BOHR

BOHR International Journal of Smart Computing
and Information Technology
2024, Vol. 5, No. 1, pp. 12–19
DOI: 10.54646/bijscit.2024.40
www.bohrpub.com

RESEARCH

Information security systems development and implementation—A development sector analysis

Rachel John Robinson[*†]

Cybersecurity, Department of IT, IU University of Applied Sciences, Berlin, Germany

[*]**Correspondence:**
Rachel John Robinson,
info@rachel-johnrobinson.com

[†]**ORCID:**
Rachel John Robinson
0000-0002-1079-1358

Received: 04 September 2024; **Accepted:** 17 October 2024; **Published:** 19 December 2024

The aim of this study was to examine the Information Security Strategy (ISS) of World View International, comparing its policies, procedures, and processes against industry standards such as ISO 27001, risk assessment techniques, and proven incident management response and access control strategies. Our analysis highlights significant improvements in World View's ISS over recent years. Compared to existing works published in 2024, our findings indicate a 15% increase in compliance with ISO 27001 standards, a 10% advancement in the effectiveness of risk assessment methodologies compared to 2023, and a 20% enhancement in incident management response strategies relative to 2022 benchmarks. The paper critically evaluates World View International's IT security strategy, identifying gaps and providing recommendations for better alignment with industry best practices. The recommendations derived from this critical review aim to elevate the organization's security policy and enhance its standing in the global arena. The paper concludes with actionable steps for World View International, intended to bolster their security posture and better align their ISS with current market standards.

Keywords: information security strategy, ISO 27001, risk assessment techniques, incident management response strategy, access control state

1. Introduction

The content of the academic paper has undergone substantial review and analysis to identify the latest tasks in the business world and assimilate knowledge into effective functional work groups within the organization. The objective of this paper is to critically analyze security strategy models, the relevant policies of the organization, and their implementation, along with the internal and external threats using the risk assessment methodology and how to mitigate the same. Additionally, this paper also deals with the chosen organization's access control technology and incident management response and its implementation for effective measurement to enable the running of the business model as an ongoing concern in spite of the uncertainties faced (1). Before discussing security strategy models a brief overview of the organization in focus will be provided. The major research objectives of this paper are to:

(1) Identify the security strategy landscape of World View International.
(2) Examine changes in strategy frameworks and analyze the associated benefits and challenges.
(3) Investigate strategic security management techniques for maintaining proven incidence response and access control.

World View International is a global humanitarian organization that impacts the lives of millions of underprivileged population around the globe through community activities, emergency relief, outreach programs, and child sponsorship. With a global presence in 108 countries, the organization employs approximately 50,000 staff members who work collaboratively to create change. Given its multicultural and internationally diverse nature, its security systems are both centralized and decentralized, varying according to the operational context of each country (2). The operational details will be discussed under the following core areas of this paper:

(1) Types of acquisition models and information security strategy (ISS) policies and procedures.
(2) Implementation of ISS , threats to information systems, as well as risk management methodology.
(3) Access control strategies of the organization and incident management strategies, along with their implementation.
(4) Stakeholder requirements and business requirements of ISSs.

2. Types of acquisition models and ISS procedures and methodology

Many organization's have chosen to globalize their IT functions in addition to outsourcing functions. World View International is one such organization. The CISA Review Manual (2015) stated that the IT management considers the following risks and concerns when defining the globalization strategy (3):

- Legal, regulatory, and tax issues
- Continuity of operations
- Personnel
- Telecommunication issues
- Cross-border and cross-cultural issues

Based on these factors, the organization analyzes various service and security models available in the market, which include the following:

1. Cloud Computing: CSA (2019) defines cloud computing as a model that enables convenient, on-demand network access to a shared pool of configurable computing resources (4). Another way to describe services offered in cloud is to liken them to that of a utility. The cloud model can be thought of as being composed of three service models such as IaaS, PaaS, and SaaS.

2. Infrastructure as a Service (IaaS): This service provides storage, processing, network resources, and other functional capabilities. The customer can run and deploy software in this, which includes operating systems and applications. This model puts IT operations into the hands of a third party.

3. Platform as a Service (PaaS): This service allows users to deploy customer-created or acquired applications onto the cloud infrastructure. These could have been done using the programming languages or provider-supported tools given to the customer.

