EXTENT OF IMPLEMENTATION OF CYBERSECURITY SOLUTIONS IN THE PHILIPPINES: BASIS FOR INNOVATIVE PROGRAM

MARJORIE ALCALA ONA
ona.marjorie88@gmail.com

Laguna State Polytechnic University (LSPU) Sta. Cruz, Laguna 4009, Philippines

Abstract

Establishing the Department of Information and Communications Technology (DICT) in 2016 is a monumental step towards the long-term goal of a secure and technologically capable Philippines. Relatively, this study aimed to provide valuable insights into cybersecurity preparedness in the Philippines' central technology agency. These insights would benefit the DICT's mission to protect critical digital assets and contribute to the broader discourse on enhancing national cybersecurity resilience in an increasingly interconnected digital world. The study explored the challenges and limitations faced by the DICT in achieving its cybersecurity objectives and examined factors such as budget constraints, the evolving threat landscape, and the ever-increasing complexity of modern information systems. It also identified areas for potential improvement and suggested recommendations to enhance the DICT's cybersecurity posture.

Keywords: Cybersecurity Solutions, Digital Threats, DICT, and Security.

Introduction

Cyberspace is a borderless area that has evolved from a peripheral issue to one of the primary security concerns of many countries worldwide. Cyberspace risks, unlike those in the physical arena, provide a unique challenge to governments due to their ambiguity, complexity, and speed. Cyber thieves have expanded in number and expertise in recent years, as few resources are required to cause damage. As globalization accelerates, the path to digitization of all services becomes unavoidable, fostering innovation while providing more space for cyber threat actors to operate. This recurring challenge continues to be a severe worry of cyberspace. Critical actors in cybersecurity, then, are tasked with leveraging the full potential of cyberspace and reducing it.

The Philippines' National Cybersecurity Plan (2022) defines cybersecurity as "the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets." This definition demonstrates the country's commitment to taking all appropriate measures to protect cyberspace, which has become central to Filipinos' way of life.

Substantive progress in cybersecurity in the country has been noted over the years. As law enforcement is vital in national development, several legislations have been created to safeguard information in networks and systems and protect end users. First on the list is the Electronic

Commerce Act of 2000 or Republic Act 8792, which recognized the digitization of services at a time when information and communications technology (ICT) became more prominent in national economic development. Second, the Anti-Photo and Video Voyeurism Act of 2009, or Republic Act No. 9995, penalizes persons who spread private photos or videos of someone on the Internet with the latter's written consent. Third, the Anti-Child Pornography Act of 2009, or Republic Act No. 9775, gives value to children and the youth by safeguarding them against malicious, abusive, and obscene acts such as pornography. Fourth, the Data Privacy Act of 2012, or Republic Act No. 10173, established the Data Privacy Commission, which oversees all functions related to securing personal information and facilitating a free flow of communication in government and private sectors. Finally, the Cybercrime Prevention Act (CPA) of 2012, or Republic Act 10175, penalizes cyber criminals who misuse and abuse all ICT devices, including illegal access to information therein and all activities done on and through the Internet for malicious and unjustified reasons. The CPA was created to prevent and address the adverse effects of technological advancement.

In an era defined by the relentless march of technology, safeguarding digital assets and critical information has never been more paramount. With the ever-increasing dependence on digital infrastructure, governments worldwide must fortify their cybersecurity defenses to protect their citizens, critical infrastructure, and sensitive data from myriad cyber threats. The Philippines is no exception to this global imperative, and its Department of Information and Communications Technology (DICT) plays a pivotal role in securing the nation's digital landscape.

Establishing the Department of Information and Communications Technology (DICT) in 2016 is a monumental step towards the long-term goal of a secure and technologically capable Philippines. As stipulated in Republic Act 10844, the DICT is tasked to be the lead government agency in planning, developing, and promoting the national ICT development agenda. As a background, efforts to establish the DICT have advanced. In 2004, former President Gloria Arroyo signed Executive Order 269, establishing the Commission on Information and Communications Technology (CICT). Several years later, in 2011, President Noynoy Aquino issued Executive Order 67, reorganizing the CICT to the Information and Communications Technology Office (ICTO) under the Department of Science and Technology (DOST). However, the desire to establish a department continued even with these initiatives. This was exemplified by the bills in Congress that were filed in 2004. The Cybersecurity Bureau mostly manages cybersecurity matters under the DICT and the Cybercrime Investigation and Coordinating Center (CICC), an attached DICT agency.

By investigating the extent of cybersecurity solution implementation within the DICT, this research aims to provide valuable insights into cybersecurity preparedness in the Philippines' central technology agency. These insights will benefit the DICT's mission to protect critical digital assets and contribute to the broader discourse on enhancing national cybersecurity resilience in an increasingly interconnected digital world. The study also explored the challenges and limitations faced by the DICT in achieving its cybersecurity objectives, examining factors such as budget constraints, the evolving threat landscape, and the ever-increasing complexity of modern information systems. Additionally, it identified areas for potential improvement and suggest recommendations to enhance the DICT's cybersecurity posture.

Theoretical Framework

The theoretical framework for studying the extent of cybersecurity solution implementation in the Department of Information and Communications Technology (DICT) in the Philippines is based on several key theoretical perspectives and concepts. These theories help guide the research and provide a structured foundation for understanding the dynamics and factors influencing cybersecurity practices within a government agency.

Diffusion of innovations theory, developed by Everett M. Rogers in 1962, explains how new technologies and other innovations spread throughout societies, from introduction to widespread adoption. This theory examines how innovations, such as cybersecurity technologies and practices, spread within an organization. It helps analyze the factors that facilitate or impede the adoption and diffusion of cybersecurity solutions within the DICT, including leadership support, the complexity of the technology, and the readiness of the organization to embrace innovation.

Cybersecurity Frameworks and Models: The research is grounded in various established cybersecurity frameworks and models, such as the NIST Cybersecurity Framework, c, and the Cybersecurity Capability Maturity Model (CMM). These frameworks provide a structured approach to assessing cybersecurity practices, including risk management, threat mitigation, incident response, and security governance. They serve as benchmarks against which the DICT's cybersecurity implementation can be evaluated.

Institutional theory explores how organizations adapt and conform to institutional norms, values, and practices. In the DICT context, this theory helps explain how government regulations, policies, and international standards influence the department's cybersecurity practices. It also considers how external pressures from the cybersecurity community and global organizations affect the DICT's implementation of cybersecurity solutions.

The Technology Acceptance Model (TAM) assesses the extent to which individuals or organizations accept and use technology. Within DICT, this model can be applied to understand the willingness of employees and stakeholders to embrace and effectively utilize cybersecurity solutions. It can help identify potential barriers to technology adoption and propose strategies to overcome them.

