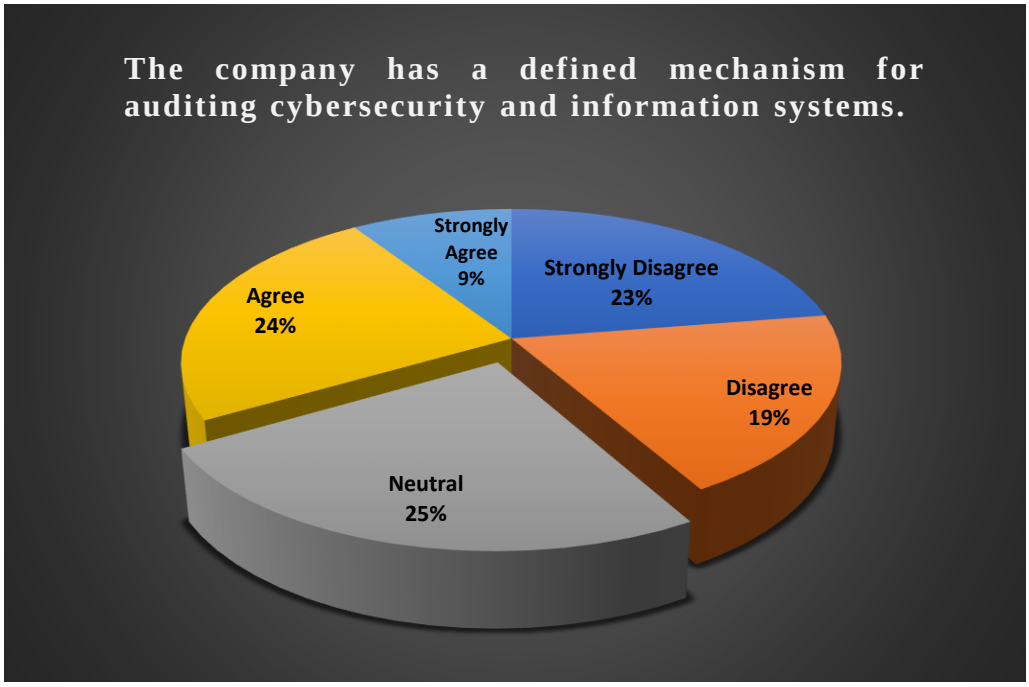


Figure 40: Survey Responses to Statement 22

Survey Statement 23: The company applies cybersecurity-related guidelines and regulations with the aim of protecting its data and digital assets.

The statistical analysis indicated that 30% of respondents agreed that KPC and its subsidiaries effectively apply cybersecurity guidelines. Furthermore, 25.8% of respondents remained neutral, while 22.5% strongly disagreed. In comparison, 14.2% disagreed, and only 7.5% strongly agreed. These results are illustrated in Figure 41 below.

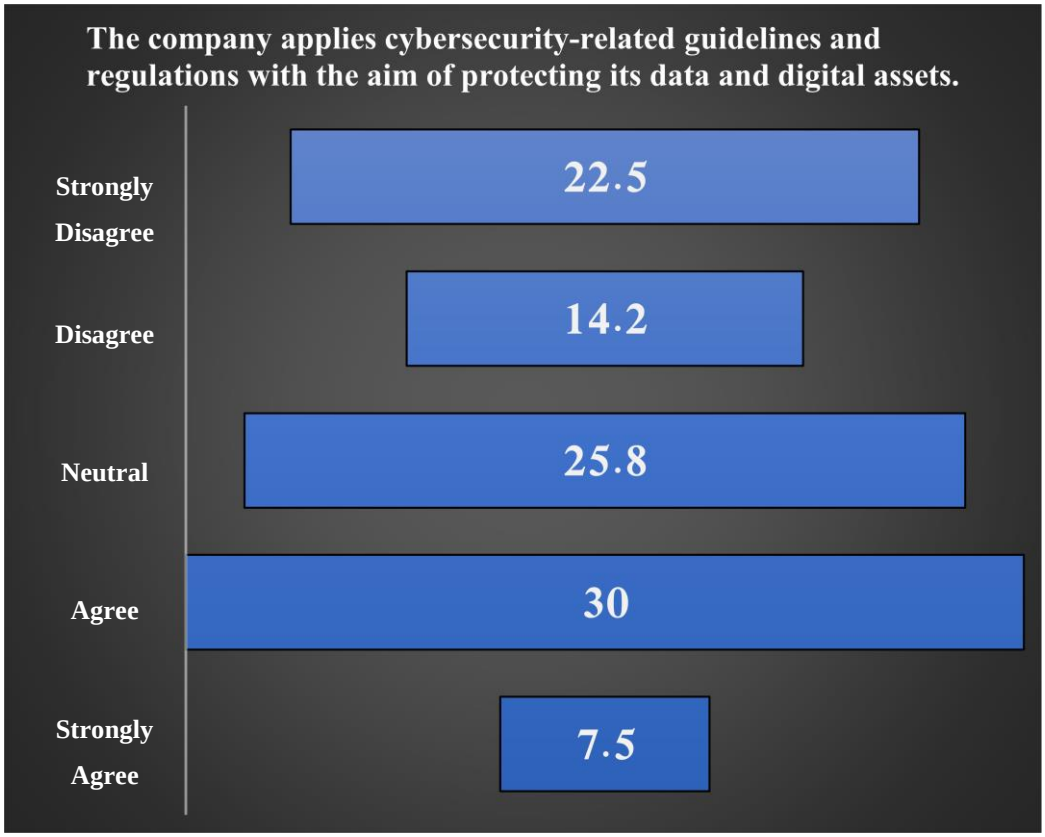


Figure 41: Survey Responses to Statement 23

Survey Statement 24: The company regularly develops cybersecurity-related requirements, guidelines, and regulations to accommodate the ongoing changes in this domain.

In an evaluation of the regular development of cybersecurity requirements, guidelines, and regulations within the companies of the oil and gas sector, the survey results revealed a range of perspectives. Specifically, the majority of respondents (28%) agreed with this statement, while 23% remained neutral. On the other hand, 21% strongly disagreed, 16% disagreed, and only 12% strongly agreed. These data are illustrated in Figure 42 below.

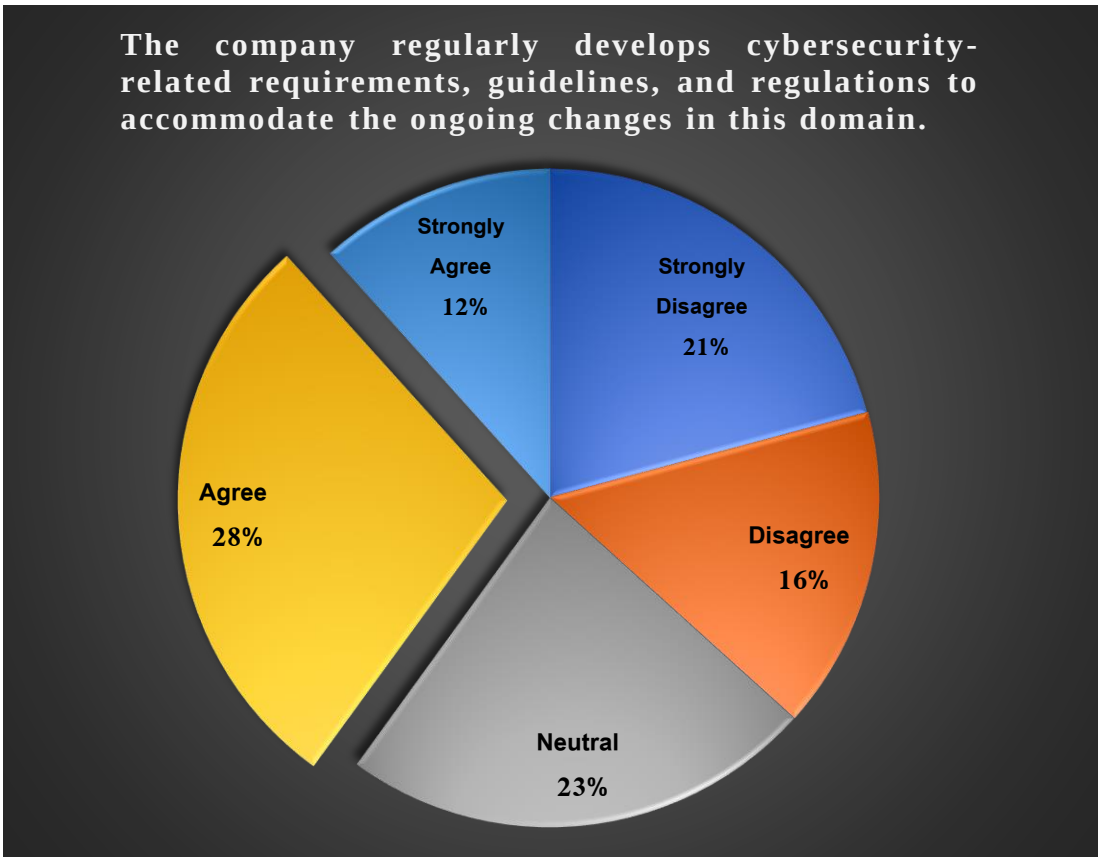


Figure 42: Survey Responses to Statement 24

V. Theme 4: Kuwait's oil and gas sector keeps pace with the latest advancements in the domain of cybersecurity and the audits of cybersecurity and information systems.

Survey Statement 25: KPC and its subsidiaries keep pace with the latest international advancements in cybersecurity.

The survey respondents had relatively close opinions on the statement that KPC and its subsidiaries keep pace with the latest cybersecurity-related advancements. The largest segment of respondents (26.7%) remained neutral, while 25.8% agreed with this statement. On the other hand, 20.8% disagreed, and 20% strongly disagreed. The smallest group of respondents, constituting 6.7%, strongly agreed with the statement, as shown in Figure 43 below.