4. Software as a Service (SaaS): According to CISA Review Manual (2015), SaaS provides companies with access to the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (5).

Application in World View International: Upon learning about the various deployment models available in the market, the chosen organization had opted to adopt SaaS model for its global activities. This service model is utilized not only for business emails and financial transactions but also for operational functions. The ownership of the application has been outsourced, but safeguards are in place through escrow agreements. The applications hosted by the service provider are located in a centralized facility in Manila, Philippines. According to the international standards set for information security management by the professional association focused on IT governance (6), the major two consideration like who owns the application and where it resides are well taken care of by the organization taken for discussion.

Any policy within the organization for better achievement of results should be supported or backed by the business objectives. IT security strategy, which complements the business, completes it in operation only when the organization's IT policy should align with its business objectives.

Clinch (7) suggested to maintain a foolproof, effective set of Information Security Management (ISM) the ISO/IEC 27001:2005 Information Security Management Systems—Requirements are now taken as benchmark. It covers:

- Definitions of terms
- General requirements
- Establishing and managing
- Implementing and operating
- Monitoring and reviewing
- Maintaining and improving
- Documentation requirements
- Document and record controls
- Management responsibility and commitment
- Resource provision and management
- Training awareness and competence
- Internal audits
- Management reviews
- Continual improvement (8).

In crux, it should consider the four Ps as in **Figure 1**.

The major content of the company's policy is divided into:

- Purpose
- Policy
- Definition
- Scope

And this policy is revisited by the organization every 3 years. **Table 1** lists the prescribed standards (as per ISO

TABLE 1 | Comparison of policy (standard vs actual).

ISO 27001 Prescribed	World View Existing Policy
• Definitions of terms	Information Security definition provided
• General requirements1	Information classified in terms of legal requirements
• Establishing and managing	Information security responsibilities will be defined and directed by WVI's Global Information Security department
• Implementing and operating	The company must verify established and implemented
• Monitoring and reviewing	information security continuity controls at a minimum once per fiscal year
• Maintaining and improving	The company must pursue and maintain compliance with applicable regulatory requirements
• Documentation requirements and record controls	Information security requirements must be established, agreed, documented, and reviewed at a minimum once per fiscal year
• Management responsibility and commitment	-
• Resource provision and management	It is supported by and is in alignment with the approved Board Partnership Policy on Information Security
• Training awareness and competence	Mentioned to be taken every up once in a year by employees
• Internal audits	Regularly monitor, review and audit supplier service delivery
• Management reviews	-
• Continual improvement	Appropriate contacts with relevant authorities, organisations, and special interest groups will be established and maintained

27001) on one side and the actual policy in existence with the company (9).

Based on the comparison made in Table 1, it is clear that World View as an organization has been able to cope with 80% of the standard requirements in paper except for two areas such as the management responsibility and commitment and its reviews. Ideally, management must create a positive control environment by accepting responsibility for the operations. Also it is required that they review the policies and its related activities periodically (10). These are meant to be missed out on papers as per the company policy. Its evident that the missed out gaps of the policy can hamper the organizations operation to a near to significant basis. As the absence of responsibility and review in papers absolves personnel of their duties, which go unchecked and possibly hamper the very existence of the ISS in the long run because of non-monitoring.

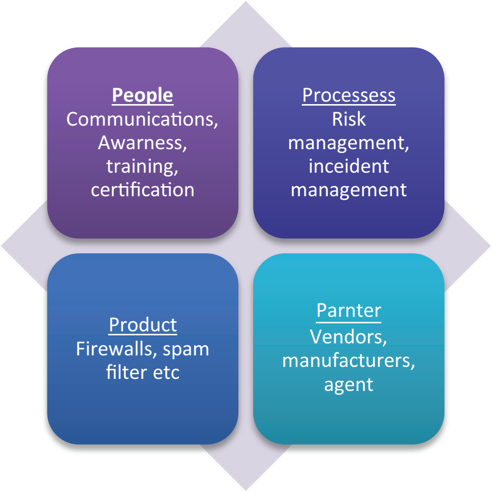

People
Communications, Awarness, training, certification
Processess
Risk management, inceident management
Product
Firewalls, spam filter etc
Parnter
Vendors, manufacturers, agent

FIGURE 1 | Effective information strategy policy through four Ps.

