THE NATIONAL CYBERSECURITY SOCIETY

IT Security Frameworks

An information security framework is a series of documented, agreed and understood policies, procedures, and processes that define how information is managed in an organization. There are frameworks that are broad and those developed specially for a sector. Following a recognized framework can lower risk and vulnerability, and align your business with industry best practices.

There are about 250 different security frameworks used globally, developed to suit a wide variety of businesses and sectors. The mostly commonly used frameworks are:

Did you know?

- √ Financial auditors often use COBIT to base their audit
- √ Understanding which framework your vendor uses is helpful in determining your level of risk when sharing sensitive information
- √ NCSS uses a modified NIST Cybersecurity Framework in the design of its educational products
- √ Use the NCSS CARES tool to assess your company's readiness and resiliency

FACT 1: International Standards Organization (ISO) 27001

One of the most widely known security standards, ISO 27001 is suitable for any organization, large or small, in any sector. This standard is especially applicable to financial, healthcare, public or IT sectors. It works well with organizations that manage a large volume of data. Developed and sustained by the International Standards Organization), it is the security equivalent of the ISO 9000 quality standards for manufacturers to achieve operational excellence.

FACT 2: Control Objectives for Information and Related Technology (COBIT)

COBIT is a high level framework focused on identifying and mitigating risk. It was developed to reduce technical risk, but it has evolved into a standard to align IT with business goals. While it's not as widely followed as others, COBIT is mostly used within the finance industry to comply with standards such as Sarbanes-Oxley, but if your business wants to adopt a formal risk management framework, it's also worth considering.

FACT 3: National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST Special Publications 800-37, 800-39, 800-53 and 800-171.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

IT Security Frameworks

The NIST Cybersecurity Framework was designed to use business drivers to guide cybersecurity activities and considers cybersecurity risk as part of the organization's risk management processes. The framework is comprised of three components - the Framework Core, the Implementation Tiers and Framework Profiles. It was devised to assist critical infrastructure owners and operators in managing cybersecurity risk. The framework is unique in that it can be tailored to fit the unique circumstances of a business. The Framework helps an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The NCSS CARES assessment is modeled after the NIST Framework.

NIST Special Publications 800-37, 800-39, 800-53 and 800-171 are publications that identify necessary controls and approaches for federal institutions, but can be used for the private sector as well. These publications are defined as: NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach; 800-39, Managing Information Security Risk, Organization, Mission and Information System Review; 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

FACT 4: Carnegie Mellon CERT Resilience Management Model

The CERT Resilience Management Model (CERT-RMM) is a process improvement approach to operational resilience management. It defines the essential organizational practices that are necessary to manage your business during a crisis event - such as a cybersecurity incident or data breach. The NCSS uses the CERT-RMM to assess your organization's NIST Framework capabilities.

By leveraging the CERT-RMM's business process approach, your organization can determine its ability to respond to stress and recover effectively.

FACT 5: ISACA Risk IT Framework

The ISACA Risk IT Framework provides an end-to-end, comprehensive analysis of risks related to the use of IT and how your organization deals with risk -- from the tone and culture at the top -- to people dealing with daily operational issues. The framework enables enterprises to understand and manage all significant IT risk types, building upon the existing risk components within the ISACA frameworks. It relies heavily on COBIT.

FACT 6: Industry Specific Standards

In addition to the common frameworks above, there are also a number of industry-specific standards such as PCI DSS (for credit card handling), HIPAA (U.S. legislation to safeguard health/medical information) European GDPR (consumer privacy protections) and the NZ Privacy Act.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

IT Security Frameworks

Adopting one of the more general security frameworks above may not make you fully compliant with these specific standards or regulations, but they will go a long way to helping you achieve compliance.

Security frameworks are vital for future success and resiliency. The decision about which to adopt should not be left to your IT team. Boards and senior management need to be fully involved and responsible in determining which framework to use to build a sustainable governance model. Information security is a business risk issue, not an 'IT problem', and should be addressed at the executive level of your organization.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.