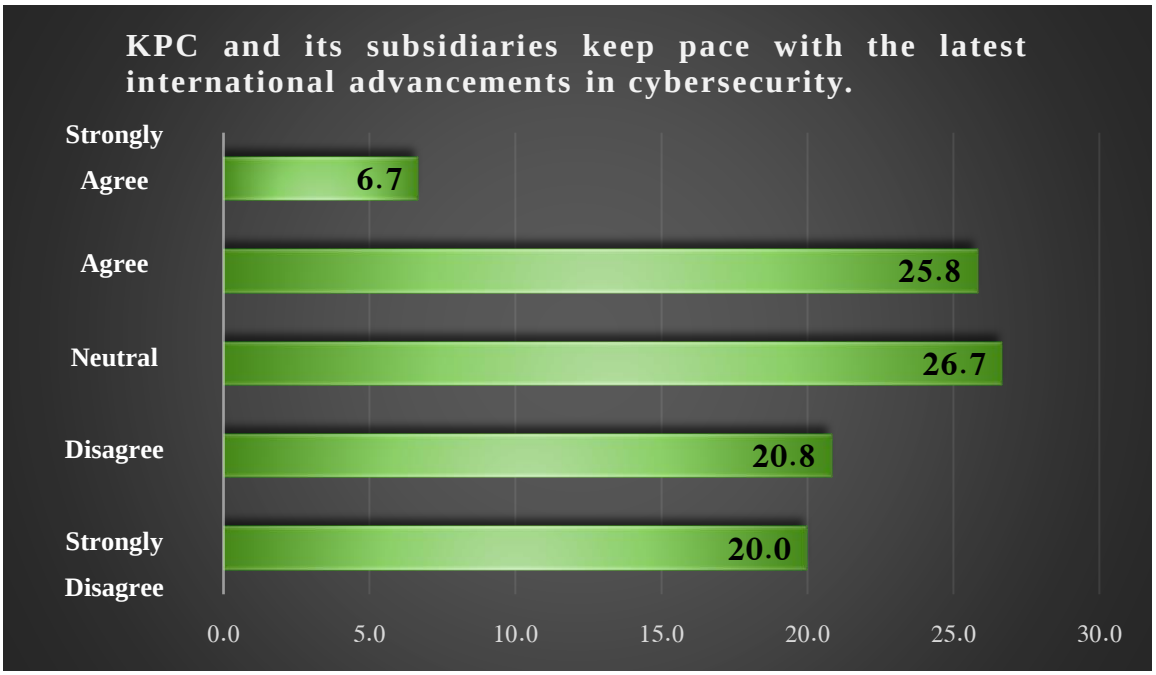


Figure 43: Survey Responses to Statement 25

Survey Statement 26: The company regularly develops its systems and infrastructure to cope with the latest advancements in this domain and prevent potential cyberattacks.

Regarding KPC and its subsidiaries regularly developing their systems and infrastructure to cope with the latest advancements in cybersecurity and prevent potential cyberattacks, the statistical results revealed that 25.8% of respondents agreed that their respective company is improving its cybersecurity operations. On the contrary, 22.5% of respondents remained neutral on this matter, 18.3% disagreed, and another 18.3% strongly disagreed. The smallest group, comprising 15%, strongly agreed. These data are illustrated in Table 17 and Figure 44 below.

Q26

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	22	18.3	18.3	18.3
	Disagree	22	18.3	18.3	36.7
	Neutral	27	22.5	22.5	59.2
	Agree	31	25.8	25.8	85.0
	Strongly Agree	18	15.0	15.0	100.0
	Total	120	100.0	100.0	

Table 17 – SPSS Analysis of Statement 26

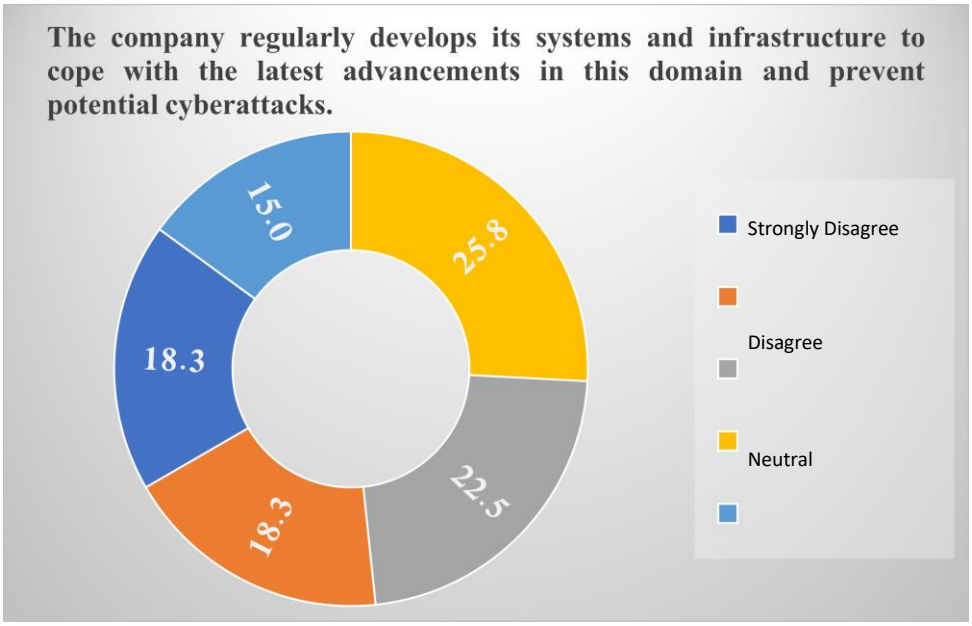


Figure 44: Survey Responses to Statement 26

Survey Statement 27: The current cybersecurity audit reports are of high quality.

Regarding the quality of current cybersecurity audit reports, findings indicated that 30.8% of respondents disagreed with the notion that these reports are of high quality, while 22.5% remained neutral. In contrast, only 20% of the sample agreed, 17.5% strongly disagreed, and a mere 9.2% strongly agreed that the current cybersecurity audit reports meet high-quality standards. These data are illustrated in Figure 45 below.

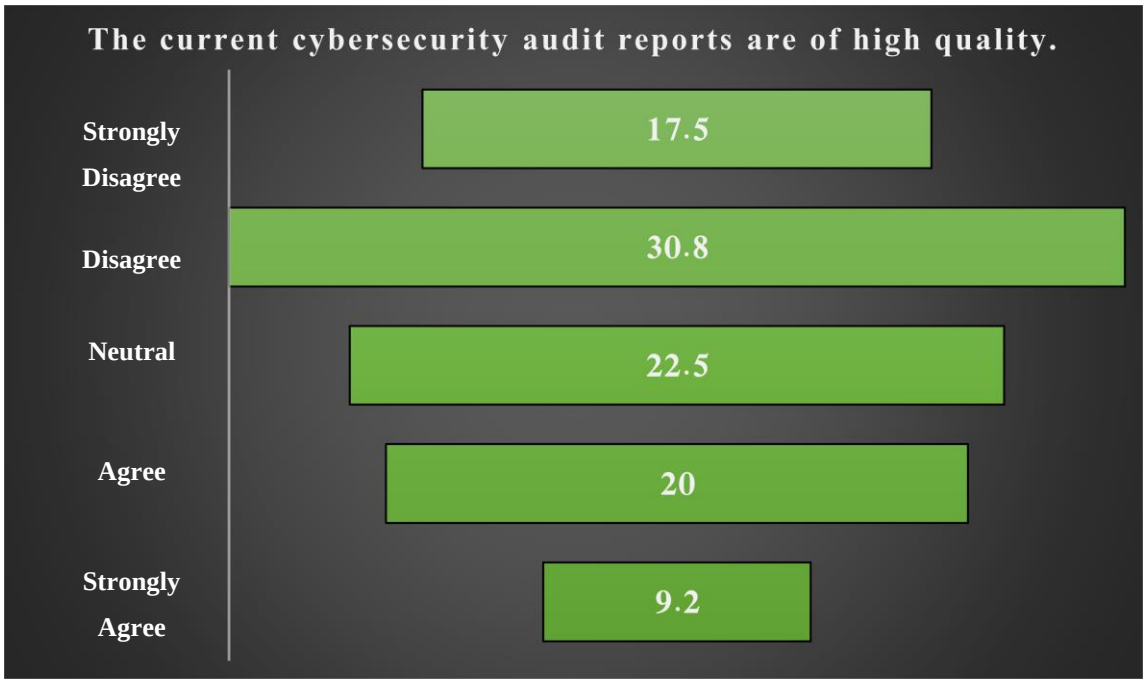


Figure 45: Survey Responses to Statement 27

Survey Statement 28: The cybersecurity audit reports currently issued by the company need further improvements and enhancements.

With respect to the quality of the company's cybersecurity audit reports, the survey results indicated that 27.5% of respondents strongly agreed that further improvements are necessary. Furthermore, 26.7% of respondents remained neutral on this matter, while 24.2% agreed. Few respondents (13.3%) disagreed that such reports need further improvements, and only 8.3% strongly disagreed. These data are illustrated in Figure 46 below.

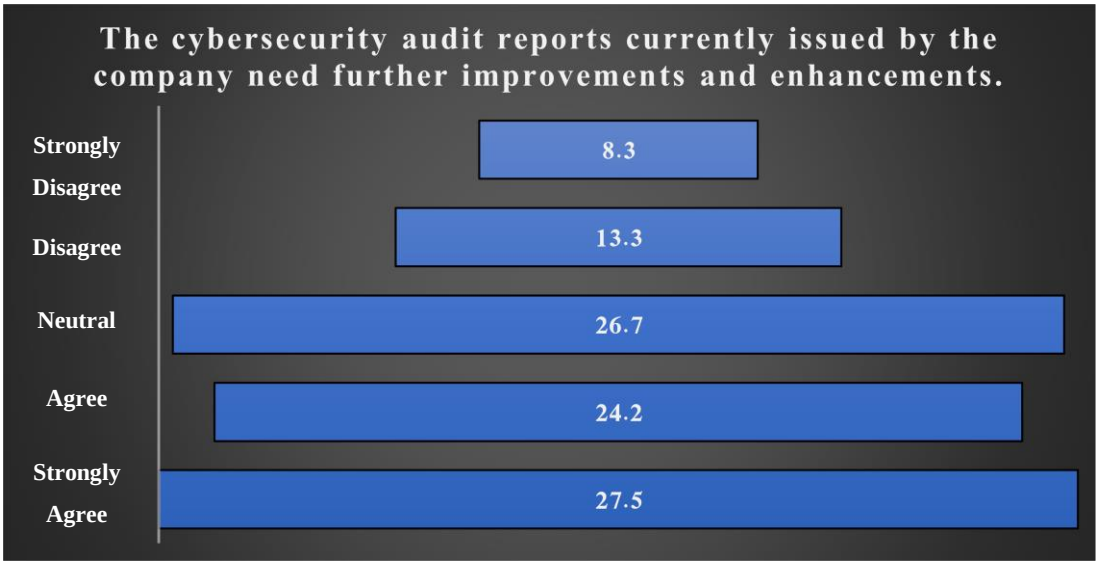


Figure 46: Survey Responses to Statement 28

Survey Statement 29: KPC and its subsidiaries have assigned dedicated teams for monitoring and following up on the latest updates in cybersecurity.