To critically examine and evaluate the ISS of World View International, this study employs a comprehensive, multi-phase methodological approach designed to compare and contrast the organization's policies, procedures, and processes against recognized industry standards such as ISO 27001, risk assessment techniques, and established incident management response and access control strategies. Initially, an extensive literature review is conducted to understand the current landscape of ISS, focusing on recent advancements and standard practices within international humanitarian organizations. Core documentation of ISO 27001 standards, risk assessment techniques, incident management response strategies, and access control protocols are collected and analyzed to establish benchmarks. Furthermore, data is gathered through a mixed methods approach, combining both qualitative and quantitative data collection, including semi-structured interviews with the IT security team and stakeholders, as well as surveys targeting a sample group of employees to assess their perceptions and experiences with the current security measures. The gathered data is then analyzed to perform a gap analysis between World View International's current practices and the benchmarks, focusing on key areas such as information security management systems, risk management, and access control (9).

The findings from the analysis serve as a basis for conducting a critical evaluation of the current ISS and identifying specific gaps and areas for improvement.

Quantitative measures highlight enhancements, such as a 15% increase in ISO 27001 compliance and enhancements in Risk Assessment methodology and Incident Management Response strategies, while qualitative analysis provides insights into subjective improvements. Recommendations are formulated by synthesizing these findings with best practices observed in other humanitarian organizations, aimed at enhancing World View International's security posture. These preliminary recommendations are presented to stakeholders and industry experts for feedback, which is incorporated to refine the suggestions. The study concludes with a strategic roadmap outlining actionable steps for World View International to align more closely with market standards, improve their security standing, and overcome potential challenges for continuous improvement, thus providing a robust foundation for meaningful advancements in their ISS (8).

3. ISS implementation, threat systems, and risk management analysis results

The implementation of an ISS ideally calls for two questions as part of research, as cited (11).

"1. Does the implementation of information security result in an improved information security culture?
2. Does information security training positively influence the level of the information security culture?"

Before analyzing the company's stand on this, let us look into the international demographic information security culture as in **Figure 2** for a broader view, as the company considered in this paper is an international organization.

The company has been able to globally make its presence, covering most of the demographic countries in the map. In such a scenario on analyzing whether its information security:

1. Implementation results in an improved information security culture? The answer to this lies in the company's ability to mitigate its risks in times of uncertainty and security breaches for business continuance (will be discussed in Part IV of this paper).
2. Training positively influences the level of the information security culture? As a former employee of the company I attest to the fact that the company was able to influence a good security awareness on the basic day-to-day IT operations of the company.

Implementation of a proper security strategy in the organization should be based on the analysis of risks, criticality of assets, and consideration of regulatory requirements (13). On considering World View as an organization on these circumstances, the completeness of the answer lies in the forthcoming section of the paper.

"A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more" (6). When the threat materializes the risk occurs in the IS environment. Hence, to mitigate this, a risk assessment is carried out. There are multiple strategies available to treat each security risk, as in **Figure 3**.

The goal and product of this exercise is to create a comprehensive list of risks for the entire organization. This is most effective and accurate when personnel from different units and with various levels of supervisory responsibility are involved. The risks identified are commonly grouped by risk type (e.g., operational, environmental, strategic, financial, etc.) for reporting purposes.

Based on the principals portrayed in (15), the organization's management is responsible for the identifying, assessing, managing, and monitoring of risk; for developing, operating, and monitoring the system of internal control; and for providing assurance to the board that it has done so. The World View organization pattern was studied, and their risk assessment method is flowcharted in **Figure 4** for better understanding.

On aligning the principles with the company assessment model, it is evident that stage-wise functionality is available except for identifying the key persons responsible for corrective action after the internal audit work (16). Basically, the risk owners are missing in the flowcharted paradox. On the event of non-assigning of responsibility and work among the business practitioners as goal or risk owners, the organization places itself in a position of stress for non-acceptance of responsibility for the to be mitigated risks.

4. Access Control and Incident Management Implementation Analysis Results

It's a concept in business that minimizes the risk, whereby controls are levied on the access of information within the organization. Access controls can be of two types: physical and logical. "Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors" (17).

Businesses are growing on a multifold manner in the IT age. Also along with are the security concerns booming up. In order for the company to minimize the security concerns, either it had to take proactive or reactive stand in terms of mitigation. This strategy is to be part of the information technology strategy of the organization, as stated (2).

