Super-Essays
-Service.com

Agency Security Regulation Compliance

Introduction

Information is a vital resource for any particular organization. The management of information and information systems remains a mandatory role for any successful institution. However, the implementation of the management system should be based on sufficient information. Monitoring and evaluation of compliance with set rules and regulations is a guiding step for these organizations. This paper will attempt to analyze the existing gap in information by implanting institution. Moreover, it will provide critical insights into the activities that foster compliance. An overview of the guidelines provided by the compliance and legal bodies will also be presented.

Existing Regulatory Requirements

Compliance with the existing laws is a major challenge for many organizations. This phenomenon is usually promoted by the lack of information on the relevant laws. Therefore, it is advisable to facilitate education and the awareness creation initiatives among agencies and various stakeholders. Among the regulations that the agency needs to be cognizant of is the Federal Information Security Management Act (FISMA). This law is established to address issues of information security. It focuses primarily on ensuring that the procedures used in preventing, mitigating, and evaluating security incidents are efficient. Its

scope includes the management of information systems, the assets used in operations both owned by the agency and other affiliated third parties.

This piece of legislation is found in title III of the E-government act passed by the 107th congress and approved by the president in December 2002. The law was drafted in recognition of the role of information security to the national security and economic interests of American citizens.

FISMA advocates risk-based policy for cost-effective security. The Act requires that federal agencies create, document, and execute an agency-wide initiative. This is done to provide information security for both information and the information systems that are used in operations. There is also the support that should include those assets managed by another agency, contractor, or other sources.

In compliance with this Act, the government agency should develop initiatives that conduct periodic risk assessments outlining their various levels of severity. Policies and strategies must be geared towards risk assessments and they should mitigate the information security risk. Further, security awareness training must be facilitated and conducted to ensure that personnel and relevant stakeholders are aware of relevant risks incidents. Periodic evaluation and testing of the efficiency of information security management in terms of procedure, strategies, and controls should be conducted regularly but no less than annually. It is also important for the government agency to come up with strategies for detecting, documenting, reporting, and responding to information

security issues. This should be followed by appropriate plans to ensure that operations of information systems continue in the event of a security incident.

Another relevant legislation that the personnel agency should be acquainted with is the Sarbanes-Oxley Act (2002). It is also referred to as the Public Company Accounting Reform and Investor Protection Act. This Act stipulates that it is a crime for companies trading publicly and non-governmental organizations to institute reactive action against whistle-blowers. An employee who provides information about financial mismanagement by the organization should not be fired, denied promotion, demoted, or harassed. However, the whistle-blower should have a reasonable suspicion of financial impropriety at the time of making the complaint.

The Act also outlines that it is a federal crime for non-governmental organizations and companies trading publicly to destroy internal documents intentionally. This should be complied with by organizations that are under government investigation to ensure that the required documents are accessible. Moreover, the law advocates policies that promote document retention, but it does not limit the destruction of all agency documents.

In line with the Act, the agency should also be aware of the need to establish a competent and independent audit committee as a company trading publicly. These committee members should be part of the organization's board and they are responsible for overseeing the auditing process and supervising the auditors themselves to ensure that

financial concerns are effectively addressed. The agencies' auditors should be rotated after every five years, which will ensure that inappropriate acts are identified. Furthermore, the agency should not also provide loans to top officials such as directors, officers, and executives.

The Sarbanes-Oxley Act provides that chief executives and chief financial officers of companies trading publicly should ensure that they certify company's financial statements. This will increase their cognizance with the financial statements before their issue. In compliance with these requirements, the agency should also disclose any other information that may include financial control, material transactions not recorded on balances sheets and financial statement changes. This information is then availed publicly.

The Gramm-Leach-Bliley Act (GLBA) is concerned with the treatment of individual non-public information about consumers by financial institutions. The Act provides that financial institutions should establish and maintain a detailed written information security program that promotes privacy, security, and integrity of the records and customer information. This calls for financial institutions to adopt strategies to enhance integrative security in networks, databases, applications, and devices. All these elements should work together towards realizing a more stringent information security prevention, mitigation, and management.

The law was enacted in November 1999. It addresses the relationship between insurance, financial institutions, privacy, home loan bank

system modernization, and other financial statutes. The Act prohibits the disclosure of non-public personal information of a consumer by a financial institution to other unaffiliated parties for marketing with the exception that notices or opt-out requirements are given and the consumer has not pre-empted the disclosure. The Act further provides that a financial institution should give notice of privacy practices and policies to its customers.

According to the Act, institutions must adhere to the reuse and re-disclosure limitations on individual information it receives from a non-affiliated financial institution. In compliance with the Act, implementation of technical and administration controls to secure customer information is used. This includes getting knowledge of what the law states first by reading the Act.

The Payment Card Industry Data Security Standard (PCI DSS) was established to facilitate cardholder data security and encourage broad acknowledgement and acceptance of globally standardized data security measures. Payment Card Industry standard security involves operational and technical requirements set by to protect cardholder data by Payment Card Industry security standards council.

Activities adopted by an organization in maintaining the Payment Card Industry data security may include building and maintaining secure networks, cardholders protection, and vulnerability management program maintenance, instituting strong access control strategies, test of networks regularly, and facilitating maintenance of a security policy for information.

