Scientific Research Publishing

Journal of Information Security, 2023, 14, 152-180
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threats in the Egyptian Downstream Oil and Gas Industry

Mohamed Shohoud[1,2]

[1]UNICAF University, Cape Town, South Africa
[2]University of East London, London, UK
Email: mshohoud@gmail.com

How to cite this paper: Shohoud, M. (2023) Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threats in the Egyptian Downstream Oil and Gas Industry. *Journal of Information Security*, **14**, 152-180.
https://doi.org/10.4236/jis.2023.142010

Received: March 20, 2023
Accepted: April 25, 2023
Published: April 28, 2023

Abstract

As Egyptian oil and gas downstream information technology has grown digitally over the past decade, security breaches against these digitally connected systems have also increased. These cyber security threats could have devastating effects on the operations and reputation of these companies. Preventing such cyberattacks is crucial. Especially, with the significance of the Egyptian oil and gas downstream sector to the local economy and the fact that many of these connected systems are sometimes managed remotely. This paper examines the value of the ISO 27001 standard in mitigating the effect of cyber threat and seeks to inspire decision-makers to the importance of the proactive measures to strengthen their organization's cybersecurity posture and protect information critical assets. The study stresses the importance of improving the local educational system to bridge the gap between supply and demand for cybersecurity specialists by implementing a structured approach that emphasizes behavior modification to get a high return on investment in cybersecurity awareness.

Keywords

Downstream, Cyberattack, Cyber Security, Mitigate, Decision-Makers, Proactive Measure, Critical Assets, Behavior Modification

1. Introduction

Background to the Study

The digital age we live in has brought about incredible advancements in technology and connectivity. However, it has also increased the risk of cybersecurity breaches and attacks. With the increasing reliance on technology, it's more im-

portant than ever to prioritize cybersecurity measures and take active steps to protect our personal and professional information. Failure to do so can cause significant financial loss and reputational damage sometimes. In this context, proactive cybersecurity measures are more important than ever before. Rather than simply reacting to threats as they arise, businesses must take a proactive approach to identify and mitigate risks before they can be exploited. This requires a comprehensive understanding of the threats that exist in the digital landscape, as well as the tools and strategies necessary to counter them. Therefore, it is vital for businesses to stay current with the latest cybersecurity trends and to invest in the tools and personnel to safeguard their digital assets through working with cybersecurity experts to implement robust access controls, monitor network activity regularly, and invest in innovative security technology, especially in critical environments, such as O&G industry.

According to [1], there are various points through which oil and gas companies are susceptible to cyberattacks, including many digital data within the corporate, upstream, midstream, and downstream sectors. This study focuses on the downstream industry, which refers to the portion of the oil and gas industry responsible for refining, distributing, and selling petroleum products to consumers. Maintaining critical business operations in the event of an emergency is essential to preventing disasters. Considering, it has focused most security efforts on the security of physical assets, rather than the security of information.

This study inspects the mechanisms behind ISO 27001 as a proactive cybersecurity framework, provides an independent and objective evaluation of an organization's ISMS includes policies, procedures, controls, and processes related to information security, as well as an assessment of the effectiveness of these measures in protecting the confidentiality, integrity, and availability of information assets. Also involves an examination of the organization's risk management practices, incident management procedures, and compliance with legal and regulatory requirements related to information security.

The study presented in this paper examines relevant surveys regarding cyber threats and cyber protection through LinkedIn, as a popular social platform to evaluate professional feedback on various discussions to support this study.

Egypt downstream gateway has transformed the oil and gas industry into Egypt Vision 2030's sustainable development strategy, which involves the creation of a business structure that mitigates the cyber threats risk by linking all holding companies and subsidiaries through a secure unity information source to support quick decision-making and grantee continuity of business. Taken into consideration, the need for talent individuals and culture change management to support the results effectively by promoting different opportunities to support 2030 development strategy vision.

2. Research Aims

- Identify common cyber threats and vulnerabilities faced by the O&G local

industry.

- Investigate the current information security practices in the O&G downstream sector.
- Evaluate the effectiveness of ISO 27001 in mitigating cyber risks in the sector.
- Identify the reasons for weak implementation of ISO 27001 in the Egyptian market.
- Propose recommendations for improving information security practices in the sector.

2.1. Research Objective

- Review the literature on cyber threats and ISO 27001 in the O&G downstream sector.
- Identify the key information assets and systems that need protection in the sector.
- Evaluate the effectiveness of ISO 27001 in managing information security risks.
- Explore the challenges and barriers to implementing ISO 27001 in Egypt.
- Develop recommendations for improving information security practices in the sector.
- Evaluating the competitive advantage of ISO 27001 compliance.

2.2. Research Hypothesis

Hypothesis: we can mitigate Cyber security threats in the downstream oil and gas industry by implementing ISO 27001. As a result, companies that successfully implemented ISO 27001 are better able to secure their cybersecurity, according to the participants who took part in successfully implemented ISO 27001 projects reported a better cybersecurity outcome against cyberthreats than those who do not implement this standard.

3. Scope of the Study

- Geography: we focused the study on the Egyptian downstream O&G industry, which refers to the sector responsible for the refining, processing, and distribution of O&G products in Egypt.
- Demographics: The study does not specify a particular demographic group but focuses on the downstream oil and gas industry. However, it may be assumed that the study will involve information technology professionals, cybersecurity experts, and stakeholders involved in the industry, including executives and managers.
- Sectors: The study is specific to the downstream oil and gas industry, which is a subset of the larger energy sector. In addition, the study will not address other segments of the O&G industry, such as upstream or midstream sectors.
- Functional areas: The study's functional scope is primarily focused on information technology (IT) and cybersecurity-related functions, including risk

assessment, threat management, security policies and procedures, and incident response.

Limitations of the Study

- Limited sample size: This study focuses on Egypt's downstream oil and gas industry, limiting generalizability.
- Access to relevant local data is limited, such as cyber security incident reports or internal security policies and procedures of Egyptian companies.
- Biases: The study may be influenced by the biases of the local participants involved in the surveys.
- The study may be limited by time constraints, which may limit the scope of the research or the depth of the analysis.
- Changes in technology and threats: The study may become outdated quickly because of the fast-paced nature of technology and the growing nature of cyber security threats.

4. Literature Review

Throughout the past few decades, technological advancements have made it possible for most of the oil and gas industries to embrace digitalization and automation to maintain safety and sustainability in all phases of their daily operations. Many advanced technologies, involving the internet of things, artificial intelligence, and machine learning, have been introduced to improve efficiency, productivity, and decision-making in the oil and gas industry to facilitate the automation of processes. They commonly referred these technologies to as the fourth industrial revolution, or Industry 4.0. This revolutionary technology has reduced human intervention in hazardous environments, operation downtime, and human error.

According to [2], there are three general categories of oil and gas infrastructure: upstream, midstream, and downstream. The upstream infrastructures support exploration and drilling operations, whereas midstream infrastructures provide a link between production and downstream dissemination by transporting oil and gas, while downstream infrastructures provide the distribution of crude oil and natural gas to consumers. Digital technologies continue to affect the oil and gas industry, for example, an industrial control system (ICS) is composed of a collection of control digital components (electrical, hydraulic, pneumatic) that work together to meet certain industrial objectives (e.g., manufacturing, transportation). In the past, these systems operated in isolation, independent of the IT infrastructure. However, because of Industry 4.0, today multiple industrial IT/OT technologies have been integrated in this sector, offering engineers the ability to remotely maintain Supervisory Control and Data Acquisition (SCADA) systems and monitor operations in real-time through digital actuators and smart sensors.

According to [3] reports, there has been an increase in the security issues as-

sociated with energy sector control systems because of new vulnerabilities in ICS equipment and the decrease in the qualified information security experts. These vulnerabilities make it even more critical to integrate these systems with other IT environments to maintain ICS security. Under [4], proactive approaches can range from technological solutions to the implementation of security standards to prevent successful attacks. That means, it is imperative that organizations improve their security processes by proactively identifying and fixing vulnerabilities that attackers can exploit.

4.1. Cybersecurity Challenges

Digital Transformation projects tempt companies to roll out new technologies without prioritizing security, which make the cybersecurity the critical consideration for organizations undertaking digital projects. According to [5], the oil and gas industry is a critical infrastructure, making it a valuable target for adversaries who are seeking to exploit any security weaknesses, including espionage, infrastructure sabotage, and data theft. Therefore, cybersecurity must be the primary concern that should be evaluated regularly. As more and more devices and systems become connected to the internet, they become potential targets for these types of cyber threats, range from simple malware attacks to highly sophisticated cyber espionage campaigns. In line with [6], in order to better understand the top ten cybersecurity threats facing the oil and gas industry, the following threats can be considered:

1) Insufficient training and awareness of cybersecurity among employees.

