Sultan Qaboos University
Journal of Arts & Social Sciences

جامعة السلطان قابوس
مجلة الآداب والعلوم الاجتماعية

Assessing Information Security Practices in Omani Ministries: Challenges and Pathways to International Standards Compliance

Said Albarami

PhD candidate
Department of Information Studies
Sultan Qaboos University
Oman
albarami@hotmail.com

Khalfan Zahran Al-Hijji

Associate Professor, Department of Information Studies
Sultan Qaboos University
Oman
khijjiz@squ.edu.om
khijjiz@yahoo.com

Raja Waseem Anwar

Assistant Professor
Department of Computer Science
German University of Technology (Gutech)
Oman
raja.waseem@gutech.edu.om

Date received: 05/10/2023
Date of acceptance: 12/06/2024

Volume (15) Issue (3), December 2024

Assessing Information Security Practices in Omani Ministries: Challenges and Pathways to International Standards Compliance

Said Albarami, Khalfan Zahran Al-Hijji, Raja Waseem Anwar

Abstract

Digital transformation in Oman has amplified the risk of cyberattacks, as evidenced by millions of attacks targeting government websites and critical infrastructures. However, Oman's current cybersecurity preparedness, particularly in policy development, is inadequate, as indicated by its moderate ranking in the National Cyber Security Index and score of 0% in cybersecurity policy development. Furthermore, prior research has not extensively covered the implementation of information security standards within Omani ministries. This study addresses this critical gap by evaluating the current state of information security policy implementation across 18 Omani ministries. A survey of 36 IT and security managers assessed current policies and practices, focusing on confidentiality, integrity, and availability. The study highlights that, although fundamental information security principles are implemented, a limited number of ministries possess international certifications. Specific deficiencies exist in advanced security measures, particularly in inadequate authentication protocols, inadequate encryption of sensitive data, and insufficient disaster recovery plans. The outcomes of this research highlight the critical necessity for Omani government agencies to embrace innovative technologies and adhere to internationally recognised information security standards to improve their security stance. This study provides significant information for policymakers and professionals aiming to strengthen the security posture of Oman's public sector.

Keywords: Information Security; Information Security Policy; Government Ministries; Oman Information Security Standards.

تقييم ممارسات أمن المعلومات في الوزارات العمانية: التحديات والمسارات للامتثال لمعايير أمن المعلومات الدولية

سعيد البرعمي، خلفان بن زهران الحجي، وسيم أنور

الملخص

شهدت سلطنة عُمان تحولًا رقميًا سريعًا، مما زاد بشكل ملحوظ من خطر الهجمات الإلكترونية التي تستهدف المواقع الحكومية والبنية التحتية الحيوية. وعلى الرغم من ذلك، لا يزال مستوى التأهب للأمن السيبراني في عُمان غير كافٍ، وهو ما يتجلى في تصنيفها المتوسط في مؤشر الأمن السيبراني الوطني. علاوة على ذلك، فإن الدراسات السابقة لم تتطرق بشكل كافٍ لمسألة تطبيق معايير أمن المعلومات في الوزارات العُمانية. هدفت هذه الدراسة إلى تقييم الوضع الحالي لمعايير أمن المعلومات في ثمانيٍ عشرة وزارة عمانية، عبر استبانة وُزّعت على ستة وثلاثين مدير تقنية وأمن معلومات. استُخدمت الاستبانة كقائمة تحقق لتقييم السياسات والممارسات الحالية لأمن المعلومات، وقياس مستوى السرية والنزاهة والتوافر. وأظهرت النتائج تطبيق معظم الوزارات لبعض الضوابط الأساسية لأمن المعلومات، إلا أن عددًا قليلاً من الوزارات المستهدفة حصل على تراخيص وشهادات دولية معتمدة. وحدد البحث بعض الفجوات في المعايير الأمنية المتقدمة، بما فيها أوجه القصور في بروتوكولات المصادقة وتشفير البيانات، واستعادة القدرة على العمل بعد الكوارث. وتؤكد النتائج على ضرورة تبني المعايير المعترف بها على الصعيد العالمي لتقييم أمن المعلومات، وبيئة تكنولوجيا المعلومات. ويوصي البحث بتنفيذ متطلبات هذه المؤسسات الدولية، وتعزيز الضوابط الأمنية لمعالجة الفجوات المحددة في البحث مما يثري فهم معايير أمن المعلومات في القطاع العام، ويقدم رؤى عملية لتعزيز الوضع الأمن التقني لهذه الوزارات.

الكلمات المفتاحية: الأمن السيبراني؛ معايير أمن المعلومات؛ حماية البيانات؛ الوزارات العمانية؛ السياسات الأمنية.

Introduction

In the digital era, the surge in online activities has necessitated robust information security (InfoSec) frameworks to safeguard sensitive data. Governments tasked with handling confidential information must evaluate and align their InfoSec practices with international standards, to ensure national security and effective governance. This study focuses on the Sultanate of Oman, assessing the implementation of InfoSec policies across its ministries against the principles of Confidentiality, Integrity, and Availability (CIA model). Increasing cyber threats highlight the timely relevance of this research, which aims to delineate Oman's cybersecurity readiness and identify areas for enhancement (Alzghaibi, 2023; Chinyemba & Phiri, 2018; Cresson Wood, 1995; Elisa, Yang, Chao, Naik, & Boongoen, 2023; Hong, Chi, Chao, & Tang, 2003; Rostami, Karlsson, & Gao, 2023).

Statement of the Problem

As digital transformation accelerates globally, cybersecurity has become a strategic priority for nations and is critical for safeguarding national security, economic stability, and public safety. The urgency of robust InfoSec practices is especially pronounced in the context of international economic relations, where the protection of critical information assets is paramount (Moon, Choi, & Armstrong, 2018; Nguyen, Koblandin, Suleymanova, & Volokh, 2022; United Nations, 2023).