In terms of having dedicated teams within KPC and its subsidiaries for auditing cybersecurity and information systems, the survey results indicated that 26.7% of respondents remained neutral. In comparison, 25.8% of respondents strongly disagreed, and 23.3% disagreed with the notion that such teams are available in their respective companies. On the other hand, only 17.5% agreed with this statement and 6.7% strongly agreed. These data are illustrated in Table 18 and Figure 47.

Q29

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	31	25.8	25.8	25.8
	Disagree	28	23.3	23.3	49.2
	Neutral	32	26.7	26.7	75.8
	Agree	21	17.5	17.5	93.3
	Strongly Agree	8	6.7	6.7	100.0
	Total	120	100.0	100.0	

Table 18 – SPSS Analysis of Statement 29

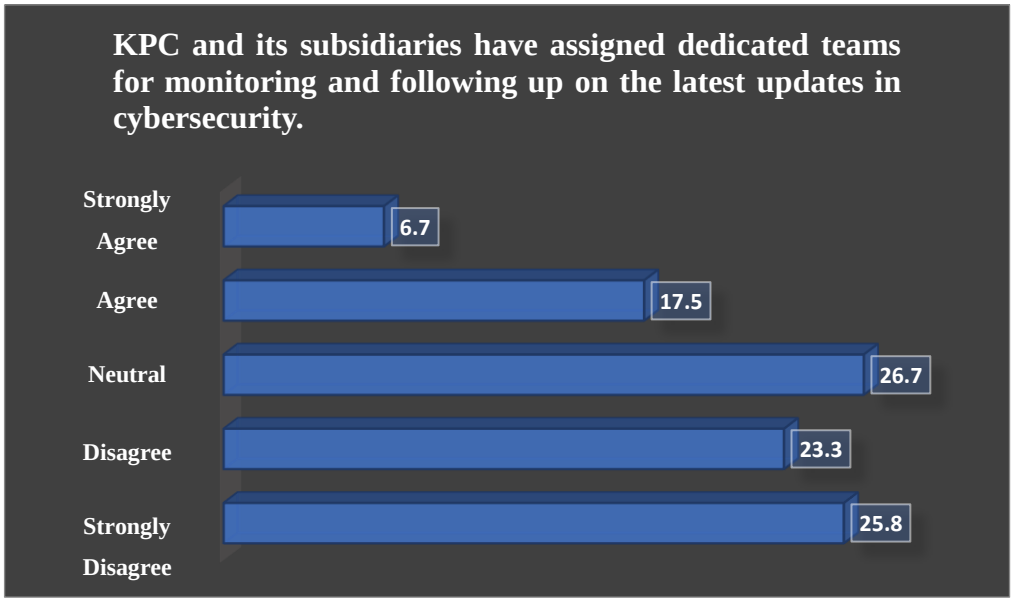


Figure 47: Survey Responses to Statement 29

VI. Theme 5: Employees of Kuwait's oil and gas sector are sufficiently trained and qualified in cybersecurity.

Survey Statement 30: The company conducts cybersecurity and information system awareness campaigns.

In terms of conducting campaigns aimed at raising awareness of cybersecurity and information systems, 27.5% of participants agreed that KPC and its subsidiaries are active in this area. Conversely, 24.2% strongly disagreed with this statement, 20.8% remained neutral, 16.7% disagreed, and 10.8% strongly agreed. These data are illustrated in Figure 48 below.

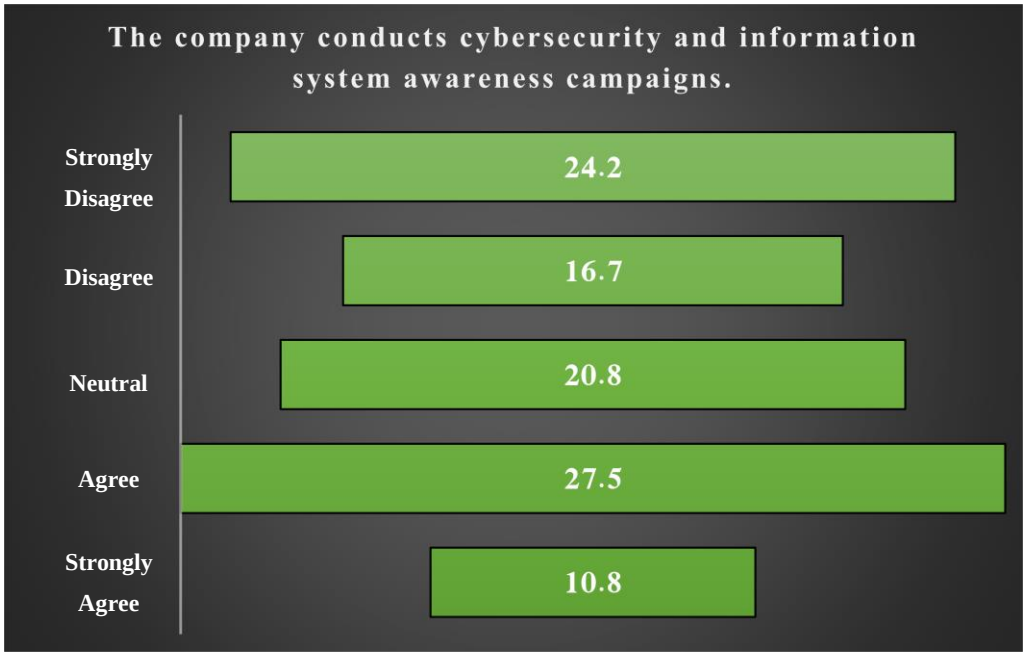


Figure 48: Survey Responses to Statement 30

Survey Statement 31: The company provides specialized training programs in cybersecurity.

According to the survey results, 26% of respondents agreed with the statement that their respective company provides specialized cybersecurity training programs. 24% were neutral on this matter, 22% strongly disagreed, 18% disagreed, and 10% strongly agreed. These results are illustrated in Figure 49 below.

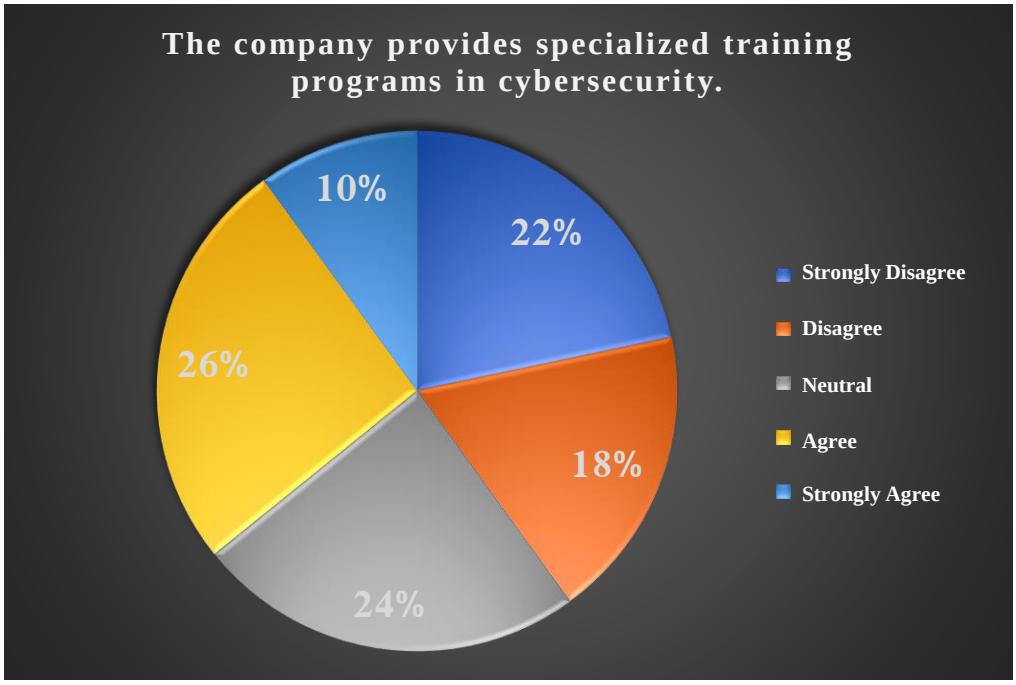


Figure 49: Survey Responses to Statement 31

Statement 32: I received sufficient training to understand the fundamentals of cybersecurity.

A notable 30.8% of respondents strongly disagreed that they had received sufficient training to understand cybersecurity fundamentals. Moreover, 25.8% of respondents remained neutral, while 20.8% disagreed. In contrast, only 13.3% agreed that their training was sufficient, while 9.2% strongly agreed. These results are illustrated in Table 19 and Figure 50 below.

Q32

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	37	30.8	30.8	30.8
	Disagree	25	20.8	20.8	51.7
	Neutral	31	25.8	25.8	77.5
	Agree	16	13.3	13.3	90.8
	Strongly Agree	11	9.2	9.2	100.0
	Total	120	100.0	100.0	

Table 19 – SPSS Analysis of Statement 32

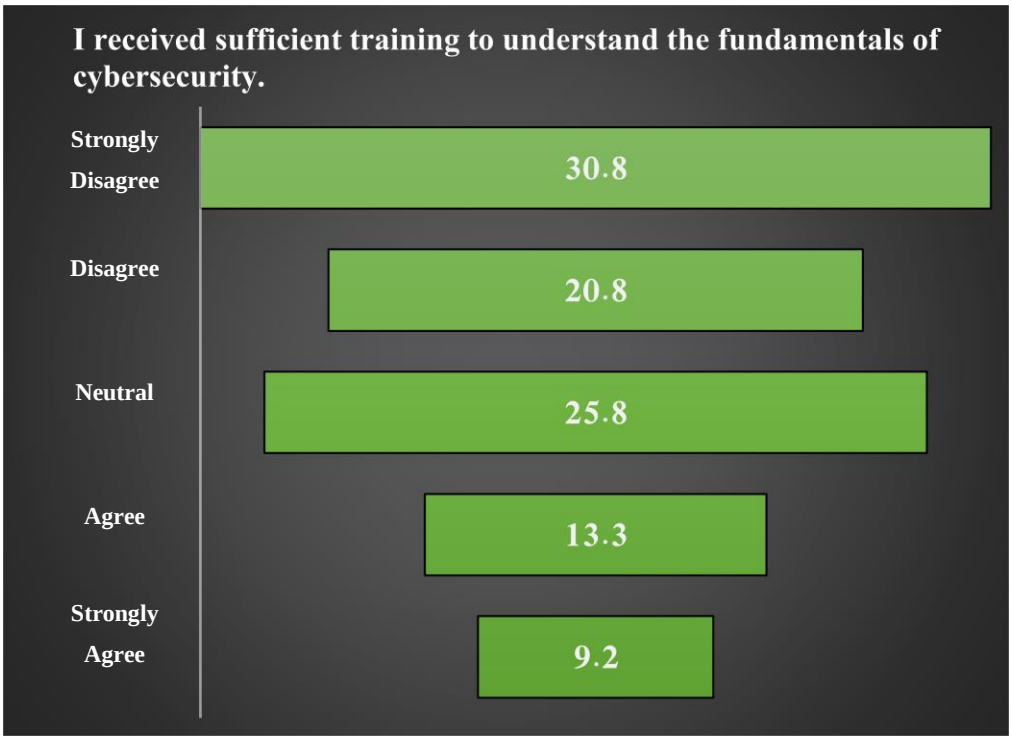


Figure 50: Survey Responses to Statement 32

Survey Statement 33: I received sufficient training to understand cybersecurity and information systems' guidelines, standards, and frameworks and how they can be applied in practice.