2) Work from a remote non-secure connection during operations and maintenance.

3) The use of IT products in production that have well-known vulnerabilities.

4) Network segmentation is insufficiently separated.

5) The use of BYOD includes storage units with no security restriction policy.

6) Outdated control systems plague the sector.

7) Cybersecurity is not a priority among vendors, suppliers, or contractors.

4.2. Downstream Industry

The Egyptian downstream oil and gas industry is an integral part of the economy, and its security is of the utmost importance. According to [7], the Egyptian vice president for cybersecurity affairs for the National Telecom Regulatory Authority (NTRA), Egypt needs to address the cyberthreats within its technological system as soon as possible, Cyber-attacks have become more frequent and sophisticated, and the country must take steps to protect information infrastructure from these threats over the current 150 technology services through the Egyptian digital platform. External threats, such as hackers or malicious software, as well as internal threats, such as employees or contractors, may make up these threats. Because of these threats, the industry can suffer financial losses, reputational damage, or even physical harm. Therefore, the industry must take steps to

protect itself from these threats. However, along with the shortage of cybersecurity professionals, it is crucial that implementing International Standard for Information Security Management will be essential. In addition, implementing cyber awareness training to the education method will be important to decrease the gap in the cybersecurity local market demand. According to [5], the downstream industry of the oil and gas industry comprises refineries and processing plants, as well as marketing and distribution companies. In these operations, it typically transformed the raw materials into finished products. These products including gasoline, diesel, heating oil, and other petroleum-based products. After these finished products have been manufactured, pipelines, tankers, and other means of transportation to customers then distributed them. The technology has had a significant impact on the business functionality inside the downstream modern world by creating an unprecedented level of interconnectedness infrastructure networks that control finished and partially refined products. According to the latest announced economic indicators reported by [8], the petroleum sector has achieved about 27% of Egypt's gross domestic product. Subsequently, strictly adhering to safety and security protocols is vital in protecting this industry and its personnel. The oil and gas industry uses a variety of systems and equipment as part of information technology (IT) to store, process, and transport data related to accounting, human resources, and communication within an organization, including computers, servers, networking hardware, and software programs. Operational technology (OT) includes sensors, control systems, and automation equipment control critical infrastructure and processes to improve the production operations by optimizing performance in real-time such as SCADA and ICS systems. To support its business operations, the oil and gas industry relies on a complex network of interconnected IT and OT systems to improve industrial activities by simplifying the process within the safety in a more cost efficiency way.

In line with [9], during designing of OT/IT systems and networks, it is important to consider cyber security risk assessments, taking into consideration the information security three pillars: confidentiality, integrity, and availability (CIA). From a business continuity management perspective, the IT network prioritizes these pillars in CIA order, however the OT network prioritizes it in AIC order. Which means the availability countermeasures is the most critical pillar in the OT systems. For that, most of the Oil and Gas organizations have significant systems redundancy in separate physical locations to protect against cyber threats. According to [10], organizations in the Oil and gas sector typically implement integrated security systems to provide visibility and control of their IT infrastructures. To implement countermeasures against these threats, these systems must be capable of detecting security threats. In accord with [11], it is essential to design, manage, and test a comprehensive cyber incident response plan to effectively mitigate the effects of any data security incident in a timely manner. Referring to [12], stated in his survey that the biggest challenge faced by OT

is the legacy technology that needs to be technically integrated with themost recent IT systems. However, the IT team lacks awareness of the operations department, making it difficult to implement this integration taken the security measurement into account.

According to [13], the number of cyberattacks continues to rise because of the use of digital technology to increase automation across vast geographical oil and gas downstream networks. This automation increased its reliance on integrating information and communication technologies (ICT) spaces with information technology (IT) and operational technology (OT). Which encourage the cyberthreats to take advantage of IT and OT vulnerabilities to occupy this space, including the challenge of zero-day attacks, and to mitigate these cyberthreat risks and improve the security posture of organizations, it is crucial to develop cybersecurity contingency and recovery plans. These plans should be implemented and tested regularly.

4.3. Cybersecurity Awareness

The increasingly adopting of IT and OT solutions in the Oil and Gas business in particular downstream sector may present an additional chance for cybercriminals to gain access to vital information by taking advantage of the lack of cybersecurity awareness within many of these organizations. According to [6], they have discovered the computer worm known as Stuxnet in July 2010, and it specifically targets computers that run critical infrastructure such as oil and gas pipelines. This worm hijacks critical infrastructure systems worldwide by utilizing compromised USB thumb drives to infect Microsoft Windows platforms so that it can gain control of the infected systems. In consonance with [14] survey, the lack of end-user cybersecurity awareness is a significant threat to cybersecurity. Top management must support the implementation of an effective cybersecurity culture in order to limit cyberattacks. It is important to invest in the resources allocated to cyber security measures. Clearly, the lack of qualified cybersecurity specialists may pose a significant challenge toward the extensive assets and sensitive data that hackers can exploit to make a personal gain or as part of a larger political or ideological agenda. Referring to [14] the cyberthreats against oil and gas companies have been increasing with high rates over the last 30 years, exploiting the unavailability of unified IS framework that secure this sector.

4.4. Cyber Security Proactive Approach

Referring to [9], the study showed the importance of the proactive cyber security approach that maintain the integrity and safety of oil and gas downstream data infrastructure based on the cyber threat risk assessments include certain measurement and legislations that designed to proactively deal with emerging cyber security threats in the OT/IT domains to secure operations against any disrupt in the production and distribution that leading to financial losses and possibly even safety issues, if a malicious attacker were to gain access to and manipulate

the refinery's control system to malfunction or shut down, resulting in costly downtime and potentially serious injury. The theft of sensitive data, such as trade secrets or financial information, could also have a significant effect on the local industry. Because of this, it is imperative for companies in the oil and gas downstream sector to be aware of and prepared to deal with cyber threats.

Developing cybersecurity standards has become an essential element of the 21st century, as cyberattacks against organizations, businesses, and individuals are on the rise. These standards provide a set of measures that organizations and individuals can use to increase their protection against malicious cyber threats. According to Gupta & Mata-Toledo (2016), a standard such as firewall protection protects ICS communications from internal and external threats and cyber incidents. Besides the proper user authentication and authorization will ensure that the data is transmitted and stored securely. An information security framework such as such as NIST SP800-82, NERC SIP, ISA99, IEC 62443 or ISO 27001 will provide organizations with the ability to mitigate cyber risks in a manner that protects sensitive data, in particular, financial information, personal data, and intellectual property, as well as ensuring compliance with regulations such as IT policies, managing risk by helping organizations identify and assess these risks, and improving efficiency by standardizing processes and procedures to provide guidance on handle data securely.

According to [15], ISO 27001 standard is a proactive approach motivating organizations to increase their cyber security in the face of modern security threats by enhancing organizations' cybersecurity measures to combat modern security risks. This standard was divided into 14 domains, which cover areas such as access control, security of data, environmental security, and risk management. The approach discusses legal, physical, and technical measures which can be taken to protect against information risks rather than merely assessing and responding to them by providing a set of controls that organizations are required to implement, including risk management, particularly when companies adopt industry 4.0 technology.

4.5. ISO 27001 Benefits

According to [16], security standards such as ISO 27001 are crucial for oil and gas assets because:

- It included a set of controls that helps organizations in the oil and gas sector to reduce cyber risk by being secure against unauthorized access, and malware attacks.
- Providing guidelines for the secure storage, access control, and destruction of sensitive data, such as financial information, trade secrets, and proprietary technology, as a key component of protecting sensitive data.
- Ensure compliance in the oil and gas industry by assisting organizations in meeting regulations and standards related to information security requirements.
- It improves the efficiency of a company's information security processes by

streamlining processes, reducing the risk of errors, and enhancing communication and collaboration among employees.

- Help organizations in the oil and gas sector to identify and assess their cybersecurity risks and put measures in place to mitigate or eliminate those risks.
- Provides guidelines for protecting against a range of cyber threats, such as unauthorized access, data breaches, and malware attacks.

Egypt's downstream oil and gas industry is vital to the country's economy, providing fuel and petroleum products to all areas of the country. Therefore, it is imperative that they remain protected from cyberattacks and other security threats. However, cybersecurity culture in the country varies depending on the individual attitudes, behaviors, and contributions of these individuals to develop their level of cybersecurity awareness. In addition, the legal and regulatory framework surrounding cybersecurity may be different among the country cities and the guideline and procedures used to respond to any cyber-attack incident. Considering technological, economic, and social factors of the country may also contribute to influencing the level of digital literacy among the population by shaping the cybersecurity culture among citizens. According to Fitch Solution report on Egypt Information Technology 2022, Egypt benefits from a rapidly developing digital ecosystem, supported by its large, tech-savvy youth population and the government placing heavy emphasis on digital transformation. Oil and gas companies across all sectors are being actively encouraged to adopt digital workflow solutions in the business process by utilizing sensors and equipment for data collection and analysis to identify medium-term opportunities through the adoption of artificial intelligence, blockchain, drones and cybersecurity. Subsequently, this make many organizations in the Egyptian industry are working to improve their defenses against cyber security threats that are becoming increasingly sophisticated by introducing different information security frameworks such as ISO 27001 to address these cyber security risks through the application of 14 controls, which cover a wide range of information security best practices assessment and treatment to protect industry information assets.