Over the past few years, the Gulf Cooperation Council (GCC) region has become one of the most significant targets of malicious cybersecurity. The primary target of the GCC is the public sector (energy sector), with 50% of attempted malicious intrusions in the Middle East targeting the oil and gas sector (Hassib & Shires, 2022). Similarly, on 6 February 2020, the National News of Saudi Arabia stated that Saudi Telecom Company counters approximately 16 million phishing and 4 million malicious connectivity attempts monthly (Sharma, 2020). In 2015, a Laziok Trojan virus attack resulted in the victimisation of 25% of the UAE's energy sector, highlighting the importance of IT security in critical infrastructure industries (Nasser et al., 2018a) . In the context of Oman, the surge in digitalization has brought about significant cybersecurity challenges. In 2022, Oman thwarted three million attempted cyberattacks, a 55% increase in global threat detection, and a 242% surge in blocked malicious files from the previous year (Oman Observer, 2023).

These statistics not only reflect the heightened vulnerability of Oman's digital infrastructure, but also the urgent need for comprehensive and strategic responses to these threats. Recent reports from the Ministry of Transport, Communications, and Technology (MTCIT) in Oman reveal that, in 2021 alone, government websites were the target of nearly 251 million cyberattacks, emphasising the severe and frequent nature of these threats (MTCIT, 2022).

Despite these challenges, Oman's preparedness for cybersecurity threats, as measured by the National Cyber Security Index (NCSI), is moderate. With a current score of 45.45, Oman ranked 80th among 193 nations, underscoring significant areas for improvement. The NCSI report reveals particularly alarming deficiencies in cybersecurity policy development, where Oman scored 0%, indicating a critical gap in the foundational aspects of the national cybersecurity infrastructure (Ncsi, 2023).

Given this backdrop, this study aims to conduct a thorough assessment of the current state of InfoSec policy implementation across Omani ministries (OMs). By pinpointing specific weaknesses and identifying effective practices, this study seeks to develop informed recommendations that will enable Oman to enhance its cybersecurity measures. This approach will not only help Oman strengthen its defences against an evolving landscape of cyber threats, but also align its practices with international standards, contributing to global efforts in cybersecurity.

Research Questions

This study aimed to answer the following questions:

- What is the status of various OMs implementing InfoSec policies?
- Do these OMs implement the best practices in the CIA InfoSec model?

Significance of the Study

Establishing robust InfoSec standards is critical amid escalating cyber threats that have become more sophisticated, targeted, and economically damaging. This is especially true in developing countries, where the digital infrastructure is often more vulnerable. Such cyber incidents are now recognised as serious

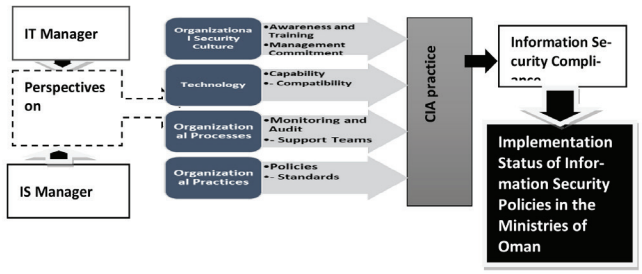
disruptions to both national and international security, catapulting cybersecurity into the global political discourse. These discussions emphasise the integral role of cybersecurity in power dynamics and international cooperation (Cavelty & Wenger, 2019).

This study is of paramount importance to the Sultanate of Oman, as it provides crucial baseline data for assessing the implementation of InfoSec policies across government ministries. It identifies both strengths and areas needing improvement, offering a clear picture of how Oman compares to international best practices. This analysis is vital for effectively enhancing digital infrastructure security, which supports Oman's broader objective of leveraging digitisation for economic and social prosperity (AlKalbani, Deng, Kam, & Zhang, 2017; Neto, Obiso, & Baayen, 2022).

Furthermore, this research maps the current risks and vulnerabilities within various ministries, enabling policymakers to develop and refine strategies to strengthen InfoSec defences. The results of this study will inform both immediate enhancements and long-term security planning, which are essential for maintaining the integrity and availability of critical government services. By advocating for continuous improvement in InfoSec practices, this study aimed to ensure that Oman remains aligned with global standards, fostering a secure and resilient digital environment.

Conceptual Framework of the Study

Figure (1): Conceptual Framework of the Study



As shown in Figure 1, Information Technology (IT) and Information Security (IS) managers of the participating OMs provided answers to InfoSec in their respective ministries. Their perceptions were collected using an expert survey instrument and the collected information was grouped into the following four categories: (a) organisational security and culture, (b) technology, (c) organisational processes, and (d) organisational practices. Awareness, training, and management commitment emphasise the organisational security culture, including training programs, planning, and other relevant activities. Technology groups focus on their capabilities and compatibility. These include infrastructure, appropriate InfoSec software, servers, and hardware.

Review of Related Studies

CIA Model

Rapid digital transformation globally necessitates robust cybersecurity measures, especially within the government sectors tasked with managing sensitive information. This literature review explores the implementation and significance of the CIA principles in governmental cybersecurity. These principles are fundamental to InfoSec practices to safeguard data against unauthorised access (Confidentiality), ensure data accuracy and protection against tampering (Integrity), and maintain system and information availability as needed (Availability). Given the increasing cyber threats, it is crucial to examine how Oman's ministries uphold these principles.

Confidentiality

Confidentiality protects sensitive information by ensuring it is accessible only to those authorised. Employing 'need-to-know' mechanisms restricts access to crucial data, thus securing personal privacy and proprietary information. For instance, Oman's MTCIT enforces strict access controls to maintain confidentiality, a practice underscored by comparative international studies highlighting the effectiveness of such measures in preventing unauthorised data disclosures (Aminzade, 2018; de Oliveira Albuquerque, García Villalba, Sandoval Orozco, de Sousa Júnior, & Kim, 2016). International comparative studies such as by and Fanelli (2016) illustrate the application of confidentiality measures, including the prevention of unauthorised data disclosure through data breaches and other cyberattack vectors.

Integrity

Integrity in governmental data systems fosters trust by ensuring that information is accurate and unaltered unless explicitly authorised. Techniques such as robust authentication protocols, error checking, and comprehensive audit trails help to maintain integrity.

Oman's adherence to stringent security policies aligns with international standards, ensuring the protection of data integrity within government systems (Guhan, Arumugham, & Janakiraman, 2019; MTCIT, 2016; Samonas & Coss, 2014)

Availability

Availability is crucial for the continuous operation of government functions, ensuring that information and services are accessible to authorised users, as needed. Measures such as network redundancy and real-time data backup are implemented to mitigate downtime and maintain service reliability, which are key to responding to prevalent threats such as denial-of-service attacks (MTCIT, 2016). These are critical for responding to network-based denial-of-service attacks, which are prevalent threats to availability (Fanelli, 2016).