In terms of employees receiving adequate training in cybersecurity and information systems to understand relevant guidelines, standards, and frameworks, the proportion of neutral was equal to that of respondents disagreeing and was 27% in both segments. Moreover, 25% of respondents strongly disagreed that they received sufficient training, while 17% agreed. Only 4% of respondents strongly agreed, representing the lowest percentage. These data are illustrated in Figure 51 below.

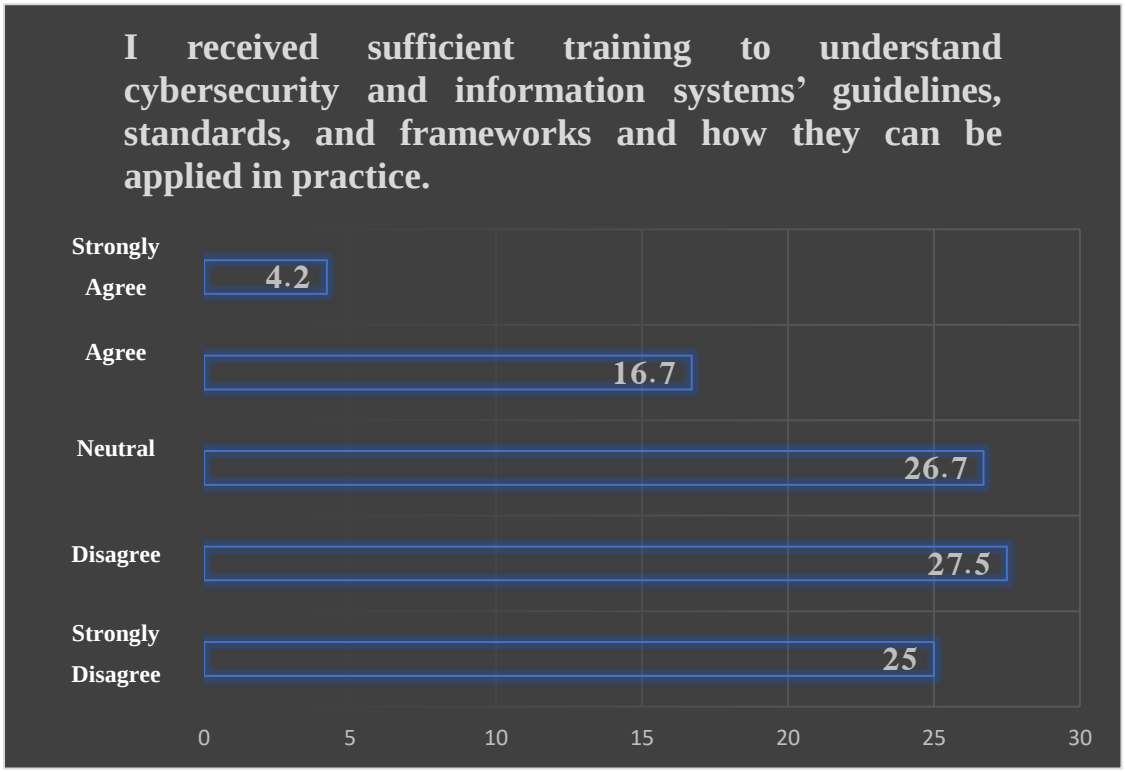


Figure 51: Survey Responses to Statement 33

Survey Statement 34: The company's employees are sufficiently qualified in the area of cybersecurity and information systems and possess the needed knowledge to prevent and rapidly respond to cyberattacks.

The statistical analysis revealed that 28.3% of respondents strongly disagreed that employees are sufficiently qualified in cybersecurity and information systems. Moreover, 23.3% were neutral, and 20.8% disagreed. Only 20% agreed, and 7.5% strongly agreed, representing the lowest proportions. These data are illustrated in Table 20 and Figure 52 below.

Q34

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	34	28.3	28.3	28.3
	Disagree	25	20.8	20.8	49.2
	Neutral	28	23.3	23.3	72.5
	Agree	24	20.0	20.0	92.5
	Strongly Agree	9	7.5	7.5	100.0
	Total	120	100.0	100.0	

Table 20 – SPSS Analysis of Statement 34

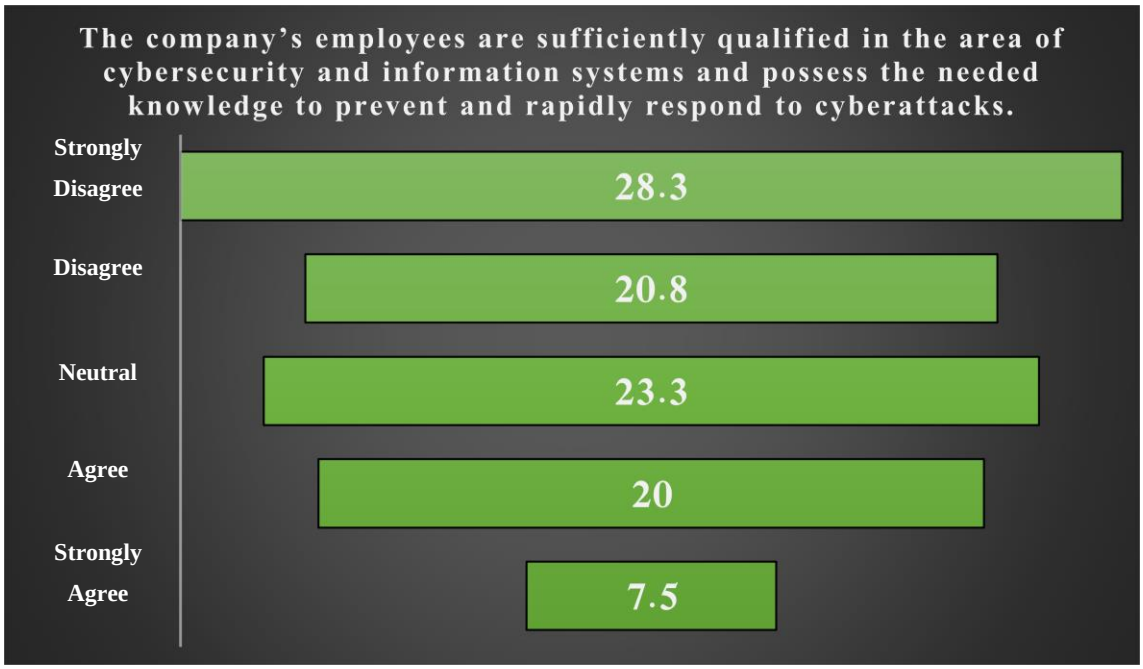


Figure 52: Survey Responses to Statement 34

Survey Statement 35: The company prioritizes investing in human capacities in the field of cybersecurity as a goal to be sought.

With respect to KPC and its subsidiaries investing in human capacity building on cybersecurity as a primary goal, a notable 27% of respondents disagreed with this statement. Moreover, 25% remained neutral, and 21% strongly disagreed. The segments of those who agreed and strongly agreed had the lowest percentages, with 18.3% and 9.2%, respectively. These data are illustrated in Table 21 and Figure 53 below.

Q35

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	25	20.8	20.8	20.8
	Disagree	32	26.7	26.7	47.5
	Neutral	30	25.0	25.0	72.5
	Agree	22	18.3	18.3	90.8
	Strongly Agree	11	9.2	9.2	100.0
	Total	120	100.0	100.0	