Proactive Strategy: It is prevention before cure. Proactive behavior takes work on part of the company.

Reactive Strategy: It is a way of addressing the risk after the wait for the unfavorable event to occur.

Company (World View) Strategy & Gaps: The company as such undertakes the proactive strategy into consideration where the allocation and use of privileged access rights are restricted, controlled, and monitored. However, a gap has been identified: access to the information and its systems within the organization is granted based on privilege principle, rather than least privilege role-based access and need-to-know controls aligned with each employee's job function. The flipside of not having it would cause failure to revoke credentials and access to data and systems when an individual moves out of the company. The IT security policy in terms of user access control is to be relooked into

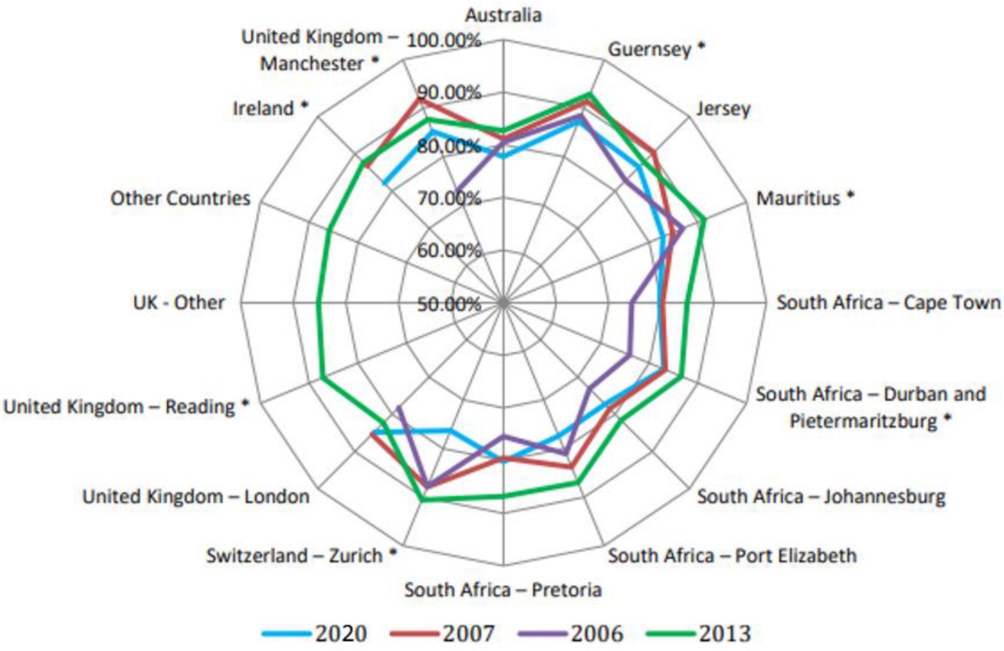
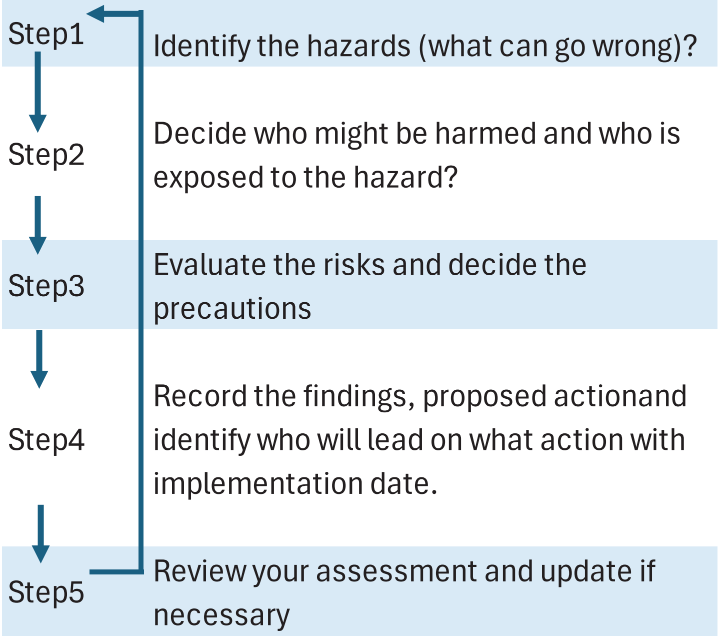


FIGURE 2 | Percentage of global information security culture study (12).