As InfoSec has become increasingly important in the processing of information by government agencies, employee awareness has also become vital. Several studies have addressed InfoSec awareness activities in Oman and their interactions with various organisational activities and events (AlMindeel & Martins, 2020; Al Shabibi & Al-Suqri, 2022; Al Shammakhi & George, 2022; Al-Shanfari, Yassin, & Abdullah, 2020; Alzubaidi, 2021).

As these studies show, countries are beginning to realise the importance of security awareness at the individual level in organisations. Thus, governments have begun to work towards national and international cybersecurity policies. In countries such as the Sultanate of Oman, the initiative is to push ministries to take individual initiatives to implement their own InfoSec policies after complying with international InfoSec policies, and then adopt best practices in InfoSec based on the CIA standard. In doing so, these countries imagine that when the full implementation of InfoSec policies is achieved, the next step in developing a standard country-level cybersecurity policy will not be far behind (Arndt, 2017; Maness & Valeriano, 2018; Wessel & Vries, 2018).

International Information Security Standards

Employing international InfoSec standards bolsters an organisation's security position and capacity to effectively address security incidents. Disterer (2013) advocated that standardised terminology and adherence to best practices are instrumental in fortifying organisational security measures. AlKalbani, Deng, and Kam (2015) further strengthened the proactive stance toward InfoSec, which promotes the integration of risk assessment, continuous improvement, and monitoring and evaluation of security protocols as the cornerstones of a proactive InfoSec approach in the digital era.

Al-Hamar (2018) highlighted the importance of InfoSec and compliance within organisations in Qatar. This study explores the development of a bespoke information management framework that considers both the technical and non-technical aspects of implementing InfoSec. In particular, it focuses on the human elements of InfoSec, addressing the challenges faced by Qatari organisations, leading to the adoption of National Information Assurance (NIA) standards by the Ministry of Transport and Communications (MOTC) and the Ministry of the Interior (MOI). However, Al-Hamar noted that, despite these efforts, the full implementation of the NIA standards in Qatar experienced challenges, indicating a need for further development (Schroeder, Chappuis, & Kocak, 2014) investigated the complexities of security sector reform and hybrid security governance by examining the ways in which domestic actors in post-conflict or fragile states assimilate, adapt, or reject international security governance norms. This study considered the applicability of such standards in the Omani context, where similar InfoSec challenges exist. InfoSec standards provide a structured approach to safeguard organisational data and are typically managed by standard bodies such as the National Institute of Standards and Technology (NIST) and International Standards Organization (ISO).

This standard is critical for bodies that handle sensitive government or related data. In the face of escalating security threats, it is essential for organisations to formulate robust security policy guidelines. These help mitigate risks and preserve the integrity, availability, and confidentiality of the information. Adherence to these standards is increasingly becoming a condition for global and national legal and audit bodies, not only to manage risk, but also to avoid potential legal and reputational repercussions (Nasser, Abdualmajed, Al-Khulaidi, Mijahed, & Aljober, 2018b).

The National Institute of Standards and Technology (NIST)

The NIST plays a crucial role in setting benchmarks for cybersecurity risk management and promoting best practices through a voluntary framework developed in collaboration with the private sector. This framework is designed to be adaptable, enabling its effective implementation in diverse environments, including Oman's governmental institutions (NIST, 2023).

For example, NIST's "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" outlines a comprehensive risk management strategy for safeguarding federal information systems. This approach underscores the need to adhere to InfoSec standards and establish baseline criteria for federal information systems, which is a viewpoint supported by Junior and Santos (2015) regarding the adoption of InfoSec in public research institutions.

The NIST pioneered the development of a voluntary framework for cybersecurity risk management created through collaboration between the government and the private sector. This framework encourages a common language and set of guidelines, promoting best practices that organisations can adopt to mitigate cybersecurity threats effectively. It strategically balances economic efficiency driven by market demand, while avoiding imposing additional regulatory burdens on businesses (Bakare, 2020; Mell & Grance, 2011; Messier, 2019).

In Oman, the alignment of NIST's best practices with government bodies is crucial for assessing cybersecurity efficacy. The adoption of these standards is a testament to their international relevance and adaptability, and acts as a foundation for building robust cybersecurity defences tailored to the unique landscape of the country's governmental sector.

International Standards Organisation

ISO/IEC 27001 provides comprehensive guidelines for implementing security controls to safeguard information assets. Part of the ISO 27000 family supports organisations in managing and mitigating InfoSec threats through a process-based approach using the Plan-Do-Check-Act (PDCA) model, highlighting its global applicability and importance in establishing robust InfoSec management systems (Accerboni & Sartor, 2019; Everett, 2011).

The concept of normative isomorphism and the applicability of ISO/IEC 27002 in various organisational settings were explored by Chinyemba and Phiri (2018), who remarked that ISO/IEC 27002 often serves as a foundational model for organisations implementing extensive training and certification procedures.

In summary, the CIA model and international InfoSec standards are pivotal for enhancing cybersecurity frameworks within government sectors. Oman's efforts to align with these standards underscore a proactive approach to national cybersecurity that addresses both current challenges and prepares for future threats. The integration of these standards provides a structured approach to safeguard organisational data, which is crucial for national security and compliance with international norms (Bawono, Soetomo, & Apriatin, 2021; Faruq, 2020; Humphreys, 2016).

Gaps in the Related Work

The field of InfoSec in OMs has reached a critical point because of the proliferation of sophisticated cyber threats and the need for effective data-protection measures. This study examines this domain, and a unique perspective on assessing OMs' compliance with the CIA Triad against international standards is an important contribution to the field. The evaluation of compliance with the CIA Triad and international InfoSec standards has been discussed in some papers, but from the human or user perspective and not from the technology and organisation perspective.

By addressing the lack of research on this topic, this study provides valuable insights into the security posture of OMs, which not only contributes to existing knowledge, but also identifies critical gaps in the current InfoSec landscape in OMs.

