IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

INTRODUCTION TO THE INFORMATION TECHNOLOGY SECTOR RISK MANAGEMENT AGENCY

DEFEND TODAY, SECURE TOMORROW

The Information Technology (IT) Sector is central to the nation's security, economy, and public health and safety as businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. These virtual and distributed functions produce and provide hardware, software, and IT systems and services, and, in collaboration with the Communications Sector, the Internet. The Sector's complex and dynamic environment makes identifying threats and assessing vulnerabilities difficult and requires that these tasks be addressed in a collaborative and creative fashion.

INFORMATION TECHNOLOGY SECTOR COLLABORATION, RESOURCES, AND TRAINING

The IT Sector Risk Management Agency (SRMA) is responsible for leveraging knowledge, expertise, and resources to coordinate and collaborate with private sector companies, the Department of Homeland Security, other relevant federal departments and agencies, as well as with critical infrastructure owners and operators and their respective associations, independent regulatory agencies, and state local, tribal, and territorial (SLTT) entities, as appropriate.

Collaboration

Sector Coordinating Council (SCC) and Working Groups convene regularly; share information; and develop tools, guidelines, and products to address risks, vulnerabilities, and emerging issues most pressing to the IT Sector. For information regarding the IT SCC, visit it-scc.org/.

Government Coordinating Council (GCC) and Working Groups composed of various federal departments coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to identify and address shared priorities and initiatives that impact the IT Sector.

The **Information Technology-Information and Analysis Center (IT-ISAC)** is the definitive source for security information affecting the IT Sector. It Is a one-of-its kind forum that assembles some of the brightest minds from the world's leading IT companies to minimize threats, manage risk, and respond to cyber incidents affecting the IT Sector. To learn more, visit it-isac.org/about.

Resources

CISA's Cyber Essentials is a guide for leaders of small businesses, as well as leaders of small and local government agencies, to develop an actionable understanding of where to start implementing organizational cybersecurity practices. Learn more at cisa.gov/publication/cisa-cyber-essentials.

Cyber Resource Hub is used to help agencies make data-informed risk decisions; CISA may conduct analysis of assessment data by providing this information to partners. The Hub can help the broader cybersecurity community gain visibility with vulnerability trends, adversarial activities, and effective mitigations to implement for better protection of their networks. Learn more at cisa.gov/cyber-resource-hub.

Training

Creating a Computer Security Incident Response Team (CSIRT) was developed for organizations and individuals that are at the beginning of their planning and implementation process for creating a CSIRT. The training provides definitions and context for defining a CSIRT framework, followed by services that may be provided and the building of an action plan.

Cloud Computing Security is a course that explores guidance from the Cloud Security Alliance (CSA), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and several Cloud Service Providers (CSPs). Topics cover cloud security risks and threats, basic operations, and incident response considerations, along with application, data, and infrastructure security concepts.