According to [17] study, ISO 27001 is a useful tool for reducing cyber security threats in the downstream oil and gas sector. Organizations in this industry can benefit from this standard as a set of best practices for information security to assess the risks associated with their operations and developing and implementing preventive, detective, and corrective controls accordingly to reduce those risks. This security framework enables organizations to monitor and evaluate the effectiveness of their controls regularly, and continually improving information security. The ISO 27001 standard provides an approach for protecting data assets and their confidentiality, availability, and integrity (CIA). To examine the effectiveness of ISO 27001 in mitigating cyber security threats in the downstream oil and gas industry in Egypt, a study by the International Association of Computer Science and Information Technology (IACSIT) found that organizations that implement ISO 27001 had a significantly lower risk of cyber security

breaches compared to those that did not. Oil and gas downstream activities as part of the global energy supply chain include refining, marketing, and distributing petroleum products, are quite vulnerable to cyberattacks. Because of the potential disruption of operations or damage to its critical infrastructure caused by cyber threats, that may disrupt operations and potentially cause harm to people and the environment. Therefore, it is imperative to take proactive steps to protect against these threats. Companies in the downstream sector should implement robust cybersecurity measures as well as regularly review and update their defenses. To accomplish this, information security management system (ISMS) best practices such as ISO 27001 should be followed, include network segmentation, timely application of security patches and updates, and training of employees in recognizing and reporting suspicious activity to manage cybersecurity risks and contribute to the prevention of breaches and the mitigation of their impact if they occur. According to [18], in terms of economic contribution, Egyptian downstream oil and gas are one of the most significant industries in the country and its cyber security landscape that constantly challenged with different techniques of cyberattacks to exploit the sector's complex distributed networks of systems and devices, including control systems, sensors, and other digital equipment. For instance, it is possible for cybercriminals to target these systems to disrupt or manipulate operations through man in the middle of attacks, which may cause serious consequences. Insider threats include employees and contractors who intentionally or unintentionally expose the organization to cyber threats. According to [19] report, Cisco lost approximately $1.4 million in employee time to appropriately audit its infrastructure and repair the damage caused by unauthorized access by a former employee. The company was required to pay a total of $1 million in restitution to affected users. This type of insider threat illustrates the negative implications of this type of threat.

4.6. Most Serious Cyberthreat

Referring to [20] found in his study that the unacceptable employee attitude is one of the major sources of internal threat that may causes security incidents within any organization, and it takes many shapes such as user security errors, negligence, and carelessness specially before cyber incident. The employer with the bad managerial to their employee may affect employee values to following standards. As reported in [14] study, insider threats and a lack of cyber security awareness are the most significant cyber threats facing oil and gas assets. Along with [21] survey on the analysis of insider incidents, the insider threat reaches 65% of total cyberthreats because of negligent insider in front of malicious insider of 35%. As well as phishing attacks that attempt to trick individuals into divulging sensitive information or clicking on malicious links, these links can negatively affect the operations in the oil and gas industry. Ransomware attacks that involve malware that encrypts an organization's data and demands payment for the decryption key. Therefore, it is importance to understand employee psy-

chology by implement the suitable change management technique that change employee motivation to comply with the organization cybersecurity policies and procedures, this behavior develops user knowledge about business expectation and willingness to behave appropriately to mitigate the negative effect of the cybersecurity internal threat. [22] go deeper in his study and found the insider motivation with malicious intent represents 54% for financial gain, 24% for business revenge and 14% because of management injustice or carelessness. In line with [23], mentioned in their study, about the importance of the regular cybersecurity awareness programs beside the other managerial measurement such as punishments and rewards, should improve employee behavior to comply with the organization standards. Also, referring to [24] study, he found the monitoring process is essential to be implemented ethically to detect and respond to any suspicious behavior even during the employment process. In line with Herath and Rao (2009), the employee behavior is difficult to be automated by technology, but the security best practices policies and procedure are well designed to manage such behavior through a group of standards that defined security roles, responsibilities, authorization, and violation consequences to all employees. Taken into consideration if the employees perceive that there is a likelihood of getting caught if they violate policies, they are most likely to follow it, especially when they feel that the top management treatment for rules is equally. According to [19], the top management effort is essential to support the employee's behavior toward information security strong culture. In equivalent to the importance of trust as a psychological contract between employer and employee, instead of high level of monitoring that reduce the trust in the workplace as reported by [25]. Because of the complexity of this environment, ISO 27001 implementation in the Egyptian downstream oil and gas sector is challenging. Organizations must consider the cost of training staff, developing policies and procedures, and applying for certification. Also, organizations should assess their current security practices and identify areas for improvement regularly. Afterward, they must develop policies and procedures, training the staff, and conduct regular audits to ensure compliance with the standard.

According to announced Egyptian energy newspapers, lately the cyber security threats have increased significantly in the Oil and Gas sector, prompting alarm, and drawing attention to the need to enhance security measures within Egypt's downstream petroleum industry. Another parameter magnifies the cyberthreats challenge in Egypt, represented by the local education systems. The weakness of the local educational system that deals with cybersecurity awareness, contribute to increase the gap between the outputs of the education system and the needs of the job market. Cybersecurity investment prospects continue to be limited by skills shortages. According to [26], Egypt can achieve greater success if it invests in human resources and takes advantage of more growth opportunities in high-skilled economic sectors. Therefore, it is necessary to recognize the problem to find ways to combat it. According to [27], upgrading the capabilities

of the local learning system methodologies is importance including the consistent of international standards. Such as implementing the NIST framework beside ISO 27001 standards in the learning cycle to decrease the gap between the Egyptian educational institutions and the businesses requirements. As showed by Capgemini Institute (2018) study, there is a growing cybersecurity skills gap by 25% between market demand and available skilled employees who are proficient in the cybersecurity talent. Several advantages and benefits are offered by the ISO 27001 domains for implementing an information security management system. As help enhance cybersecurity posture to support competitive advantage in the market, mitigate cyber risks, and increase awareness of standards. As well as providing information about how to develop and implement the ISMS, organizations can access tools and templates to help them get started and collaborating and sharing best practices.

4.7. ISO 27001 Implementation Challenges

In line with the points discussed in the literature review, implementing ISO 27001 in the oil and gas downstream industry faces several challenges, such as

- Infrastructure complexity: managing hundreds of individual technologies and cloud services can be more challenging to secure, making it more susceptible to data breaches.
- Require more resources, which significantly increases the cost of implementation.
- Legacy Infrastructure: include compatibility issues, limited resources, inconsistent security controls, limited visibility, and the need for specialized training and education.
- Lack of corrective action for known system vulnerabilities: such as missing patches, and unlicensed software.
- Inadequate asset management and visibility due of the incomplete hardware and software assets inventory, limited tracking capabilities include software updates, system modifications such as hardware replacement or new system configuration.
- Silently accepting cybersecurity risks: insufficient security controls awareness, incomplete risk assessments, and lack of compliance.
- Limited budgets and qualified personnel: Limited budgets can make it difficult to invest in cybersecurity measures, such as staff training, security tools, and systems upgrades.

In this study, we conducted a series of surveys to assess the effectiveness of ISO 27001 in the O&G local sector, using LinkedIn polls, to prove the efficiency of ISO 27001 toward cybersecurity in the Egyptian O&G downstream sector.

5. Methodology

5.1. Introduction

To evaluate the effectiveness of ISO 27001 in mitigating cyber security threats in

the Egyptian downstream oil and gas sector, a mixed-methods research approach has been used, containing both quantitative and qualitative methods of data analysis. In the previous chapter of the literature review, we have discussed cybersecurity challenges in the oil and gas sector, as well as the benefits of ISO 27001 in mitigating cyber threats. The here below surveys will be conducted among a sample of companies in the O&G downstream sector.

- Evaluate the benefits of implementing ISO 27001 to mitigate cyber threats.
- Exploring the potential risks of cyber security threats in the Egyptian O&G industry.
- Examine the implementation obstacles of ISO 27001 in the Egyptian O&G sector.

