Security Awareness Compliance Requirements

Updated: 11 October, 2017

Executive Summary

The purpose of this document is to identify different standards and regulations that require security awareness programs.

ISO/IEC 27001 and 27002

8.2.2: *All employees of the organization and, where relevant, contractors and third-party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.*

Learn more at: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

PCI DSS

12.6: *Make all employees aware of the importance of cardholder information security.*

- *Educate employees (for example, through posters, letters, memos, meetings, and promotions).*
- *Require employees to acknowledge in writing that they have read and understand the company's security policy and procedures.*

Download the PCI DSS standard at: https://www.pcisecuritystandards.org/document_library

Download the PCI DSS Security Awareness Program Guidelines at: https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Federal Information Security Management Act (FISMA)

§3544.(b).(4).(A),(B): *Securing awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks.*

Learn more at: http://www.dhs.gov/fisma

Gramm-Leach Bliley Act

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. Depending on the nature of their business operations, firms should consider implementing the following practices: Employee Management and Training. The success of your information security plan depends largely on the employees who implement it.

GLBA Overview: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Safeguards Rule: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Health Insurance Portability and Accountability Act (HIPAA)

§164.308.(a).(5).(i): *Implement a security awareness and training program for all members of its workforce (including management).*

Learn more at: http://www.hhs.gov/hipaa/for-professionals/index.html

Red Flags Rule

§16 CFR 681.1(d)-(e): Employees should be trained about the various red flags to look for and any other relevant aspect of the organization's Identity Theft Prevention Program.

Learn more at: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule

NERC CIP

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standard. *CIP-004-5.1 R1 - Each Responsible Entity shall implement one or more documented processes that collectively include security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.*

Learn more at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

CobiT

PO7.4 Personnel Training: *Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls, and security awareness at the level required to achieve organizational goals.*

§DS7: *Management of the process of educate and train users that satisfies the business requirement for IT of effectively and efficiently using applications and technology solutions and ensuring user compliance with policies and procedures is: […] 3 Defined when a training and education program is instituted and communicated, and employees and managers identify and document training needs. Training and education processes are standardized and documented. Budgets, resources, facilities, and trainers are established to support the training and education program. Formal classes are given to employees on ethical conduct and system security awareness and practices. Most training and education processes are monitored, but not all deviations are likely to be detected by management. Analysis of training and education problems is applied only occasionally,*

Learn more at: https://cobitonline.isaca.org/

U.S. State Privacy Laws

Many states in the United States have individual privacy laws. You can find a listing of most of those state privacy laws at the Morrison & Foerster's Privacy Library. Many of these privacy laws require some type of awareness training or at a minimum that the privacy requirements are communicated to employees in that state.

Learn more at: https://www.mofo.com/privacy-library

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is the latest data security legislation in the European Union, it takes effect 25 May, 2018. The European Union has directed all European member countries to develop and define laws regarding the protecting of personal privacy of the citizens of their respective country. This regulation has specific requirements for data breach notification (within 72 hours) and fines up to 4% of the organization's global revenues. Although each country's implementation of this regulation is different and unique, the regulation does require a security awareness program. Under Article 39:

The data protection officer shall have at least the following tasks: ... (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; ..."

Learn more at: http://www.eugdpr.org

Australian Government InfoSec Manual

§0252: Information security awareness and training: Revision: 2; Updated: Nov-10; Applicability: U, IC, R/P, C, S/HP, TS; Compliance: must

Agencies must provide ongoing information security awareness and training for personnel on information security policies including topics such as responsibilities, consequences of noncompliance, and potential security risks and countermeasures.

Download the manual at: http://www.asd.gov.au/infosec/ism

PAS555 Cyber Security Risk: Governance and Management

PAS 555 is a UK standard that offers a framework that defines the outcome of good cyber security practice. It extends beyond the technical aspects of cyber security risk to encompass physical and people (behavioral) security aspects as well.

Clause 4: Commitment to a Cyber Security Culture: *The organization's top management shall define and demonstrate how it engenders a culture of cyber security within the organization. (Note: A cyber security culture is one in which values, attitudes, and behaviors are the foundation of day-to-day life in the organization. It is one where being careless about (cyber) security is not acceptable. It is recognized that it takes time to achieve a culture change and cannot be immediate.)*

*Cl*ause 7: Capability Development Strategy: *The organization shall have cyber security awareness programs, training, and development so that all individuals in the extended enterprise have the awareness and competence to fulfill their cyber security role and contribute to an effective cyber security culture.*

Learn more at http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030261972