Introduction.....2

Importance of Information Security Governance 3
security management 5
Risk assessment Risk management in Information Security 5
Risk assessment in information security involves several steps. 5
Cybersecurity framework 7
National Institute of Standard (NIST) 7
COBIT 9
ITIl or Information Technology Infrastructure Library, is a framework that provides best practices for managing IT services. 10
Implementation 10
Encryption 11
The future 12
Contingencies Planning 12
In conclusion, ... 12
References 14
What is Qualitative Risk Analysis? 19
Make Organizational Charts in PowerPoint with Templates from SmartDraw 19

Data security Assignment

Importance of Information Security Governance

Information security governance is not just an IT issue; it requires the commitment of the entire organisation's workforce to uphold their responsibility in protecting valuable information assets. To achieve effective information security governance, organisations must establish an environment that fosters management commitment, leadership, organisational structures, user awareness, and commitment. Policies, procedures, technologies, and compliance enforcement mechanisms must work together to ensure that the confidentiality, integrity, and availability of electronic assets are maintained. This comprehensive approach to information security governance will help in addressing the increasing challenges posed by cyber threats and risks. Furthermore, it is vital for organizations to learn from global initiatives for cybersecurity.

In today's digital age, information has become one of the most valuable assets for organisations. The ISO 27799 is based on ISO 27001 and ISO 27002 which ensure that an appropriate level of information security management is in place to protect these assets (Sari K, P. et al., 2022) as illustrated in the figure Below.

(blogarama.com 2021)

With the increase in cyber threats and data breaches, organisations need to implement effective strategies, policies, and standards to safeguard their information assets. These standards help organizations ensure that they have appropriate security measures in place to protect their information, enabling best practices to be embedded in their procedures (Dutta, N., 2022)

By adopting ISO 27001 and ISO 27002, organizations can demonstrate their commitment to information security and gain the trust of their stakeholders as well complies with Law

and regulations. Even so complying on its own shouldn't be the organisation's main goal. ISO 27001 is a comprehensive standard that sets out the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System within the context of the organisation. ISO 27001 focuses on identifying and managing information security risks, vulnerabilities, and threats to organisational assets (Safitri, M, E. et al., 2021) .ISO 27002, on the other hand, provides guidance on implementing information security controls based on best practices (Safitri, M, E. et al., 2021).

security Management

Information security management encompasses the development and implementation of strategies, policies, and standards to protect an organization's information assets. These strategies, policies, and standards are designed to identify and mitigate potential risks and vulnerabilities, ensuring the confidentiality, integrity, and availability of information. Effective information security management involves several key components, including:

Risk assessment Risk management in Information Security

Risk assessment is a critical component of information security. It involves identifying, analysing, and evaluating potential risks to an organisation's information assets. Risk assessment helps organizations understand the vulnerabilities and threats that could impact their information security. By conducting a risk assessment, organizations can prioritize their efforts and allocate resources effectively to mitigate and manage these risks. (Teixeira, A, G., Silva, d, M, M. and Pereira, R., 2019)

Risk assessment in information security involves several steps.

First, organizations need to identify the assets that need to be protected. These assets can include sensitive data, systems, networks, infrastructure, and intellectual property. Once the assets are identified, organisations need to assess the potential threats that could compromise the confidentiality, integrity, and availability of these assets. (ISO/IEC 27002:2022 - Information security, cybersecurity and privacy ..., 2022)

This can include threats such as unauthorised access, data breaches, malware attacks, physical theft, and natural disasters. After identifying the threats, organizations need to assess the vulnerabilities that exist within their systems and processes. This involves evaluating the weaknesses and potential points of failure in their information security

controls, such as outdated software, weak passwords, lack of employee awareness, or insufficient physical security measures. (Park, S. and Lee, K., 2014)

This involves evaluating the effectiveness of security measures, such **as access controls, network defenses, and encryption protocols.** Based on the identified threats and vulnerabilities, organizations can then determine the **likelihood** and impact of potential security incidents. (Goosen, R. and Rudman, R., 2013)