5.2. The Research Design

Data was collected through a LinkedIn survey, by using a set of simple questions that targeted many qualified cybersecurity LinkedIn groups. In addition, Microsoft Excel has been used to analyze the collected data to justify the study objectively. We developed the survey questions using the following 14 domains of ISO 27001 as the basis for the development of the survey.

1) Information security policy.
2) Organization of information security.
3) Asset management.
4) Human resources security.
5) Environmental security.
6) Communications and operations management.
7) Authentication.
8) Purchasing, developing, and maintaining information systems.
9) Management of information security incidents.
10) Management of business continuity.
11) Achieving compliance.
12) Business continuity management and information security.
13) Relationships between suppliers and information security.
14) Management of incidents in information security.

5.3. Research Philosophy

To achieve the objectives of the research philosophy, data collection and interpretation were limited to facts based on positivism. In this study, we examined the positive impact of ISO 27001 implementation on mitigating cyber threats on the downstream oil and gas sector in Egypt.

5.4. Research Type

As part of this study, we employed an inductive approach as well as a mixed methods method through qualitative and quantitative analysis to examine how cyber threats it can mitigate in the downstream oil and gas industry. Next, we

collected a quantity of data over the study period to identify patterns of reasoning observations about the benefits of ISO 27001, as well as to develop explanations of how these benefits can be enhanced by the cybersecurity posture of Egypt.

5.5. Data Collection Method

Surveys were used to generate the data that will be used in the quantitative analysis, in which structured questionnaires were distributed to participants to discuss the fourteen domains of ISO 27001. These unified questions have been used to collect information from a large group of people quickly, and efficiently to draw conclusions about how ISO 27001 standard help to mitigate the cyberthreats in the Oil and gas downstream industry. The collected answers have been reviewed and cleaned by removing any errors or outliers and ensuring that the data is accurate and complete. Then Microsoft Excel and SPSS have been used to analyze and determine the best visualize way to present the survey collected data.

We constructed survey questions using the SWOT analysis to show the current cybersecurity performance in the Egyptian oil and gas downstream sector in terms of strengths, weaknesses, opportunities, and threats. t-tests have been used to investigate the relationship between compliance with ISO 27001 and non-compliance toward cybersecurity posture inside the sector, to find a relation between the companies that had suffered from data breaches and comparing it to companies that have implemented ISO 27001, in a way to identify whether there is a correlation between compliance with this standard and reduced data breaches. To gain a deeper understanding of the challenges associated with implementing ISO 27001 in the Egyptian market, we have started a structured interview during Egypt petroleum show (EGYPS 2022). This local show is one of the most prominent oil and gas events in North Africa and the Mediterranean. During the event, we met professional cybersecurity individuals who are knowledgeable in considering Egyptian cyber threats of the Oil and gas downstream sector. In these interviews, the here below topics have been discussed.

- Briefly describe the cyberthreats facing Egyptian oil and gas corporations.
- The benefits of implementing cybersecurity measures, such as ISO 27001 to combat cyber threats.

5.6. The Methodological Limitations

Despite methodology advantage that has been used in this study from the Quantitative methods that provided statistical data that is often seen as more objective and reliable, to the Qualitative methods, such as EGYPS interviews which provide rich and detailed data that can provide deeper insights into the research topic. We have noted that some limitations in method that has been used especially reaching the desired sample size which have negatively affected the representativeness of engagement. Because of the low response rate, selection bias, and self-reported data. Besides the complexity and difficulty of the multiple

analysis techniques that have been used in the study. However, we tried to minimize these limitations by designing the survey question in a way that was clear, concise, and well-written. In addition, we tried to ensure that we administered the survey to an appropriate cybersecurity expert through LinkedIn's top hashtags in the Egyptian market.

6. Finding

6.1. Evaluate the Effectiveness of ISO 27001

The thesis' aim is to provide the results of surveys done on the LinkedIn platform to learn more about how well ISO 27001 contributes to reduce cyber security risks in the Egyptian downstream oil and gas industry. The purpose of the poll was to collect information and opinions from a group of experts in the pertinent cybersecurity subject to clarify the current cybersecurity trends, cybersecurity challenges, and market opportunities in the local oil and gas sector. Then we analyzed the survey's results using statistical measurement to give a thorough overview of the major conclusions that may provide suggestions based on the knowledge gained from these surveys to support future decisions positively toward cybersecurity. The results then presented in a well-organized manner, under the research method arrangement, beginning with a discussion of ISO 27001 benefits from a security perspective, followed by current cybersecurity measurements in the oil and gas industry, and then an overview of the key difficulties in implementing ISO 27001 in Egypt. Visual aids, such as tables, figures, and charts, have been used to clarify the data and facilitatean objective understanding of the study. Based on the results of survey one, this survey presents in an easy and understandable manner how ISO 27001 can mitigate the risk of cyber-attacks. Figure 1 illustrates that ISO 27001 provides a comprehensive framework for managing information security and helping organizations mitigate the risk of cyberattacks. Further, it responds to cyber-attacks as soon as they occur by ensuring the readiness of business continuity plans.

A further objective of the study is to evaluate current protection measures against cyberthreats in both the oil and gas foreign and local markets to gain a deeper understanding of the market trend. To accomplish this, we conducted another survey among participants in group two in the oil and gas industry in

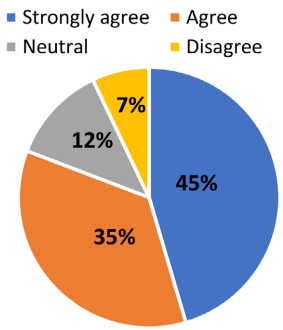

Figure 1. A summary result of Evaluate the effectiveness of ISO 27001.

the foreign and local markets. In this survey, we tried to evaluate the standard compliance to ISO 27001 toward an organization's reputation, production disruptions and financial protection during their day-to-day work. As shown in Figure 2 and Figure 3, the summary of the survey in the foreign market was as follows:

Along with the oil and gas market trend toward the protection against cyberthreats, we found a lot of attention is being paid toward the effectiveness of compliance to ISO 27001 standard approach to protect sensitive information. To achieve the measurement of this effectiveness, survey three has grouped for foreign and local market for evaluate "how far the compliance with the ISO 27001 standard provides organizations with a significant cybersecurity level to mitigate cyber threats?"

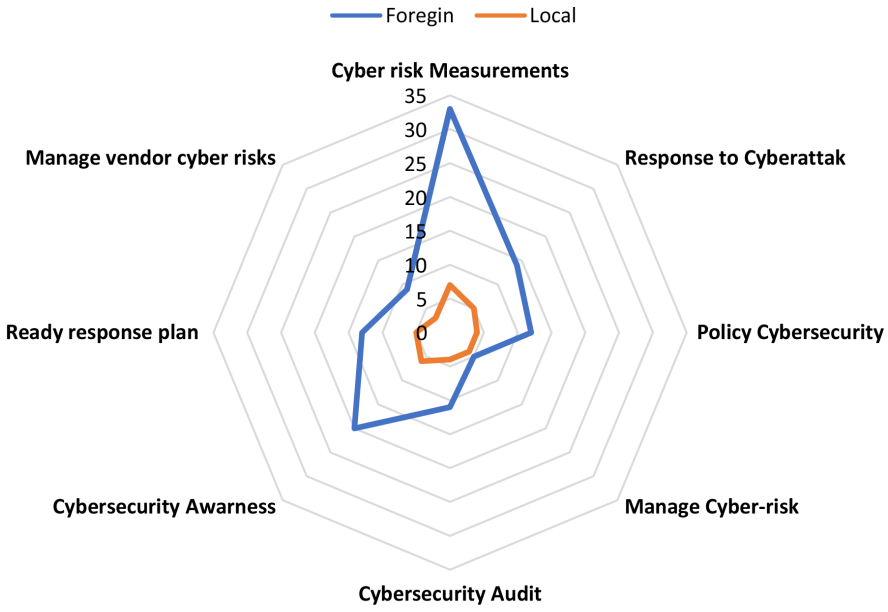

Figure 2. Oil and gas protection measurement (foreign vs. local market).