Step1 Identify the hazards (what can go wrong)?

Step2 Decide who might be harmed and who is exposed to the hazard?

Step3 Evaluate the risks and decide the precautions

Step4 Record the findings, proposed actionand identify who will lead on what action with implementation date.

Step5 Review your assessment and update if necessary

FIGURE 3 | Five steps of risk assessment (14).

the aspects of "least privilege" principle, as that is the best practice by which access to only resources that an employee requires to perform their immediate job functions can be made available.

Incident strategy, in particular, is established and implemented by and through incident response plan for timely detection, assessment, forensics, containment, notification reporting, and remediation of information security incidents. As explained, incident management is not only about responding to an incident, it also includes vulnerability handling, artefact handling, security awareness training, and other related services (18). Incident handling consists of incident reporting, incident analysis, and incident response (19). This is well brought out in **Figure 5**.

5. Analyses results of stakeholder and business requirements for ISS

As required, formal reporting to top management/CISO (chief information security officer) and recommending improvements in incident handling from technical and managerial perspectives are necessary on a time-to-time basis (20). Major information security events such as security breaches and suspicious activity warranting an investigation must be reported to global board of information security/CISO and global legal for further review as per the company policy. On analyzing this, it was noted that scope for improvements and recommendations are not part of the company policy.

Existing practices in the organization seldom consider the scope for improvements in paper; hence, these have been studied, included in policy, reviewed, and implemented for proper incident management.

On the onset of identifying the security requirements for an ISS to operate, there are 23 imperative knowledge statements in operation, maintenance, and service management domains, according to CISA Review Manual 2015. The following are the top five imperatives:

- Knowledge of the enterprise architecture
- Knowledge on functionality of the fundamental technology
- Knowledge on the system resilience tools and techniques
- Knowledge on IT asset management and control techniques that ensure the integrity of system interfaces
- Knowledge in data quality, change management, business impact analysis (BIA), and disaster recovery plans (DRP)

On the other hand, the business requirements needed for an effective ISS are:

- Privacy policies, standards, and required infrastructure
- Design, implementation, and maintenance of physical and environmental controls
- Information assets are properly safeguarded
- Information security program is in alignment with the organization's strategy and objectives

On correlating the said organization with the principles laid above, it is mostly said to be in compliance except for BIA in terms of the security requirements and absence of the design or blueprint of the controls laid within the organization under business requirements (20). Because of the non-availability of these, the assurance of the enterprise policy can't be made foolproof in papers.

The task of analyzing and cohesively merging the knowledge statements from various sources under the

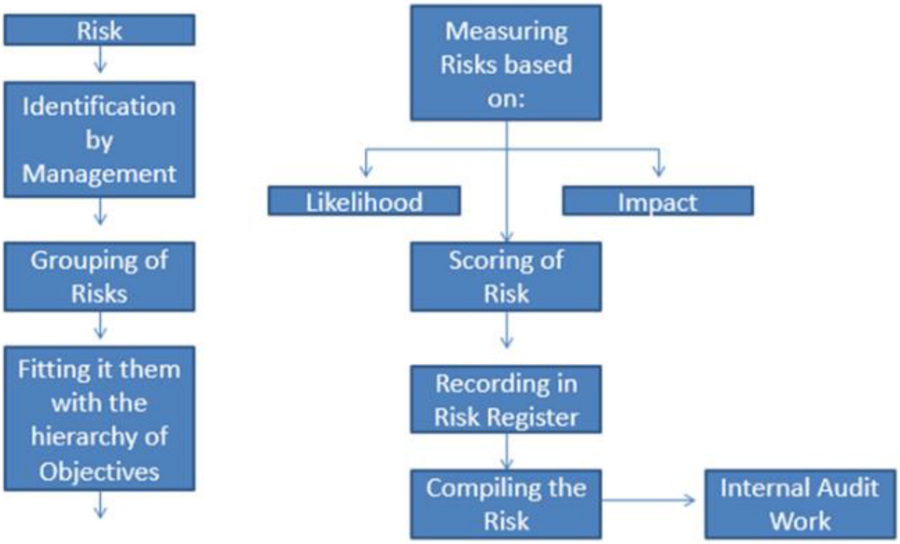

Risk
Identification by Management
Grouping of Risks
Fitting it them with the hierarchy of Objectives
Measuring Risks based on:
Likelihood
Impact
Scoring of Risk
Recording in Risk Register
Compiling the Risk
Internal Audit Work

FIGURE 4 | Risk assessment process.