Table 21 – SPSS Analysis of Statement 35

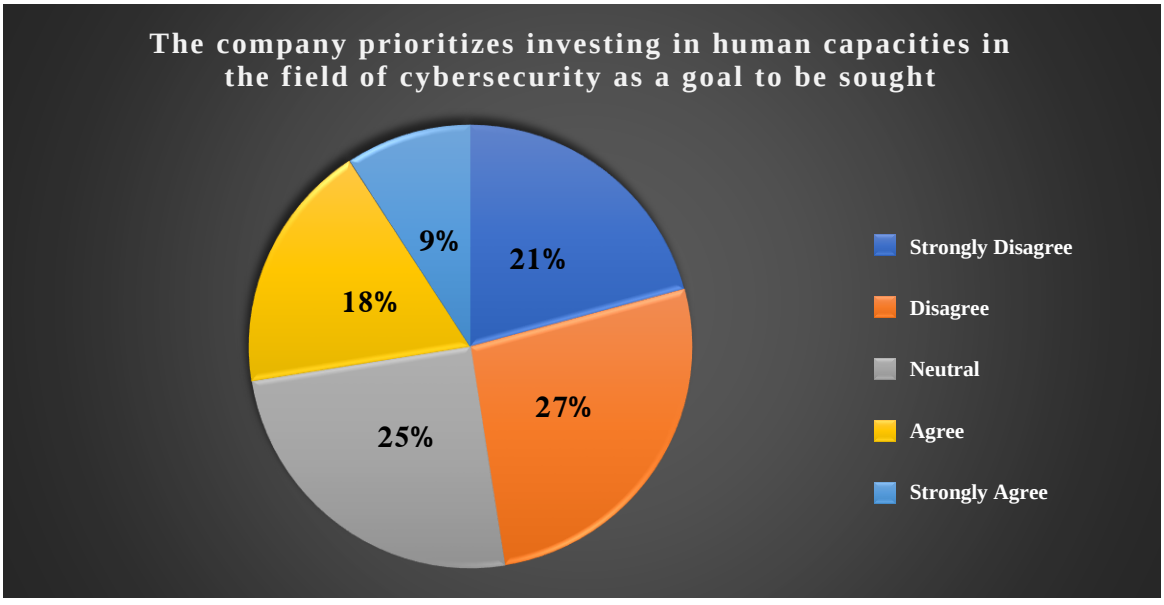
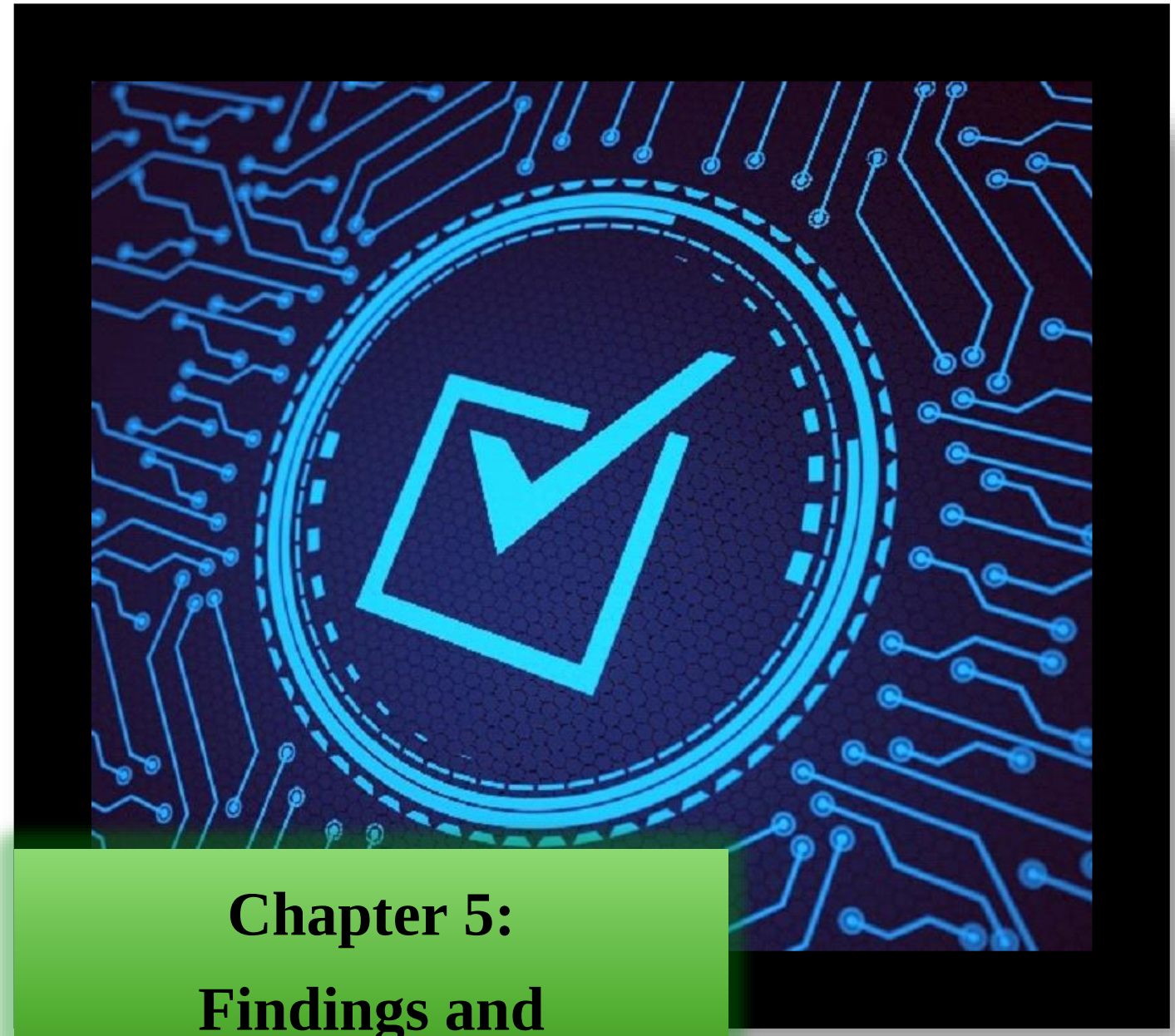


Figure 53: Survey Responses to Statement 35



Chapter 5:
Findings and Recommendations

Chapter 5

Findings and Recommendations

In this chapter, the researcher will present the findings of the study following the analysis outlined in Chapter 4. The findings will be presented in detail, highlighting the key relationships and trends identified during the research. This chapter will also provide practical and reasonable recommendations based on the study findings, contributing to actionable and applicable conclusions that benefit both the community and the research field.

1. Findings:

The researcher has conducted a field study using a web-based survey distributed via the SurveyMonkey platform. The questionnaires were disseminated through a shared link to auditors of SAB's Independent Bodies Audit Sector, specifically targeting the auditors of the Oil Bodies Production and Manufacturing Audit Department as well as the Independent Bodies of Financial and Investment Affairs Audit Department. The questionnaires were also distributed to professionals working at the Kuwait Petroleum Corporation (KPC) and its subsidiaries as per the specific categories outlined in this study. The collected data were subsequently analyzed using the SPSS statistical software, leading to the following key findings:

I. Findings related to the Primary Theme of the survey – Cybersecurity KPIs contribute to enhancing the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector

- The field study found that the employees of Kuwait's oil and gas sector lack sufficient knowledge of cybersecurity KPIs. This was indicated by 48.4% of the study sample, representing nearly half of the survey respondents. The survey results demonstrate that

awareness of the concept of cybersecurity KPIs and their types is limited to 8.3%, which is an exceptionally low percentage. Furthermore, a substantial proportion of respondents (43.3%) indicated that the Kuwait Petroleum Corporation (KPC) and its subsidiaries do not measure cybersecurity KPIs. This highlights the critical need to implement the measurement of cybersecurity KPIs in Kuwait's government oil and gas sector.

- The field study also found that Kuwait's government oil and gas sector lacks a defined classification system for cybersecurity activities, as reported by 49% of the respondents- a notably high percentage. This finding indicates that measuring cybersecurity KPIs and assessing cybersecurity risks may be challenging without a clear classification of cybersecurity activities.
- With regard to the contribution of cybersecurity KPIs measurement to decision-making, the field study revealed that 26.7% of the respondents remained neutral on this matter. On the other hand, 35.8% of the respondents agreed that the measurement of cybersecurity KPIs contributes to decision-making, which is a relatively satisfactory percentage, reflecting the positive impact of cybersecurity KPIs measurement on decision-making processes in the oil and gas sector. The field study also revealed that the cybersecurity-related information and data available in the oil and gas sector are found to be insufficient for the measurement of cybersecurity KPIs. A significant proportion of respondents (45%) reported that the sector lacks the necessary data and information to support the implementation of cybersecurity KPIs measurement. This finding highlights the critical need for providing relevant, high-quality data to support the sector in the measurement of cybersecurity KPIs.
- The field study revealed that the measurement of cybersecurity KPIs enhances the quality of audit outcomes. This was reported by a significant percentage of respondents (46%), reflecting

the importance of measuring KPIs and their positive impact on the quality of audit outcomes in Kuwait's oil and gas sector. Although 24.2% of the respondents remained neutral, 41.7% of the sample agreed that there is an apparent relationship between cybersecurity KPIs and the quality of audits. These findings, therefore, reflect the strong correlation between audit quality and the measurement of cybersecurity KPIs.

II. Findings related to Theme 1 of the survey – Kuwait's oil and gas sector is marked for adopting a well-defined strategy for the measurement of cybersecurity KPIs

- The field study revealed that 51.6% of the sample lacked sufficient knowledge about Kuwait's National Cybersecurity Strategy. This is a remarkably high percentage, exceeding half of the research sample, and indicates insufficient awareness of the said strategy. This finding reflects the critical need to enhance awareness of the National Cybersecurity Strategy within Kuwait's oil and gas sector in order to effectively achieve its strategic objectives at the national level and guide individual efforts toward protecting various sectors of the country, including the oil and gas sector. Furthermore, the findings showed that 37% of the sample agreed that the sector's cybersecurity strategy comprises cybersecurity KPIs, while an equal percentage (37%) disagreed. This parity indicates a lack of clarity regarding the content and comprehensiveness of the strategy within the sector.
- The results showed that 48.4% of the sample lacked sufficient awareness of the sector's cybersecurity strategy, reflecting a significant knowledge gap among employees in the sector. Additionally, a high proportion of the sample (50%) lacked knowledge of cybersecurity frameworks and their implementation mechanisms for achieving cybersecurity strategic objectives. These results underscore the urgent need to provide training and expand knowledge and awareness of cybersecurity frameworks and their implementation mechanisms. This step

is critical for enabling the sector to achieve its strategic goals and prevent potential cyberattacks.

- The field study revealed that 57% of the research sample- an exceptionally high percentage- lacked sufficient knowledge of the professional guidelines issued on cybersecurity and their implementation mechanisms. This indicates a significant gap in knowledge and awareness of cybersecurity-related matters, which adversely affects the sector's ability to respond promptly to cyberattacks and undermines the quality of cybersecurity audit outcomes. Indeed, such professional guidelines play a critical role in enhancing the quality of outcomes in Kuwait's oil and gas sector.
- The results also revealed that Kuwait's oil and gas sector is working on finding strategic solutions to mitigate cybersecurity risks, as indicated by 39% of the sample. This moderate percentage suggests that the sector is steadily improving in the domain of cybersecurity and actively working toward finding suitable solutions that serve the industry. Furthermore, 42.5% of the sample agreed that the cybersecurity strategy in the oil and gas sector contributes to achieving cybersecurity and information systems objectives. This demonstrates adequate awareness of the importance of having a cybersecurity strategy in place to meet the objectives of Kuwait's oil and gas sector.

III. Findings related to Theme 2 of the survey – The measurement of cybersecurity KPIs contributes to elevating the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector

- The field study results revealed that measuring cybersecurity KPIs enhances the quality of audit outcomes, as reported by 43.4% of the study sample. This substantial percentage demonstrates the positive impact of the measurement of cybersecurity KPIs on improving audit

outcomes. The results also showed that a significant proportion of the respondents (40%) believe that measuring these KPIs contributes to establishing a well-defined plan for auditing cybersecurity and information systems. This result reflects employees' awareness of the importance of measuring cybersecurity KPIs prior to developing the audit plan. Implementing such a measurement at an early stage would directly enhance cybersecurity awareness in Kuwait's oil and gas sector and strengthen its digital stability by facilitating the development of a precise audit plan for cybersecurity and information systems in the sector.