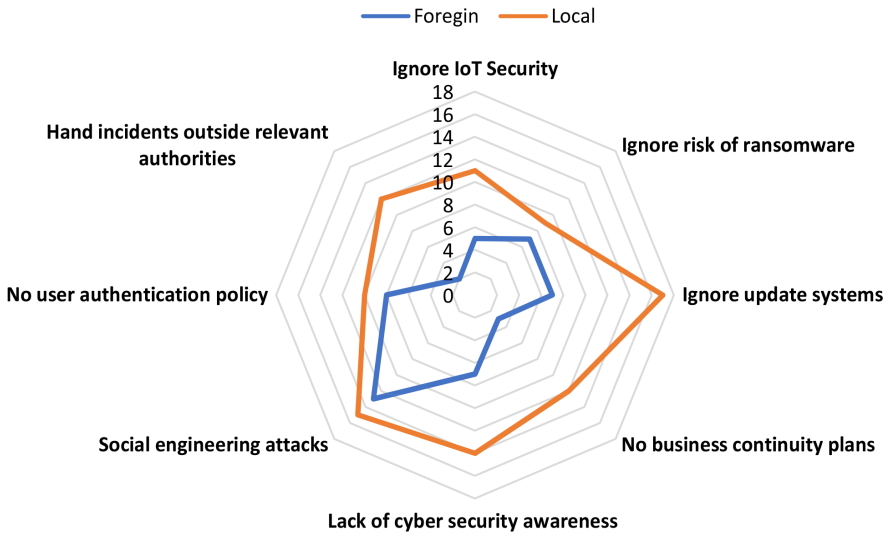

Figure 3. Oil and gas Cyberthreats (foreign vs. local market).

6.2. ISO 27001 Compliance Benefits

The statistical hypothesis test has been used to answer this question using "t-test" statistical method to determine the relationship between compliance to ISO 27001 toward mitigation of cyberthreats in the Egyptian oil and gas downstream sector. By introducing the null hypothesis (H0) and the alternative hypothesis (Ha) as shown here below:

Null hypothesis (H0): ISO 27001-compliant organizations are not better secure than non-compliant organizations in both local and foreign oil and gas downstream market. Alternative hypothesis (H1): ISO 27001-compliant organizations are better secure than non-compliant organizations in both local and foreign oil and gas downstream markets.

The t-test as a statistical test will be used to compare the means of two groups of data, whether there is a significant difference between the mentioned hypothesis (H0 and H1). Table 1 and Table 2 illustrate the manual calculations to

Table 1. Results of the group three survey (foreign market).

	ISO 27001 Compliance vs. Protection (Foreign Market) LinkedIn Hashtag Group 3		Deviation of Mean $(x_i - \bar{x})$	Deviation Squared $(x_i - \bar{x})^2$
1	Significant difference	4	1.13	1.28
2	Somewhat significant	3	0.13	0.02
3	Somewhat significant	3	0.13	0.02
4	Marginally significant	2	−0.87	0.76
5	Significant difference	4	1.13	1.28
6	No significant difference	1	−1.87	3.50
7	Significant difference	4	1.13	1.28
8	Significant difference	4	1.13	1.28
9	Somewhat significant	3	0.13	0.02
10	Marginally significant	2	−0.87	0.76
11	Marginally significant	2	−0.87	0.76
12	Marginally significant	2	−0.87	0.76
13	Significant difference	4	1.13	1.28
14	Marginally significant	2	−0.87	0.76
15	Somewhat significant	3	0.13	0.02
	Mean	2.8667		
	MS. Excel (STDEV.S)	0.9904	$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$	
	Standard Deviation	0.9904		
	Variance	0.981		
	(n)	15		

Table 2. Results of the group three survey (local market).

	ISO 27001 Compliance vs. Protection (Local Market) LinkedIn Hashtag Group 3		Deviation of Mean $(x_i - \bar{x})$	Deviation Squared $(x_i - \bar{x})^2$
1	No significant difference	1	−0.67	0.44
2	Marginally significant	2	0.33	0.11
3	Somewhat significant	3	1.33	1.78
4	Marginally significant	2	0.33	0.11
5	No significant difference	1	−0.67	0.44
6	Marginally significant	2	0.33	0.11
7	Marginally significant	1	−0.67	0.44
8	Marginally significant	2	0.33	0.11
9	No significant difference	1	−0.67	0.44
10	No significant difference	1	−0.67	0.44
11	No significant difference	1	−0.67	0.44
12	Marginally significant	2	0.33	0.11
13	Somewhat significant	1	−0.67	0.44
14	No significant difference	1	−0.67	0.44
15	Somewhat significant	4	2.33	8.44
	Mean	1.6667		
	MS. Excel (STDEV.S)	0.8997	$s = \sqrt{\frac{\sum (x_i - \bar{x})^2}{n-1}}$	
	Standard Deviation	0.8997		
	Variance	0.8095		
	(n)	15		

evaluate the effect of ISO 27001 protection.

Considering, the STDEV.S Function as a statistical function in Excel that has been used to calculate the standard deviation based on the coded samples that were collected from group two and group three surveys. The STDEV.S function accepts two arguments "number 1" and "number 2" representing the first and the second value of the sample data, respectively.

In order to calculate the t-test, the variance of the two samples must be determined first. If the variance between the larger and smaller is less than four, then we can assume that the variances are approximately equal, which allows us to estimate the T-value. In the cross-tabulation between Table 1 and Table 2, V1 = 0.9810, and V2 = 0.8095, which indicates that the variances between the two groups are approximately equal. Therefore, the significance level (Alpha α) or the critical level, is ready to be 8 to evaluate the strength of evidence that must be retrieved from the distribution table before the null hypothesis can be affirmed

or rejected. It is important to use significance levels during hypothesis testing to determine the data support which hypothesis. We considered significance level as 5%, which means the study result has a 5% chance of being just a coincidence.

The hypothesis does not signify the direction of interaction or difference, so we will use the two-tailed (sides) of a normal distribution to checking the relations between variables and justify the null hypothesis testing. The significance level included in the t-distribution table should provide the critical values where the column (probability) and row (degree of freedom) intersect and define by the following values: degrees of freedom (total number of participant − 2), number of tails of the t-test (two-tailed), significance level of the t-test (we will use 0.05), Microsoft Excel function has been used to calculate alpha value "T.INV.2T (Probability, Degree of Freedom)".

There is a relationship between the smaller the p-value, and the stronger the evidence that the null hypothesis should be rejected. Based on the sample collected from 30 participants (n = 30) then the degree of freedom (df) should be 28 (n − 2). Besides the traditional probability threshold suggest the statistical significance should be 0.05. Then, according to the t-distribution table, the significance level (alpha α) critical value should be 2.048. Using the collected data, we can now calculate the t value manually, as shown in Table 3.

Using the following equation to determine the t-value of the collected samples (V1/V2 < 4 *i.e.* the samples with equal variance, then the following equation will determine the t value):

$$t = \frac{x_1 - x_2}{\sqrt{\frac{(s_1)^2}{n_1} + \frac{(s_2)^2}{n_2}}}$$

T test statistic value = (2.867 − 1.667)/SQRT (0.981/15 + 0.81/15) = 3.473 Using MS Excel to calculate p-value (2 tailed) = t.dist.2t (3.473, 28) = 0.002 As shown in Figure 4, the t-distribution table shows the calculated t (3.473) corresponding to the degree of freedom (28) demonstrate t-distribution p-value of 0.002 (two tailed). The t value (3.473) exceeds the critical value (2.048), so the means of local group and local group are significantly different at p = 0.05 and the null

Table 3. T-values calculation based on cross-tabulations of Table 1 & Table 2.

Group	Oil and Gas Foreign Market	Oil and Gas Egyptian Market
Sample	(4 3 3 2 4 1 4 4 3 2 2 2 4 2 3)	(1 2 3 2 1 2 1 2 1 1 1 2 1 1 4)
Mean	X1 = 2.8667	X2 = 1.6667
Standard Deviation	S1 = 0.9904	S2 = 0.8997
Variance (V1, V2)	V1 = 0.9809	V2 = 0.8095
n	15	
Degree of Freedom	28	
Critical Value	2.048	

hypothesis (H0) should be rejected, and alternative hypothesis (H1) should be accepted. In other words, ISO 27001-compliant organizations are better secure that non-compliant organizations.

Using IBM SPSS statistics software, we will confirm the preview calculation as follows:

Open SPSS application, from "variable view"', we need to create the following two variables: Variable Name: Group / Values: 1.00 = "Foreign Market", 2.00 = " Local Market" From Data view, enter the survey coded data as shown in Table 4, considered the group field will have only values of one or two and the score value will be the survey score. Set the percentage of confidence intervals to 95% and click OK. Then generate the results as shown in Table 4.