Policy Implementation theory examines the process of translating policy objectives into concrete actions. The DICT context helps analyze how national and departmental cybersecurity policies are implemented, including allocating resources, decision-making processes, and enforcing security measures.

Combining these theoretical perspectives provides a comprehensive framework for understanding the extent of cybersecurity solution implementation within the DICT. It considers internal and external factors and the complex interplay of technology, organizational behavior, and policy implementation. This framework will guide the research in assessing cybersecurity practices within the DICT and formulating recommendations for improvement.

Literature Review

In the public sector, capacity building and readiness for cybersecurity can be enhanced through digital technologies and simulation tools. This paper summarizes six years of experience (2011-2016) at the Ministry of Transport, Information Technology and Communication and the National Revenue Agency to develop capacity and cybersecurity readiness. Cyber security standards are based on several projects that adopt a consistent approach to change management and public administration restructuring. In addition, this paper outlines how digital technologies and simulation tools have been employed in cyber security development as an example of good practices in public sector information. Using computer-assisted exercises, a special technical platform and a training and exercise management system provide an integrated framework across the public sector that enhances effectiveness and achieves interoperability and analytical capability (Nikolova, 2017).

In the digital era, governments are considered high-value targets, chased not only by financially motivated criminals but also to commit acts of espionage, terrorism, and warfare. One of the most important technologies developed is network access control (NAC), which implements policy-based access control to handle entry to the network. This research focuses on the application of network access control in government institutions and the numerous benefits of its adoption. Exploring the challenges of the government in adopting a budget that prioritizes cybersecurity will allow us to analyze if the solutions offered in the market are achievable for big and small cities. This paper explores the budgets of six cities, and three NAC solutions are offered to help the government increase its cybersecurity and comply with regulations. It is considered a protocol, tool, or mechanism that helps manage the security entry to devices that try to connect to a network. NAC is implemented to help in many security aspects, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus programs, host or gateway firewalls, user or system authentication, and network security enforcement. One of the most important aspects of NAC is that before access, it checks the security of the endpoint and policy compliance. After granting access, it controls the location and behavior (Santana & Barsoum, 2022).

According to Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021), the ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The systematic review of ISO/IEC 27001 helps to clarify the main themes and results elaborated in almost 15 years of academic research on the standard. Emerging clearly from the literature is that (1) a structured approach to information and cybersecurity requires the integration of multiple standards; (2) the motivations to pursue the ISO/IEC 27001 certification are also related to governmental incentives and market demands; (3) implementation entails several challenges due to guidelines that are generic by design, different approaches/internalization levels are possible; (4) there is limited evidence demonstrating the outcomes of the certification; (5) integration of ISS standards, motivations, implementation and outcomes are dependent on a series of contextual factors, including the technological environment in which the organization operates. Overall, the paucity of empirical studies on ISO/IEC 27001 is striking, especially in light of significant public efforts to sustain the diffusion of the certification.

Methods

The study utilized the descriptive quantitative research method to gather data from respondents using a survey questionnaire. The objective is to determine the level of implementation of Cybersecurity Solutions to the Department of Interior and Local Government in the Central Office and CALABARZON. This research method is most appropriately designed for this study since the researcher wanted to determine the impact of implementing Cybersecurity Solutions. The instrument used to gather data was a questionnaire for selected personnel. The questionnaires, as research instruments, adopted a four-point scale. Pilot testing was also conducted as the instrument underwent validation among research experts. After the pilot testing, the data collected were submitted to the statistician for the reliability test.

In this study, the random sampling technique was also used because there are some instances whereby the population members do not belong to the same category, class, or group. This type of sampling can be advantageous when reaching a targeted sample and where sampling proportionality is the main concern. This design is based on choosing individuals as samples according to the researcher's controls. An individual is chosen as part of the sample because of good evidence that he represents the total population.

Results

Table 2 presents the test results with the Cronbach Alpha, which were excellent overall.

Table 2. Reliability Result

VARIABLES	CRONBACH ALPHA	
CYBERSECURITY SOLUTIONS	VALUE	REMARKS
Network Security	.883	Good
Cloud Security	.911	Excellent
Endpoint Security	.934	Excellent
Application Security	.879	Good
EFFECT OF CYBER SECURITY		
Incident Response Time	.908	Excellent
Security Policy Compliance	.968	Excellent
Security Tools and Technology	.920	Excellent
EFFECTIVENESS OF IMPLEMENTATION GUIDELINES		
Assemble an implementation team and plan	.937	Excellent
Initiate the ISMS and Scope	.932	Excellent
Baseline Security Control	.874	Good
Risk management and treatment plan	.886	Good
Measure, monitor, and review	.942	Excellent
Overall	.966	Excellent

Perceived Level of Acceptability of Cybersecurity Solutions

Table 3. Perceived Level of Acceptability of Cybersecurity Solutions in terms of Network Security

INDICATOR	MEAN	SD	INTERPRETATIO N
1. Network security helps DICT safeguard digital assets, devices, and systems from unauthorized access.	3.60	0.498	Very Highly Aware
2. Acts as the primary defense against cybercriminals by protecting a DICT's sensitive data and critical systems from potential cyberattacks.	3.37	0.615	Very Highly Aware
3. It provides the means of detecting, classifying, and investigating incidents while enabling quick and effective containment and mitigation of their impacts on DICT.	3.47	0.507	Very Highly Aware
4. It continuously monitors the network of DICT for anomalies and potential threats.	3.50	0.572	Very Highly Aware
5. It helps DICT employ deep packet inspection and analysis to identify and prioritize critical data traffic.	3.50	0.630	Very Highly Aware
Weighted Mean	3.49	0.460	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

The primary objective of the study is to assess the respondents' perceived level of acceptability of cybersecurity solutions in terms of network, cloud, endpoint, and application security.

Based on the respondents' perceived level of implementation of cybersecurity solutions regarding network security, the majority have very high awareness, as seen in the composite mean of 3.49 (SD=.460) in Table 3. Adapted from the discussion of Forcepoint (2023), network security is a term that refers to a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies. The results indicate a very high level of implementation of cybersecurity solutions, such as safeguarding digital assets, protecting DICT data, detecting, classifying, and investigating incidents, and constant monitoring and inspection.