- The field study results further demonstrated that measuring cybersecurity KPIs improves the quality of cybersecurity audits of the sector, as indicated by a high percentage of the survey respondents (42.5%). This result particularly underscores the importance of measuring cybersecurity KPIs to enhance the quality of audits. Furthermore, a substantial proportion of the sample (47%), representing nearly half of the research sample, reported that cybersecurity KPIs are not considered when making critical decisions in the company. This indicates that the sector does not rely on cybersecurity KPIs in critical decision-making processes. Addressing this issue is essential, particularly in future decision-making related to the sector's mega projects. Taking such a step would contribute to safeguarding public properties and national security against cyber threats.
- The field study results revealed that Kuwait's oil and gas sector does not prepare specific reports on cybersecurity, as indicated by 48.3% of the respondents. This significant percentage indicates the need for the sector to adopt such reports. The study also showed that cybersecurity activities are not systematically classified to enhance the quality of information, as reported by 41.7% of the respondents. This finding highlights the need to classify cybersecurity activities

to improve the quality of information as well as the audit outcomes within Kuwait's oil and gas sector.

IV. Findings related to Theme 3 of the survey – There are defined requirements for integrating cybersecurity into audit practices within Kuwait's oil and gas sector

- The field study results indicated that the respondents' company does not have dedicated guidelines for auditing cybersecurity and information systems, as noted by 39.2% of the respondents. While this represents a moderate percentage, it highlights the need to prioritize the development and issuance of comprehensive cybersecurity audit guidelines. Such a guide would align the sector with international best practices followed by leading global oil and gas companies and Supreme Audit Institutions (SAIs). Furthermore, 42% of the respondents also indicated that there is no mechanism in place for auditing cybersecurity and information systems within the sector. Such a high percentage highlights the need for the sector to establish a cybersecurity audit mechanism, providing a well-defined framework for employees of the sector to perform their functions in this domain.
- Additionally, the results showed that a moderate percentage of respondents (37.5%) agreed that Kuwait's oil and gas sector applies cybersecurity-related guidelines and regulations with the aim of protecting data and digital assets. This demonstrates the sector's adequate awareness of the importance of implementing cybersecurity guidelines and regulations and their positive impact on operational efficiency and asset protection within the sector.
- The results of the field study showed that Kuwait's oil and gas sector regularly develops cybersecurity-related requirements, guidelines, and regulations. This was supported by 40% of the survey respondents, which is a satisfactory percentage, demonstrating the sector's commitment to continuous development and improvement in this domain.

V. Findings related to Theme 4 of the survey – Kuwait's oil and gas sector keeps pace with the latest advancements in the domain of cybersecurity and the audits of cybersecurity and information systems

- The field study results indicated that Kuwait's oil and gas sector is developing its systems and infrastructure in an effort to keep up with the latest advancements in this domain and avoid cyberattacks, as reported by 40.8% of the respondents. This satisfactory percentage demonstrates that the sector is committed to keeping pace with the latest developments in order to enhance the protection against cyber threats and safeguard the digital data of the sector. These efforts involve enhancing cybersecurity infrastructure, promoting innovation, and establishing a more secure and reliable work environment.
- The results also showed that the current cybersecurity audit reports issued by KPC and its subsidiaries are not of high quality. This finding was supported by 48.3% of the respondents, representing a significant proportion close to half the sample. Therefore, it is necessary for the sector to enhance the quality of its cybersecurity audit reports.
- The study results revealed that 32.5% of the respondents agreed that their companies apply cybersecurity-related guidelines and regulations to secure the sector's digital data and assets. This result highlights the companies' awareness of the need to ensure the application of guidelines to protect the sector from cyberattacks. Additionally, 51.7% of the respondents agreed that the current cybersecurity audit reports should be further improved to enhance their quality. Such a significant percentage evidently reflects a need to enhance the quality of cybersecurity audit outcomes within Kuwait's oil and gas sector.
- The study results further pointed out the absence of dedicated cybersecurity teams within the State's oil companies, as confirmed by 49% of the respondents. Such a significant percentage

reflects the critical need to dedicate specialized teams within those companies to handle cybersecurity-related tasks.

VI. Findings related to Theme 5 of the survey – Employees of Kuwait's oil and gas sector are sufficiently trained and qualified in cybersecurity

- The study results indicated a convergence of opinions regarding cybersecurity and information system awareness campaigns. 38% of the respondents agreed that their companies are conducting awareness campaigns in this field, whereas 40.9% disagreed. Despite being close, these percentages highlight the need for more targeted awareness campaigns for employees in the oil and gas sector, focusing on cybersecurity and information systems. It is also necessary to invest in human capital within the oil and gas sector.
- The results of the field study also indicated the critical need for further specialized training programs in cybersecurity and information systems since 40% of the sample reported insufficient training provided in this domain. Such a significant percentage highlights that providing additional training in this domain is essential to achieve several benefits, namely keeping pace with technological advancements, enhancing cybersecurity awareness in the oil and gas sector, and ensuring a rapid response to and protection against cybersecurity threats. The findings also revealed a significant shortfall in training on the fundamentals of cybersecurity. This was highlighted by 51.6% of the respondents, who indicated that they had not received sufficient training to understand the basic principles of cybersecurity. This notably high percentage, exceeding half of the respondents, indicates a significant knowledge gap and the lack of a clear training plan on cybersecurity fundamentals in Kuwait's oil and gas sector.
- The results further revealed that over half of the respondents, specifically 52.5%, had not received sufficient training to understand cybersecurity and information systems' guidelines,

standards, and frameworks and how they can be applied in practice. Meanwhile, a smaller percentage, 20.90%, indicated that they had received adequate training in this area. This emphasizes the importance of establishing a comprehensive training plan within Kuwait's oil and gas sector to educate the staff on cybersecurity-related guidelines, standards, and frameworks. Such a plan would enhance employees' knowledge, empower them to address cybersecurity challenges, and ensure effective investment in human capital within the sector.

- Finally, the results indicated that 49.1% of the respondents are inadequately qualified in the area of cybersecurity and information systems. They lack sufficient knowledge to effectively counter and respond rapidly to cybersecurity threats. This underscores the importance of investing in human capital and providing sufficient training for employees of Kuwait's oil and gas sector to enhance their capacity to respond rapidly to such challenges. Additionally, the study revealed that Kuwait's oil and gas sector, particularly Kuwait Petroleum Corporation, does not currently prioritize investing in human capacities in the field of cybersecurity and information systems as a goal to be sought. This finding was supported by a significant percentage of respondents, 48%, reflecting the need for the sector to develop targeted solutions and approaches to investing in human capital in this critical domain. Therefore, Kuwait's oil and gas sector must prioritize these efforts as a core objective, recognizing that human capital is the backbone of the sector and serves as the first line of defense against advanced cybersecurity threats.

2. Recommendations:

1. Implement cybersecurity and information systems audits in order to protect information assets, national data, and information networks in KPC, its subsidiaries, and SAB.
2. Develop a cybersecurity strategy and update it once achieved. Most importantly, put the strategy into effect in order to prevent cyberattacks on sensitive national information in Kuwait's oil and gas sector since such information is entirely confidential and the cybersecurity strategy would contribute to its protection.
3. Provide support for the national staff in KPC, its subsidiaries, and SAB in cybersecurity and information systems audits. Such support is essential given that cybersecurity and information systems auditors form the first line of defense in detecting vulnerabilities and developing recommendations to address these vulnerabilities in the future, thereby protecting national information assets.
4. Identify and document all relevant to sensitive information assets such as software, hardware, and databases to enhance the results of cybersecurity and information systems audits in KPC and its subsidiaries.
5. Update and inventory information assets to enhance and facilitate the audit of cybersecurity and information systems in Kuwait's oil and gas sector in general and KPC and its subsidiaries in particular.
6. Appropriate a budget for the protection of information assets in the oil and gas sector in Kuwait.
7. Ensure firm management of personal profiles and access authorization, as they can be the main gateway to most attacks. Two-factor authentication should also be added, which is one

of the most effective ways to prevent cyberattacks in the oil and gas sector in general and in KPC and its subsidiaries in particular.

8. Develop a list of authorized software, tools, and applications for use in Kuwait's oil and gas sector. The list must be reviewed and updated periodically to prevent future attacks and vulnerabilities.

9. Measure cybersecurity KPIs in KPC and its subsidiaries, as that would reflect positively on the cybersecurity audit plan. The measurement of KPIs would also contribute to the periodical and consistent review and improvement of procedures, as KPIs can be an effective tool for such purposes. Furthermore, KPIs can protect KPC and its subsidiaries against cyberattacks and enhance the results of SAB's audits in the sector.

10. Enhance preventive measures related to cybersecurity and information systems.

11. Promote the field of cybersecurity and information systems in the sector by setting clear and strategic plans for the following:

    a. The maintenance of information assets for KPC and its subsidiaries.
    b. The disposal of information assets in KPC and its subsidiaries upon examining appropriate disposal technologies.
    c. Employee training at KPC and its subsidiaries on the need for cybersecurity and the importance of separating personal information from work-related information.
    d. The establishment of tight restrictions on the use of hardware and the exchange of data and information in KPC and its subsidiaries.

12. Assess and analyze cybersecurity risks to enable internal auditors and SAB auditors to reach effective audit results when auditing cybersecurity and information system-related matters. Furthermore, internal and SAB auditors should advise KPC and its subsidiaries on the need to address and monitor cybersecurity risks effectively.

13. Manage and detect security vulnerabilities in KPC and its subsidiaries by auditing cybersecurity and information systems and using risk-based examination and analysis to develop a methodology and a proactive plan to prevent the recurrence of such vulnerabilities.

14. Maintain an event and control log as part of the network security management in the oil and gas sector. By using the log, the auditor would be able to track the most critical events and security vulnerabilities to prevent cyberattacks, which is achieved by improving the status of information assets in KPC and its subsidiaries. The log would also enhance the results of SAB's audits in the sector as it keeps a record of the remarks that would contribute to future work development and improvement.

15. Keep abreast of the latest developments in cybersecurity and information systems audits. This is in order to adopt the best practices in this field and utilize modern tools that contribute to enhancing the process of auditing cybersecurity and information systems. As a result, such an approach would facilitate the protection of national security and the State's primary source of income in the oil and gas sector.

