Security Awareness Compliance Requirements

Executive Summary

The purpose of this document is to identify some of the most common standards, regulations, and frameworks that require security awareness programs. We do not consider this list comprehensive, new standards are constantly being developed with many specific to certain countries or industries.

ISO 27001:2022

ISO 27001 is an international standard that outlines best practices for an Information Security Management System (ISMS). Developed and published by the International Organization for Standardization (ISO), it is a controls-based framework for organizations to manage and protect their information assets. In addition, it is part of a larger series of documents known as 27000. In many cases 27001 is optional, but you must pay for a copy of the document.

Annex A 6.3: *Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function*.

Learn more at: https://www.iso.org/standard/27001

Center for Internet Security (CIS) Controls

Center for Internet Security is a non-profit providing numerous security resources for the community. One of those resources is the 18 CIS Critical Security Controls, a controls-based framework to managing risk. In most cases the standard is optional, and the Critical Security Controls are free for organizations to download and use.

14. Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Learn more at: https://www.cisecurity.org/controls/cis-controls-list

NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework is a globally recognized framework enabling organizations to effectively manage their risk and benchmark against others. While developed by the United States government (specifically the National Institute of Standards and Technology) the strategic framework is freely available for any organization to use. PR.AT (Protection / Awareness & Training) defines the Security Awareness and Training requirements.

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security–related duties and responsibilities consistent with related policies, procedures, and agreements.

Learn more at: https://www.nist.gov/cyberframework

PCI-DSS

PCI-DSS stands for Payment Card Industry Data Security Standard. It is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. PCI-DSS is required for any organization handling card-holder data and is administered by the Payment Card Industry Security Standards Council (PCI SSC).

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

PCI-DSS is one of the few standards to provide guidelines specifically for Security Awareness Programs:
https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in the European Union (EU) on May 25, 2018. It replaced the 1995 Data Protection Directive and significantly changed how data is protected and managed across the EU and the world. GDPR has had a global impact, affecting any organization worldwide that handles the personal data of individuals residing in the EU.

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: https://gdpr.eu/

NIST SP 800-53 Rev. 5

NIST SP800-53 is the primary controls document for United States federal departments and agencies. SP800-53 aligns with the NIST Cybersecurity Framework. AT-1 thru AT-6: Awareness and Training specify the requirements for Security Awareness and Training.

Learn more at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a United States federal law that primarily affects financial institutions and how they handle consumers' private financial information. The Safeguards Rule, a component of GLBA, 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 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

NERC CIP

NERC CIP refers to the Critical Infrastructure Protection standards developed by the North American Electric Reliability Corporation (NERC). These standards are a set of requirements designed to secure the assets required for operating North America's bulk electric system. Most countries have similar regulations for their electric / power generation systems and industry.

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: https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA, or the Health Insurance Portability and Accountability Act, is a United States federal law enacted in 1996. One of the key purposes of HIPAA is in the protection and confidential handling of protected health information (PHI). This part of the law, often referred to as the HIPAA Privacy Rule, sets national standards for the protection of individual medical records and other personal health information. It applies to health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically.

§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

COBIT

COBIT (Control Objectives for Information and Related Technologies) is a framework for the governance and management of enterprise IT. It provides guidelines and best practices to help organizations ensure effective and efficient use of IT in achieving their business goals. COBIT is widely recognized and used by organizations globally for IT governance. Developed by ISACA (Information Systems Audit and Control Association), COBIT is designed to be used by businesses of all sizes and sectors.

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.

Learn more at: https://www.isaca.org/resources/cobit

Australian Government InfoSec Manual

The Australian Government Information Security Manual (ISM) is a set of guidelines and best practices issued by the Australian Cyber Security Centre (ACSC) to assist in the protection of Australian government information systems and data. The ISM is designed for Australian government agencies, but its principles can also be valuable for private sector organizations seeking guidance on effective information security practices.

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

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: https://www.cyber.gov.au/acsc/view-all-content/ism

PAS 555 Cyber Security Risk: Governance and Management

PAS 555, officially known as PAS 555:2013 Cyber security risk - Governance and management - Specification, is a framework created by the British Standards Institution (BSI), the National Standards Body. It is designed to help organizations manage their exposure to cybersecurity risks. The PAS (Publicly Available Specification) provides a set of guidelines that defines the overall outcomes of effective cybersecurity, incorporating various measures such as technical, physical, cultural, and behavioral, in conjunction with effective leadership and governance.

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.)

Clause 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: https://knowledge.bsigroup.com/products/cyber-security-risk-governance-and-management-specification