Fisma Report

Student Name

Institution Affiliation

Professor

Course

Due Date

**Fisma Report**

The Information Security Management Act (FISMA) was enacted by the United States government with the aim of safeguarding governmental data and operations. The risk management methodology in question was initially integrated into the Electronic Government Act of 2002 and has subsequently undergone revisions, as per Granetto's (2019) account. Initially designed to primarily encompass federal agencies, the scope of FISMA has expanded to encompass state agencies responsible for federal programs, in addition to private businesses and service providers operating under U.S. government contracts, since its inception in 2002. In the eight years following the enactment of FISMA, publicly accessible security metrics placed emphasis on agency compliance. Compliance scores reached their highest point in 2008, with all three metrics exceeding 90% (Granetto, 2019). The aforementioned metric was ascertained based on the proportion of systems present in the agency's FISMA inventories that had undergone successful certification and accreditation, had executed and evaluated contingency plans, and had executed and evaluated security controls. The Federal Information Security Management Act (FISMA) mandates the submission of yearly reports to Congress regarding the current state of information security management initiatives.

Since 2002, the Office of the Inspector General (OIG) has been performing yearly autonomous evaluations of agency information security programs in compliance with the Federal Information Security Modernization Act (FISMA). The FISMA metrics for both the Chief Information Officer (CIO) and the Independent Government (IG) have been developed through a collaborative approach involving the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and their interagency partners. The Office of Management and Budget (OMB) engages in a collaborative effort with the Federal privacy community to establish metrics that are intended for use by the Senior Agency Official for Privacy (SAOP). According to Wilshusen (2015), the integration of these three sets of metrics offers a comprehensive perspective on a company's cybersecurity status. During the identical time frame, wherein a tendency towards enhanced information security measures was observed among federal agencies, the quantity of security incidents disclosed by these entities underwent a surge of over 750%. The frequency of cyber-attacks and other forms of threats targeting government networks, systems, and infrastructure has increased. As a result, Congress is currently engaged in ongoing efforts to amend FISMA or introduce new legislation aimed at enhancing information security for government entities. This is primarily being achieved through incentivized disclosure of vulnerabilities.

**Office of Management and Budget (OMB)**

 **Compliance and Reporting**

Most businesses place a high importance on providing effective security protection for information systems and other assets due to the critical enabling role that information security plays in the execution of mission activities and business operations. Federal government entities are required to abide by a number of security and privacy laws and regulations, whilst private businesses are given more freedom to take whatever precautions they see fit to safeguard the personal information and other sensitive data of their clients. The process of making sure compliance, which is covered by the agency's information security program, is ultimately the responsibility of each agency's head. Organizations must strictly adhere to the FISMA regulations. In addition to gathering, managing, and submitting agency-wide security information reported to prove compliance, the day-to-day operations of the agency's information security program must involve compliance with these rules. Consistent reporting and compliance practices can help manage the risks related to information security.

**Agency Reporting Requirements**

According to the Federal Information Security Management Act (FISMA), every federal agency is required to produce an annual report "on the sufficiency and effectiveness of information security policies, procedures, and practices" as well as a report on how effectively the agency complies with all applicable laws and regulations. In addition to incorporating comparable data into their budget formulation, information resource management, program performance monitoring, financial management, internal auditing, and administrative contingency plans, agencies are also required to include comparable data in their plans and reports. This is necessary in order for the agencies to fulfill additional requirements. In accordance with the Federal Information Security Management Act (FISMA), the OMB (and, as of 2010, the DHS) releases recommendations to federal agencies detailing the data and metrics required for reporting on security initiatives on an annual basis (Trzeciak, 2021).

In addition, FISMA reporting activities encompass a range of measures such as monthly automated data feeds of security information from each agency to CyberScope, written responses to a set of questions directed towards chief information officers, senior agency officials for privacy, and inspectors general, and involvement in "CyberState" meetings organized by DHS to aid agencies in evaluating their existing security stance and devising recommendations and action plans for enhancing security. According to Trzeciak (2021), there exists a practice of reporting security information on a monthly or quarterly basis. This practice has been in place since 2010 and has since evolved to incorporate automated data feeds for reporting security metrics. The trend is currently moving towards more frequent reporting. The annual reporting requirement is referenced in both FISMA and the reporting instructions that are disseminated to agencies. The CyberScope platform facilitates the effortless retrieval of current reporting templates and the management of document-based submissions by agency officials. Despite its restricted nature, the summary FISMA report of each agency is incorporated into publicly accessible annual reports submitted to Congress.