The gaps in the literature on InfoSec policy implementation in organisations, particularly in public sector InfoSec policy implementation studies, are limited and offer opportunities for further research. The review could benefit from exploring how the CIA Triad has evolved over time with technological advancements and changing cyber threat landscapes and could offer insights into the adaptability and resilience of InfoSec practices.

Literature notes the growth of cybersecurity implementation frameworks worldwide. However, further research on national cybersecurity is required. Owing to the paucity of studies evaluating InfoSec in the Sultanate of Oman, this study aims to fill this gap.

Contribution

For IT and InfoSec managers, this research offers a roadmap for compliance with the CIA Triad and international standards. This highlights the areas of strength and concern that can guide decision-making processes and investments in technology. Multiple evaluation criteria were used to assess the CIA of information in the sample. The researcher and supervisors then analysed the results and provided feedback on strengths, weaknesses, and recommendations. This evaluation can lead to several potential contributions.

This study developed a method to identify vulnerabilities, and assessments have helped ministries to identify vulnerabilities and gaps in InfoSec policies. This study also revealed the security gaps and outdated protocols. It contributes to risk assessment by reviewing InfoSec rules to aid firms in estimating their risk. Evaluating current policies helps determine risk exposure and prioritise areas for improvement. This study opens new avenues for compliance and regulatory adherence. InfoSec policies can be used to measure an organisation's compliance with submission and regulatory criteria. This approach can identify policy alignments with industry best practices and legal requirements in order to ensure corporate compliance. Moreover, the study created a new benchmark that enables a comparison of InfoSec policies across ministries. This benchmark enables ministries to compare their approaches to industry standards and competitors, identify areas for improvement, and implement best practices.

The results of this study will aid IT and IS managers in making informed recommendations for their organisations' high-level management to improve their InfoSec policies. These recommendations may involve changes, adjustment of rules to address evolving threats, or advocating for additional security measures and protocols. In addition, evaluating an organisation's InfoSec policy can help assess its readiness to handle security incidents. A thorough review of incident response plans and procedures can enhance an organisation's ability to detect and respond to events and facilitate recovery.

Materials and Methods

This study adopts an exploratory research methodology to investigate the implementation of InfoSec policies and adherence to CIA standards within various OMs. Given the limited literature on the specific state of InfoSec policies in these ministries, an exploratory approach is necessary to establish a foundational understanding of current practices and challenges, serving as a baseline for future research.

Research Population

The research population consisted of IT and InfoSec managers from 18 of the 20 OMs, providing a broad spectrum of insights into the state of InfoSec within these government entities. These managers are pivotal in implementing and overseeing InfoSec practices because of their strategic roles and comprehensive knowledge of both national and international security standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF). Their involvement ensures that the collected data reflect the realities of organisational InfoSec management, capturing the effectiveness, challenges, and existing gaps in the ministries' InfoSec practices.

The selection of participants was based on their direct involvement in the decision-making processes concerning InfoSec, making them valuable contributors to understanding and evaluating the implementation of security measures and policies. Two ministries did not participate in the study because of confidentiality concerns regarding their data. Each participating ministry was represented by one IT and one InfoSec manager, totalling 36 participants. As suggested by Tegan (2022), to enhance comprehension of the subject matter through exploratory research, a set of inquiries is formulated and disseminated to facilitate the establishment of connections between ideas and gain a deeper understanding of the foundational aspects of the research being conducted.

Research Tools

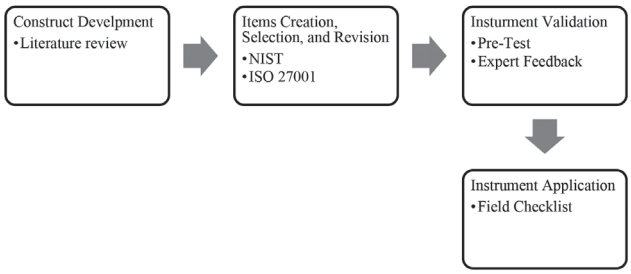
The checklist questions are Likert-type questions with response anchors described as "Do Not Know", "Not Implemented", "Partially Implemented and No Plan to Fully Implement", "Partially Implemented and Plan to Fully Implement", and "Implemented", thus capturing

the degree of implementation and planning within ministries. Furthermore, the checklist addresses the InfoSec practices of participating ministries, which are related to their implementation of the CIA Triad, including authentication, encryption, inventory, and validation.

Before distribution, the checklist was validated by field experts to ensure that it accurately reflected the study objectives and was free from biases that could lead to misinterpretation. This validation process was crucial for enhancing the reliability of the survey and the generalisability of findings. Following validation, the checklist was disseminated to respondents, and the responses were subsequently collected and analysed to assess the current state of InfoSec implementation in OMs (Boparai, Singh, & Kathuria, 2018). This methodological approach, leveraging expert knowledge and a validated survey tool, provides a robust framework for exploring the intricate dynamics of InfoSec implementation in the government sector, paving the way for targeted improvements and strategic developments in national cybersecurity policies.

The flowchart in Figure 2 visualises these stages, highlighting the methodological approach used to develop a robust instrument for this exploratory study.

Figure (2): Development and Validation of the Expert Survey Instrument



Finally, to complete the research methodology used in this study, an expert survey was combined with a literature review, meta-analysis of relevant existing studies, and supplementary interviews with experts to enrich the findings. The methodology used in this study is shown in Figure 3 below.

Figure (3): Two-Component Research Methodology of the Study

Data Collection and Analysis Methods

Respondents were requested to provide insights based on their practical knowledge and the current state of InfoSec practices in their respective organisations. The numerical data gathered through the checklist enables statistical analysis, allowing for the detection of prevailing trends, areas of non-compliance, and strengths and weaknesses in current InfoSec practices. The collected data were analysed using the SPSS statistical tool to quantify the adherence to and effectiveness of the InfoSec standards across the participating ministries. This analysis provides insights into the current state of cybersecurity practices in the government sector and enables informed recommendations to be made to improve the resilience of the InfoSec frameworks.

The questions posed to the study sample were based on the ISO 27001 checklist and the NIST. The researcher studied all the questions in these international standards separately and concluded that the methods that suit the needs and levels of InfoSec in the Sultanate of Oman should be based on multiple criteria rather than a single scale, resulting in the development of 37 questions: Confidentiality - 17 questions; Integrity - 9 questions; and Availability - 11 questions.