Qualitative risk assessment involves assessing risks based on severity or impact, likelihood or probability, and the effectiveness of existing controls. As shown in the following table

Likelihood		Very Likely	Likely	Unlikely	Highly Unlikely
Severity	Fatality	High	High	High	Medium
	Major	High	High	Medium	Medium
	Minor	High	Medium	Medium	Low
	Negligible	Medium	Medium	Low	Low

(Safety control, 2023)

Quantitative risk assessment, on the other hand, involves assigning numerical values to risks and calculating their potential financial impact. Once the risks have been assessed, organisations can prioritise them based on their significance and likelihood (Chuma, G, K. and Ngoepe, M., 2021)

These strategies can include implementing firewalls and intrusion detection systems, conducting regular security audits, training employees on information security best practices, and backing up data regularly to ensure its availability in case of a security incident (Winter, d, J. et al., 2019). Furthermore, organizations should develop clear

information security policies and standards that outline the required security measures and behaviours for employees, contractors, and third-party vendors. ISO 27001 provides a framework for establishing, implementing, maintaining, and continuously improving an information security management system. (Krekora-Zając, D., Marciniak, B. and Pwlikowski, J., 2021)

Cybersecurity framework

A comprehensive cybersecurity framework is crucial for organizations to effectively manage information security risks. This framework should include:

"Identifying threats and vulnerabilities" (Chajduga, T., Ingaldi, M. and Klimecka-Tatar, D., 2021) Establishing incident response plans and procedures to effectively respond to security incidents - Conducting regular audits and assessments to ensure compliance with policies and standards - Providing ongoing training and education for employees to promote awareness and understanding of information security best practices (Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review, 2021) With the increasing reliance on technology and the rise of cyber threats, organizations must have a robust information security strategy in place.

National Institute of Standard (NIST)

offers a widely recognized cybersecurity framework that provides guidelines for organizations to manage and improve their cybersecurity posture. This framework consists of five core functions:

- Identify,
- Protect,
- Detect,
- Respond,
- Recover. (Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review, 2021)

The "Identify" function involves understanding and managing cybersecurity risks to systems, assets, data, and his includes conducting thorough risk assessments, identifying critical assets and their vulnerabilities, and establishing processes to manage those risks effectively.

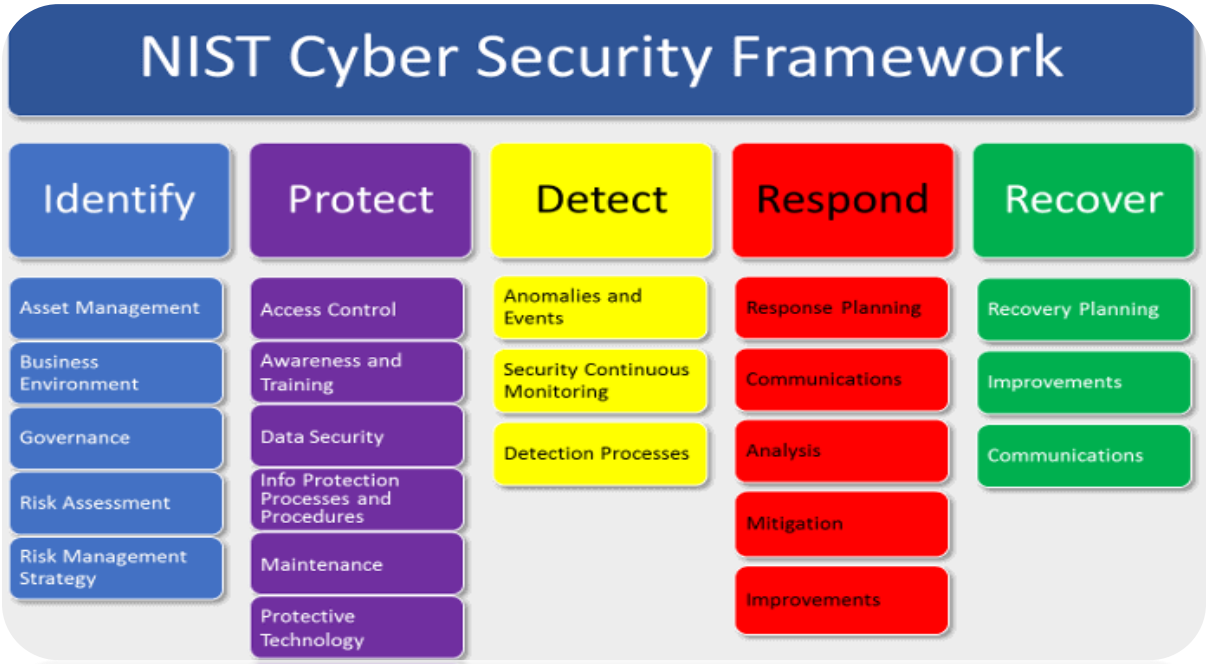
The "Protect" function focuses on implementing safeguards to ensure the security and resilience of systems and data. detect potential threats and vulnerabilities by

