DOI: 10.31703/girr.2021(IV-IV).04 **URL:** http://dx.doi.org/10.31703/girr.2021(IV-IV).04

p-ISSN: 2788-5054 **e-ISSN:** 2788-5062 **Vol.** IV, **No.** IV (Fall 2021) **Pages:** 22 – 30

GLOBAL INTERNATIONAL RELATIONS REVIEW

Cite Us

Information Security Policy Development: the Mechanism to Ensure Security Over Information Technology Systems

Maryam Saadat* Muhammad Umar Abbasi†

Abstract

Information security is still in its embryonic phase. The reason is that there are certain malevolent actors in the network that are always looking for loopholes in the system and can harm organizations with their malicious activities. The development of information security policy is very important. It lays the foundations of certain significant standards and procedures that help mitigate the potential risks associated with the organization or its network. The following article has discussed information security policy and its respective development cycle for the implementation of policy infrastructure that could help secure vital data and information in an organization. A framework is explained that demonstrates the construction of a policy, keeping in mind the implementation of an effective security policy. It has elaborated the significance of auditing measures focusing on ISO-27001, the policy specifically designed for information security.

Heading

Key Words: Information, Network, ISO-27001, Information Technology, Information Security, Policy, Audit

Introduction

In order to develop a policy, it is first vital to analyze why there is a requirement to build policy in that domain. In the case of Information Security, it is to ensure that all the vital digital or analog forms of information are protected. Securing information in the Information Technology domain embraces network security and infrastructure, as well as auditing and testing. It helps prevent unauthorized individuals from accessing private information not meant to be disclosed to them and ensures the confidentiality, availability and integrity of information. It is also worthwhile to mention that protection of cyberspace and protection of information is not the same, the former is more focused on protection against Internet-based threats, whilst the latter includes a broader range of protection mechanisms such as cryptography, social media, and mobile computing. It even assures information security during non-person-based threats such as system failures.

In the case of a computer network being hacked, there are mainly three objectives that can be achieved. First, data could be stolen from that computer. This would mean any plans of secret strategy present in those files would be accessed by the attacker. Secondly, misuse of credentials, the id of the computer owner could be stolen and

* Bs, Department of International Relations, National Defence University, Islamabad, Pakistan.
Email: maryamsaadat311998@gmail.com
† Assistant Professor, Department of International Relations, National Defence University, Islamabad, Pakistan.

Citation: Saadat, M., & Abbasi, M. U. (2021). Information Security Policy Development: The Mechanism to Ensure Security Over Information Technology Systems. *Global International Relations Review*, *IV*(IV), 22-30. https://doi.org/10.31703/girr.2021(IV-IV).04

the attacker could even enable themselves to access other departments, they could steal all the money in their credit cards, etc. Lastly, they could hijack resources. It is possible for the hackers to hijack any resource that is regulated by a computer having access to the Worldwide Web.

Unlike before, now we live in an era where significant technological advancements have shifted traditional methods of attacks in the international system. Now is the time when the one who obtains more information about their adversary is considered to hold power. Hence it is a time of information warfare. As information technology has certain branches that are still in their development stages and would always be, the need to identify the potential threats associated with each development is vital to ensure that it could ultimately prevent any kind of loss to the organization. Every technology at a certain level has the capacity to get hacked, and for that, the security systems should always be updated that could help fight back against the fraudulent attempts of hackers.

Many researchers have identified that the need for information technology (IT) has become dominant. IT has the capability of making things easy, maximizing speed, increasing convenience, and helping organizations in effective decision making. However, there are potential threats that can impose harsh penalties on organizations for their insecure data that is linked with many lives. Cybercrimes such as high-scale data breaches, online payment fraud, data theft, phishing attacks, and malware injections, etc. are done to compromise the highly confidential and sensitive information of an organization. The number of cybercrimes is increasing every day and demands stringent security measures and procedures that could help mitigate these risks with a very dedicated and tailored approach.

Challenge in the Development of Effective is Policy Structure

As per researchers, the major problems faced by current information security development processes correspond to a lack of guidance to the members regarding security contents. There is a lack of guidance to provide regarding information security that could help take into consideration an appropriate yet full-fledged flow to implement policy. Considering this challenge in information security, a standard information security policy needs to be developed that makes its importance and understanding easy for the practitioners.