16. Promote training programs related to the audit of cybersecurity and information systems in the oil and gas sector through the following:

a. Maintaining exchange of expertise and participation in local and external training courses for employees of the oil sector to expand their knowledge in the field of cybersecurity and information systems;

b. Training and educating employees of KPC and its subsidiaries on the importance of cybersecurity through intensive training and educational activities;

c. Developing training programs in the oil and gas sector that address the principles of cybersecurity and information systems and the relevant audits to raise employees' awareness of the importance of this field. Additionally, employees need to understand how this awareness can be employed at all stages of the audit process in order to ensure an effective execution of all procedures;

d. Developing training programs in the oil and gas sector dedicated to cybersecurity KPIs and their measurement. This step is necessary since employees' knowledge of such an effective tool would enhance the control of cybersecurity and information systems within the sector, preventing potential cyberattacks proactively;

e. Providing sufficient training for sector employees on cybersecurity frameworks and the mechanism for their implementation, which would enhance the employees' performance in audit tasks. Having frameworks to follow would contribute to improving the quality of audit outcomes within the sector and achieving strategic objectives; and

f. Organizing awareness-raising seminars and workshops for auditors that include practical and realistic case studies to introduce the concepts of Cybersecurity and Cybersecurity KPIs and their connection to the quality of cybersecurity and information systems audits.

17. Emphasize the importance of cybersecurity KPIs in assessing cybersecurity risks, in addition to developing a plan to apply KPI measurement and cybersecurity and information systems audits and operate them in KPC and its subsidiaries to enhance the audit work environment.
18. Develop a set of guidelines for auditing cybersecurity and information systems by SAB to help auditors follow a precise methodology to protect public funds from cyberattacks. KPC should also develop guidelines on auditing cybersecurity and information systems for Kuwait's oil and gas sector.
19. Publish the recommendations issued by organizations and agencies specialized in the field of cybersecurity and information systems audit and the measurement of cybersecurity KPIs while urging auditors to use these recommendations in examination and auditing tasks.
20. Consider developing a specific methodology and guidelines for auditing cybersecurity and information systems in KPC and its subsidiaries that align with the latest developments in the control and audit of cybersecurity and information systems.
21. Periodically and effectively measure cybersecurity KPIs and categorize cybersecurity activities in KPC and its subsidiaries to improve the quality of audit outcomes.
22. Work on enhancing information related to cybersecurity and information systems in KPC and its subsidiaries to facilitate the measurement of cybersecurity KPIs. It is also necessary to urge employees to rely on the results of KPI measurement in decision-making in the sector to improve decision accuracy.
23. Raise awareness among employees of Kuwait’s oil and gas sector in relation to the National Cybersecurity Strategy and the cybersecurity strategy of the oil and gas sector. This would

contribute to enhancing and promoting awareness of cybersecurity in general, thus facilitating the achievement of the strategic vision and objectives.

24. Establish a connection in the field of cybersecurity between KPC and its subsidiaries in order to enhance the sector's cybersecurity infrastructure, advise solutions, and establish a highly secure and complex network.

25. Prepare a comprehensive cybersecurity plan that would contribute to improving the information in the oil and gas sector and the employees' knowledge of this domain. Such a plan would include the development of cybersecurity-related training programs, guidelines, methodologies, and frameworks, as well as their implementation mechanism. This would eventually lead to raising awareness among employees on cybersecurity and the need to put all plans and strategies in KPC and its subsidiaries into effect.

26. Rely on the results of the measurement of cybersecurity KPIs during the development of the annual audit plan for KPC and its subsidiaries in order to improve the quality of audit outcomes and their results.

27. For KPC and its subsidiaries, set a prevention plan and appropriate solutions to protect information assets and databases in the event of cyberattacks in order to reduce their risks. A prevention plan would contribute to enhancing cyber-resilience and taking proper measures in the event of a cyberattack.

28. Urge KPC subsidiaries to periodically update the requirements, guidelines, and regulations relevant to cybersecurity to conform to global developments in this domain. This would contribute to improving the infrastructure, maintaining information assets, and protecting Kuwait's sole source of income.

29. Invest in the adoption of advanced methods and solutions in the field of cybersecurity in order to modernize the systems and infrastructure and keep pace with the latest developments in the field. This would also improve responsiveness in the event of a cyberattack on the sector.

30. Improve the quality of the audit reports issued by KPC and its subsidiaries in the field of auditing cybersecurity and information systems by engaging field specialists in preparing the reports and investing in measuring cybersecurity KPIs to enhance audit results.

31. Emphasize the importance of investing in human talents in the field of cybersecurity and information systems in the oil and gas sector. Owing to the fact that the sector is the state's sole source of income, and the protection of its funds is an objective that KPC and its subsidiaries seek to reach, then the investment in the human element must be an indispensable part of the road to achieving that objective.

References

References

(Listed according to APA 7th Edition referencing style)

7 Cybersecurity Frameworks that Help Reduce Cyber Risk (List & Resources). (2024, January 15). *Bitsight*. Retrieved January 15, 2024, from https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk

Al-Burzangi, S. Y. A. & Al-Saqqa, Z. H. Y. (2023). Requirements of Internal Audit for Enhancing Cybersecurity in Economic Entities in Light of the Institute of Internal Auditors (IIA). *Tikrit Journal of Administrative and Economic Sciences, 19 (63,2), 94-112*. Retrieved from https://doi.org/10.25130/tjaes.19.63.2.5

Al-Khaldi, A. (2023, October 22). 46 Government Entities Vulnerable to Cybersecurity Risks. *Al-Qabas Newspaper*. Retrieved from https://www.alqabas.com/article/5922102-46/

Al-Matari, O. M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2020). Integrated Framework for Cybersecurity Auditing. *Information Security Journal: A Global Perspective*, 30(4), 189-204. Retrieved from https://doi.org/10.1080/19393555.2020.1834649

Al-Samhan, M. (2020). Cybersecurity Requirements for Management Information Systems at King Saud University. *Journal of the College of Education, 111*

Ameerhum, D.J. (2022). The Impact of Internal Audit Quality on Mitigating Cybersecurity Risks and its Role in Rationalizing Investors' Decisions (Field Study). *Journal of Financial and Commercial Research* (3,23).

Benetis, V. (2018, March 9). *Tips on Cybersecurity Auditing*. Retrieved from https://www.linkedin.com/pulse/tips-cyber-security-auditing-vilius-benetis?utm_source=share&utm_medium=guest_mobile_web&utm_campaign=copy

Britannica. (2021). *Resources and Power*. Retrieved November 26, 2021, from https://www.britannica.com/place/Kuwait/Resources-and-power

Challenges of Internal Audit. (2020). National Audit Office of Bahrain. Retrieved January 1, 2024, from https://www.nao.gov.bh/uploads/1wcht4u0_5yo.pdf

CITRA. (2016). *Kuwait National Cybersecurity Strategy (2017-2020).* (1st ed., Vol. 1).

Communications, Space and Technology Commission. (2020). *Cybersecurity Regulatory Framework (CRF) for Service Providers in the Information and Communications*

Technology Sector (1st ed., Vol. 1). Communications, Space and Technology Commission (CST).

Core Cybersecurity Controls. (2018). National Cybersecurity Authority – NCA.

Cybersecurity Status Report. (2nd ed.). (2023). National Cybersecurity Center.

Cyber Resilience in the Oil and Gas Industry: Playbook for Boards and Corporate Officers. (2023, November 2). World Economic Forum. Retrieved from https://www.weforum.org/publications/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers/

Cyber Risk to the Oil and Gas Industry Threat-Analysis-Report. (2022, August 29). New Jersey Cybersecurity & Communications Integration Cell. Retrieved January 10, 2024, from https://www.cyber.nj.gov/threat-analysis-reports/cyber-risk-to-the-oil-and-gas-industry

Cybersecurity Frameworks 101- The Complete Guide.(2022, June 3).*Prey Blog*. Retrieved from https://preyproject.com/blog/cybersecurity-frameworks-101

Cybersecurity Guidelines for Contractors. (2019). KNPC. Retrieved from https://ktendering.com.kw/esop/kuw-kpc-host/public/attach/cybersecurity_guidelines_for_contractors.pdf

Cybersecurity in the EU and its Member States. (2020). [PDF]. Contact Committee of the Supreme Audit Institutions of the European Union. Retrieved from https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf

Cybersecurity Program Audit Guide. (2023). GAO. Retrieved from https://www.gao.gov/assets/d23104705.pdf

CyberTalents. (2024). Top 15 Cybersecurity Metrics and KPIs for Better Security. *CyberTalents Blog*. Retrieved from https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry. (2017). Natural Gas Council. Retrieved from https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf

FAA Digital and Technology Audit. (2018). Financial Audit Authority (FAA). Retrieved March 31, 2024, from https://www.faa.gov.ae/ar/what-we-do/digital-and-technology-audit

General Audit Guideline.(2020). State Audit Bureau of Kuwait.

Global Cybersecurity Index 2020. (2020). Retrieved from https://www.scpd.gov.kw/archive/%D8%AA%D9%82%D8%B1%D9%8A%D8%B1%20%D9%85%D8%A4%D8%B4%D8%B1%20%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%202020.pdf

High-risk Issues Report (3rd ed., Vol. 3).(2023). The State Audit Bureau of Kuwait.

ISACA. (2016). Auditing Cybersecurity. *ISACA Journal, Vol.1*. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/auditing-cybersecurity

ISACA. (2016). Auditing for FISMA and HIPAA: Lessons Learned Performing an In-house Cybersecurity Audit. *ISACA Journal, Vol.5*. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/auditing-for-fisma-and-hipaa-lessons-learned-performing-an-in-house-cybersecurity-audit

ISACA. (2018, April 18). Cybersecurity Risk. *ISACA Journal. Retrieved from* https://journal.isca.org.sg/2018/04/12/cybersecurity-risk/pugpig_index.html

ISACA. (2022).The Evolution of Information Systems Audit. *ISACA Journal, 1*. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-evolution-of-information-systems-audit

KNPC Increases Cybersecurity Protection with Matrox Extio 3. (2021). *Hydrocarbon Processing Magazine*. Retrieved from https://www.hydrocarbonprocessing.com/news/2021/10/knpc-increases-cybersecurity-protection-with-matrox-extio-3

KPMG. (2021, October 1). *Industrial Cyber Defense*. KPMG. Retrieved from https://assets.kpmg.com/content/dam/kpmg/sa/pdf/2021/industrial-cyber-defense-arabic-final.pdf

Mahrous, R., & Saleh, A. A. (2022). Using the Agile Approach in Developing Internal Audit Performance to Confront Cybersecurity Risks. *Journal of Financial and Commercial Research* (3,23).