implementing security controls such as firewalls, intrusion detection systems, and antivirus software. (Krekora-Zając, D., Marciniak, B. and Pawlikowski, J., 2021)

The "Detect" function focuses on continuously monitoring and identifying cybersecurity events to enable timely detection of potential security incidents. This may involve implementing security monitoring tools, conducting regular vulnerability assessments, and analyzing network traffic for signs of malicious activity. (Chajduga, T., Ingaldi, M. and Klimecka-Tatar, D., 2021)

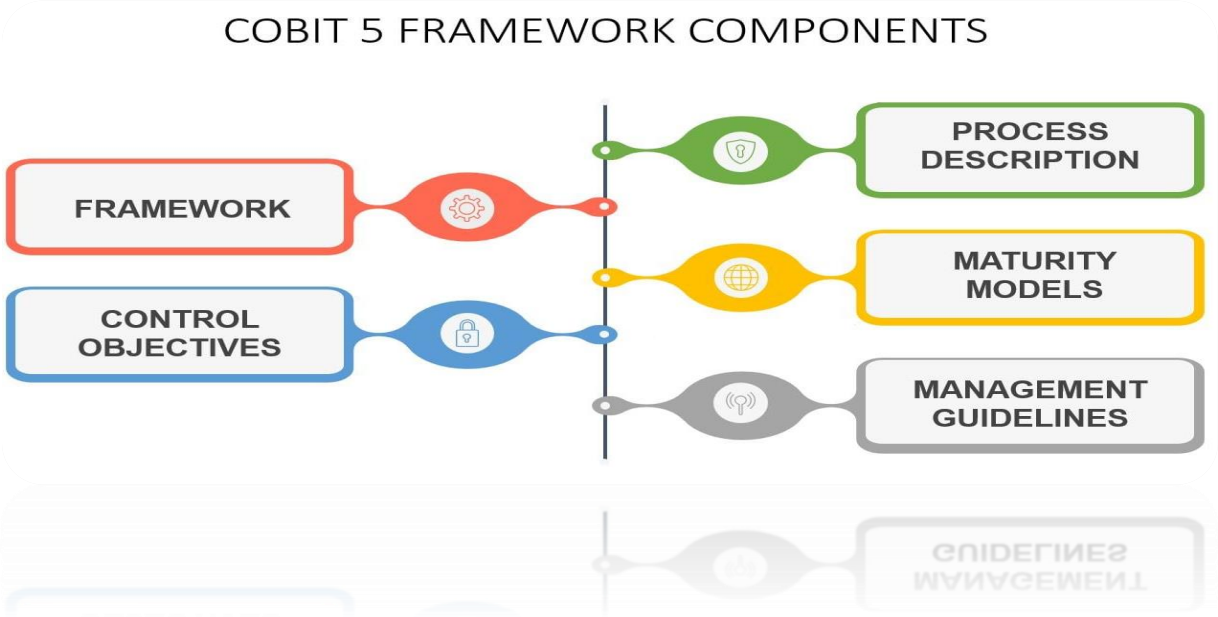
The "Respond" function involves developing and implementing an effective incident response plan to contain and mitigate the impact of a security incident. This includes establishing clear roles and responsibilities, defining communication protocols, and conducting drills and exercises to ensure a swift and coordinated response (Goosen, R. and Rudman, R., 2013).

