**FISMA REPORT**

Student’s Name

Institutional Affiliation

Course

Professor’s Name

Date

**FISMA REPORT**

The Federal Information Security Management Act (FISMA) of 2002 is a vital piece of legislation enacted in the United States to improve the security of federal information and information systems. FISMA was created in retort to the growing importance of information technology and the need to guard delicate data and critical infrastructure from cyber threats. FISMA founds a framework for national agencies to grow, document, and implement comprehensive information security programs. These plans are intended to ensure the discretion, honesty, and availability of federal info and the information systems that store, process, and convey that data. FISMA plays an essential role in enhancing the security of federal information and information systems by establishing a framework for federal agencies to develop comprehensive information security programs and acquiesce numerous reports, including System Security Plans (SSPs), Security Assessment Reports (SARs), Plan of Actions and Milestones (POA&Ms), and Annual Security Reports (ASRs), which are crucial for identifying susceptibilities, improving security controls, and monitoring the growth of security wits within the federal government

FISMA incorporates numerous integral components meant for enhancing the security of federal information and information systems. These components form the framework through which federal agencies develop inclusive information security programs and fulfill reporting necessities (Barret et.al., 2020). Risk managing stands at the essential of FISMA, emphasizing the need for agencies to adopt risk-based tactics in identifying, evaluating, and extenuating information security risks. Observance to security standards and guidelines, mostly those established by the National Institute of Standards and Technology (NIST), is authorized by FISMA. These rules provide thorough orders on selecting, applying, and evaluating security controls across several fields.

Another key factor is the development and maintenance of System Security Plans (SSPs) for each information system. These plans serve as blueprints, documenting system boundaries, architecture, operational environment, and implemented security controls. Security assessments play a crucial role in evaluating the effectiveness of security measures. Federal agencies are required to conduct regular assessments, which involve technical testing, vulnerability scanning, and manual reviews (USAID, 2020). The findings and recommendations from these assessments are documented in Security Assessment Reports (SARs). When vulnerabilities are identified, agencies develop Plan of Actions and Milestones (POA&Ms) that outline the steps and milestones to address and remediate the weaknesses. Continuous monitoring is encouraged to ensure ongoing evaluation and maintenance of security controls and the security status of information systems. Reporting and accountability are also fundamental to FISMA, with agencies producing Annual Security Reports (ASRs) that assess the overall state of their information security programs and provide transparency and accountability to stakeholders. By embracing these components, federal agencies can effectively protect sensitive information, mitigate risks, and ensure the integrity, confidentiality, and availability of critical government data.

FISMA reports support the sharing of best practices, lessons learned, and information on emerging threats across federal agencies. By analyzing the findings and recommendations from these reports, agencies can enhance their security programs, update policies and procedures, and allocate resources effectively to mitigate potential vulnerabilities. Over the years, FISMA has evolved, and additional guidance has been provided by NIST to support agencies in implementing the law's requirements. According to USAID, (2020) NIST Special Publication 800-53 and 800-37, among others, provide detailed guidelines on developing SSPs, conducting security assessments, and preparing FISMA reports.

One of the main aims of FISMA reports is to validate compliance with FISMA requirements. These necessities outline the essential steps and measures that federal agencies must commence to defend their information assets. By preparing and submitting FISMA reports, agencies provide evidence of their adherence to these requirements, showcasing their commitment to maintaining a robust and secure information infrastructure. FISMA reports typically involve a comprehensive evaluation of various aspects of an agency's information security program (Weber, 2019). This evaluation includes the assessment of security controls, risk management practices, incident response capabilities, system inventory, and continuous monitoring processes. By thoroughly examining these areas, FISMA reports help identify strengths and weaknesses within an agency's security posture.

The examination of security controls is a perilous component of FISMA reports. This assessment focuses on determining whether the applied controls line up with industry best applies and fulfill the relevant security standards. Agencies must prove that they have applied appropriate safeguards to guard sensitive information and preserve the discretion, integrity, and availability of their systems (Weber, 2019). Risk management is another vital aspect covered in FISMA reports. Agencies are needed to conduct regular risk assessments to identify potential vulnerabilities and assess the impact and likelihood of various threats. FISMA reports examine the agency's risk management practices, assessing the efficiency of risk assessment methodologies, risk mitigation strategies, and the implementation of security controls to address identified risks.