The results show p-value 0.002 was less than the alpha value (0.005), that means the null hypothesis (H0) should be rejected, whereas the alternative hypothesis (H1) should be accepted. Which means, there is a difference between

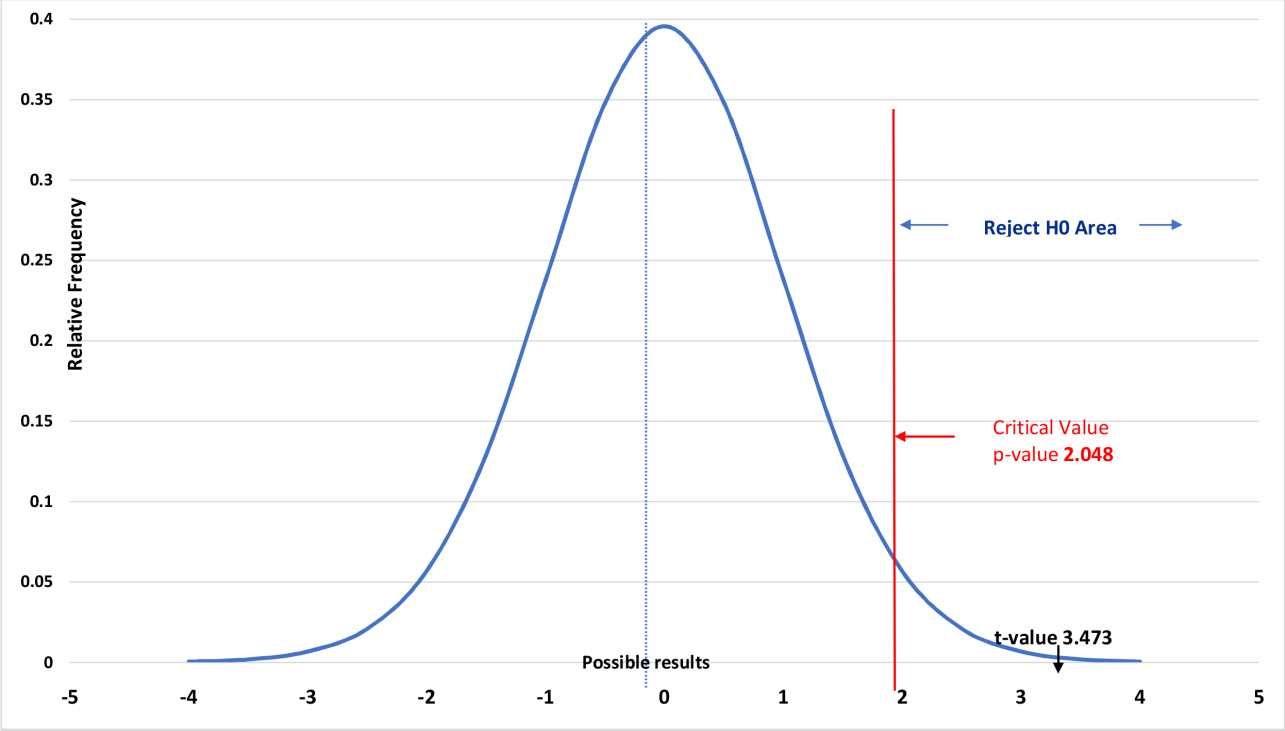

Figure 4. T-distribution and the critical point.

Table 4. t-test group statistics using SSPS (foreign/local market).

	Group	N	Mean	Std Deviation	Std Error Mean
Score	Foreign Market	15	2.8667	99043	25573
	Local Market	15	1.6667	89974	23231

		F	Sig	t	df	Sig (2t)
Score	Equal variances assumed	388	538	3.473	28	0.002
	Equal variances not assumed			3.473	27.746	0.002

compliant organizations and non-compliant organizations with ISO 27001 from the security perspective.

6.3. EGYPS 2023 Interviews

We implemented a structured interview during the oil and gas local event "EGYPS" to learn more about the benefits of ISO 27001 in mitigating the cyber-security threats in the Egyptian downstream sector. In the show, we have spoken with cybersecurity experts in the oil and gas who are familiar with the Egyptian cyber risks in the downstream sector. The interview covered the discussion about cyberthreats that Egypt's oil and gas downstream sector is facing, and their experiences before, during, and after putting cybersecurity measures such as ISO 27001 in place to counter cyber-attacks. The results then coded on the cyber risk scale of 10% - 100% towardISO 27001 implementation timeline, then presented these results once again as shown in Figure 5.

During the interview, we discussed the cybersecurity gap between demand and supply in the Egyptian oil and gas market. There is a discrepancy between the rising demand for cybersecurity products and services and the country's shortage of certified cybersecurity providers. We have introduced group four survey during EGYPS event to identify the causes behind low level of ISO 27001 implementation in Egypt and we found the reasons for the local market cyber-security gap in the following points:

- Internal resource has difficulty implementing security controls effectively.
- Local organizations have difficulty to identify and prioritize risks effectively.
- Local organizations have trouble maintaining standard compliance over time.
- The culture of information security is not well adapted by local organizations.
- Local organizations struggle to measure the effectiveness of security controls.
- Resources are limited locally because of financial constraints and insufficient

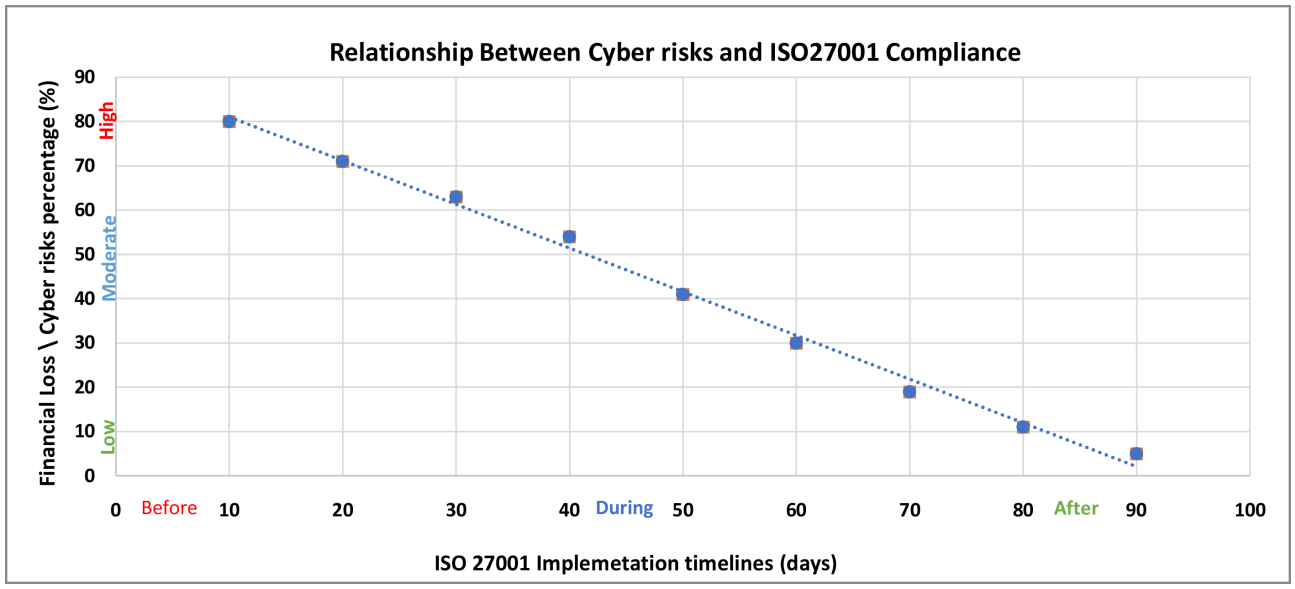

Figure 5. Relation between cyber risks, financial loss and ISO 27001 implementation.

expertise.

- Employees are resistant to changes and procedures required by the standard.
- Failing to continuously monitor systems to ensure they comply with standards.
- Local organizations neglect to educate staff about information security best practices.
- Local organizations have trouble documenting their information and procedures.

6.4. Cybersecurity Local Gap

According to group four survey results, we found the main reason of what these points have in common, the Egyptian education method is the one of the main reasons for the absence of cybersecurity experts on the local market. According to Louisa Loveluck (2012) research paper, the Egyptian educational approach is to blame for the lack of cybersecurity specialists in the local market and is one of the key factors causing the industry's persistently high unemployment rate because of the mismatch between the demands of the cybersecurity labor market and the educational system's outputs, resulting in a shortage of skilled workers and limiting cybersecurity investment opportunities.

7. Discussion

In this study, we conducted surveys and interviews with cybersecurity experts and professionals in the oil and gas downstream industry in Egypt. The survey questions focused on the level of cyber protection in the industry and the extent of cybersecurity awareness among employees. The findings provide a valuable insight into how ISO 27001 use in shaping a best-practice approach to information security inside the Egyptian oil and gas downstream sector as following:

- Despite the high level of cyber threats facing the local industry, the survey results showed a limited level of cyber protection.
- The interviews revealed that organizations in the industry face several challenges in adopting ISO 27001, such as the cost of implementation and the lack of expertise in cybersecurity.
- It also found the lack of cybersecurity awareness among employees to be one of the main reasons for the cyber threats in the O&G local market.