The "Recover" function focuses on restoring normal operations and services after a security incident, minimizing the impact on the organization and its stakeholders. This may involve conducting forensic investigations, restoring backups of compromised data, and implementing measures to prevent similar incidents in the future. (Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review, 2021) .



COBIT

The Control Objectives for Information and Related Technologies is a framework developed by ISACA to help organizations effectively manage and control their information technology resources. COBIT provides a comprehensive set of best practices and standards for IT governance, risk management, and information security (Nejabatkhah, F. et al., 2020) COBIT focuses on aligning IT objectives with business goals, ensuring the effective use of IT resources, and providing a framework for managing risks and improving processes related to information security. COBIT includes guiding conducting risk assessments, implementing control objectives, and monitoring and measuring the effectiveness of controls (Goosen, R. and Rudman, R., 2013).



One of the key elements of COBIT is its focus on establishing and maintaining a strong control environment. This includes identifying and implementing the necessary controls to mitigate risks, regularly assessing the effectiveness of these controls, and monitoring compliance with relevant policies and standards. Another important aspect of COBIT is its emphasis on continuous improvement. (Goosen, R. and Rudman, R., 2013)

ITIl or Information Technology Infrastructure Library, is a framework that provides best practices for managing IT services.

The IT Infrastructure Library is a framework that provides best practice guidelines for IT service management. ITIL focuses on the delivery of high-quality IT services that meet the needs of the business. This includes defining and documenting IT service processes, establishing service level agreements, and continuously improving service delivery through monitoring and measurement. (Winter, d, J. et al., 2019) ITIL also emphasises the importance of incident management, problem management, and change management processes to ensure the efficient and effective resolution of IT issues and the implementation of changes while minimising risks. (Goosen, R. and Rudman, R., 2013)

In the context of information security, COBIT and ITIL can be valuable frameworks for organizations to establish effective governance and management practices (Sahd, L. and Rudman, R., 2016). These frameworks provide guidance on developing clear policies and good practices for information security and addressing risk management and control objectives. (Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review, 2021)

Implementation

Based on the scenario for this assignment, the organisation needs to comply with health standards. Implementing ISO 27001 to address Bring Your Own Device concerns is an important step in ensuring data security and privacy within an organisation. Assessing the current BYOD policies and practices against the requirements of ISO 27001 is essential for identifying gaps and areas for improvement. In this process, it is crucial to evaluate how well the existing BYOD policies align with the controls and requirements set forth in ISO 27001.

This includes assessing the access controls, encryption methods, device management, and user awareness programs in place to mitigate the risks associated with BYOD. "*According to the HIPAA (2013), 91% of cyber-attacks in the healthcare industry come from phishing emails. Hackers send phishing emails to a healthcare employee along with a seemingly legitimate reason for revealing their login credentials*" (Rothstein and Talbott 2015) found that approximately 25 million requests are made annually in the United States for access to health records. Concerns about the security of patients' health data were also reported by respondents in Denmark, Germany, and New Zealand (Zurita & Nøhr 2007)

Furthermore, the company should involve identifying any potential non-compliance with ISO 27001 and developing a plan to address these issues. This may involve updating policies, implementing new security measures, or providing additional training for employees on BYOD best practices. (Mayayise, O, T., 2021).

By conducting a thorough assessment as per the guidelines of ISO 27001, the company can ensure that their BYOD environment meets the necessary information security standards and protocols, mitigating potential risks and safeguarding sensitive data. By implementing ISO 27001 for BYOD, organisations can effectively address security risks and protect sensitive data. HIPAA compliance should also be considered when implementing BYOD in the healthcare industry. "Bring your own device " policy. risk associated with BYOD are mitigated and sensitive data is protected through the implementation of ISO 27001 security standards.