Incident response capabilities and processes are also evaluated in FISMA reports. These assessments gauge an agency's readiness to detect, respond to, and recover from security incidents. The reports evaluate the competence of incident response plans, incident handling measures, and the coordination of incident response efforts. They also assess the agency's incident reporting practices to guarantee timely and precise reporting of security incidents. Furthermore, FISMA reports encompass the evaluation of the agency's system inventory. This includes assessing the accuracy and completeness of the inventory, ensuring that all information systems are properly identified and categorized (Syafrizal, et.al., 2020) The system inventory analysis provides insights into the scope of the agency's information security responsibilities and assists in identifying potential gaps or areas of improvement in securing the systems.

Continuous monitoring is a vital element of FISMA reports. Agencies must establish processes for ongoing monitoring, assessment, and improvement of their information security controls. FISMA reports evaluate the agency's continuous monitoring practices, including the tools and technologies utilized, the frequency of monitoring activities, and the effectiveness of monitoring in detecting and responding to security incidents (Barret et.al., 2020). In addition to assessing the existing state of an agency's data security program, FISMA reports also provide references for improvement. These endorsements are based on the findings and remarks from the assessment process. They guide agencies in enhancing their security posture, addressing identified vulnerabilities, and implementing measures to mitigate risks effectively.

FISMA reports play an important role in promoting transparency, accountability, and information sharing within the federal government. They offer crucial information to agency leadership, Assembly, auditors, and other stakeholders concerning the agency's information security program's effectiveness and compliance with regulatory requirements. Furthermore, FISMA reports may encompass an evaluation of the agency's security incident response exercises and simulations (Syafrizal et.al., 2020). These exercises test the agency's incident response procedures, coordination among stakeholders, and the effectiveness of incident response plans. The report assesses the agency's performance during these exercises and identifies areas for improvement, ensuring that the agency is adequately prepared to handle and respond to real-world security incidents.

Another aspect that FISMA reports may address is the agency's supply chain risk management practices. This includes evaluating the processes in place to identify and mitigate potential risks arising from third-party vendors, contractors, and other external entities that have access to the agency's information systems. Assessing supply chain risks helps ensure the security and integrity of the agency's information assets and prevents unauthorized access or compromise through external connections. FISMA reports also play a crucial role in facilitating information sharing and collaboration among federal agencies (Barret et.al., 2020). They serve as a platform for agencies to learn from each other's experiences, share best practices, and identify common challenges. The reports provide insights into successful security initiatives and strategies implemented by agencies, promoting knowledge exchange and fostering a culture of continuous improvement in information security practices across the government.

Moreover, FISMA reports contribute to the overall cybersecurity posture of the nation. The compilation of data and insights from these reports allows for a broader analysis of the state of federal information security. It allows policymakers and regulators to recognize trends, developing threats, and areas where extra guidance or possessions may be needed to strengthen information security at a national level. It is important noting that FISMA reports are not motionless documents but rather part of a continuing process (Ahamas $ Rajpu, 2020). Federal agencies are required to review and update their reports frequently, reflecting changes in their information security programs, evolving threats, and emerging technologies.

To crown it all, FISMA reports serve as complete assessments of federal agencies' information security programs, providing a detailed assessment of their acquiescence with FISMA requirements and the effectiveness of their security controls. These reports play a crucial role in promoting transparency, responsibility, and information sharing within the government, allowing agencies to validate their obligation to protecting federal information and information systems. By evaluating several components such as security controls, risk management applies, occurrence response capabilities, system inventory, and ongoing monitoring processes, FISMA reports identify strengths, weaknesses, and areas for improvement in an agency's security posture. Additionally, these reports contribute to the broader national cybersecurity landscape by facilitating knowledge exchange, promoting best practices, and enabling policymakers and regulators to assess the state of federal information security. FISMA reports are not static documents but rather part of an ongoing process, encouraging agencies to continuously enhance their information security programs and adapt to evolving threats. Ultimately, FISMA reports play a crucial role in strengthening the overall security posture of federal agencies, safeguarding sensitive information, and ensuring the resilience of the nation's critical information infrastructure.

**REFERENCES**

Ahmed, S. M., & Rajput, A. (2020). Threats to patients’ privacy in smart healthcare environment. In *Innovation in Health Informatics* (pp. 375-393). Academic Press.

Barrett, M., Barrett, M., Marron, J., Pillitteri, V. Y., Boyens, J., Quinn, S., ... & Feldman, L. (2020). *Approaches for Federal Agencies to Use the Cybersecurity Framework*. US Department of Commerce, National Institute of Standards and Technology.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432.

USAID, U. (2020). Usaid Fisma quarterly reporting update-FY 2020 Q1 quarterly report.

Weber, R. (2019). IG review of FISMA requirements says DOD lacks cybersecurity oversight. *Inside the Pentagon*, *35*(3), 12-12.