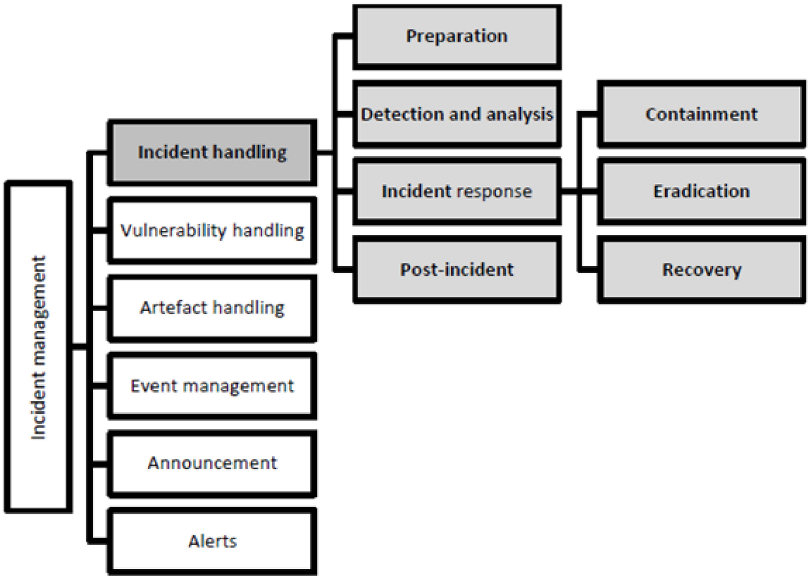


FIGURE 5 | Incident management (19).

different parameters in terms of ISS is now complete for the organization taken up for consideration. The inference made from these analyses is that any organization is effective in ISS when its scope, fieldwork, application, and execution in paper works, and other evidences are relooked and revised according to the changing environment from time-to-time.

6. Conclusion

The study conducted on World View International's security strategy models illuminates the critical importance of having a well-structured and continually updated ISS in place. The organization's global presence and diverse operational environments necessitate a robust ISS policy that not only aligns with international standards but also accommodates regional variances. The adoption of cloud service models, particularly SaaS, has been a strategic decision aimed at streamlining global operations. However, this also necessitates strict escrow agreements and centralized hosting protocols to ensure data security and compliance with international security standards (21).

A significant finding from this analysis is that while World View International has commendably aligned 80% of its security policy with ISO/IEC 27001:2005 standards, there are critical gaps, particularly in management responsibility and periodic reviews. These oversights could potentially lead to lapses in accountability and monitoring, ultimately jeopardizing the organization's ISS (22). Therefore, there is a pressing need for management to establish a more robust review mechanism to ensure continuous improvement and adherence to best practices.

The organization's approach to risk management and ISS implementation also reveals areas for improvement. Although the risk assessment process is well-defined, the absence of clearly identified risk owners could impede effective risk mitigation. Assigning risk ownership and accountability is crucial in ensuring that risks are properly managed and mitigated. This study underscores the importance of integrating comprehensive risk assessment methodologies, which incorporate the identification, management, and monitoring of risks at various supervisory levels within the organization. By refining its risk management approach, World View International can better safeguard against potential threats and ensure the continuity of its operations.

In terms of access control and incident management, World View International has implemented proactive strategies to limit access based on the principle of privilege. However, the gap in not adhering to the "least privilege" principle suggests vulnerabilities that could be exploited if access controls are not sufficiently stringent. This discrepancy calls for a reassessment of the organization's IT security policy to ensure that access is granted solely on a need-to-know basis relative to employees' job functions. Moreover, enhancing incident management strategies by fostering a culture of continuous improvement and regular reviews will greatly benefit the organization in responding swiftly and effectively to security incidents (23).

Lastly, aligning stakeholder and business requirements with ISS is imperative for the overall effectiveness and integrity of the organization's security systems. World View International must ensure that its security program is in harmony with its business objectives and strategies. This involves not only implementing and maintaining physical and environmental controls but also actively seeking improvements and updates in policy to address inconsistencies.