These standards provide a framework for addressing BYOD concerns by incorporating best practices in information security management. The implementation of ISO 27001 for BYOD ensures that the organisation follows internationally recognized standards and best practices in managing information security. the cloud services provided by the organization is also a relevant factor to consider when assessing the implementation of ISO 27001 for BYOD. Chhana Bhai and Holt (2007:8) found that 202 participants (73.3%) expressed concerns about the compatibility issues, privacy, and security of patients' data. According to Papoutsi, (Reed, Marston,et al (2023)

Encryption

Encryption plays a vital role in ensuring the security and confidentiality of information. Encryption is the process of encoding data or ensuring that the information is structured to be accessed in a restricted manner. decrypted by authorized individuals who have the appropriate encryption key. (Chajduga, T. et al 2021) Encryption algorithms use complex mathematical computations to transform plain text into cipher text, making it unreadable to anyone without the proper decryption key. Encryption helps protect sensitive data from unauthorized access or interception, especially when data is transmitted over networks or stored in vulnerable databases. In the context of information security, organizations often rely on encryption to safeguard their valuable data from unauthorized access or interception. To effectively implement encryption, organizations should establish clear encryption policies and standards that outline the specific algorithms, key lengths, and encryption methods to be used (Shang, Y., 2022) in different scenarios. These policies and

standards should also address key management practices, such as key generation, distribution, storage, and rotation, to ensure the ongoing effectiveness of encryption measures. (Winter, d, J. et al., 2019)

The future

The future of information security is constantly evolving to keep up with the ever-changing landscape of technology and cyber threats. Organizations will need to stay proactive and adaptive in their approach to information security, continuously assessing and managing risks, as well as keeping up with emerging technologies (Ivanova, R., 2022) and trends in order to effectively protect their valuable data. Furthermore, with the increasing adoption of Internet of Things technology in various sectors, including smart cities, there are new challenges that need to be addressed in information system security management. One such challenge is the sheer volume of data generated by IoT devices in smart cities. This data needs to be securely managed and protected from unauthorised access or manipulation. (A Guide to the Updated ISO/IEC 27002:2022 Standard, Part 2 - ISACA, (2021)

Contingencies Planning

Contingencies planning is an essential aspect of information security strategy. It involves developing and implementing plans to address potential risks and threats that could impact the confidentiality, integrity, or availability of information. These plans often include measures to mitigate the impact of cyber-attacks, natural disasters, system failures, or other unforeseen events. Contingencies planning should include steps to identify critical assets and systems, assess potential vulnerabilities and their likelihood of occurrence, prioritize risks based on their potential impact and likelihood, and develop response strategies and recovery plans.

In conclusion,

Information security is of utmost importance in today's dynamic and interconnected world. Organisations must prioritise the confidentiality, integrity, and availability of their data to protect against cyber threats. To achieve effective information security, organisations should implement robust strategies, establish comprehensive policies and standards, conduct regular risk assessments, and employ encryption techniques to

safeguard sensitive data. They should also stay informed about emerging technologies and evolving threats to continuously update and improve their security measures. In summary, information security is a critical requirement for organisations to safeguard their valuable data from security threats (Gyllensten, K., Törner, M. and Pousette, A., 2022).

Overall, information security is a complex and multifaceted process that requires a comprehensive approach. Organizations must adopt a strategic mindset, establish clear policies and standards, and regularly assess and manage risks to ensure the confidentiality, integrity, availability, and accountability of their information assets. Thus, information security is a vital aspect of any organization's operations. It is crucial for organizations, especially government organizations, to prioritize information security as it directly impacts the continuity and growth of the organization (AlMindeel, R. and Martins, T, J., 2020).

However, while information security is undoubtedly important, some argue that organizations should be cautious about prioritizing security measures over innovation and efficiency. Overly stringent security protocols can sometimes hinder collaboration and the adoption of new technologies, ultimately limiting an organization's ability to stay competitive in a rapidly evolving market. Additionally, dedicating significant resources to information security can strain budgets and divert attention from other crucial aspects of business operations.