Discussion of the Results

The checklist on the current InfoSec conditions in OMs received 36 responses, with an average score of 3.81. This score suggests an established consensus, either strong or moderate, concerning the potential adverse consequences of unlawful data disclosure by the ministry or country. The calculated standard deviation of 0.40 suggests that the responses exhibit a relatively small dispersion from the mean value. The lowest score seen in the dataset was 3, but a significant majority of the responses (75%) were rated 4 or higher. The median and 75% score were 4 and 4, respectively. The upper limit of the scoring system was 4. The findings indicated a consensus among all participants regarding the statement, albeit to varying degrees. Table (1) summarises the major findings related to the ministry's evaluation based on the CIA Triad.

Table (1)

Ministry Evaluation Based on the CIA Triad

Ministry Code:	Confidentiality Score	Integrity Score	Availability Score
Ministry 1	3.17	2.78	4.06
Ministry 2	3.72	3.22	3.89
Ministry 3	3.22	3.33	3.00
Ministry 4	3.97	4.11	4.44
Ministry 5	4.44	4.33	3.89
Ministry 6	3.58	4.22	3.89
Ministry 7	4.67	4.28	4.78
Ministry 8	3.56	3.67	3.33
Ministry 9	4.17	3.67	3.94
Ministry 10	2.58	3.06	3.39
Ministry 11	3.19	2.94	3.00
Ministry 12	3.11	3.89	4.56
Ministry 13	3.89	3.33	4.39
Ministry 14	2.94	2.83	3.78
Ministry 15	4.17	4.22	4.78
Ministry 16	3.31	3.94	4.06
Ministry 17	3.50	3.11	3.22
Ministry 18	2.83	2.33	3.50

Table (1) depicts the following results. Confidentiality: Ministries, such as 7 and 5, have very high average scores (approximately 4.67 and 4.44, respectively), indicating robust measures for ensuring confidentiality. Meanwhile, ministries 10 and 18 have lower scores (approximately 2.58 and 2.83, respectively), signalling room for improvement.

Integrity: Ministries 15 and 7 had the highest integrity scores (roughly 4.22 and 4.28, respectively), suggesting strong data integrity measures. Ministry 18 had the lowest score (2.33), indicating the need for better data-integrity solutions.

Availability: Ministries 15 and 7 also score highly in regard to availability, with scores of 4.78 and 4.77, respectively. Ministries 11 and 3 have lower scores (approximately 3.00), indicating that data availability is a potential area for improvement.

The ministries with scores below the median in each category were as follows:

- Low Confidentiality Scores: Ministries 1, 10, 11, 12, 14, 16, 17, 18, and 3
- Low integrity score: Ministries 1, 10, 11, 13, 14, 17, 18, 2, and 3
- Low Availability Scores: Ministries 10, 11, 14, 17, 18, 2, 3, 5, and 8.

Assessing Compliance with International Information Security Standards

Insights from the OM participants revealed a trend towards only partial implementation of InfoSec's best practices and policies. This trend is significant when considering the strategic goals of Oman Vision 2040. The unified viewpoint among IT and InfoSec managers, despite their differing roles, suggests a widespread recognition of deficiencies in the adoption of international InfoSec standards. This realisation raises critical questions regarding the preparedness of OMs in the face of evolving cyber threats and their alignment with global security benchmarks.

Confidentiality

An analysis of the data on confidentiality measures in OMs shows a dichotomy in their implementation. While foundational elements, such as Virtual Local Area Networks (VLANs) and Active Directory policies, are well established and reflect a commitment to data security, the variation in implementing other confidentiality measures, such as encryption and strong authentication, indicates a need for a more comprehensive and unified approach. This disparity not only highlights areas for improvement but also poses a question: How effective are current measures in protecting the sensitive data of OMs against sophisticated cyber threats?

IT and InfoSec Managers agreed on the significance of confidentiality, echoing previous research findings (Aminzade, 2018; de Oliveira Albuquerque et al., 2016) However, the previously noted gap in encryption practices calls for a comprehensive policy. Conversely, the widespread application of active directories and group policies could provide a solid basis for future integration.

The ministries' commitment to InfoSec was reflected in their adherence to various confidentiality measures, as indicated by scores close to five. Their high adherence is particularly evident in the deployment of VLANs to protect sensitive information, implementation of Active Directory and group policies for user management, use of intrusion detection and prevention systems to thwart unauthorised access, and enforcement of role-based access control to ensure that individuals can only access information pertinent to their roles. These measures collectively signify a sophisticated and proactive approach to safeguard confidential data, suggesting that ministries have established a robust security infrastructure to effectively manage confidential information.

However, adherence levels vary. Practices such as authentication, data classification, and encryption received moderate scores between three and four, indicating room for improvement. Critical controls, such as authentication, authorisation, and accounting servers (AAA), full-disk encryption, and Privileged Access Management (PAM) systems, are still under implementation, with scores near or below 3. AAA servers and PAM were particularly inadequately addressed, with scores below 3, revealing substantial vulnerabilities that require immediate attention. Additionally, periodic updates to the inventory of confidential information, comprehensive audit logging to track security-related events, secure remote connectivity to allow safe access from outside the network, and timely revocation of access rights upon termination of an employee are essential practices that have not yet achieved optimal adherence. These practices are in place but require further refinement and consistent application to elevate the level of confidentiality assurance.

These findings highlight the need to strengthen these areas. These low scores underscore significant vulnerabilities and urge ministries to focus on enhancing these critical areas, as recommended by the literature review (Abukari & Bankas, 2020; Mattei, 2017). It is imperative to address these weaknesses promptly to mitigate the risks associated with the inadequate protection of confidential information.

The aspect of confidentiality in InfoSec is highlighted through various concerns and initiatives expressed by the participants. Challenges in encryption and PAM directly affect the ability to safeguard sensitive information. Remote working policies and adherence to international security standards are essential for ensuring confidentiality, particularly in contexts in which data exposure and compliance with security policies are significant concerns. These insights demonstrate the ongoing efforts and challenges faced in maintaining the confidentiality of information among OMs.

