Cybersecurity Assessment Foundations

Assessors demonstrate competence by providing security assessments, which outline the controls and sanctions clients should follow for protection. Security professionals must possess knowledge of laws, policies, and accepted practices before providing services to clients.

The National Institute for Standards and Technology (NIST) has collaborated with the Small Business Administration and the Federal Bureau of Investigation to raise awareness about information security in small businesses. As part of this effort, NIST has created a reference guideline for small businesses called NISTIR. The purpose of this document is to explain the basics of information security programs for small businesses using simple language that is easy to understand.

Ensuring the security of information, systems, and networks is vital for small businesses to earn the trust of their customers, employees, and trading partners. Even nonprofit organizations fall under "Small Enterprise" or "Small Organization." While the size of a small business can differ depending on the type, it typically refers to a business or organization with up to 500 employees. Neglecting security measures can cause harm to all stakeholders involved.

To mitigate potential hazards, the President of the United States has prioritized improving the security and resilience of the country's critical infrastructure while promoting efficiency, innovation, and economic growth. To assist organizations in managing cybersecurity risks, NIST has developed a voluntary, risk-based Cybersecurity Framework and a set of industry standards and best practices. This framework has been created through collaboration between the government and private sector, using a language easily understood and cost-effective for businesses to implement without imposing additional regulatory requirements. It aims to maintain a cyber environment prioritizing safety, security, business confidentiality, privacy, and civil liberties.

This two-part presentation will review the documents' tenets and provide non-technical templates to enhance small businesses' cybersecurity posture. Part one will explain the foundational attributes of Cybersecurity. Part two will compare Risk Management and Cybersecurity Frameworks. Please download and review the following documents before the lectures.

Part One: One-Hour

Small Business Information Security: The Fundamentals Small Business Information Security: the Fundamentals (nist.gov)

Standards for Security Categorization of Federal Information and Information Systems. https://doi.org/10.6028/NIST.FIPS.199

Minimum Security Requirements for Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Security and Privacy Controls for Information Systems and Organizations SP 800-53R5 Security and Privacy Controls for Information Systems and Organizations (nist.gov)

Part Two: One-Hour

Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy NIST SP 800-37r2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

NIST Cybersecurity Framework 2.0. U. S. Department of Commerce. Public Draft: The NIST Cybersecurity Framework 2.0