**FISMA Report**

Students Name

Institutional Affiliation

Professor’s Name

Course Name

Due Date

**FISMA Report**

FISMA is a piece of U.S. government legislation establishing a comprehensive framework for safeguarding sensitive data, activities, and assets. FISMA, enacted in 2002 and revised in 2014, stipulates a certain level of security for government networks. Programs for security awareness education are intended to help employees identify security vulnerabilities and take the proper action, enhancing the organization's overall security posture. Several public and private sector industries need or advocate yearly security awareness instruction. The Federal Information Security Modernization Act of 2014 (FISMA) is an example of a law that governs cybersecurity in the United States and is an official contribution from the National Institute of Standards and Technology. It is not protected by American copyright. In the Workshop on Security Information Workers (WSIW) 2022 on August 7 in Boston, Massachusetts, USA, government workers and contractors were required to give comparable awareness training under the General Data Protection Regulation of the European Union.

The Department of Homeland Security's responsibilities for managing the application of information security policies for Federal Executive Branch civilian agencies, monitoring adherence to those policies, and aiding OMB in establishing such policies are codified under FISMA 2014 ( Jacobs et al., 2022, July). Under OMB principles and procedures, the legislation grants the Department the authority to create and supervise the execution of legally binding operational instructions for other agencies ( Jacobs et al., 2022, July). Additionally, it: enables DHS to offer operational and technical support to other civilian federal executive branch departments upon request; binds DHS to operate the federal information security incident centre (a duty now performed by US-CERT); enables the introduction of DHS technology onto the networks of other agencies (upon request from those agencies); Directs OMB to update its guidelines for notifying those who

the government may impact

Organizations may gather metrics regarding their security awareness programmes for obligatory reporting purposes, to justify funding, or to show overall programme success. The number of organizational workers who complete the training, or compliance with the training requirements, is a standard metric used to assess the performance of security awareness programmes. These compliance indicators, however, might not show if staff security behaviours and attitudes have improved (Jacobs et al., 2022, July). According to earlier research and industry surveys, security awareness programmes frequently fail to alter behaviour, partly because they need help with quantifying programme impact. With an understanding of the impact, security awareness programmes may be able to pinpoint the changes required to encourage behaviour change while addressing employee and organizational needs ( Jacobs et al., 2022, July). Few studies have started to investigate methods and difficulties for evaluating organizational security awareness programmes, particularly in compliance-focused industries.

Security awareness programmes must be successful; measuring that accomplishment can be difficult. Even if the information is not a guarantee of behaviour, few studies offer specific advice on evaluating the long-term efficacy of security awareness programmes beyond knowledge-based tests. The reliance of organizations on adherence to awareness policies (like FISMA) may contribute to the need for adequate measurement ( Jacobs et al., 2022, July). When the focus should be on behaviour modification, compliance-focused organizations mistakenly use training completion rates as a measure of success.

Researchers advise using a combination of practical measures for a comprehensive evaluation, including the quantity and types of security incidents related to training topics, user-initiated incident reporting, click rates for phishing simulations, views and engagement with security awareness materials, and stakeholder feedback via surveys and interviews ( Jacobs et al., 2022, July). According to I.T. specialists in small and medium-sized firms, measurement systems should use a semi-automated approach, combining data obtained by automated tools or processes and gathered via staff surveys or interviews ( Jacobs et al., 2022, July). A supporting visualization component should be included to communicate metrics to stakeholders straightforwardly. Additionally, to address alleged deficiencies, awareness personnel should suggest corrective actions. The cybersecurity training centre SANS discovered that businesses that benchmark their programmes against competitors typically have more vital executive support for security awareness training and, consequently, tremendous success ( Jacobs et al., 2022, July). The five-level Security Awareness Maturity Model is an example of a maturity model that can be used as a peer benchmark.

The research on compliance and the design of security rules is currently dwarfed by recent studies on security breaches using the expanding datasets of security failures. The current body of academic and industrial research on control catalogues emphasizes how well they are implemented and whether they improve security results (Stiles, 2018). Organizations take the promised effectiveness of the control catalogues for granted and do not question it. For several reasons, there may be little research on the effectiveness of security compliance control catalogue architectures (Stiles, 2018). Obtaining specific information on compliance solutions can be challenging since the security compliance industry is still very young.