Integrity

The implementation of data integrity measures across various ministries reveals a heterogeneous landscape in InfoSec. This disparity, which ranges from robust policies to significant vulnerabilities, has become increasingly concerning in the light of escalating cyberattacks. The findings of this study regarding hash verification and digital signatures, which are crucial elements of data integrity, suggest opportunities for enhancement through the incorporation of BC technology, as suggested by Fanelli (2016).

Our analysis shows that the adoption level of digital signatures reflects a commitment to secure transactions. However, we found a clear correlation between strict adherence to international standards and the overall effectiveness of integrity controls. Notably, encryption has emerged as a vital area that requires significant improvement, as emphasised by participants.

In the realm of data management and security, the contrast is stark between high adherence to data modification controls, with a joint score of 4.39, and less rigorous adherence to updating access-control policies. The latter, especially in the InfoSec sector, highlights the need for more frequent reviews to address evolving security threats effectively.

Areas of moderate adherence, such as data input validation and monitoring data changes, with scores of approximately 3.5, suggest that these practices are good, but can be improved. Lower scores on unauthorised transfer monitoring indicate a pressing need for enhanced strategies to mitigate the risks associated with data exfiltration.

The alarmingly low scores for cryptographic control policies, hash verifications, and international cryptographic mechanisms indicate major vulnerabilities. These critical areas, essential for

upholding global security standards, urgently require strategic improvement. This need for overhaul is reinforced by the critical perspectives of experts such as Gordon and Hernandez (2016) likewise the observations noted in the literature review by Patel (2018).

In conclusion, these scores not only provide a measure of current compliance but also serve as a roadmap for strategic improvements. Addressing these identified vulnerabilities is crucial for strengthening the security posture of both the IT and InfoSec departments and ensuring more robust protection against the evolving landscape of cyber threats.

Availability

An investigation of the availability of the CIA Triad across OMs uncovered a spectrum of adherence levels in relation to best practices. High scores in areas such as protection against power failures and regular data backup reflect a strong commitment to maintaining service continuity. However, moderate-to-low adherence in areas such as teleworking policies and disaster recovery plans reveals gaps that could jeopardise ministries' abilities to deliver continuous public services, especially in the face of natural disasters or cyber incidents. This finding calls for an urgent review and enhancement of these critical areas to ensure service resilience and reliability, as recommended (CIS, 2023; ISO/IEC 27001, 2022; MTCIT, 2017; NIST, 2023).

The adherence scores across various IT and InfoSec practices offer insightful benchmarks for compliance. Notably, high adherence to protection against power failures signifies keen awareness and proactive measures among ministries to mitigate system disruptions. However, moderate adherence to implementing comprehensive backup and disaster recovery plans raises concerns about the overall readiness and resilience of the IT infrastructure. This contrast between different areas of adherence underscores the need for a more holistic and strategic approach to fortifying OMs' IT and InfoSec capabilities. Regarding protection from power failure, both IT and InfoSec managers showed high adherence with a notable score of 4.72. This demonstrates the strong commitment to safeguard systems against power-related disruptions. Backup policies and processes are also given due importance, with IT scoring slightly higher at 4.67, compared to the InfoSec managers at 4.06, indicating a robust approach to data preservation in the event of system failures.

The high scores for regular automatic data backups reflect commendable practices in OMs, showcasing a forward-thinking approach to data security. However, relatively low scores in areas such as secure remote connectivity and periodic reviews of backup effectiveness indicate potential vulnerability. These findings suggest that, while OMs are adept at certain aspects of data preservation, there is room for improvement in ensuring comprehensive data security, particularly in a rapidly evolving digital landscape.

Areas with moderate adherence, such as periodic checks of the restoration process, highlight critical gaps in the current OMs fossil practices. The varying scores between the IT and InfoSec managers in this domain indicate a potential disconnection or uneven emphasis on certain security practices. This inconsistency calls for a unified approach to InfoSec, ensuring that all aspects from the data backup to the restoration process receive equal and adequate attention.

Low adherence to the development of robust teleworking policies and standards, especially those critical to the current landscape of remote work, is a glaring concern. This gap not only highlights a reactive approach to emerging work trends but also suggests potential risks in data security as remote working becomes more prevalent. Addressing this gap is essential for OMs to adapt to new ways of working while maintaining stringent security standards, with scores just below the moderate score of 2.94. The adherence levels for disaster recovery and business continuity plans underscore the significant vulnerability of OMs. Considering the pivotal role that these plans play in organisational resilience, especially in regions prone to natural disasters and cyber threats, low scores are alarming. This finding suggests an urgent need for OMs to prioritise the development and implementation of robust disaster recovery strategies, not only as a compliance measure but also as a critical component of their overall risk management and security framework. This indicates a significant area in which attention is required to fortify unforeseen events in contrast to the studies mentioned in the literature review (CIS, 2023; Fanelli, 2016; ISO/IEC 27001, 2022; NIST, 2023; Shave, 2018).

The availability of InfoSec among the government entities in Oman has been addressed through various strategic and operational measures. The establishment of a centralised government entity, development of robust disaster recovery and business continuity plans, and implementation of secure remote working policies are all considered crucial for ensuring the continuous availability of services. Challenges in implementing security standards and concerns regarding centralised data centres as single points of failure also directly impact service availability. These insights demonstrate the ongoing efforts and complexities involved in ensuring that critical systems and data remain accessible and functional in the face of various challenges and disruptions.

In summary, although foundational availability practices are in place, there is a paramount need for a unified and strategic approach to cybersecurity in OMs. Such an approach is essential not only to meet and surpass global InfoSec benchmarks but also to align with the strategic direction of Oman Vision 2040. The findings underscore the national importance of bolstering cybersecurity infrastructure, suggesting that addressing these gaps is not just a matter of organisational efficiency, but also of national security and resilience.

Conclusion and Recommendations

Based on the analysis and generalisations of the findings, it is clear that OMs have started implementing best practices to stay current with the latest developments in InfoSec. However, it is also evident that more work needs to be done to achieve the full implementation of these policies. The results indicate that plans are underway to achieve 100% compliance with the CIA Model of InfoSec, but there are areas that require serious attention, such as implementing a server for AAA, full disk encryption, PAM, an international cryptographic mechanism for enterprise data, and functional disaster recovery and business continuity plans. The collected data show that, while ministries are making progress in many areas of InfoSec, they must prioritise areas that have been overlooked to achieve full policy implementation. As this study failed to obtain the full participation of all ministries, governments, and private entities, it is recommended that a follow-up study be conducted for all other ministries that were not included in the study and that their responses be compared with the data collected from this study to further determine the status of the implementation of InfoSec policies concerning the entire population of ministries in the Sultanate of Oman.

