**FISMA Report**

Name

Institution

Instructor

Date

**FISMA Report**

A FISMA report is a report created under the Federal Information Security Management Act (FISMA). FISMA is U.S government legislation that defines a comprehensive framework to protect government information, operations and assets against threats. It was signed into law in 2002 and updated in 2014 and it requires that federal systems meet a set level of security requirements. FISMA was introduced to strengthen cybersecurity defenses of federal information networks and systems and it applies to any organization within the federal information network. FISMA makes the National Institute of Standards and Technology responsible for developing cybersecurity standards and guidelines. Government agencies must review their cybersecurity program each year as part of their FISMA compliance reporting requirements and submitting their performance report to the Office of Management and Budget.

A FISMA report include an assessment of the information of the agency`s security controls, risk management practices and compliance with security standards. The reports help identify weakness in the agency and guide the implementation of appropriate measures taken to mitigate the identified deficiencies.

Security compliance is often an integral part of every Federal IT pro`s decision making process. FISMA compliance defines a vast and detailed set of security requirements. FISMA compliance was initially applicable to federal agencies, however it is now applicable to state agencies involved in federal programs and companies that are in a contractual relationship with federal agencies.

The government controls a lot of information and letting the information fall into wrong hands can lead to dire consequences. Because the risk of catastrophe is high, the standard for protecting that data needs to be high. The controls put in place to protect government information must match the risk and potential scale of harm that could transpire if the data were accessed, distributed or manipulated by a malicious source. Potential consequences for not following FISMA compliance can be huge and any agency that fails to comply to the FISMA guidelines runs the risk of losing federal funding. A government contractor can lose the entire business or miss out on future bids for government-funded projects.

There is a vast set of security requirements to be fulfilled by agencies to become FISMA compliant and FISMA has outlined several steps to be followed with an intent to help reduce security risks for agencies. An inventory of all information systems needs to be maintained by every federal agency and entities working in collaboration with the government. In addition, the agencies also need to maintain an inventory of interdependencies between the systems and the interdependence between internal systems and systems not under the control of the agency.

All agency data and IT systems must be categorized according to risk-low, moderate or high. A low impact system is generally information which does not contain sensitive information that requires safeguarding. A moderate impact system may contain such information and will require a greater degree of safeguarding. A high impact system contains information where it has been determined that a loss or compromise of such information would present a grave risk to the U.S government.

Certification and accreditation. Agencies need to go through a four-phased process to achieve certification and accreditation. The four- phase are initiation, planning, certification and monitoring. The certification process is outlined in NIST SP 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems.”

Utilize security controls. There are multiple security controls recommended for FISMA compliance however agencies should not implement all the security controls. They need to assess the security requirements of their organization and accordingly implement the appropriate security controls relevant to their organization. The organizations also need to document the chosen security controls in the system of the security plan. The range of security controls include risk assessment, certification and accreditation assessments, security planning, configuration management and personnel security.

All agencies must develop and maintain a system security plan. The System Security Plan (SSP) defines how the agency will implement security controls and it must be updated regularly including a Plan of Action and Milestones (POA&M). The security plan should outline the plan of action and security that have already been deployed within the organization.

Continual assessment and monitoring. The threat landscape is constantly evolving which means that agencies need to implement the appropriate security measures from time to time. FISMA compliance demands regular monitoring of systems which makes agencies well-prepared to avert and respond to any kind of attacks. The types of monitoring include configuration management, file integrity monitoring, vulnerability scanning and log analysis.

Conduct risk assessment. Every agency must validate the successful implementation of its security controls through risk assessments. During this risk assessments, agencies also determine if additional controls are necessary to provide extra protection for any information or IT systems. The NIST guidelines requires agencies conduct a three-tiered risk assessment to detect risks at all levels such as organizational level, business process level and the information system levels.

FISMA metric domains are aligned to the five functions outlined in NIST`S cybersecurity framework. They are: identify, protect, detect, respond and recover. In identification, metric focuses on measuring an agency`s ability to identify, manage and map systems and networks. This function also focuses on the diagnosis of network issues and systems.

In protection, the metric records the level of safeguarding for networks and systems. The function helps an organization understand its ability to contain a cybersecurity incident, protecting the rest of the network. In detection, metric deal with the process of detecting and discovering system and network breaches or changes.

The metric focuses on policies to respond to cybersecurity incidents including the creation and testing of response plans. The metric collects information and recovery plans in place to respond to cybersecurity breaches or disruption to networks. These are known as the core functions of the framework and represent the key steps to achieving effective cybersecurity.

A FISMA report should include documentation such as audit logs. A FISMA audit is a program which ensures that government agencies as well as private agencies with government affiliations or contracts properly secure and store sensitive data. FISMA also requires the information systems utilized by these organizations to be equally protected and monitored. Federal contractors are the responsible for conducting audits annually to assess the continued efficacy of their compliance programs and to document their ongoing efforts to maintain compliance.

There are key steps involved in conducting a FISMA audit. Federal contractors should identify all relevant internal systems and software applications. Failure to comply can lead to exposure of sensitive information of the government data to malicious intrusion. Identification of internal system helps avoid such consequences. There should be also identification of all relevant external systems and facilities to avoid external exposure of sensitive data.

Examination of federal contractor`s FISMA compliance documentation. Federal contractors need to ensure that their compliance documentation remains adequate in light of any changes to their operating environments. As new threats arise, these may necessitate changes to contractors and FISMA compliance programs as well. Reviewing of the contractor`s certifications and accreditations is also done in FISMA audits.

A FISMA report is an essential component in ensuring the security and protection of federal information systems and data. FISMA enhances compliance for effectiveness of the security system. FISMA compliance provides a good starting point for security implementation. This increases the security of federal information and it will protect exposure of sensitive information to unauthorized individuals. Compliance also ensures there are best security policies for businesses in the private sector. A FISMA report helps evaluate an agency`s compliance to security requirements and provides insights to the effectiveness of their security measures.

The FISMA report identifies and assesses potential risks and vulnerabilities within an agency`s information system. It helps identify weaknesses and gaps that can be used by attackers and provide recommendations to mitigate those risks. This assessment helps boost the security system therefore it safeguards sensitive information from sabotage by outsiders.

A FISMA report serves as a record of an agency`s security posture, documenting their efforts to protect sensitive information. This helps demonstrate compliance to auditors, stakeholders and the public. This enhances accountability of agencies to the security of their information systems hence a security practice.

The FISMA report helps agencies in budget and resource allocation since the FISMA report identifies areas and gaps where additional resources need to be allocated. This helps further investments and also facilitate informed decisions regarding budget allocation for information security initiatives.

In conclusion, a FISMA report provides a detailed assessment on cybersecurity and helps avoid cyber threats within an organization or government agency since it plays a crucial role in ensuring sensitive information are protected. The FISMA report highlights the strengths and weaknesses of an organization and provides a stage for enhanced security measures. By adhering to the guidelines outlined in the FISMA report, organization can boost their security system and safeguard their information assets.

**References**

. Malin, A., & Van Heule, G. (2013). *Continuous monitoring and cyber security for high performance computing*. <https://doi.org/10.1145/2465808.2465810>

.Johnson, L. R. (2015). Security Controls Evaluation, Testing, and Assessment Handbook.*Elsevier eBooks*. <https://doi.org/10.1016/c2013-0-13416-2>

Cebula, J. E., Popeck, M., & Young, L. R. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*. <https://doi.org/10.21236/ada609863>

Howard, P. (2016). FISMA Principles and Best Practices. In *Auerbach Publications eBooks*. <https://doi.org/10.1201/b10782-5>