Research paper on security policy

Business, Management

Security Policy

Creation and implementation of information security policies should be a top priority for any firm, organization or a federal agency that depends on integrated information systems and networks to perform it day-to-day activities. It is most important for government agencies to address information security issues in order to gain the public trust. An improvement in information technology, communication systems, and the use of the internet is a necessary drive for government agencies to change the procedures of carrying out its business and execution of its functions to the public. Without proper policies and security measures to safeguard sensitive information, the agencies run a high risk of unauthorized data access, data manipulation, fraud, system disruptions, and attacks.

The IRS is an example of a government agency that handles the sensitive public information (tax information) which demands a high degree of trust and confidence. The IRS has to ensure that it undertakes the appropriate measures and policy security standards to protect and safeguard public information from an authorized access, use, inspection, manipulation, or disclosure to other parties. This paper will examine the security standards adopted by IRS, compare and contrast them with another independent standard and conclude the overall effectiveness of the standards.

The IRS has adopted the (NIST) National Institute of Standards and Technology Special Publication (SP) 800-53 to implement its information security polices to safeguard the taxpayers information. Alongside the NIST SP 800-53, the IRS also includes in its use the recommended security controls for Federal Information systems (FIS). The IRS implements the two standards with an aim to satisfy the minimum-security requirements by Federal Information Security Management (FISMA) for federal information systems. The requirements include limit and detection of access to sensitive information, Protection from unauthorized disclosure, system integrity management, software safeguards against alterations, segregation of duties to avoid access to information in the whole system and contingency plans to follow in case of emergencies.

ISO 27001 is another example of an information security standard. It is among a series of ISO standards by the international organization for standardization. It recognized among the internationally best standards for an information security management systems (ISMS). It helps organizations and businesses to develop a secure information management system. The design of ISO 27001 standards is meant to harmonize all other standards in the ISO series such as ISO 9001: 2008, 14001, 2004, and 20000. The ISO standardization outlines the specific security and policy requirements that an organization must achieve in order to receive an ISO certification. Implementation of the requirement protects the organizational systems and networks from attacks, unauthorized use and the unnecessary loss of sensitive information due to lack of proper safeguard measures. ISO standardization acts as a yard stick for measuring an organization’s effectiveness in the implementation of Information Security Management System (ISMS).

The NIST SP 800-53 used by the federal government is a design that targets federal information systems. It provides the controls for information access, use, storage, and alterations by federal agents. It outlines the requirements and criteria for office management and budgets in federal such as the IRS. The SP aims at providing a guide to the selection, implementation, and continuous assessment for improvement of an information system throughout its life cycle. Security controls in the SP are in 18 families. Each family has a unique identifier assigned to it and a responsibility area. It outlines the actions to execute to remedy specific threat occurrences. The major disadvantage is the SP standard has a limited application in the private industry. It is common in federal agencies only. ISO standardization on the other hand is very widely applicable in the private sector. It provides the measure of achieving Information Security Management System efficiency. It makes sure that an organization continually upgrades their information systems through the various ISO series. Maintenance requirements and high certification costs are a major disadvantage to this standard.

The SP 800-53 used by IRS and the ISO 27001 have a similarity in their goals for an organization. They both aim at ensuring that organizations meet some specified standards that will ensure the protection and safeguarding of information in an organization’s system. They both offer the criteria and ways of reaching the minimum requirements for certification. While the ISO 27001 standard focuses on the long term and continuous upgrading of an organization’s information system, the SP 800-53 standard places its emphasis on the continuous assessment of information systems to ensure that they meet the current standards. The two standards have a difference in the organization target for which they are designed. The NIST SP 800-53 standard functions well in federal agencies. It designers targeted federal agencies and other government institutions to protect and guard its information. On the other hand, ISO 27001 targets and functions well in private businesses and other non-governmental bodies in protecting and improving their information systems.

In conclusion, IRS should fully implement the NIST SP 800-53 standards through an appropriate framework provided by Federal Information Security Management (FISMA) and the Federal information systems control (FIS). This will improve the public trust and the safety of tax information by IRS as a federal institution.

References:

(GAO) United States, C. o. (2005). Information security Internal Revenue Service needs to remedy serious weaknesses over taxpayer and Bank Secrecy Act data : report to the Committee on the Judiciary House of Representatives. Washington DC: DIANE Publishing.

IRS. (2012, 09 12). Security, Privacy and Assurance. Retrieved from Internal Revenue Service Policy On Limited Personal Use Of Government Information Technology Resources: http://www. irs. gov/irm/part10/irm_10-008-027. html

ltd, I. G. (2012, 09 12). ISO 27001 & Information Security. Retrieved from Specialist services and solutions for IT governance, risk management, compliance and information security. : http://www. itgovernance. co. uk/iso27001. aspx