Future work

Based on these conclusions, the following recommendations are proposed for future research: A thorough gap analysis of the ministries involved in identifying areas that require enhancement regarding the execution of InfoSec policies. This analysis can help to prioritise areas that require prompt attention and resource allocation.

Participating ministries should implement targeted training and awareness programs that focus on areas requiring improvement. These programs can enhance personnel's cognitive abilities and proficiency in optimal InfoSec protocols, while fostering heightened awareness of the significance of adhering to the CIA model. Technical implementation assessments were conducted to evaluate the effectiveness of the mechanisms and the best practices of the ministries involved. The evaluation can detect any vulnerabilities or weaknesses in the current systems and provide recommendations for improvement. The objective involves thoroughly evaluating the InfoSec policies currently in place within the concerned ministries to identify any gaps or shortcomings that may require revision or improvement. This measure can guarantee that policies conform to the present industry norms and upcoming risks.

A subsequent investigation should be conducted to include all ministries excluded from the previous examination of InfoSec policy implementation. This comprehensive approach will provide a more complete picture of the current state of InfoSec in all ministries of the Sultanate of Oman. A comparative analysis of recent research and primary data will help to identify patterns and evaluate advancements over time. It is recommended that ministries collaborate and share information to foster continuously improving culture. A systematic process for regular audits and monitoring should be implemented to ensure ongoing adherence to the InfoSec policies, including periodic evaluations, vulnerability scans, and incident-response exercises. Decentralised technology should be created to store

and disseminate information on security policies and procedures. The implementation of the current security standards is facilitated by ministries through this measure.

Develop a systematic approach to periodically evaluate the efficacy of InfoSec policies. This measure facilitates the identification of any domain for which the policies require updating or enhancement.

References

Abukari, A., & Bankas, E. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific & Engineering*. *11*(Issue 4). Retrieved from https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond/citations.

Accerboni, F., & Sartor, M. (2019). ISO/IEC 27001. In *Quality management: Tools, methods and standards*. https://doi.org/10.1108/978-1-78769-801-720191015

Al Shabibi, A. M., & Al-Suqri, M. N. (2022). Cybersecurity awareness among students during the COVID-19 digital transformation of education: A case study at the Muscat (Oman) schools. In *The Sharjah international conference on education in post COVID-19* (pp. 39–51). Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-99-1927-7_4

Al Shammakhi, B., & George, L. (2022). Analysis of the awareness of the sultanate of Oman government's social protection coverage program among self-employed orange taxi drivers. *Journal of Positive School Psychology*. Retrieved from https://journalppw.com/index.php/jpsp/article/view/12127.

Al-Hamar, A. (2018, January 1). Enhancing information security in organisations in Qatar. Retrieved from https://repository.lboro.ac.uk/articles/thesis/Enhancing_information_security_in_organisations_in_Qatar/9406472?file=170.

AlKalbani, A., Deng, H., & Kam, B. (2015). *Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure*. Paper presented at the Pacific Asia Conference on Information Systems (PACIS) *CORE Reader*. Retrieved from https://core.ac.uk/reader/301365270.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management*. https://doi.org/10.1515/dim-2017-0006

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People*, *34*(2), 770–788. https://doi.org/10.1108/itp-06-2019-0269.

Al-Shanfari, I., Yassin, W., & Abdullah, R. (2020). Identify of factors affecting information security awareness and weight analysis process.*International Journal of Engineering and Advanced Technology (IJEAT)*, *9*(3), 534–542. https://doi.org/10.35940/ijeat.C4775.029320.

Alzghaibi, H. A. (2023). An examination of large-scale electronic health records implementation in primary healthcare centers in Saudi Arabia: A qualitative study. *Frontiers in Public Health*. https://doi.org/10.3389/fpubh.2023.1121327

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016.

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, *2018*(5), 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Arndt, T. (2017). International Organization for Standardization. In *Lexikon der Medizinischen Laboratoriumsdiagnostik* (pp. 1–1). https://doi.org/10.1007/978-3-662-49054-9_1603-1

Bakare, A. A. (2020). *A methodology for cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model* [Doctoral dissertation, University of Cincinnati]. http://rave.ohiolink.edu/etdc/view?acc_num=ucin1583247043269043

Bawono, M. W. A., Soetomo, M. A., & Apriatin, T. (2021). Analysis correlation of the implementation framework COBIT 5, ITIL V3 and ISO 27001 for ISO 10002 customer satisfaction. *Acmit Proceedings*. https://doi.org/10.33555/acmit.v7i1.105

Boparai, J. K., Singh, S., & Kathuria, P. (2018). How to design and validate a questionnaire: A guide. *Current Clinical Pharmacology*, *13*(4), 210–215. https://doi.org/10.2174/1574884713666180807151328.

Chinyemba, M. K., & Phiri, J. (2018). An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector. *Journal of Computer Science*. https://doi.org/10.3844/jcssp.2018.1389.1400

CIS. (2023). CIS critical security controls. (2023). Retrieved from https://www.cisecurity.org/controls.

Cresson Wood, C. (1995). The Charles Cresson Wood file. *Information Management & Computer Security*, *3*(4), 23–26. https://doi.org/10.1108/09685229510097278

de Oliveira Albuquerque, R., García Villalba, L. J., Sandoval Orozco, A. L., de Sousa Júnior, R. T., & Kim, T. H. (2016). Leveraging information security and computational trust for cybersecurity. *Journal of Supercomputing*, *72*(10), 3729–3763. https://doi.org/10.1007/s11227-015-1543-4

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*. https://doi.org/10.4236/jis.2013.42011

Cavelty, M. D., & Wenger, A. (2019). Cyber security meets security politics: complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Elisa, N., Yang, L., Chao, F., Naik, N., & Boongoen, T. (2023). A secure and privacy-preserving e-government framework using blockchain and artificial immunity. *IEEE Access*. https://doi.org/10.1109/access.2023.3239814

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(11)70005-7

Fanelli, R. (2016). Cyberspace offense and defense. *Journal of Information Warfare*, *15*(2), 53–65. https://search.proquest.com/docview/1968022288?accountid=27965

Faruq, B. A. (2020). Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT services and Security Management system. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3514–3531. https://doi.org/10.30534/ijatcse/2020/157932020.