The statement that network security helps DICT safeguard digital assets, devices, and systems from unauthorized access obtained the highest weighted mean of 3.60 (SD=.498), interpreted as highly aware. This indicates that respondents perceived a very high level of implementation directed at safeguarding digital assets, devices, and systems from unauthorized access. The findings are supported by the research results by Ali and Kasowaki (2024), which stated the importance of adopting a comprehensive approach to protecting information assets from unauthorized access. However, they also highlighted that aside from implementing these cybersecurity solutions, there is also a need for a cultural shift within the organization that prioritizes data privacy and security. Ali and Kasowaki (2024) further recommended constant attention and investment in these activities as it is not a one-time thing but an ongoing effort.

Table 4. Perceived Level of Acceptability Implementation of Cybersecurity Solutions in terms of Cloud Security

INDICATOR	MEAN	SD	INTERPRETATION
1. It helps DICT to ensure user and device authentication, data and resource access control, and data privacy protection.	3.50	0.509	Very Highly Aware
2. Protect DICT's data from distributed denial of service (DDoS) attacks, malware, hackers, and unauthorized user access or use.	3.43	0.568	Very Highly Aware
3. It helps DICT save on costs and reduce the risks of hiring an internal security team to safeguard dedicated hardware.	3.43	0.568	Very Highly Aware
4. It gives DICT a centralized location for data and applications, with many endpoints and devices requiring security.	3.50	0.572	Very Highly Aware
5. It allows DICT to scale with new demands, providing more applications and data storage whenever they need it.	3.57	0.504	Very Highly Aware
Weighted Mean	3.49	0.438	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

Table 4 shows the perceived level of implementation of cyber solutions in terms of cloud security. It obtained a composite mean of 3.49 (SD=.438), interpreted as highly aware. Box (2019) defined cloud security as a collection of security measures to protect cloud-based infrastructure, applications, and data. This result implies that most respondents observed a very high level of implementation of measures relating to ensuring user and device authentication, protecting data privacy and DICT's data, helping DICT save costs and reduce risks, and allowing them to scale with new demands.

The indicator stating that the cloud security cybersecurity solutions implemented allow DICT to scale with new demands and provide more applications and data storage whenever needed obtained the highest weighted mean of 3.57 (SD=.504). According to Khansa and Zobel (2014), underlying technologies that compose the cloud, like service-oriented architectures, updating on the Web, AI, and other improvements, are essential to consider additional innovations targeted at securing the cloud.

More data breaches will continuously occur if innovations and upgrades are not done. In 2022 alone, Thales Cloud Security Study (2023) reported that 39% of businesses experienced data breaches in their cloud environment. Cloud Security Alliance (2023) mentioned that numerous cloud platforms continue to be neglected, granting unauthorized access to sensitive data. Frequently, organizations place a higher value on flexibility and cost savings than on security challenges. It is essential to receive training in cloud security posture management to prevent security intrusions and avoid common misconfigurations. It is imperative to adhere to optimal methodologies when managing the security posture of a cloud.

Endpoint security, as defined by Modern Office Methods (2024), protects endpoints or entry points of end-user devices such as laptops, desktops, mobile devices, and other connected hardware from being exploited by malicious authors and campaigns.

Table 5 presents the perceived level of implementation of Cybersecurity solutions in terms of endpoint security, which obtained the composite mean of 3.47 (SD=.434), interpreted as highly aware. This implies that respondents perceived a very high level of implementation in web security, data classification, and data loss prevention, as well as providing antivirus solutions, blocking phishing, and providing DICT's centralized endpoint management platform.

Table 5. Perceived Level of Acceptability of Cybersecurity Solutions in Terms of Endpoint Security

INDICATOR	MEAN	SD	NTERPRETATION
1. It gives DICT proactive web security to ensure safe browsing on the web.	3.43	0.504	Very Highly Aware
2. It provides data classification and data loss prevention to prevent data loss and exfiltration of DICT.	3.40	0.498	Very Highly Aware
3. It gives DICT advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems.	3.57	0.504	Very Highly Aware
4. Provide an email gateway to block phishing and social engineering attempts targeting DICT's employees.	3.37	0.615	Very Highly Aware
5. Provide DICT's centralized endpoint management platform to improve visibility and simplify operations.	3.57	0.504	Very Highly Aware
Weighted Mean	3.47	0.434	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

The indicators stating that the implemented endpoint security cybersecurity solutions give DICT advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems and provide DICT's centralized endpoint management platform to improve visibility and simplify operations both obtained the highest weighted mean of 3.57 (SD=.504) interpreted as very highly aware. The results indicate that DICT's implemented endpoint security solutions effectively provide advanced antimalware and antivirus protection alongside centralized management for streamlined operations.

Just like what was mentioned in the study by Althamir et al. (2024), advances in endpoint security, like machine learning-based techniques, are being used to detect malware in endpoint security, offering total protection for all endpoints, real-time detection, and centralized management. However, these methods may produce false positives, be resource-intensive, and restrict protection. Endpoint security should be used with other security measures to defend against cyberattacks completely. It is crucial to acknowledge that machine learning-based methodologies are not a panacea and may present drawbacks such as the potential for false positives and substantial processing power and memory requirements.

George et al.'s study (2021) mentioned XDR or Extended Detection Response, an evolution of Endpoint Detection Response (EDR) that enhances visibility and control across all endpoints, network connectivity, and cloud workloads. XDR provides contextualized threat analysis, enabling quick remedial efforts.

Table 6. Perceived Level of Acceptability of Cybersecurity Solutions in terms of Application Security

INDICATOR	MEAN	SD	NTERPRETATION
1. Confirming a DICT user's identity is valid and necessary to enforce identity-based access.	3.43	0.504	Very Highly Aware
2. Converting DICT's information or data into code to prevent unauthorized access to individual files or an entire project.	3.43	0.626	Very Highly Aware
3. Examining DICT activity to audit incidents of suspicious activity or breach.	3.43	0.504	Very Highly Aware
4. Making sure that DICT data is entered and processed meets specific criteria.	3.43	0.568	Very Highly Aware
5. Limiting DICT's access to applications based on IP addresses or authorized users.	3.37	0.669	Very Highly Aware
Weighted Mean	3.42	0.462	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

Application security, defined by Synopsis (n.d.), is the processes, practices, and tools used to identify, repair, and protect against application vulnerabilities throughout the software development life cycle (SDLC). Table 6 shows the perceived level of implementation of cybersecurity solutions in terms of application security. Based on the findings, a composite mean of 3.42 (SD=.462) was obtained, interpreted as highly aware. This implies that the respondents perceived a very high level of implementation of measures relating to validating a user's identity, preventing unauthorized access, auditing suspicious activities or potential breaches, quality checks, and limiting DICT's access to authorized users only.