**Information Security Program Evaluation**

As per the Federal Information Security Modernization Act (FISMA), federal agencies are mandated to furnish information security metrics and program data for government-wide oversight, and conduct yearly autonomous evaluations to gauge the efficacy of their information security programs. The aim of these analyses is to assess the effectiveness of the agencies' information security programs in safeguarding confidential information. The evaluations in question pertain to the degree of adherence exhibited by an organization with respect to security and privacy regulations such as FISMA, as well as other pertinent rules, policies, and guidelines (Wilshusen, 2015). Furthermore, an assessment is conducted on the security policies, processes, and practices that have been implemented within the information systems of the agency. The assessment of the information security program is frequently carried out by an external auditor who is not affiliated with the organization, the inspector general of the pertinent government agency, or both. The FISMA report conducted by the inspector general on the information security program of the agency has the potential to serve as a valuable tool for internal program evaluation. The report's alignment with administration priorities, FISMA metrics, and baseline questions established for FISMA reporting may prove beneficial. Additionally, agencies may consider broadening the scope of FISMA metrics and topic areas to address program characteristics that hold the greatest significance for them. The reason for this is that FISMA reporting necessitates an evaluation of the information security program vis-à-vis management priorities, FISMA metrics, and baseline inquiries. Inspectors general are obligated to provide answers to inquiries that are based on mandates from the Department of Homeland Security, which possesses the power to oversee the security of operations within executive agencies. The aforementioned guidelines prioritize the demonstration of security control efficiency and risk assessment alignment with Special Publication 800-39, rather than emphasizing compliance as the primary objective (Wilshusen, 2015). The results of evaluations of information security programs and the feedback provided to individual agencies during CyberState reviews can be utilized by said agencies to identify areas of vulnerability, formulate security strategies that encompass the entire organization, and enhance activities related to information systems security and risk management. \

Moreover, FISMA provides federal agencies with a recommended set of security control prerequisites necessary to protect information within an information system.22 According to Wilshusen (2015), it is imperative for federal agencies to assess and analyze the potential hazards to their personally identifiable information (PII) and ensure that appropriate security measures are implemented to ensure an adequate level of safeguarding. Consequently, it is possible that CSPs will need to comply with specific security protocols in the event that they collect, retain, or manipulate personally identifiable information (PII) on behalf of the United States government. The security protocols are based on the accessibility, secrecy, and consistency of the data, which are evaluated through a security classification conducted by either the CSP or the federal agency.

In summary, the adoption of the FISMA cybersecurity architecture and reporting yields numerous tangible advantages that extend beyond mere legal compliance. While there may be financial advantages associated with achieving compliance with the Federal Information Security Modernization Act (FISMA), such as facilitating private sector contractors' interactions with federal agencies, it is widely recognized that the legal standards outlined in FISMA represent industry best practices for devising a comprehensive information security strategy. The Office of Management and Budget (OMB) bears the responsibility of overseeing the information security programs of federal agencies. As a result, the Federal Information Security Modernization Act (FISMA) mandates that these agencies furnish yearly reports to Congress, outlining their level of adherence to the provisions of the statute. Moreover, it is mandated by the Office of Management and Budget that government agencies furnish details pertaining to their extant information security programs. The yearly FISMA reports presented to Congress furnish comprehensive and agency-specific statistics on various information security management elements. The particular metrics are subject to alteration annually, in line with the evolving objectives and priority areas of the federal government concerning information security.

**References**

Granetto, P. J., Marsh, P. A., Blair, E. A., Ball, C. M., Adams, M., Smythe, B., ... & Hart, E. (2019). Defense Finance and Accounting Service Kansas City Federal Manager's Financial Integrity Act, Federal Financial Management Improvement Act, and Federal Information Security Management Acting Reporting of FY 2005. INSPECTOR GENERAL DEPT OF DEFENSE ARLINGTON VA.

Gupta, S. (2020). Assuring compliance with government certification and accreditation regulations. Cloud Computing Security, 387-394.

Trzeciak, A. (2021). Office of Inspector General US Government Accountability Office Semiannual Report to CongressOctober 1, 2020, through March 31, 2021. GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

Wilshusen, G. C., Crosland, L., Businsky, C., Guerrero, R., Glover, N., Ip, A., ... & Wallace, S. (2015). Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs. United States Government Accountability Office.