Gordon, A., & Hernandez, S. (2016). *The official (ISC)2 guide to the SSCP CBK: 9781119278634: Computer Science Books @ Amazon.com*. Sybex. Retrieved from https://www.amazon.com/Official-ISC-Guide-SSCP-CBK/dp/1119278635.

Guhan, S., Arumugham, S., & Janakiraman, S. (2019). A trio approach satisfying CIA triad for medical image security. *A trio approach satisfying CIA triad* (January). https://doi.org/10.1007/978-3-030-00665-5.

Hassib, B., & Shires, J. (2022). Cybersecurity in the GCC: From economic development to geopolitical controversy. *Middle East Policy*, *29*(1). https://doi.org/10.1111/mepo.12616

Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard, Second edition* (second). Retrieved from https://uk.artechhouse.com/Implementing-the-ISOIEC-27001-ISMS-Standard-Second-Edition-P1790.aspx.

ISO/IEC 27001. (2022). Retrieved from https://www.iso.org/standard/27001.

Junior, A. E. de A., & Santos, E. M. d. (2015). Adoption of information security measures in public research institutes. *Journal of Information Systems and Technology Management*. https://doi.org/10.4301/s1807-17752015000200006

Maness, R. C., & Valeriano, B. (2018). International cyber conflict and national security. In D. S. Reveron, N. K. Gvosdev, & J. A. Cloud (Eds.), *Oxford handbook of national security* (Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190680015.013.25

Mattei, T. A. (2017). Privacy, confidentiality, and security of health care information: Lessons from the recent WannaCry cyberattack. *World Neurosurgery*. https://doi.org/10.1016/j.wneu.2017.06.104

Mell, P. M., & Grance, T. (2011, January). *The NIST definition of cloud Computing*. https://doi.org/10.6028/nist.sp.800-145.

Messier, R. (2019). CEH V10 certified ethical hacker study guide. *Wiley.com*. Retrieved from https://www.wiley.com/en-gb/CEH+v10+Certified+Ethical+Hacker+Study+Guide-p-9781119533269.

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, *40*. https://doi.org/10.1016/j.ijinfomgt.2018.01.001

MTCIT. (2016). *Information Technology Authority*. http://www.ita.gov.om/ITAPortal/ITA/

MTCIT. (2017). *Data and information systems security classification mapping*. https://www.mtcit.gov.om/ITAPortal/Pages/Page.aspx?NID=2038&PID=7415&LID=30

MTCIT. (2022). *Ministry of Transport, Communications and Information Technology*. Retrieved from https://www.mtcit.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=144.

Nasser, Abdualmajed A. Al-Khulaidi, Mijahed N. Aljober. (2018b). "Measuring the Information security maturity of enterprises under uncertainty using Fuzzy AHP", International Journal of Information Technology and Computer *Science (IJITCS)*. https://doi.org/10.5815/ijitcs.2018.04.02.

Nasser, M., Ahmad, R., Yassin, W., Hassan, A., Zainal, Z., Salih, N., & Hameed, K. (2018a). Cyber-Security Incidents: A review cases in Cyber-Physical systems. *International Journal of Advanced Computer Science and Applications*, *9*(1). https://doi.org/10.14569/ijacsa.2018.090169.

Ncsi. (2023). *Oman*. National Cyber Security Index. Retrieved September 11, 2023, from https://ncsi.ega.ee/country/om/

Neto, I., Obiso, M., & Baayen, M. (2022). How tailored national cybersecurity strategies enable safe, inclusive and sustainable digital development. *World Bank Blogs*. https://blogs.worldbank.org/digital-development/how-tailored-national-cybersecurity-strategies-enable-safe-inclusive-and

Nguyen, T. A., Koblandin, K., Suleymanova, S., & Volokh, V. (2022). Effects of “digital” country’s information security on political stability. *Journal of Cyber Security & Mobility*, *11*(1). https://doi.org/10.13052/jcsm2245-1439.1112

NIST. (2023). Retrieved from https://www.nist.gov/.

Oman Observer. (2023). Over 12m cyber threats thwarted in Oman in 2022. https://www.omanobserver.om/article/1139857/oman/over-12m-cyber-threats-thwarted-in-oman-in-2022

Patel, V. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal*, *25*(4), 1398–1411. https://doi.org/10.1177/1460458218769699.

Rostami, E., Karlsson, F., & Gao, S. (2023). Policy components – a conceptual model for modularizing and tailoring of information security policies. *Information & Computer Security*, *31*(3), 331–352. https://doi.org/10.1108/ICS-10-2022-0160.

Samonas, S., & Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. Retrieved from https://www.jissec.org/Contents/V10/N3/V10N3-Samonas.html.

Schroeder, U., Chappuis, F., & Kocak, D. (2014). Security sector reform and the emergence of hybrid security governance. *International Peacekeeping*. https://doi.org/10.1080/13533312.2014.910405

Sharma, A. (2020). Saudi Telecom working on strategy to safeguard 5G network from cybercriminals. *The National News*. https://www.thenationalnews.com/business/technology/saudi-telecom-working-on-strategy-to-safeguard-5g-network-from-cyber-criminals-1.975128.

Shave, L. (2018). The CIA of security and access. Retrieved from https://search.informit.org/doi/abs/10.3316/informit.706387331405083.

Tegan, G. (2022). *Exploratory research/definition/guide/and examples*. Scribbr. https://www.scribbr.com/methodology/exploratory-research.

United Nations. (2023). *Fighting the industrialization of cyber crime*. https://www.un.org/en/chronicle/article/fighting-industrialization-cyber-crime.

Wessel, R. I., & Vries, H. J. d. (2018). Business impacts of international standards for information security management. Lessons from case companies. *Journal of ICT Standardization*. https://doi.org/10.13052/jicts2245-800x.112.