The four indicators obtained the highest weighted mean of 3.43, highlighting that there are efforts focused on validating user identity, preventing unauthorized access, auditing suspicious activities or potential breaches, and quality checks. This suggests that significant efforts are dedicated to critical aspects of cybersecurity, including authentication of user identities, preventing unauthorized access, auditing suspicious activities or breaches, and maintaining quality checks. This highlights the proactiveness of implementing cybersecurity solutions, resulting in a high awareness level among respondents. According to Crowdstrike (2023), security controls related to application security can keep disruptions to internal processes at a minimum, respond quickly in case of a breach, and improve application software security for businesses. They can also be tailored to each application so a business can implement standards for each as needed. Reducing security risks is the most significant benefit of application security controls. Different controls include authentication, encryption, logging, validity checks, and access controls, which help businesses enforce security policies and prevent unauthorized access.

Perceived Effect of Implementation of Cybersecurity Solutions

This objective aims to measure the perceived effect of implementing Cybersecurity solutions in terms of incident response time, security policy compliance, and security tools and technologies.

Table 7. Perceived Effect of Implementation of Cybersecurity Solutions in terms of Incident Response Time

INDICATOR	MEAN	SD	INTERPRETATION
1. Define clear communication channels, implement response checklists, and provide staff with quality cybersecurity training.	3.40	0.498	Very Highly Aware
2. Assess whether an event is a cyber-attack, evaluate its intensity, and classify the cybersecurity incident based on the nature of the attack.	3.43	0.504	Very Highly Aware
3. Isolate the affected systems and impede the incident from propagating further.	3.40	0.563	Very Highly Aware
4. Investigating the incident's root cause and eradicating any threats from the system.	3.47	0.507	Very Highly Aware
5. Strengthen security posture by continuously testing and evaluating incident response plans to ensure they remain current and effective in the face of ever-evolving cyber threats.	3.53	0.507	Very Highly Aware
Weighted Mean	3.45	0.432	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

Table 7 shows the perceived effect of implementing Cybersecurity solutions regarding incident response time. It obtained a composite mean of 3.45 (SD=.432), interpreted as very highly aware. This implies that respondents perceived a very high level of awareness of implementing cybersecurity solutions regarding incident response time. It focuses on the activities relating to defining clear communication channels, assessing and evaluating the intensity of a cyber-attack, isolating affected systems, investigating the root cause of the incident, and evaluating the incident response plan to strengthen security posture.

The indicator stating that continuous testing and evaluating incident response plans are done to ensure that they remain current and effective in the face of ever-evolving cyber threats to strengthen security posture obtained the highest mean of 3.53 (SD=.507) interpreted as highly aware. This result suggests that the organization places high importance on regularly testing and evaluating its incident response plan to ensure efficiency in addressing cyber threats. Data Guard (n.d.) supported this and explained that regular testing and updating an incident response plan is crucial for addressing evolving cyber threats. This involves conducting drills, exercises, and simulations to validate the plan, identify gaps, and refine procedures. Periodic assessments, audits, and scenario-based exercises help organizations adapt to new threats and mitigate potential damages. Secure JavaScript practices are essential for web application testing, as modern cyber-attacks target vulnerabilities in web interfaces.

Table 8. Perceived Effect of Implementation of Cybersecurity Solutions in terms of Security Policy Compliance

INDICATOR	MEAN	SD	INTERPRETATION
1. Adapting a security compliance program within your organization can assist in improved security with better collaboration across your organization, from security and compliance teams to HR, IT, and the C-suite	3.40	0.498	Very Highly Aware
2. Good security compliance includes automated security controls that help streamline adherence to DICT regulations, standards, and frameworks and improve security posture.	3.37	0.490	Very Highly Aware
3. Identify DICT's current risks and vulnerabilities and a plan for recovery in the event of a data breach.	3.50	0.509	Very Highly Aware
4. New risks evolve, and regulations change frequently; continuous monitoring is essential for effective security compliance.	3.50	0.509	Very Highly Aware
5. Conduct a risk assessment regularly to stay aware of the current threats to your network and system.	3.47	0.571	Very Highly Aware
Weighted Mean	3.45	0.475	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

Table 8 shows the perceived effect of implementing cybersecurity solutions regarding security policy compliance, which obtained a composite mean of 3.45 (SD=.475), which is interpreted as very highly aware. This implies that respondents perceived a very high level of awareness of implementing cybersecurity solutions regarding security policy compliance. It focuses on the efforts focused on adapting security compliance programs, automated security controls, identification of current risks and vulnerabilities, frequently changing regulations in connection to new risks evolved, and conducting a risk assessment.

The indicator stating that identifying DICT's current risks and vulnerabilities and a plan for recovery in the event of a data breach and new risks evolve, and regulations change frequently, continuous monitoring is essential for effective security compliance both obtained the highest mean of 3.50 (SD=.509) interpreted as very highly aware. Respondents are very highly aware of the importance of identifying current risks and vulnerabilities and developing a comprehensive recovery plan for a data breach. In addition, they also recognize the need for continuous monitoring to address evolving risks and regulatory changes.

Rainbow Secure (2023) explained that IT risk assessments are crucial for organizations' cybersecurity and information security management. They help identify potential threats and their business impact, preventing disruptions and compliance penalties. Common attack types include insecure design, software, data integrity failures, and server-side request forgery.

Moreover, Gibbard (2024) stated that organizations must remain current on the constantly shifting regulatory environment and industry standards to manage compliance and mitigate risks. Analyzing industry standards and monitoring regulatory changes is essential to facilitating strategic planning and ensuring compliance measures align with anticipated changes.

Table 9 shows the effect of implementing Cybersecurity solutions in terms of security tools and technology, which obtained a composite mean of 3.49 (SD=.435), interpreted as very highly aware. This implies that respondents perceived a high level of awareness of implementing cybersecurity solutions regarding security tools and technology. It focuses on the efforts focused on identifying external network threats, detecting non-compliant activities and security failures, continuously monitoring potential security risks, decoding or encoding streams of data, and preventing unauthorized user access on the intranet.

The indicator states that continuous monitoring of the potential security risks of web applications to reveal security flaws and vulnerabilities by scanning websites and preventing unauthorized users from accessing the company intranet can be implemented as hardware, software, or a hybrid of the two. Both obtained the highest mean of 3.57 (SD=.504), interpreted as highly aware. This result implies that the respondents are very aware of the organization's effort to prioritize the importance of continuously monitoring security risks associated with web applications.