In compliance with the set standards, the government agency should ensure that it adopts the strategies of best practices proposed by the Payment Card Industry security standards council. The process entails a three-phased procedure in a sequential fashion. This process includes assessment of the card used, payment card processing assets, and checking for vulnerabilities to the data of the cardholder. Another phase of the standard would involve fixing the vulnerability while ensuring that no storage uses data unless necessary. Finally, it involves submission of reports of compliance with the organization one makes transactions with. A list of vulnerabilities fixed may also be compiled and submitted if they are applicable.

The Health Insurance Portability and Accountability Act also known as the Administrative Simplification was enacted in 1996. It is concerned with the protection of privacy and security of some health information through regulations development by the United States health and human service department.

The Act is grounded on some five fundamental rules that are aimed at administrative simplification. They include privacy through regulation of protected health information use and disclosure, secondly transactions and code set rule that requires health plans to conduct health care transactions in a standardized manner. Another canon is the security rule that focuses on ensuring privacy of specifically electronic protected health information.

Health Insurance Portability and Accountability (HIPAA) also provides for a unique identifier rule that requires the norm that covered entities

must use only the national provider identifier to determine the healthcare providers covered in conducting standard transactions. The enforcement rule, which is a crucial facet of HIPAA, outlines the consequences to those who violate the HIPAA rules by giving methods of systematically investigating incidents of violation.

Business organizations are charged with the responsibility of ensuring that the private healthcare information of an individual is not disclosed. Upon realization of a violation of this Act, the organization should take decisive steps towards fixing or ending the violation. This involves measures of safeguarding the confidentiality, integrity, and availability of healthcare information stored or transmitted by the organization or agency.

The United States Constitution provides for exclusive rights to authors and innovators to their inventions and creations. Intellectual property law covers the regulation for protecting and enforcing legal rights to inventions, designs, and artistic works. The main objective of the legislation is to encourage people who are creative and who contribute to society to benefit from their work without a threat misuse by other third parties.

Through Article 1 Section 8 of the Constitution, Congress is given the mandate to regulate interstate and foreign commerce. These laws passed by the government are implemented by the U.S Patent and Trademark Office and the Copyright Office. Patents can be used by innovators or inventors to profit from their products by selling them to another party or trading the product on the market. This right to patent

may be valid to up to 20 years. They may include improvements in technology, a range of manufactured goods, or even the appearance of a product. On the other hand, trademarks involve protection of symbols, slogans, or names uniquely identifying a good or service. Trademarks are aimed at creating a unique identity for a product, eradicating any form of existing confusion by consumers.

A copyright is a set of intellectual property laws that protect writings, music, motion pictures, architecture, and other intellectual and artistic expressions. The copyright is based on the act of creation and they may range from 70 years to a creator's period of living.

Security Methods and Controls to Ensure Compliance

Compliance remains a main challenge for many organizations. Partial implementation or omission of some of the prerequisites is one of the main problems. Further, this results in the breach of legal requirements or the infringement of rights. Several measures may be adopted to ensure that organizations comply with these requirements. Security control can ensure that the organizations comply with set rules and regulations. Through preventive, detective, and corrective control the incidents of security breach can be realized.

Education and creation of awareness among personnel may improve

their assertiveness in advocating their rights. This is a provocative approach that should be utilized by organizations to ensure compliance. Other physical measures may be instituted to regulate the access to assets and information. By classifying information, establishing authorization and authentication mechanisms access to assets is regulated. Only legitimate users can utilize a set of information, for example, medical records. In line with logic compliance, physical systems may also be used to facilitate compliance, which may include physical systems like building walls, locking assets, etc.

In the context of intellectual property, the compliance with set rules may be facilitated through a strict legal system. Drafting of a formidable legislation and efficient coordination with enforcement agencies such as police will enhance compliance. Breach of intellectual property rights and access to classified information should be punished strictly. Laws against hacking and use of illegally solicited information should be adopted timely and effectively. All these activities should be undertaken by qualified and tech savvy professionals. In foreign countries, the rights should be enforced through interagency and intergovernmental collaboration and partnerships.

Guidelines Provided by Regulatory Bodies

The National Institute of Standards and Technology (NIST) provides a guideline to the implementation and management of information security. Through the issuance and approval of federal information processing standards, it ensures that the standards are binding and they must be adhered to. Moreover, the development of special publications (SP's) provides the guidance and recommendation documents that must be complied with by federal institutions or government agencies and national security programs and systems. NIST also provides inter agency reports that give technical information about its activities. The process of compliance with these security standards is established in policies, directives, or memoranda by the office of management and budget.

The general outline of guidance provided by NIST in information security includes categorizing information systems, selecting the appropriate security controls that are followed by the implementation of the controls. Upon implementation, an assessment authorization and monitoring of the security controls should be conducted by the government agency to improve its efficiency.

The U.S department of Health and Human Services also is greatly involved into the implementation and management of information security strategies. This is done through a number of activities ranging from appropriate use of certified electronic health records, release of educational material and tools, which enable hospitals to minimize the

security incidents in their practice.

Conclusion

The enforcement of an effective regulation in relation to protecting assets and information is an integral part of any organization. Security remains a major issue in the use and conveyance of information in the 21st century. Therefore, it is imperative that all organizations comply with these regulations. Further, the responsibility rests on the enforcement agencies to promote its efficiency. Professionalism and acquisition of relevant contemporary skills to cope with the emerging issues should be prioritized. To ensure compliance and protection of assets, the approach to be taken should always be bipartisan. This serves to protect the mutual interests of both parties and promote safe use of emerging technologies in society.