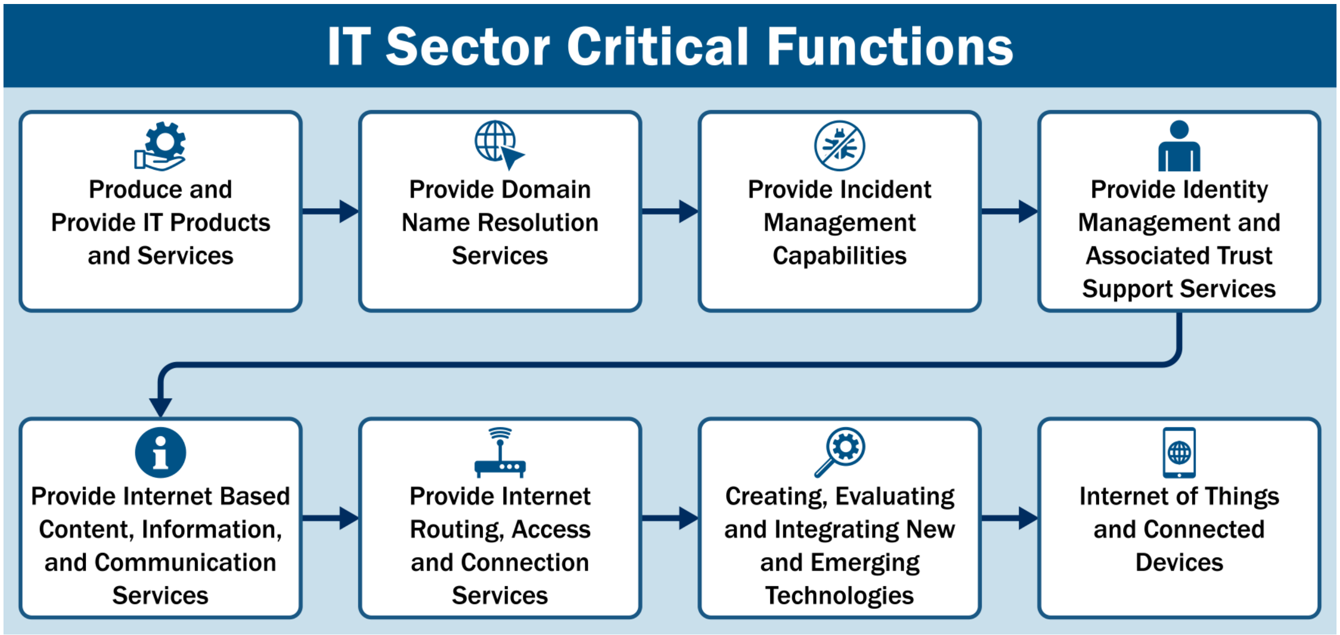
Cyber Essentials is a course that provides an overview of cyber essentials from a leadership perspective and is designed to introduce the six essential elements of building a culture of cyber readiness.

SECTOR PROFILE

The IT Sector provides products and services that support the efficient operation of today's global information-based society, and is integral to the operations and services provided by other critical infrastructure sectors. Comprised of small and medium-sized businesses, as well as large multi-national companies, the IT Sector, unlike many critical infrastructure sectors, is a functions-based sector comprised of physical assets and virtual systems and networks that enable key capabilities and services in both the public and private sectors.

Critical Sector Functions

IT Sector functions encompass the full set of processes involved in creating IT products and services, including research and development (R&D), manufacturing, distribution, upgrades, and maintenance. Eight critical functions support the Sector's ability to provide high assurance IT products and services for various sectors. These functions are required to maintain or reconstitute networks (e.g., the Internet, local networks, and wide area networks) and their associated services. Provided by a combination of entities—often owners and operators and their respective associations who provide IT hardware, software, systems, and services—IT services include development, integration, operations, communications, testing, and security.



IT Sector Critical Functions

Produce and Provide IT Products and Services

Provide Domain Name Resolution Services

Provide Incident Management Capabilities

Provide Identity Management and Associated Trust Support Services

Provide Internet Based Content, Information, and Communication Services

Provide Internet Routing, Access and Connection Services

Creating, Evaluating and Integrating New and Emerging Technologies

Internet of Things and Connected Devices

CRITICAL INFRASTRUCTURE SECURITY CONSIDERATIONS

- **Cyberattacks:** Key cyber risks include cyberattacks that target inadequate security controls, outdated patches, and unknown vulnerabilities; social engineering attempts designed to gain operator credentials; and intrusions from insider threats. All such attempts could allow attackers to access critical control systems and disrupt or control physical components and processes. For information on reducing the risk of a successful cyberattack, visit cisa.gov/cyber-hygiene-services.
- **Cybercrime:** Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse. As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks, such as corporate security breaches, spear phishing, and social media fraud. Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. For information on combating cybercrime, visit cisa.gov/combating-cyber-crime.
- **Ransomware:** A type of malicious software or malware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by a victim unknowingly visiting an infected website. For ransomware guidance and resources, visit cisa.gov/ransomware.

FOR MORE INFORMATION ON THE INFORMATION TECHNOLOGY SECTOR

Contact the IT SRMA at ITSector@cisa.dhs.gov or learn more at cisa.gov/sector-specific-agencies. For additional information about the IT Sector, please view the IT Sector-Specific Plan at cisa.gov/publication/nipp-ssp-information-technology-2016.