Table 9. Perceived Effect of Implementation of Cybersecurity Solutions in terms of Security Tools and Technology

INDICATOR	MEAN	SD	INTERPRETATION
1. Identify external network threats by detecting and preventing attacks that originate from the DICT's intranet.	3.47	0.507	Very Highly Aware
2. Detects non-compliant activities and security failures and notifies system administrators to take corrective actions.	3.47	0.507	Very Highly Aware
3. Continuously monitor the potential security risks of web applications to reveal security flaws and vulnerabilities by scanning websites.	3.57	0.504	Very Highly Aware
4. Decode or encode data streams at rest or in transit, making them safe and unreadable by unauthorized individuals.	3.37	0.490	Very Highly Aware
5. Prevent unauthorized users from accessing the company intranet, which can be implemented as hardware, software, or a hybrid.	3.57	0.504	Very Highly Aware
Weighted Mean	3.49	0.435	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

Likewise, the emphasis on preventing unauthorized access to the company intranet indicates a dedication to protecting sensitive internal resources from potential threats.

The study of Ami and Malav (2013) enumerated the five dangerous security risks of web applications. This included SQL injection, inclusion attacks, cross-site scripting, brute force attacks, and insecure cryptographic storage. In support of this, the research of Torkura et al. (2023) mentioned that cloud infrastructure is constantly evolving, increasing the complexity of managing and securing it. Early detection of malicious changes is crucial for IoC (Internet of Cloud Computing). Continuous monitoring and auditing strategies are essential to detect IoC and provide security visibility.

On the other hand, Khan (2023), in his research, further explains the concept of unauthorized access and how important it is to protect sensitive data from cyber-attacks. Unauthorized access occurs when attackers exploit infrastructure vulnerabilities or steal login credentials. Techniques include brute force, software vulnerabilities, and phishing. Once infected, they can exfiltrate sensitive information, install malware, or disrupt operations. To protect against unauthorized access, strong security measures like passwords, software patching, two-factor authentication, monitoring, data backup, and incident response plans are crucial.

Implementation Guidelines

This objective aims to measure respondents' assessments of the implementation guidelines considered regarding the assembly of the implementation team and plan, Initiating ISMS and Scope, Baseline Security Control, Risk Management and Treatment Plan, and Measuring, monitoring, and Review adapted from ISO 27001 (2021).

Table 10. Assessment of Respondents on the Implementation Guidelines in terms of the Assembly of Implementation Team and Plan

INDICATOR	MEAN	SD	INTERPRETATION
1. Appoint a project leader to oversee the implementation of the ISMS.	3.67	0.479	Very Highly Aware
2. Have a well-rounded knowledge of information security and the authority to lead a team and give orders to managers.	3.53	0.571	Very Highly Aware
3. Create a project mandate to achieve the objectives.	3.63	0.490	Very Highly Aware
4. Use the project mandate to create a more detailed outline of information security objectives, plans, and risk registers.	3.60	0.498	Very Highly Aware
5. Raise awareness of the project through internal and external communication.	3.53	0.507	Very Highly Aware
Weighted Mean	3.59	0.450	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

As presented in Table 10, respondents' Assessments of the implementation guidelines regarding the assembly of the implementation Team and Plan obtained a composite mean of 3.59 (SD=.450), interpreted as Very Highly Aware. This indicates that respondents assessed a very high level of awareness of the implementation guidelines focused on assembling the implementation team and plan.

The indicator stating that a project leader is appointed to oversee the implementation of the Information Security Management System (ISMS) obtained the highest weighted mean of 3.67 (SD=.479), interpreted as very highly aware. This result implies a high level of awareness of an Information Security Management System headed by a project leader. Ondzaghe (2023) stresses that implementing an ISMS is crucial, especially in safeguarding valuable assets and mitigating risks. Project leaders' and managers' roles are crucial in maintaining secure and sustainable computing. The results of the study by Choi (2016) emphasize the importance of transformational leadership by information security managers in improving the effectiveness of information security systems (ISS) used by e-governments. It also highlights the relevance and enforcement of information security policies as mediators between the transformational leadership of information security managers and ISS effectiveness.

As presented in Table 11, the assessment of respondents on the Implementation Guidelines regarding the initiating Information Security Management System (ISMS) and Scope obtained the composite mean of 3.43 (SD=.464), interpreted as Very Highly Aware. This indicates that respondents were highly aware of the implementation guidelines for initiating an Information Security Management System (ISMS) and Scope.

The indicator stating that an Information Security Management System (ISMS) policy was created and focused on outlining what the implementation team wants to achieve and how to plan to do it obtained the highest weighted mean of 3.43 (SD=.464) interpreted as very highly aware.

Table 11. Assessment of Respondents' Implementation Guidelines in Terms of Initiating the ISMS and Scope

INDICATOR	MEAN	SD	INTERPRETATION
1. Determine which continual improvement methodology to use.	3.43	0.504	Very Highly Aware
2. Use any model provided the requirements and processes are clearly defined, implemented correctly, and reviewed and improved regularly.	3.47	0.507	Very Highly Aware
3. Create an ISMS policy outlining what the implementation team wants to achieve and how to plan.	3.50	0.509	Very Highly Aware
4. Identify where information is stored, whether physical or digital files, systems, or portable devices.	3.37	0.556	Very Highly Aware
5. Correctly defining scope is essential to your ISMS implementation project.	3.40	0.498	Very Highly Aware
Weighted Mean	3.43	0.464	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

This finding suggests that significant efforts in DICT were spent in creating ISMS policy with details on the goals and plans for implementation. Robinson (2023) explained that this is important since implementing an ISMS framework will help organizations address both internal and external security threats, ensuring that a robust defense is in place to safeguard against unauthorized access, data breaches, and other security incidents. These policies outline the organization's commitment to security management, defining the security requirements and expectations for employees, suppliers, and other stakeholders. The framework also encompasses risk assessments, identifying potential risks to the organization's assets and allowing for informed decisions on security controls and measures.

Table 12. Assessment of Respondents' Implementation Guidelines in Terms of Baseline Security Control

INDICATOR	MEAN	SD	INTERPRETATION
1. A minimum level of security is required to ensure that the organization operates securely.	3.27	0.583	Very Highly Aware
2. Identify security baseline with the information gathered in ISO 27001 risk assessment.	3.30	0.466	Very Highly Aware
3. Identify your organization's most significant security vulnerabilities and the corresponding ISO 27001 control to mitigate the risk.	3.33	0.479	Very Highly Aware
4. Document each control's tailoring efforts in the security and privacy plans.	3.37	0.490	Very Highly Aware
5. Develop a strategy for continuously monitoring security control effectiveness and any proposed or actual changes to the information system and its operation environment.	3.43	0.504	Very Highly Aware
Weighted Mean	3.34	0.421	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

As presented in Table 12, respondents' assessment of the Implementation Guidelines in terms of the Baseline Security Control obtained a composite mean of 3.34 (SD=.421), interpreted as Very Highly Aware. This indicates that respondents assessed a very high level of awareness of the implementation guidelines focused on initiating Baseline Security Control.