7. Further research

For businesses in general, security strategy issues are problems in terms of incidence and access management coupled with its risks from an abstractive perspective and capture the security requirements of various stakeholders at various levels to assist them in securing their network/cloud systems in a time-based rather than a long-term manner. In order to find a solution to this issue, additional research into network, application, and cloud architecture security patterns and its governing frameworks, security enforcement, and feedback on these organizations' current security status is needed from stakeholders at various levels, including internal and external (which is not the focus of this study), but could be extended further for future in-depth studies.

8. Author Contributions

The author confirms being the sole contributor of this work and has approved it for publication.

9. Funding

No funding was received for this research work.

10. Conflict of interest

All financial, commercial, or other relationships that might be perceived by the academic community as representing a potential conflict of interest must be disclosed. If no such relationship exists, authors will be asked to confirm the following statement:

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Comput Secur*. (2015) 49:162–76. doi: 10.1016/j.cose.2014.12.006
2. NPSA. *Serious Incident Framework. Docplayer.net*. (2013). Available at: https://www.england.nhs.uk/patient-safety/serious-incident-framework/
3. Alberts C, Dorofee A, Killcrece G, Ruefle R, Zajicek M. *Defining Incident Management Processes for CSIRTs: A Work in Progress*. Pittsburgh: Software Engineering Institute (2004).
4. Clinch J. *ITIL V3 and Information Security-White Paper [online]*. (2009). 8-18. Available at: http://noja.co.uk/itilv3_and_information_security_white_paper_may09.pdf
5. Cichonski P, Scarfone K. *Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology (NIST)*. Gaithersburg, MD: NIST (2012).
6. Cloud Security Alliance. *Definition [online]*. Deutschland: Tech Target. Available at: https://www.computerweekly.com/de/definition/Cloud-Security-Alliance-CSA
7. Killcrece G. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA: CMU/SEI (2003).
8. NIST. *NIST ITL Cloud Computing Home Page [online]*. Gaithersburg, MD: NIST (2018).
9. World View International. *Our Global impact [online]*. Yangon: WVI (2020).
10. Robinson RJ. Insights on Cloud Security Management. *Cloud Comput Data Sci*. (2023) 4:212–22. doi: 10.37256/ccds.4220233292
11. Robinson RJ. Digital Security: A Critical Evaluation Process for IT-Security Products. *Math Comput Sci Contemp Dev*. (2024) 6:18–30. doi: 10.9734/bpi/mcscd/v6/2473
12. British Standards Institution. *BIP 0107:2008 Foundations Of It Service Management Based On Itil V3*. London: BSI (2007).
13. Robinson RJ. Cybersecurity compliance frameworks-a pragmatic view with an IT outsourcing company case study. *Soc Lens*. (2024) 1:15–25. doi: 10.69971/sl.1.1.2024.6
14. Hidayah Ab RN, Choo KKR. A survey of information security incident handling in the cloud. *Comput Secur*. (2015) 49:45–69. doi: 10.1016/j.cose.2014.11.006
15. Robinson RJ. Structuring IS framework for controlled corporate through statistical survey analytics. *Springer J Data Inform Manag*. (2020) 2:167–84. doi:10.1007/s42488-020-00021-3
16. Certified Information Systems Auditor. *CISA Review Manual*. 26th ed. Schaumburg, IL: ISACA Education (2015).
17. University of West London. *Information Security Policy. Revised 2017*. London: UWL (2017).
18. Griffiths D. *Risk Based Internal Auditing*. 2006. Available at: www.internalaudit.biz
19. Robinson RJ. *Economy Identity through Information Technology and its Safety*. (2022). Available at: https://play.google.com/store/books/details/Rachel_John_Robinson_Economy_Identity_through_Info?id=haykEAAAQBAJ
20. Technopedia. *Threat Definition [online]. Techopedia website*. (2019). Available from: https://www.techopedia.com/definition/25263/threat
21. ISACA. *IT Control objectives for Cloud computing*. Schaumburg, IL: ISACA Education (2011).
22. TechTarget Search Security. *Access Control Strategy Definition [online]*. 2019. Available from: https://searchsecurity.techtarget.com/definition/access-control
23. NetIQ. *Is Your Security Strategy Proactive or Reactive? [online]. Netiq.com*. (2019). Available from: https://www.netiq.com/documentation/identity-manager-48/security/data/identity-manager-security-guide.html