Information Security Policy

The role of Information security is quite significant as far as the identification of organizations' s vital assets are concerned. There is a need to protect them in order to eradicate suspicious activities. The main role of Policies are as follows:

- Protecting organization and privacy
- Mitigation of threats
- To define those steps for staff to fight against any suspicious attempt
- Making of infrastructure for access to intimate information
- Defining the responsibilities and roles of every individual

In order to counter threats to ensure information protection, organizations should not focus on how to deal with every individual threat that arises; instead, they should build up security mechanisms that can withstand any cyber-attack thrown at the organization (Flowerday, 2022). This is so because cybercriminals have methodologically similar patterns of targeting systems; hence building up security systems to account for how the organization is targeted would suffice as more profitable rather than just focusing on each individual attack itself. Some of the ways to ensure this is by:

Support the Cyber Security Staff

Senior members of organizations rarely invest in security updates in their cyberspace as they assume information security as an operational cost and do not ponder upon the benefits of investing in it. They fail to realize the better the information security is ensured, the less time they would get to spend fixing data breaches that could potentially occur. It is best to keep up to date with the requirements of the IT team to ensure better and more security of the organization.

Making Risk Assessment a Priority

In order to understand the potential vulnerabilities the systems of an organization may face, it is best to first do a risk assessment. Here penetration testing might be of some assistance. Penetration testing allows a simulated virtual attack to take place on the systems in order to dig out any sort of vulnerabilities existing within the system which could damage the organization in the long run. It is also significant to follow the instructions of the International Standard for Information Security Management ISO 27001. It allows the organization to understand threats and solutions in order to better ensure the information security of their organization. This will be explained in detail in this research article.

Types of Information Security Policies

There are different types of Information security policies depending on the scope and need of an organizational infrastructure.

"Enterprise Information Security Policy(EISP)"

This type is related to the organization's security effort. The main purpose of this type is to generate guidelines for the implementation and management.

"Issue-Specific Security Policies (ISSP)"

The function of this type is to give members detailed instructions for the usage of resources to protect data.

System Specific Security Policies (SysSP)

SysSP is different from other policies as they focus on particular standards or functions that need to be configured and maintained to protect the network. It includes firewall installation in the organization whose ultimate purpose is to protect the network from bad traffic, bad access, or bad actor. Firewalls help protect the network from cyber-attacks. There are two types of SysSP.

One is the "Management Guidance," in which a managerial level document is designed that incorporates guidance regarding the implementation and management of certain technology. The second one is "Technical Specification SysSP," which highlights the need for managerial policy that could be created by system administrators or managers to ensure stronger protection in the organization. This one focuses on making authentication processes more strong to avoid any credential stuffing or similar malicious attempts to access the system outside of the organization.

Approaches towards Information Security Policy Implementation

There are various techniques and procedures to implement the policy of information security.

The top-down and bottom-up approaches to implementing information security policies are both viable options. Bottom-up methods are mostly started by Engineers and Managers of the organizations. It is also used by system administrators.

Because In the top management they do not integrate planning, such as cooperation between divisions and allocation of appropriate funds, this technique is rarely successful. In a top-down strategy, there is coordinated planning from top management, as well as a dedicated advocate who provides financing and proposes a mechanism for execution. The role of Top management is to assign resources, policies, operations and methods.

Policies, Procedures, and Standards

Within an organization, policies are a collection of rules that define what is and is not acceptable conduct. How technology should be utilized is governed by policies. Senior executives should design the information security policy, which is made up of high-level declarations that refers to the safety of information across the company. The policy outlines security roles and obligations, as well as the types of information that must be safeguarded. They should not make specific statements about how software or equipment should be used. Other types of documentation, such as rules, processes, recommendations, and policies, should provide this type of information. The link between rules,

regulations, and activities is depicted in the diagram. Guidelines are a precise description of what has to be done to comply with policies.

The standards assist in enforcing an information security program and make it easier to do so. They aid in ensuring the organization's security consistency, and they often define the security measures associated with the adoption of certain technologies, equipment, or applications. Policies are implemented by practices, procedures, and guidelines that detail how personnel will adhere to them. Standards are supported by guidelines, which are made up of suggested controls. Standards should be viewed as highly suggested best practices. Processes are step-by-step directions for putting policies, norms, and recommendations into action. For example, a method may describe how to install Windows safely by laying down the specific procedures that must be performed in order to protect the OS and ensure that it complies with the relevant policy, norms, and recommendations.