The indicator stating that a strategy was developed for continuous monitoring of the effectiveness of security control and any proposed or actual changes to the information system and its operation environment obtained the highest weighted mean of 3.43 (SD=.504), interpreted as very highly aware. This result implies that DICT has placed considerable emphasis on developing a strategy for continuously monitoring security controls and adapting to changes in the information system and operational environment. Yadav (2023), in an article, highlights that continuous monitoring is a proactive approach to cybersecurity that involves constantly monitoring and analyzing system activity to detect and respond to potential threats in real time. This approach is essential to maintain confidentiality, integrity, and availability of information assets. By identifying vulnerabilities and assessing risks in real-time, security teams can prevent security breaches, detect anomalies, and respond to threats as soon as possible.

Continuous monitoring tools and techniques involve automated security controls, such as intrusion detection and prevention systems, firewalls, and security information and event management (SIEM) systems. These tools provide real-time visibility into system activity and allow security teams to monitor, analyze, and respond to potential threats in real time. By leveraging these automated tools, organizations can reduce the likelihood of data loss or system downtime and better protect their critical information assets.

Table 13. Assessment of Respondents' Implementation Guidelines in Terms of the Risk Management and Treatment Plan

INDICATOR	MEAN	SD	INTERPRETATION
1. Establish risk acceptance criteria, i.e., the damage threats will cause and the likelihood of occurring.	3.43	0.504	Very Highly Aware
2. Select a threshold for the point at which a risk must be addressed.	3.43	0.504	Very Highly Aware
3. ISO 27001 requires organizations to complete an SOA *(Statement of Applicability)* documenting which of the Standard's controls are selected and omitted and why those choices are made.	3.30	0.466	Very Highly Aware
4. Check that staff can operate or interact with the controls and know their information security obligations.	3.47	0.507	Very Highly Aware
5. Develop a process to determine, review, and maintain the competencies necessary to achieve your ISMS objectives.	3.47	0.507	Very Highly Aware
Weighted Mean	3.42	0.418	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

As presented in Table 13, respondents' assessment of the Implementation Guidelines regarding the Risk Management and Treatment Plan obtained a composite mean of 3.42 (SD=.418), interpreted as Very Highly Aware. This indicates that respondents assessed a very high level of awareness of the implementation guidelines focused on initiating risk management and treatment plans.

The indicators stating that staff are evaluated on their ability to operate or interact with the controls, know their information security obligations, and develop processes to determine, review, and maintain the competencies necessary to achieve your ISMS objectives both obtained the highest weighted mean of 3.47 (SD=.507) interpreted as very highly aware. This implies that the organization has placed significant efforts into evaluating staff members' proficiency in operating and interacting with security control and ensuring that they understand information security obligations.

Security awareness training is crucial for organizational security, preventing phishing attacks, detecting insider threats, adhering to regulatory requirements, enhancing data security, reducing human errors, fostering a strong security culture, identifying social engineering attacks, protecting company reputation, improving incident response, and reducing costs. It helps employees recognize and thwart threats, reduces human errors, and enhances incident response, ultimately minimizing the impact of data breaches on the organization's reputation and public image (The Security Company, 2023).

As presented in Table 14, respondents' assessments of the Implementation Guidelines in terms of Measure, Monitor, and Review obtained a composite mean of 3.47 (SD=.398), interpreted as Very Highly Aware. This indicates that respondents assessed a very high level of awareness of the implementation guidelines focused on initiating measuring, monitoring, and reviewing.

The indicators stating that an internal audit of ISMS is regularly conducted and evaluating the Certification body as a member of the International Accreditation Body (IAF) obtained the highest weighted mean of 3.47 (SD=.507), interpreted as highly aware.

Table 14. Assessment of Respondents Implementation Guidelines in terms of Measure, Monitor and Review

INDICATOR	MEAN	SD	INTERPRETATIO N
1. Do at least an annual review that can closely monitor the evolving risk landscape.	3.47	0.507	Very Highly Aware
2. Use quantitative analysis to identify the financial costs or time.	3.40	0.498	Very Highly Aware
3. Conduct regular internal audits of ISMS.	3.53	0.507	Very Highly Aware
4. Ensures that the review is by ISO 27001 instead of uncertified bodies, which often promise to provide certification regardless of the organization’s compliance posture.	3.43	0.504	Very Highly Aware
5. Check that the certification body is a member of the IAF (International Accreditation Body).	3.53	0.507	Very Highly Aware
Weighted Mean	3.47	0.398	Very Highly Aware

Legend: 4.00-3.26 Very highly aware; 3.25-2.51 Highly aware; 2.50-1.76 Low aware; 1.75-1.00 Very low aware.

The findings may imply that significant effort is being put into regularly conducting internal audits and ensuring that the certification body is affiliated with a reputable IAF. Ronalds (2022) explained that security audits would help protect critical data, identify security loopholes, create new security policies, and track the effectiveness of security strategies. Regular audits can help employees stick to security practices and catch new vulnerabilities. Moreover, security audits measure an information system’s performance against criteria. A vulnerability assessment is a comprehensive study of an information system, seeking potential security weaknesses. Penetration testing is a covert approach in which a security expert tests to see if a system can withstand a specific attack. Each approach has inherent strengths, and using two or more in conjunction may be the most effective approach.

Correlation between Perceived Effect of implementation and the types of Cybersecurity Solutions

This objective aims to test the correlation between the perceived effect of implementation and the types of cybersecurity solutions.

Table 15. Correlation between Perceived Effect of Implementation and the Cybersecurity Solutions

Effect of Cybersecurity Solutions	Cybersecurity Solutions			
	Network Security	Cloud Security	Endpoint Security	Application Security
Incident Response Time	.708** Moderate	.779** Moderate	.792** Moderate	.728** Moderate
Security Policy Compliance	.518** Moderate	.603** Moderate	.654** Moderate	.562** Moderate
Security Tools and Technology	.430* Moderate	.552** Moderate	.567** Moderate	.492** Moderate

Note. * p < .05, ** p < .01, *** p < .001

Table 15 presents the Correlation between the Perceived Effect of implementation and Cybersecurity Solutions. The majority of the p-values obtained are significant at .01 except for the relationship between security tools and technology and network security, obtaining p-values significant at .05. This indicates that the hypothesis stating that there is no significant relationship between the level of awareness of the implementation and the types of cybersecurity solutions is rejected.