The t-test results showed a direct correlation between conformance to ISO 27001 and reduced cyber risks in the local and foreign downstream oil and gas industries. This finding suggests that organizations that adopt ISO 27001 are better equipped to deal with cyber threats and protect their information assets. The case studies conducted as part of the study also confirmed the importance of ISO 27001 in enhancing the security posture of organizations in the oil and gas downstream industry to identify and mitigate cyber risks more effectively and reduce the probability of security breaches and data leaks. Survey stage one shows that over 46% of respondents strongly agree that ISO 27001 reduces the

risk of cyberattacks significantly by enhancing organization's information security posture through a good security framework that identifying, analyzing, and addressing information security risks in an organized manner to reduce the likelihood of security breaches and data leaks. In the second stage of the survey, we tried to see whether there were any differences between the foreign and local markets in how cybersecurity measured in relation to cyber risks in the oil and gas sector. According to Figure 2, we found a difference between both markets concern the cyber protection and cyber threats they exposed to. According to the results of survey three, there is a direct correlation between conformance to ISO 27001 and a reduction in cyber risks in both the local and foreign downstream oil and gas industries.

Besides this, EGYPS interviews proved that conforming to ISO 27001 standards is an effective way to reduce cyber threats, as shown in the interviews results which are represented in figure five. The figure shows how the implementation of ISO 27001 standards protects information systems, helps companies in identifying and reducing security threats, and helps avoid financial loss by continuously maintaining a strong security posture.

Although complying with security standards might help minimize cyber threats, we discovered during EGYPS interviews the main reasons for the limited implementation of ISO 27001 in the Egyptian oil and gas industry. Identifying these reasons is a critical starting point for solving this limitation in the standard implementation. For instance, it's likely that many businesses in the Egyptian oil and gas sector are unfamiliar with the value of the ISO 27001 standard for enhancing their information security management system, which may make people hesitate to invest time and money in implementing ISO 27001. Several organizations in the Egyptian oil and gas sector have difficulty finding qualified cybersecurity employees, and they might not have the budget to spend implementing the standard. The local organization's current information security management system may need to be improved to implement ISO 27001, which follow by increase in the organization's resistance to change and hinders adoption of new practices. Also, the Egyptian government does not enforce the oil and gas sector to comply with ISO 27001 standards, this lack of governmental pressure, businesses may not feel as obligated to implement the standard. During EGYPS interviews, we spoke about the significant gap between the demand and supply for qualified cybersecurity professionals in the Egyptian oil and gas industry. One of the major factors contributing to this gap is the lack of a formal cybersecurity education system in Egypt, which led to this shortage in the qualified professionals in the local market. Another factor contributed to this gap is the lack of awareness among oil and gas organizations of the importance of cybersecurity. According to Louisa (2012) research report, this absence of cybersecurity specialists in the Egyptian market should encourage the Egyptian educational authorities to implement formal programs in the cybersecurity through a careful, cautious, and transparent initiatives to achieve a good balance between the qual-

ity of the cybersecurity education in line with the cyber security market demands.

According to the [28], Oando PLC orientation toward the mitigation of cyber threats, as a case study show a good example of the positive effective of ISO 27001 in mitigating cyberthreats. The company conducted a risk assessment to identify the potential vulnerabilities in the company's systems and processes. Based on the results of the risk assessment, Oando corporation developed a comprehensive information security management system (ISMS) that included policies, procedures, and controls to mitigate identified risks. Following with the establishment of incident management process to respond to any security breaches that occurred. The Oil & Gas Company Oando becomes the first in Nigeria to receive ISO 27001 certification. Now the Oando's board of directors believes that ISO 27001 significantly reduces the risk of network cyber-attacks and protects sensitive information from unauthorized access. The company has protected its reputation by demonstrating the effectiveness of the standard certification to strengthen its commitment to its customers.

Avanceon Oil and Gas Consultant is another, empirical evidence supports the argument of the ISO 27001 effective in mitigating cyber threats in the oil and gas sector. According to the [29], Avanceon is a consulting company provides key solutions to Oil and Gas downstream industries including data integration with PLC/DCS, IT/OT convergence, Manufacturing Execution System (MES), Industrial Automation as a Service (IAAS) and IIOT solutions for analysis control, quality assurance and production monitoring for making informed decisions. They have worked on more than 300 oil and gas industry projects in 14 nations, offering cutting-edge solutions to this industry. As part of Avanceon commitment of transparency to its customers and partners. As a result of implementing ISO 27001, the company was certified as compliant, and all their data and systems are protected against breaches and cyberattacks. However, ISO 27001 has some limitations, such as the difficulty of being understood by small and medium-sized organizations without dedicated information security staff. Besides the limited budget for the implementation particularly for smaller organizations. And the standard narrow scope that does not cover all cybersecurity aspects such as physical security or personnel security.

8. Conclusions

Based on a quantitative and qualitative analysis of the information gathered through surveys, interviews, case studies, and research papers, ISO 27001 was found to be an effective standard that reduces cyber security threats in the downstream oil and gas sector. However, implementing this standard faces several challenges in the Egyptian O&G downstream sector, which should be approached in the following manner:

- Infrastructure complexity should be planned carefully to improve the security posture of the sector and protect critical infrastructure from cyber threats.

- Management needs to modernize and upgrade legacy infrastructure, as well as implement effective security controls that are ISO 27001 compliant.
- Conducting regular vulnerability assessments to identify and remediate vulnerabilities in the system, besides regularly monitoring and reporting on compliance with security standards and policies and implementing remedial measures as necessary.
- Ensuring that all software used is licensed and receiving regular security updates.
- Establishing robust employee training and education programs that focus on security best practices and adherence to security policies.
- Implementing a system for tracking changes to the system, including software updates, system modifications, and hardware replacements.
- Introduce the concept of cyber security readiness team, especially the Cybersecurity Incident Response Team (CSIRT) and Computer Emergency Response (CERT) in the O&G downstream sector to take correction action towards security vulnerability findings, understanding cybersecurity incident root causes and communicated it to all relevant stakeholders for the prevention action.
- Adequate resources and support to maintain and support the IT system effectively, by investing in cybersecurity measures such as staff training, security tools, systems upgrades, and encouraging a culture of security awareness and vigilance among employees and stakeholders.
- Prioritizing cybersecurity spending by allocating more of their budgets to cybersecurity measures such as staff training, security tools, and systems upgrades.
- Organizations inside the sector may need to collaborate transparency with other companies in the sector to share cybersecurity expertise and resources.
- Companies may need to consider outsourcing some cybersecurity functions to third-party service providers to augment their internal capabilities.

The research clearly illustrates the benefits of ISO 27001 toward cybersecurity, but also raised the root causes behind the gap between the demand and supply of cybersecurity professionals in the Egyptian oil and gas market. This gap was the root cause behind the limitation in implementing this standard in the local industry. To bridge this gap, several measures can be taken, include the investing in formal cybersecurity education and training programs, providing opportunities for professional development and advancement, investing in cybersecurity infrastructure and technology, and increasing awareness of the importance of cybersecurity among organizations. Thus, further research is necessary to confirm that the results still apply. Time constraint is another type of limitation we have faced in this study that may have affected the accuracy of the results. However, based on the findings, the action sheet in **Table 5** offered some recommendations as a guidance on how this research can provide a suggest future directions as follow:

Table 5. Strategic, tactical, and operational recommendations.

Issue	Person Responsibility	Result of Request	Resource Needed	Time Frame
Strategic1 (Governmental)	Upper Management	Develop regulations to promote cybersecurity. Enforcing regulations of cybersecurity standards. Promote cybersecurity awareness in education.	Approvals	Long Term (06 - 12 months)
Strategic 2 (CEO)	Upper Management	Maintaining compliance with the standard. Plan to manage the change. Provide the necessary resources for compliance.	Approvals Budget	Long Term (06 - 12 months)
Strategic 3 (CTO/CIO)	Upper Management	Ensure ISO 27001 compliance. Taking corrective action for non-compliance. Inform stakeholders of the level of compliance on regular basis.	Budget Skilled Workers Facilities, Safety.	Medium Term (03 - 6 months)
Tactical 1	HR Manager	Selecting the right candidates for duties. Train the cybersecurity team appropriately. Employees coaching to help improvement.	Skilled Workers Facilities, Utilities Safety.	Medium Term (03 - 6 months)
Tactical 3	IT Manager	Ensure IT policies comply with standards. Ensure IT systems comply with IT policies. Conducting security vulnerability assessments. Monitor compliance with standards regularly. Develop Incident Response Team.	Qualified Workers Facilities, Utilities Equipment, Safety Insurance.	Medium Term (03 - 6 months)
Operational 2	Team Leader	Understand and communicate the standard. Providing training on security awareness. Continuous improvement cybersecurity culture. Solving problems and resolving conflicts. Goal management.	Qualified Workers Facilities, Utilities Safety, Insurance.	Short Term (01 - 03 months)
Operational 3	Auditors	Conducting assessments with relevant IT polices and report non-compliance issues to senior. Management and take action to remediate security vulnerability finding.	Qualified Workers Facilities, Utilities Safety.	Short Term (01 - 03 months)

It is important to note that the results of the study subject are extremely positive and offer significant insights into the effectiveness of ISO 27001 to mitigate cyber security threats in the Egyptian downstream oil and gas industry. A future study should examine the nature and scope of cybercrime in Egypt, as well as trends, types of attacks, and their impact on businesses and individuals. In addition, identify the root causes of this cybercrime in the country, as well as the risks and challenges associated with emerging technologies. In parallel with the effort to transform into a safer digital environment.