Success Factors

Adopting an information security program may help a company not only become more secure but also mitigate the chances of inappropriate use of the firm's data sources. There are various aspects that must be controlled and guided in order for sensitive information to be implemented successfully. There are a lot of critical aspects that play a role in strengthening an organization's data security. Information and education, supervisory support, finance, information security management implementation, and corporate mission are all critical elements.

Awareness and Training

Organizational information security may be readily obtained by increasing awareness by providing education to all personnel. A security awareness program refers to the knowledge and instructions provided to all members of the organization in order to help them carry out their responsibilities safely.

Enforcement of Information Security Policy

The policy helps identifies the assets of an organization that need to be protected by all means and ensure controlled access over the network. The policy might require revisions and updates as technology evolves.

Information Technology Auditing Process

The auditing process is considered critically important when it comes to the maintenance of compliance and regulatory obligations with the security standards in Information Technology. With increased digitization, the need to employ strong security measures such that any malevolent activities could be mitigated. A huge volume of data is generated every day, and therefore, it is necessary to keep track of this data to avoid any confusion and make it aligned with the rules and regulations defined by regulatory authorities for information security (Boehmer, 2008). These security standards are very interconnected with each other with the ultimate purpose of keeping everything secure and clean in the digital world. It necessitates compliance with multiple security standards, and for that, auditing protocols become important to comply with the requirements of regulatory bodies. ISO standards are one of the most popular IT auditing standards that will be discussed in detail.

In an auditing process, auditors employ a set of multiple procedures and techniques of auditing that involves the observation, research, collection, and analysis processes against which statistical data is obtained. Interviews, observations, questionnaires, analysis, and sampling are all strategies that may be used to gather evidence. The auditors' initial goal is to give an entrance briefing in which the scope of the audit and what they will accomplish are defined. The approach of auditors must be very straightforward and fair enough throughout the audit, where they will be using uniform standards and processes. They will gather information regarding the physical security of all the digital components and sensitive and may perform assessments in network vulnerability, application security analysis, operating system and access control auditing, and other assessments during the comprehensive auditing process. The audit team should stick to their protocols all through the process but keep a lookout for any unforeseen issues.

It is the responsibility of auditors to take into account the assumptions and expectations about the data based on which the standards are applied to properly analyze the data and deduce results accordingly. Upon the completion of the audit, the auditors provide an exit presentation to ensure that the administration is aware of any issues that require attention. To avoid giving the wrong perception about the audit's findings, managerial questions are answered in a broad manner. It should be noted at this point that the auditors may not be able to offer definitive answers. Post completion of the audit process, any final replies are delivered. The auditor's next step is to go over their checklist and analyze their findings using security vulnerabilities software to identify the loopholes that exist in the system and how they could be mitigated to avoid any potential threats that could lead to serious circumstances.

An initial meeting is usually conducted to assist in concentrating on the outcomes of the assessment. The auditors can figure out the potential issues and remedies throughout this meeting. The audit report should be very short and straightforward but should cover all important parameters with concrete findings and quantifiable solutions to the found flaws. A set of procedures and components are followed, depending on audit checklists using which the auditors can offer a complete report. The audit results should be organized in one-page spreadsheets for each found concern in a straightforward and rational fashion.

The audit team's final stage is to compile the document as quickly and accurately as possible in response to the issues uncovered during the assessment. Examiners are to be prepared to assist audit organization employees in fixing flaws and measuring the efficacy of these actions based on corporate policy. A client examines a supplier to check the integrity of transactions, compliance, internal controls, or the entire relationship in the external audit. To put it another way, the company audits its customer or the other way around. The purpose is to guarantee that they provide the performance goals as outlined in their agreements. IT general controls (ITGC) are also included in the auditing process.

Need for Security Audit Report

An information security auditing report is a thorough record that provides an evaluation of an organization's or business security conditions. It is important in order to mitigate the potential security risks and protect the system by all possible means. Its goal is to discover the business's security vulnerabilities and gaps, making it a crucial report that may assist an organization in securing itself.