The results revealed that there is a moderately significant relationship between cybersecurity solutions in terms of network security (r=.708; p-value<.01), cloud security (r=.779; p-value<.01), endpoint security (r=.792; p-value<.01), application security (r=.728; p-value<.01), and incident response time. This indicates that as the implementation of a cybersecurity solution increases, incident response time increases. When the level of network security improves, incidents related to cybersecurity are swiftly addressed, which results in improved incident response time. Enhanced network security solutions can help in the early detection and prevention of security incidents, leading to more efficient and effective responses from the incident response team. In the Serrano et al. (2024) study, the critical nature of incident response time, particularly in security management and risk analysis, and how traditional solutions are now unsuitable for practical use. Their utilization of quantum algorithms in the study resulted in faster incident response time and further suggested that quantum algorithms have the potential to solve certain security incident management challenges efficiently, especially when dealing with large volumes of data.

The results revealed that there is a moderately significant relationship between cybersecurity solutions in terms of network security (r=.518; p-value<.01), cloud security (r=.603; p-value<.01), endpoint security (r=.654; p-value<.01), application security (r=.562; p-value<.01), and security policy compliance. This indicates that security policy compliance increases as a cybersecurity solution is implemented. Implementation and investment in cybersecurity solutions positively influence the organization's adherence to security policies. The literature by Ogunjiimi et al. (2018) shows that the cybersecurity solutions used influence adherence to security policies in SMEs. Based on the context of small and medium enterprises (SMEs), the researchers stated that success depends on alignment with the SMEs' specific requirements. Expert recommendations and structured dialogues with SME representatives facilitate effective implementation. Continuous review and reflection on cybersecurity controls enhance the overall cybersecurity posture, prioritizing cybersecurity capabilities based on perceived importance and resource availability.

The results revealed that there is a moderately significant relationship between cybersecurity solutions in terms of network security (r=.403; p-value<.01), cloud security (r=.552; p-value<.01), endpoint security (r=.567; p-value<.01), application security (r=.492; p-value<.01), and security tools and technologies. This indicates that security tools and technologies increase as cybersecurity solutions are implemented. The increasing implementation of cybersecurity solutions acts as an indication for the adoption and use of different security measures, demonstrating a proactive commitment to addressing cybersecurity concerns. Smith (2018) emphasizes the significance of security automation in dealing with cybersecurity issues. According to them, security automation is a tool widely used to remove security decision responsibility from workers. It can identify and address specific dangers, such as fraudulent emails. It provides ongoing surveillance of systems, enabling IT personnel to concentrate on irregularities. This approach emphasizes that implementing cybersecurity solutions demonstrates a proactive approach to cybersecurity.

Correlation between Perceived Level of Implementation Guidelines and the Perceived Effect of Cybersecurity Solutions

The primary goal of this objective is to test the correlation between the perceived level of implementation guidelines and the perceived effect of CyberSolutions.

Table 16. Correlation between Perceived Level of Implementation Guidelines and the Perceived Effect of Cybersecurity Solutions

Implementation Guidelines	**Effect of Cybersecurity Solutions**		
	Incident Response Time	Security Policy Compliance	Security Tools and Technology
Assemble an implementation team and plan	.753** High	.640** Moderate	.679** Moderate
Initiate ISMS and its scope	.810** High	.907** High	.743** High
Baseline Security Control	.881** Moderate	.823** High	.775** High
Risk management and treatment plan	.888** High	.850** High	.733** High
Measure, monitor, and review	.637** Moderate	.507** Moderate	.742** High

Note. * *p* < .05, ** *p* < .01, *** *p* < .001

Table 16 presents the Correlation between the perceived level of implementation guidelines and the perceived effect of CyberSolutions. All p-values obtained are significant at .01. This indicates that the hypothesis stating that there is no significant relationship between the perceived level of implementation guidelines and the perceived effect of CyberSolutions is rejected.

The results revealed that there is a high to moderate significant relationship between the effects of cybersecurity solutions in terms of incident response time (r=.753; p-value<.01), security policy compliance (r=.640; p-value<.01), security tools and technology (r=.679; p-value<.01) and assemble and implementation team and plan. This implies that when organizations strengthen the effectiveness of their cybersecurity solutions through shorter incident response time, compliance with security policy, and investment in security tools and technology, they have a higher capability of implementing plans and policies. In the same manner as the results of the research of Khan and Khandaker (2016), professional and technical resources are mentioned as one of the elements that affect policy implementation. Though different in the study area, this supports the implication of the findings revealed in the study. This highlights the importance of enhancing the effectiveness of cybersecurity solutions, allowing transparent implementation of the organization's plans, programs, and policies.

The results revealed that there is a highly significant relationship between cybersecurity solutions in terms of network security (r=.810; p-value<.01), security policy compliance (r=.907; p-value<.01), security tools and technology (r=.743; p-value<.01), and Initiate ISMS and its scope. This implies that when organizations enhance the effectiveness of the cybersecurity solutions employed, this also increases the chances of initiating ISMS and its scope. It was mentioned by Robinson (2023) that ISMS framework implementation will help organizations address both internal and external security threats, ensuring that a robust defense is in place to safeguard against unauthorized access, data breaches, and other security incidents. Technology, tools, and security policy go together to address any organizational risk.

The results revealed that there is a moderate to high significant relationship between cybersecurity solutions in terms of incident response time (r=.881; p-value<.01), security policy compliance (r=.823; p-value<.01), security tools and technology (r=.775; p-value<.01), and baseline security control. This implies that as organizations ensure effectiveness in cyber security solutions, the baseline security control of the organization is also increased. The faster incident response time, practical tools and technology, and even compliance with security can fortify the baseline security employed in an organization. This also indicates that if the company loses its high level of security lines during a data breach, then the baseline or the most basic protection is still strong, securing it from any cybersecurity attacks. This is supported by the findings of Mughal (2018), stating that by conducting risk assessments, prioritizing investments, updating policies, monitoring and responding to incidents, and evaluating security measures, organizations can effectively mitigate risks and minimize the impact of potential security incidents.

The results revealed that there is a highly significant relationship between cybersecurity solutions in terms of incident response time (r=.888; p-value<.01), security policy compliance (r=.850; p-value<.01), security tools and technology (r=.733; p-value<.01), and risk management and treatment plan. The findings reveal that as there is enhanced effectiveness in cybersecurity solutions, there is also increased implementation of risk management and treatment plans. Risk management and treatment plans are essential in organizations as it addresses the full spectrum of the organization’s significant risks by understanding the combined impact of risks rather than addressing the risks only within silos (Stine et al., 2020).