Moreover, critics of extensive information security measures argue that the resources allocated to cybersecurity could be better utilized in areas that directly contribute to an organization's growth and success. For example, investing in research and development, marketing initiatives, or employee training programs may yield higher returns on investment compared to allocating resources solely towards information security

While it is valid to consider the trade-offs between prioritizing information security and other business initiatives, it is important to recognize that breaches in cybersecurity can be significantly detrimental to an organization. A single security breach can result in costly legal ramifications, damage to reputation, and loss of customer trust and loyalty. These repercussions can far outweigh the initial investment in robust information security measures.

Furthermore, in today's interconnected world, where cyber threats continue to evolve, organizations must recognize that achieving a balance between security and innovation is paramount. Embracing innovative technologies while ensuring robust security measures

are in place, is not mutually exclusive. By adopting a proactive approach to information security, organizations can mitigate risks, protect their valuable information assets, and maintain the trust of their customers and stakeholders

References

Bolek, V. et al. (2016) Factors Affecting Information Security Focused on SME and Agricultural Enterprises. Available at: https://scite.ai/reports/10.7160/aol.2016.080404. (Accessed 12 November 2023)

Sari, K, P. et al. (2022) Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. Available at: https://doi.org/10.3390/healthcare10122531. (Accessed 14 November 2023)

Dutta, N. (2022) A Tracking Solution of IT Assets and Resources Management. Available at: https://doi.org/10.47191/ijmcr/v10i7.08. (Accessed 27 November 2023)

Safitri, M, E. et al. (2021) An Analysis of Physical and Environmental Security in Communication and Information Department Mojokerto. Available at: https://doi.org/10.1051/e3sconf/202132804012.
Shaping the Future Through Standardization (2020). Available at: https://scite.ai/reports/10.4018/978-1-7998-2181-6. (Accessed 12 November 2023)

Safitri, M, E. et al. (2021) An Analysis of Physical and Environmental Security in Communication and Information Department Mojokerto. Available at: https://scite.ai/reports/10.1051/e3sconf/202132804012. (Accessed 11 December2023)

Pedreira, V., Barros, D. and Pinto, P. (2021) A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. Available at: https://doi.org/10.3390/s21155189. (Accessed 19 December2023)

Teixeira, A, G., Silva, d, M, M. and Pereira, R. (2019) The critical success factors of GDPR implementation: a systematic literature review. Available at: https://doi.org/10.1108/dprg-01-2019-0007. (Accessed 11 December2023)

Ivanova, R. (2022) INFORMATION AND THE PROTECTION OF ITS INVIOLABILITY IN THE CONDITIONS OF DIGITALIZATION OF THE EDUCATION IN THE UNIVERSITIES IN BULGARIA. Available at: https://doi.org/10.51508/intcess.202260. (Accessed 20 December2023)

Nejabatkhah, F. et al. (2020) Cyber-Security of Smart Microgrids: A Survey. Available at: https://doi.org/10.3390/en14010027. (Accessed 20 December 2023)

ISO/IEC 27002:2022 - Information security, cybersecurity and privacy ... (2022). Available at: https://www.iso.org/standard/75652.html. (Accessed 28 December2023)

Park, S. and Lee, K. (2014) Advanced Approach to Information Security Management System Model for Industrial Control System. Available at: https://doi.org/10.1155/2014/348305. (Accessed 11 December2023)

Goosen, R. and Rudman, R. (2013) The development of an integrated framework in order to address King III's IT governance principles at a strategic level. Available at: https://doi.org/10.4102/sajbm.v44i4.171. (Accessed 11 December2023)

Chuma, G, K. and Ngoepe, M. (2021) Security of electronic personal health information in a public hospital in South Africa. Available at: https://doi.org/10.1080/19393555.2021.1893410. (Accessed 21 December2023)

Winter, d, J. et al. (2019) Will vehicle data be shared to address the how, where, and who of traffic accidents?. Available at: https://doi.org/10.1186/s40309-019-0154-3. (Accessed 11 December 2023)