The information security auditing report is one of the most significant papers used to evaluate the vulnerabilities as well as the strengths of the organization. A security audit report generally lists all of the conclusions gathered by the audit team, which may include vulnerabilities issues, exploits, or other security flaws in the system. Based on the results obtained, loopholes are secured to protect the system from potential threats. The audit report also advises the relevant administration on how to strengthen the cyber security of their firm (Hemantha, 2014).

Use Cases of IT Security Auditing

Below are mentioned some potential use-cases of security reports:

1. Standards and Compliance
2. Local and Global Regulations
3. Customer Reputation and Trust

The Important Parts of a Security Audit Report

One of the key objectives of any audit is to offer meaningful recommendations to the customer so that they may strive to improve their cyber security. This information is provided in the form of a report created at the conclusion of the test.

An internal security audit may be divided into numerous components. A section with data about the objectives, audit scope, time frames, specifics about the testing procedure, conclusions, and suggestions, for example, should be included. An audit report is created by a group of security auditors who conduct an audit on firms or organizations to ensure that they are in compliance with applicable laws. The majority of the time, companies use external security

auditors to conduct an audit and generate an audit report (Kozhakhmet, 2014).

Information Security Audit - ISO 27001

The International Organization for Standardization and the International Electrotechnical Commission jointly produce ISO/IEC 27001, which is an information security management standard to ensure enhanced security over information technology systems. ISO 27001 establishes comprehensive guidelines and standards that demonstrate the ways enterprises should manage the risk of cyber security risks, including strategies, processes, and training of employees.

Cyber security rules, criteria meant to safeguard an organization's data assets and prevent them from potential loss such as unauthorized access trying to access the sensitive information. All practices are recognized as a way of confirming their devotion to information security via certification that is defined within the ISO 27001 standard. ISO 27001 certification involves various risk assessment procedures, technical and physical protection, organizational structure, access control procedures, IT policies, reporting and monitoring, and IT classification.

Due to increasing cyber-attacks and threats to the information system, the need is to employ stringent security mechanisms that help streamline the security processes and procedures. A security review may be conducted for a variety of purposes, such as completing compliance obligations, fulfilling all the regulatory requirements, acquiring a better knowledge of the security of the firm based on security standards, or increasing overall security. Information Technology security auditing is a crucial element of the security of any organization and testing of network infrastructure; thus, choosing the right IT security auditing is a difficult choice.

Because of its extremely sophisticated technical nature, IT security auditing is frequently considered an important part of any organization and for that purpose, ISO has defined the set of procedures and standards for organizations to follow. The steps take into consideration the evaluation and testing of each function and operation of an organization to protect it from potential threats and security hazards. With the ultimate purpose of protecting the organization from cyber attacks, ISO compliance helps mitigate the potential risks (Montesino, 2011).

Benefits of ISO 27001

For the effective administration and seamless running of your organization, protecting its information is vital. For this, many security standards are defined that help protects the organization from data loss, and ultimately ISO 27001 helps companies manage and preserve their important data and information assets. The companies receive numerous and consistent benefits by getting ISO 27001 certification and procedures implementation. Some of the potential benefits of ISO 27001 are:

- It helps keep highly confidential and sensitive organizational information secure from unauthorized access.
- It provides the stakeholders and customers confidence in order to manage the potential risks associated with the organization and the ones connected to the firm's operations.
- Allows organizations and employees to exchange information in a highly secure manner.
- It helps organizations comply with standard security procedures and regulations to mitigate potential risks that can cause heft losses.
- It provides companies a competitive advantage over others as it increases the credibility of following security standards.
- Maximizes customer satisfaction that increases client retention to a significant level.
- Consistent delivery of products and services and minimizes the exposure to risks and manages it seamlessly.
- It protects the organization, stakeholders, assets, and directors.

ISO 27001 certification is appropriate for any company, large or small, in any industry. Any industry using digital services of any kind

needs to take into consideration the security standards defined by ISO in such a way that the loopholes and vulnerabilities could be mitigated and enhanced protection could be provided to an organization. The standard is particularly well suited to industries where data security is vital. Therefore all industries require ISO 27001 certification and security deployment which includes banking and finance, health sector, information technology, and government sector. The guideline also applies to businesses that manage huge amounts of data or information in favor of others, such as computer servers and IT outsourcing firms (Vroom, 2004).