Finally, the results revealed that there is a moderate to high significant relationship between cybersecurity solutions in terms of incident response time (r=.637; p-value<.01), security policy compliance (r=.507; p-value<.01), security tools and technology (r=.742; p-value<.01), and measure, monitor and review. This implies that effective cybersecurity strategies are related to measuring, monitoring, and reviewing organizational performance. Cybersecurity crimes, data theft, and many more may be affected when there is no effective cybersecurity solution in the organization.

The results revealed that there is a moderate to high significant relationship between cybersecurity solutions in terms of incident response time (r=.637; p-value<.01), security policy compliance (r=.507; p-value<.01), security tools and technology (r=.742; p-value<.01), and measure, monitor and review.

Conclusions

The following are the conclusions based on the findings of the study:

1. The hypothesis that there is no significant relationship between the level of implementation awareness and the types of cybersecurity solutions is rejected.

2. The hypothesis that there is no significant relationship between the perceived level of implementation guidelines and the perceived effect of Cybersecurity Solutions is rejected.

3. It can be concluded that the respondents have a high level of awareness and perceived implementation of cybersecurity solutions in various areas. Respondents believe implementing these solutions is crucial in protecting information assets from unauthorized access. There is also a need for a cultural shift within organizations to prioritize data privacy and security. The respondents are highly aware of the implementation guidelines for Information Security Management (ISMS) and the importance of continuous risk management.

Recommendations

The following are the recommendations based on the findings and conclusion of the study:

1. Strengthen the implementation of cybersecurity solutions focused on application security by developing a program to strengthen further existing measures focused on validating user identity, preventing unauthorized access, auditing suspicious activities, and ensuring quality checks.

2. Improve the implementation of baseline security controls by documenting control and developing a strategy to monitor security control effectiveness continuously.

3. Organize training conducted at least twice a year to enhance the capabilities of incident response teams.

4. Given the high level of awareness and implementation of cybersecurity solutions and guidelines observed in this study, it is recommended that the study be extended and replicated in other institutions, such as universities. This would provide valuable insights to like-minded researchers on the effectiveness of cybersecurity practices across a different sector.

BIBLIOGRAPHY

ABDULLAYEVA, F. J. (2022). Distributed denial of service attack detection in E-government cloud via data clustering. *Array*, *15*, 100229. https://doi.org/10.1016/j.array.2022.100229

ALI, H., & KASOWAKI, L. (2024). Data Protection in the Digital Age: Safeguarding Information Assets [Unpublished master's thesis].

ALTHAMIR M., ALBUALI, A. A., RIAD, K., & ALBUALI A. (2024). Enhancing Malware Detection Efficacy: A Comparative Analysis of Endpoint Security and Application Whitelisting. Journal of Theoretical and Applied Information Technology, 102(6),2451-2465. https://www.jatit.org/volumes/Vol102No6/18Vol102No6.pdf

AMI P. V., & MALAY, S. C. (2013). Top Five Dangerous Security Risks over Web Applications. International Journal of Emerging Trends & Technology in Computer Science.

APPLICATION SECURITY: Threats, tools and techniques - CrowdStrike. (2023). Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/application-security/

CHOI, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability*, *8*(7), 638. https://doi.org/10.3390/su8070638

CULOT, G., NASSIMBENI, G., PODRECCA, M., & SARTOR, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal. https://doi.org/10.1108/TQM-09-2020-0202

GIBBARD, M. (2024). *Navigating Complexity: Compliance and Risk Management Essentials.* LinkedIn. https://www.linkedin.com/pulse/navigating-complexity-compliance-risk-management-max-gibbard-oddgc/

KHAN, M. J. (2023). Securing network infrastructure with cyber security. *World Journal of Advanced Research and Reviews*, *17*(2), 803-813. https://doi.org/10.30574/wjarr.2023.17.2.0308

KHANSA, L., & ZOBEL, C. W. (2014). Assessing innovations in cloud security. *Journal of* Computer Information Systems, 54 (3), 45
56. https://doi.org/10.1080/08874417.2014.11645703

RAINBOW SECURE. (2023, September 25). *Importance of IT risk assessments for cybersecurity*. LinkedIn. https://www.linkedin.com/pulse/importance-risk-assessments-cybersecurity-rainbowsecure/

ROBINSONS, A. (2023). *Developing your ISMS framework*. Thought Leadership & Blogs. https://blog.6clicks.com/developing-your-isms-framework

NIKOLOVA I. (2017). Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector. Information & Security, 38, 79-92. https://doi.org/10.11610/ISIJ.3806

ONGZHAGE, S. (2023, May 26). Important key recommendations for: Implementing an effective information security management system (ISMS). LinkedIn. https://www.linkedin.com/pulse/important-key-recommendations-implementing-effective-ondzaghe-mba

SANTANA, N. A., & BARSOUM, A. (2022). Network Access Control for Government: An Analytical Study. *International Journal of Cyber Research and Education (IJCRE)*, *4*(1), 1-11. https://doi.org/10.4018/ijcre.309686

STINE, K., QUINN, S., WITTE, G., & GARDNER, R. (2020). Integrating cybersecurity and enterprise risk management (ERM). https://doi.org/10.6028/nist.ir.8286-draft2

YADAV, S. (2023, May 5). *Maximizing cybersecurity with automated continuous monitoring: Benefits and best practices*. LinkedIn. https://www.linkedin.com/pulse/maximizing-cybersecurity-automated-continuous-monitoring-yadav

Electronic Sources

CLOUD Misconfigurations that lead to data breaches. (2023, October 11). Cloud Security Alliance.https://cloudsecurityalliance.org/blog/2023/10/11/the-common-cloud-misconfigurations-that-lead-to-cloud-data-breaches

Cyber security incident response plan. (n.d.). DataGuard. https://www.dataguard.co.uk/cyber-security/incident-response-plan/#:~:text=update%20the%20plan-,Regular%20testing%20and%20updating%20the%20incident%20response%20plan%20are%20essential,on%20feedback%20and%20lessons%20learned

Importance of its security audit. (2022, October 13). Ronalds. https://ronalds.co.ke/importance-of-it-security-audit/#:~:text=Security%20 audits%20will%20help%20 protect,and%20can%20catch%20new%20 vulnerabilities

IT disaster recovery, cloud computing and information security news. (2023, July 6).Continuity central. https://www.continuitycentral.com/index.php/news/technology/8663-39-percent-of-businesses-experienced-a-data-breach-in-their-cloud-environment-last-year#:~:text=This%20year's%20study%20found%20that,55%20 percent)%20of%20the%20surveyed

THE SECURITY COMPANY. (2023, October 17). Why is it important to support my staff with security awareness training? LinkedIn. https://www.linkedin.com/pulse/why-important-support-my-staff-security-awareness-training-kzyke