Main page of the Financial Audit Authority Website. (2018). Retrieved March 2, 2024, from https://www.faa.gov.ae/ar/Pages/default.aspx

Mansour, A. (2021). Impacts of Cybersecurity on Internal Audit and the Economic Entity- A Survey of Auditors and Accountants from the Ministry of Higher Education and Academic Research. The Journal of Administration & Economics. Retrieved from https://doi.org/10.31272/JAE.44.2021.127.15

Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). *Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective*. ACM Transactions on Cyber-Physical Systems, 6(3), 1–27. Retrieved from https://doi.org/10.1145/3548691

Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure. (2022, November 17). U.S. GAO. Retrieved from https://www.gao.gov/products/gao-23-105789

O'Flaherty, K. (2023, December 18). *What are the most-targeted industries for cyber attacks?.* IT Pro. Retrieved from https://www.itpro.com/security/cyber-attacks/what-are-the-most-targeted-industries-for-cyber-attacks

Parliament Assigns SAB to Prepare a Report on Government IT and Cybersecurity Measures. (2022, August 14). *Al-Rai Media.* Retrieved January 7, 2024, from:https://www.alraimedia.com/article/1602244/%D9%85%D8%AD%D9%84%D9%8A%D8%A7%D8%AA/%D9%85%D8%AC%D9%84%D8%B3-%D8%A7%D9%84%D8%A3%D9%85%D8%A9/8-%D8%AA%D9%83%D9%84%D9%8A%D9%81%D8%A7%D8%AA-%D9%85%D9%86-%D9%85%D8%AC%D9%84%D8%B3-%D8%A7%D9%84%D8%A3%D9%85%D8%A9-%D9%84%D8%AF%D9%8A%D9%88%D8%A7%D9%86-%D8%A7%D9%84%D9%85%D8%AD%D8%A7%D8%B3%D8%A8%D8%A9-%D8%AE%D9%84%D8%A7%D9%84-%D8%A7%D9%84%D9%81%D8%B5%D9%84-%D8%A7%D9%84%D8%AA%D8%B4%D8%B1%D9%8A%D8%B9%D9%8A-%D8%A7%D9%84%D8%B3%D8%A7%D8%AF%D8%B3-%D8%B9%D8%B4%D8%B1

RSA Conference. (2020, February 26). *The Journey of Cybersecurity in Kuwait's Oil and Gas Industry* [Video]. YouTube. https://www.youtube.com/watch?v=OiZFx1RldHg

Results of the Examination and Audit of the Budget Implementation and Final Accounts of Independent Entities for FY 2022-2023. (3rd ed., Vol. 3). (2022). The State Audit Bureau.

Results of the Examination and Audit of the Budget Implementation and Final Accounts of Independent Entities for FY 2022-2023. Part III: KPC and its Subsidiaries. (2022nd-2023rd ed., Vol. 3). (2023). The State Audit Bureau.

Sabillón, R. (2022). *Audits in Cybersecurity*. In IGI Global eBooks (pp. 1–18). https://doi.org/10.4018/978-1-6684-3698-1.ch001

Sengupta, S. (2022, November 23). *Top Cybersecurity KPI Examples & Best Practices*. Crashtest Security. Retrieved from https://crashtest-security.com/cyber-security-metrics/

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of Cybersecurity Audit. *International Journal of Accounting Information Systems*, 44, 100548. Retrieved from https://doi.org/10.1016/j.accinf.2021.100548

State Audit Bureau: Five Government Entities Excel in Cybersecurity. (2023, October 24). *Al-Qabas Newspaper*. Retrieved from https://www.alqabas.com/article/5922206-%D8%A7%D9%84%D9%85%D8%AD%D8%A7%D8%B3%D8%A8%D8%A9-5-%D8%AC%D9%87%D8%A7%D8%AA-%D8%AD%D9%83%D9%88%D9%85%D9%8A%D8%A9-%D8%AA%D8%AA%D9%81%D9%88%D9%82-%D9%81%D9%8A-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A

Technologies, S. (2023, April 13). *Igniting Attacks: Cybersecurity in the Oil and Gas Industry*. Sangfor Technologies. Retrieved from https://www.sangfor.com/blog/cybersecurity/cybersecurity-in-the-oil-and-gas-industry

WGITA-IDI Handbook on IT Audit for SAIs 2022 (2nd ed.). (2022). IDI INTOSAI. Retrieved from https://www.idi.no/ar/elibrary/relevant-sais/lota/wgita-idi-handbook-on-it-audit-for-sais/1632-wgita-idi-handbook-on-it-audit-for-sais-2022-en#:~:text=%D9%81%D9%8A%20%D8%B9%D8%A7%D9%85%202014%20%D8%8C%20%D8%B9%D9%85%D9%84%20%D8%A7%D9%84%D9%81%D8%B1%D9%8A%D9%82%20%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D9%84%20%D8%A7%D9%84%D8%AA%D8%A7%D8%A8%D8%B9,%D8%A8%D8%B4%D9%83%D9%84%20%D9%85%D8%B4%D8%AA%D8%B1%D9%83%20%D9%84%D8%A5%D9%86%D8%AA%D8%A7%D8%AC%20%D8%A3%D9%88%D9%84%20%D8%AF%D9%84%D9%8A%D9%84%20%D8%B9%D9%86%20%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.

What is Cybersecurity?. (2022). National Cybersecurity Center of Bahrain. Retrieved from https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html

Appendix

Appendix

Web-based Survey Form

The Role of Cybersecurity KPIs in Enhancing the Quality of Cybersecurity and Information System Audit in Kuwait Oil and Gas Sector;

A research project submitted as part of the ARABOSAI 14th Scientific Research Competition in the Field of Financial Auditing.

You are kindly requested to complete the web-based survey accurately and objectively, as it is essential to the success of this study. Your participation will contribute to enhancing the role of cybersecurity KPIs in elevating the quality of cybersecurity and information system audits in Kuwait's oil and gas sector.

Please note that all responses will be handled with complete confidentiality and used solely for scientific research purposes.

Thank you for your kind cooperation!

Researcher/

Fatima Nabeel Jaafar

Please read the following statements and place a checkmark (✓) in the box next to the statement that aligns with your response.

- **Section (1)**

Job Title	
□	Internal Auditor
□	Accountant
□	Computer Engineer
□	Financial Manager
□	Cybersecurity Expert
□	Auditor at SAB's Oil Bodies Production and Manufacturing Audit Department or the Oil Bodies Marketing and Investment Audit Department

Academic Qualification	
□	Degree in Accounting
□	Degree in Business Administration
□	Degree in Cybersecurity
□	Degree in Computer Engineering
□	Degree in Information Systems

Years of Experience	
□	Less than 5 years
□	5-10 years
□	11-15 years
□	More than 15 years

- **Section (2)**

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
Primary Theme	**Cybersecurity KPIs contribute to enhancing the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.**					
1	I have sufficient knowledge of the types of cybersecurity KPIs and their measurement mechanisms.					
2	The company measures cybersecurity KPIs.					
3	The company has a defined classification for cybersecurity activities, which makes it easier to measure cybersecurity KPIs and assess cybersecurity risks.					
4	Measuring cybersecurity KPIs contributes to decision-making within the company.					
5	The cybersecurity-related information					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
	and data available at the company are sufficient for the measurement of cybersecurity KPIs.					
6	Measuring cybersecurity KPIs enhances the quality of audit outcomes.					
7	There is a correlation between cybersecurity KPIs and the quality of audits.					
Theme 1	**Kuwait's oil and gas sector is marked for adopting a well-defined strategy for the measurement of cybersecurity KPIs.**					
8	I have sufficient knowledge of Kuwait's National Cybersecurity Strategy.					
9	Kuwait's oil and gas sector has a comprehensive and well-defined strategy for cybersecurity that comprises cybersecurity KPIs.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
10	I have sufficient knowledge of the cybersecurity strategy of Kuwait's oil and gas sector.					
11	I have sufficient knowledge of cybersecurity frameworks and their implementation mechanisms for achieving the objectives of the sector's cybersecurity strategy.					
12	I have sufficient knowledge of the professional guidelines issued on cybersecurity and information systems audits and a good understanding of how they can be adopted to achieve the objectives of the sector's cybersecurity strategy.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
13	The company is working on finding suitable strategic solutions to mitigate cybersecurity.					
14	The cybersecurity strategy contributes to achieving the sector's cybersecurity and information systems objectives.					
Theme 2	**The measurement of cybersecurity KPIs contributes to elevating the quality of cybersecurity and information systems audits in Kuwait's oil and gas sector.**					
15	Measuring cybersecurity KPIs enhances the quality of audit outcomes within the company.					
16	Measuring cybersecurity KPIs contributes to establishing a well-defined plan for auditing the company's cybersecurity and information systems.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
17	The definition and measurement of cybersecurity KPIs contribute to improving the quality of cybersecurity and information systems auditing within the company.					
18	The measurement of cybersecurity KPIs is considered when making critical decisions in the company.					
19	The company prepares reports on cybersecurity KPIs.					
20	The company classifies cybersecurity activities and measures the relevant KPIs in order to improve the quality of information as well as the audit outcomes.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
Theme 3	**There are defined requirements for integrating cybersecurity into audit practices within Kuwait's oil and gas sector.**					
21	The company has dedicated guidelines for auditing cybersecurity and information systems.					
22	The company has a defined mechanism for auditing cybersecurity and information systems.					
23	The company applies cybersecurity-related guidelines and regulations with the aim of protecting its data and digital assets.					
24	The company regularly develops cybersecurity-related requirements, guidelines, and regulations to accommodate the ongoing changes in this domain.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
Theme 4	**Kuwait's oil and gas sector keeps pace with the latest advancements in the domain of cybersecurity and the audits of cybersecurity and information systems.**					
25	KPC and its subsidiaries keep pace with the latest international advancements in cybersecurity.					
26	The company regularly develops its systems and infrastructure to cope with the latest advancements in this domain and prevent potential cyberattacks.					
27	The current cybersecurity audit reports are of high quality.					
28	The cybersecurity audit reports currently issued by the company need further improvements and enhancements.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
29	KPC and its subsidiaries have assigned dedicated teams for monitoring and following up on the latest updates in cybersecurity.					
Theme 5	**Employees of Kuwait's oil and gas sector are sufficiently trained and qualified in cybersecurity.**					
30	The company conducts cybersecurity and information system awareness campaigns.					
31	The company provides specialized training programs in cybersecurity.					
32	I received sufficient training to understand the fundamentals of cybersecurity.					

Sr.	Survey Statements	Scale of Agreement				
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
		1	2	3	4	5
33	I received sufficient training to understand cybersecurity and information systems' guidelines, standards, and frameworks and how they can be applied in practice.					
34	The company's employees are sufficiently qualified in the area of cybersecurity and information systems and possess the needed knowledge to prevent and rapidly respond to cyberattacks.					
35	The company prioritizes investing in human capacities in the field of cybersecurity as a goal to be sought.					