ISO 27001 Controls

ISO 27001 highlights potential requirements for organizations along with advanced technological solutions to protect firms from loss. The list of control sets for organizations to ensure security includes:

- Information security policies to implement in all processes and operations
- Security of Human resource department by providing them security training
- Information security implementation based on the business continuity management
- Communications security to ensure secure data transfer in between the transit
- Operations security and management by evaluating each process and operation
- Information security to protect data and incident management to avoid risks
- Access control to ensure protection against unauthorized access
- Asset management to manage assets and protect them
- Physical as well as environmental security to avoid risks
- System acquisition, maintenance, and development
- Management of supplier relationships
- Cryptography to protect data from strong cryptography has functions that ensure the security of data.
- Compliance with all the procedures and functions.

Steps for ISO 27001 compliance involve:

- Scoping the project by identifying the functions and processes of the system.
- Identify the budget and secure all the management commitments to an extent.
- Identifying all the involved parties, whether they be legal, contractual or regulatory requirements.
- Conduct risk assessment procedures to identify and eliminate the risks.
- Implementation of the security controls that vary from review to evaluation.
- Development of proper documentation that aligns well with the security procedures.
- Conduct training programs for staff and employees to deal with security hazards in an organization.
- Reporting and monitoring of risk assessment plans.
- Review, measure, monitor, and audit the procedures.

Based on all these mentioned components, the security of the organization is evaluated. It helps protect the organization from data breaches, cyber-attacks, denial of service, phishing attacks, and online fraud.

Conclusion

Information security policy plays a vital role in helping organizations streamline all of their processes and help evaluate them to ensure the loopholes are all identified and protected against potential threats so that high-scale data breaches and phishing attacks can be mitigated. Information security demands the identification and evaluation of all the operations of an organization. The loopholes are identified in order to eliminate the risks and provide enhanced security. Similarly, there exists a mechanism to ensure the protection of IT systems. These are set at the International Standard by the ISO group publishing the ISO 27001 regulations. ISO 27001 provides stringent security standards that define security procedures to exploit vulnerabilities and deploy security software. Information security auditing and ISO 27001 also ensure three important components of information security. First is confidentiality, which refers to restricting access to information

and dissemination to authorized users while prohibiting unauthorized users from accessing or transmitting data. Second is the availability of a criterion meant to ensure that processes work swiftly and that authorized persons are not refused service. The third is integrity which refers to the credibility of data resources, ensuring that data has not been modified unlawfully, whether by mistake or on purpose.

References

Flowerday, S. (2022). Information Security Policy Development and Implementation: A content analysis approach. *Accessed January 10*, 2022. https://www.researchgate.net/publication/303061017_Information_Security_Policy_Development_and_Implementation_A_content_analysis_approach

Herath, H. S., & Herath, T. C. (2014). IT security auditing: A performance evaluation decision model. *Decision Support Systems*, *57*, 54–63. https://doi.org/10.1016/j.dss.2013.07.010

Layton, T. P. (2007). "CHAPTER 3 Security Policy: Development and Implementation." Essay. In *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton: Auerbach Publications,

Moneer, A. (2022). Information Security Policy: A Management Practice Perspective. https://www.researchgate.net/publication/341579953_Cybersecurity_A_Generic_Reference_Curriculum.

Montesino, R., & Fenz, S. (2011, August). Information security automation: how far can we go?. In *2011 Sixth International Conference on Availability, Reliability and Security;* 280-285.

Montesino, R. & Fenz, S. (2011). "Information Security Automation: How Far Can We Go?," 2011 Sixth International Conference on Availability, Reliability and Security, 2011,. 280-285, doi: 10.1109/ARES.2011.48.

University of Surrey. (2022). Information security policy. Accessed January 10, 2022. https://www.surrey.ac.uk/sites/default/files/2020-12/information-security.pdf.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & security*, *23*(3), 191-198.

Wiseman, May. (2022). Implementation of information security policies in public organizations. Accessed January 10, 2022. https://www.diva-portal.org/smash/get/diva2:1133654/FULLTEXT01.pdf.

Boehmer, W. (2008). "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001," 2008 Second International Conference on Emerging Security Information, Systems and Technologies, 2008, pp. 224-231, doi: 10.1109/SECURWARE.2008.7.