Acknowledgements

I would like to use this opportunity to express my sincere gratitude to my project's supervisor, Prof. Dr. Ashwini Atul, for her direction and support. Your guidance and expertise were invaluable in helping me navigate the research and complete it successfully.

Also, I would like to thank UNICEF and the University of East London for their support and patience during the challenging times of the study. Your trust

in my abilities was a constant source of inspiration and has helped me to achieve my academic goals.

I would like to extend a special thank you to the EGYPS organizers for their help in organizing several study interviews during the Egypt petroleum show. Your team's support and guidance were invaluable, and I could not have managed it without your help.

It is also my pleasure to extend my gratitude to my loving wife Eman and my daughters Aya, Gana, and Mariam, who have enabled me to conduct my research in a calm environment. I would like to express my sincere gratitude to those members of my family and friends who have encouraged me along this journey so far. Your support means a lot to me.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Imran, H., Salama, M., Turner, C. and Fattah, S. (2021) A Systematic Literature Review on the Technical and Non-technical Cyber Risk Management Models in the Oil and Gas Sector. *Economic and Social Development*: *Book of Proceedings*, Varazdin, 3 June 2021. https://www.proquest.com/conference-papers-proceedings/systematic-literature-review-on- technical-non/docview/2545671144/se-2

[2] Stergiopoulos, G., Limnaios, E., *et al.* (2020) Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. *IEEE Access*, **8**, 128440-128475. https://ieeexplore.ieee.org/ielx7/6287639/8948470/09136701.pdf https://doi.org/10.1109/ACCESS.2020.3007960

[3] Goncharov, E. (2022) ICS Cyberthreats in 2023—What to Expect. Kaspersky ICS CERT. https://ics-cert.kaspersky.com/publications/reports/2022/11/22/ics-cyberthreats-in-2023-what-to-expect

[4] Mehan, J. (2014) Cyberwar, Cyberterror, Cybercrime and Cyberactivism (2nd Edition): An In-Depth Guide to the Role of Standards in the Cybersecurity Environment. IT Governance Ltd., Ely. https://ebookcentral.proquest.com/lib/UNICAF/reader.action?docID=1778762&ppg=183

[5] Carmony, M. (2020) Analyzing Cybersecurity Risks within Critical Infrastructures: Threats and Challenges in the Oil and Gas Industry. ProQuest Dissertations, Utica College, Utica. https://www.proquest.com/dissertations-theses/analyzing-cybersecurity-risks-within- critical/docview/2485483134/se-2

[6] Polyakov, A. (2016) Oil and Gas Security. Infosec Institute, Elmwood Park. https://resources.infosecinstitute.com/oil-and-gas-cyber-security-101

[7] Ahmed, A. (2022) Egypt among 20 Most Vulnerable Countries to Cyberattacks. *Daily News*. https://dailynewsegypt.com/2022/09/27/egypt-among-20-most-vulnerable-countries-to-cyber-attacks-ntra

[8] Ahmed, F. (2020) El Molla: Petroleum Sector Contributes 27% of GDP. Egypt Oil &

Gas.
https://egyptoil-gas.com/news/el-molla-petroleum-sector-contributes-27-of-gdp

[9] Kosmowski, K.T., Piesik, E., Piesik, J. and Śliwiński, M. (2022) Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies*, **15**, 3610. https://doi.org/10.3390/en15103610

[10] Lewis, L.D., Morris, L.D. and Simpson, N.O. (2020) Managing Cyber Security for the Downstream Oil and Gas Industry. *CIO Magazine*.
https://www.cio.com/article/3523699/managing-cyber-security-for-the-downstream-oil-and-gas-industry.html

[11] LogRhythm (2022) The State of the Security Team.
https://gallery.logrhythm.com/analyst-reviews-and-reports/logrhythm-na-the-state-of-the-security-team-research-report-2022.pdf

[12] Nozomi Networks (2022) OT/IoT Security Report a Deep Look into the ICS Threat Landscape.
https://www.nozominetworks.com/downloads/Nozomi-Networks-OT-IoT-Security-Report-2022-2H.pdf

[13] Herve, P. (2022) Securing Pipeline Endpoints against Rising Global Threats. *Pipeline & Gas Journal*, **249**, 64.
https://www.proquest.com/trade-journals/securing-pipeline-endpoints-against-rising- global/docview/2673380472/se-2

[14] Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B.A., Dalaklis, D. and Karamperidis, S. (2021) Perspectives on Cyber Security for Offshore Oil and Gas Assets. *Journal of Marine Science and Engineering*, **9**, 112.
https://doi.org/10.3390/jmse9020112

[15] Gurbani, V.K. (2019) Cyber Security Management System: A Review of Literature. *International Journal of Engineering Research & Technology*, **8**.

[16] Howard, S. and Wallaert, T. (2015) Improving Cybersecurity Defenses in Oil and Gas Applications. *Pipeline & Gas Journal*, **242**, 46-48.
https://www.proquest.com/trade-journals/improving-cybersecurity-defenses-oil-gas/docview/1654945948/se-2

[17] Amran, A., Deilami, A. and Benlamri, R. (2019) Cyber Security Risk Management in the Oil and Gas Industry. *International Conference on Digital Economy*, 337-358.

[18] Moustafa, M.I. (2015) An Analysis of the Privatization of the Oil and Gas Industry in Egypt: A Focus on Equity and Legal Implications. ProQuest Dissertations Publishing.

[19] Oost, D. and Chew, E. (2007) Investigating the Concept of Information Security Culture. University of Technology Sydney, Sydney.

[20] Leach, J. (2003) Improving User Security Behaviour. *Computers & Security*, **22**, 685-692. https://doi.org/10.1016/S0167-4048(03)00007-5

[21] Ponemon Institute LLC (2018) Cost of Insider Threats: Global. Ponemon Institute, Traverse City.
https://www.insiderthreatdefense.us/pdf/Ponemon%20Institute%202018%20Report%20-%20The%20True%20Cost%20Of%20Insider%20Threats%20Revealed.pdf

[22] Munshi, A., Dell, P. and Armstrong, H. (2012) Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents. *Hawaii International Conference on System Sciences*, Maui, 4-7 January 2012, 2402-2411.
https://doi.org/10.1109/HICSS.2012.326

[23] Back, S. and Guerette, R.T. (2021) Cyber Place Management and Crime Prevention:

The Effectiveness of Cybersecurity Awareness Training against Phishing Attacks. *Journal of Contemporary Criminal Justice*, **37**, 427-451. https://doi.org/10.1177/10439862211001628

[24] Hampton, A.J. and DeFalco, J.A. (2022) The Frontlines of Artificial Intelligence Ethics. Routledge, London. https://doi.org/10.4324/9781003030928

[25] Joinson, A.N., Houghton, D.J., Vasalou, A. and Marder, B.L. (2011) Digital Crowding: Privacy, Self-Disclosure, and Technology. Springer, Berlin. https://doi.org/10.1007/978-3-642-21521-6_4

[26] Loveluck, L. (2012) Education in Egypt: Key Challenges. Chatham House, London. https://www.semanticscholar.org/paper/Education-in-Egypt%3A-Key-Challenges-Loveluck/67481746ba3653f62228a230b44fb15512e6db40

[27] Provost, C. (2011) Egypt: Tackling Youth Unemployment. *The Guardian*. https://www.theguardian.com/global-development/2011/aug/03/egypt-education-skills-gap

[28] Orient Energy Review (2020) Oando Becomes First Oil and Gas Company in Nigeria to Be ISO 27001 Certified. Oandoplc Media Release. https://www.oandoplc.com/oando-becomes-first-african-oil-gas-company-to-be-iso-27001-certified/#:~:text=Blog-,Oando%20Becomes%20First%20Oil%20%26%20Gas%20Company%20in,to%20be%20ISO%2027001%20Certified

[29] Avanceon (2022) TUV Austria's ISO 27001:2013 Certification. TUV Austria Bureau of Inspection and Certification (Pvt.) Lt. https://www.avanceon.ae/tuv-austria-endorses-avanceons-information-security-management-system-with-iso-27001-certification