Nevertheless, the structure of the compliance standards and the fundamentals of security compliance is crucial for enabling efficient online commerce. Compliance frameworks, such as control catalogues, are created by organizations called "trust frameworks" (Stiles, 2018). Business procedures between organizations are governed by a shared set of rules developed by trust frameworks. The benefit of a shared framework is that it eliminates the requirement that each participating organization perform due diligence on all other participating organizations while establishing standard data transmission formats, processing guidelines, and levels of information security.

An extensive control inventory frequently accompanies frameworks for information security. Control catalogues is a term used to describe a set of computer security procedures intended to safeguard systems and data (Stiles, 2018). A control is described as "a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements" in the control catalogue created to comply with the Federal Information Security Management Act (FISMA) (Stiles, 2018). The frameworks compile a list of these specific safeguards and arrange them according to a process or control purpose.

The security compliance frameworks for federal contractors and agencies, businesses engaged in credit card processing, cloud service providers wishing to store federal data, and healthcare organizations and their business partners include control catalogues. Control catalogues are also included in voluntary compliance frameworks like the ISO 27000 series and the omnibus compliance certification HITRUST (Stiles, 2018). These frameworks offer a classic collection of security best practices for organizations to use to satisfy various security needs. As each catalogue develops to suit various data protection regulations, the objective of a single set of best practices may still need to be achieved.

The variation in approaches to the same protection can be seen by comparing a control across several control libraries. Nearly all control catalogues address passwords since they are a common control. The reference control for passwords in the ISO 27002:2013 standard provides instructions on seven requirements (Stiles, 2018). The International Organisation for Standardisation lists five qualities that make a good password, including "easily remembered" and "not vulnerable to dictionary attacks." For FISMA compliance, the Identification and Authentication Control (IA-5) goes further. IA-5 lays out ten requirements for a company to create an authenticator (Stiles, 2018). Four control improvements are also included in a moderate implementation. Control improvement IA-5(1) outlines five password standards, including that the organization establishes password complexity, uses only encrypted passwords for storage and transmission and forbids password reuse.

PCI-DSS version 3.2 The password requirements are more fully described in requirement eight. The 24 components of Requirement 8 give the organization less latitude. According to the PCI Security Standards Council (2016), complexity is defined as "at least seven characters" and "contains both numeric and alphabetic characters." This diversity of organizational advice shows no universal method for the straightforward control of creating a user password (Stiles, 2018). Implementing a single information security framework is a must for most organizations. An organization that maintains or processes data on individuals must use at least one of these control catalogues, thanks to the U.S.'s sectoral approach to privacy and security regulation and individual contract obligations (Stiles, 2018). A small business was born from mapping these controls from one compliance framework to another. One such framework is the HITRUST framework, which offers certifications across its meta-framework, which includes the HIPAA, PCI-DSS, and ISO catalogues (Stiles, 2018). To address the issue of compliance with various control catalogues, certifications for people to map controls from one catalogue to another have been created.

In general, regulation-mandated control catalogues affect an organization's security outcomes differently. Because control catalogues are effective at delivering certification to build trust between organizations, regulations based on them continue to be in place. It's possible that evaluating an organization based on its capacity to apply a particular set of best practices will yield unreliable or even enough indicators of the security outcomes of the organization. Replace the control catalogues with systems that require the information security team to gather more data directly from business operations and personnel as one potential solution. While fully supporting the information security objectives, a different approach to conveying this information might create a stronger foundation for informed trust between information trading partners.

**References**

Jacobs, J. L., Haney, J. M., & Furman, S. M. (2022, July). Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022) 8th Workshop on Security Information Workers (WSIW 2022). This workshop aims to develop and stimulate discussion about security information workers., Boston, MA, U.S*.

Stiles, R. (2018). *Information security trust and outcomes: a case study of compliance in a complex system* (Doctoral dissertation).