Krekora-Zając, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on the GDPR art.40. Available at: https://doi.org/10.3389/fgene.2021.711614. (Accessed 11 November 2023)

Chajduga, T., Ingaldi, M. and Klimecka-Tatar, D. (2021) Management of the Documentation Release by the Programmable Electrical Energy Flow-Individually Made Machine Called Documentomat. Available at: https://doi.org/10.3390/en14175304. (Accessed 18 November 2023)

of Smart Cities: A Review (2021). Available at: https://doi.org/10.25046/aj060213. (Accessed 16 November 2023)

Goosen, R. and Rudman, R. (2013) The development of an integrated framework in order to address King III's IT governance principles at a strategic level. Available at: https://scite.ai/reports/10.4102/sajbm.v44i4.1718 (Accessed 14 November 2023)

Guo, H., Ding, L. and Xu, W. (2022) Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-α Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment. Available at: https://doi.org/10.1109/access.2022.3169133. (Accessed 11December 2023)

A Guide to the Updated ISO/IEC 27002:2022 Standard, Part 2 - ISACA (no date). Available at: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-12/a-guide-to-the-updated-iso-iec-27002-2022-standard-part-2. (Accessed 11December 2023)

Gyllensten, K., Törner, M. and Pousette, A. (2022) The impact of psychosocial working conditions on information security behaviour in the nuclear industry. Available at: https://scite.ai/reports/10.1108/ics-05-2022-0089. (Accessed 31December 2023)

Kamrani, A. et al. (2021) Fast Chaotic Encryption Scheme Based on Separable Moments and Parallel Computing. Available at: https://scite.ai/reports/10.21203/rs.3.rs-992868/v1. (Accessed 21December 2023)

AlMindeel, R. and Martins, T, J. (2020) Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Available at: https://scite.ai/reports/10.1108/itp-06-2019-0269. (Accessed 1December 2023)

McCann, E. 2013. Kaiser reports second fall data breach. Healthcare IT News, 26 November 2013. Available from: https://www.healthcareitnews.com/news/kaiser-reports-second-fall-databreach (Accessed 17 November 2023).

NHS CfH .2010. Introduction to ISO 27000. Available from:URL:http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards /iso (Accessed 24 November 2023).

Ponemon Institute. 2016. Sixth annual benchmark study on privacy & security of healthcare data. Available from: https://www.ponemon.org/library/sixth-annual-benchmark-studyon-privacy-security-of-healthcare-data-1(Accessed 13 October 2023).

Ponemon Institute. 2017. Cost of Data breach Study: United State. Available at: https://ponemon.org/library/2017-cost-0f-data-breach-study-united-states. (Accessed on 19 November 20023)

Siwicki, B. 2016. "Tips for Protecting Hospitals from Ransomware as Cyberattacks Surge," downloaded 8/27/16. Available from http://www.healthcareitnews.com/news/tipsprotecting-hospitals-ransomware-cyber-attacks-surge (Accessed 30 November, 2023).

Deloitte Report: How Enterprise Collaboration Improves Business (cmswire.com)

Deloitte Report: How Enterprise Collaboration Improves Business

MARCH 2, 2011

Software Engineering (BCS PGD) Guidance from Ms.Dilshara Weerasinghe (bcspgdse2.blogspot.com)

Free Network Diagram Tools (blogarama.com)

https://safetyculture.com/topics/qualitative-and-quantitative-risk-analysis/

Published 23 Oct 2023

What is Qualitative Risk Analysis?

Make Organizational Charts in PowerPoint with Templates from SmartDraw

Org Chart Templates for PowerPoint

ICION 2016 - Cyber Security Governance | PPT (slideshare.net)

https://image.slidesharecdn.com/7254da11-0df5-4f24-b926-7dabbdbc60ac-160306071426/75/icion-2016-cyber-security-governance-20-2048.jpg?cb=1667976943

Cyber Security Governance | PPT (slideshare.net)