Getting Started In Information Security

Information Assurance Security | SPCC

Information Security

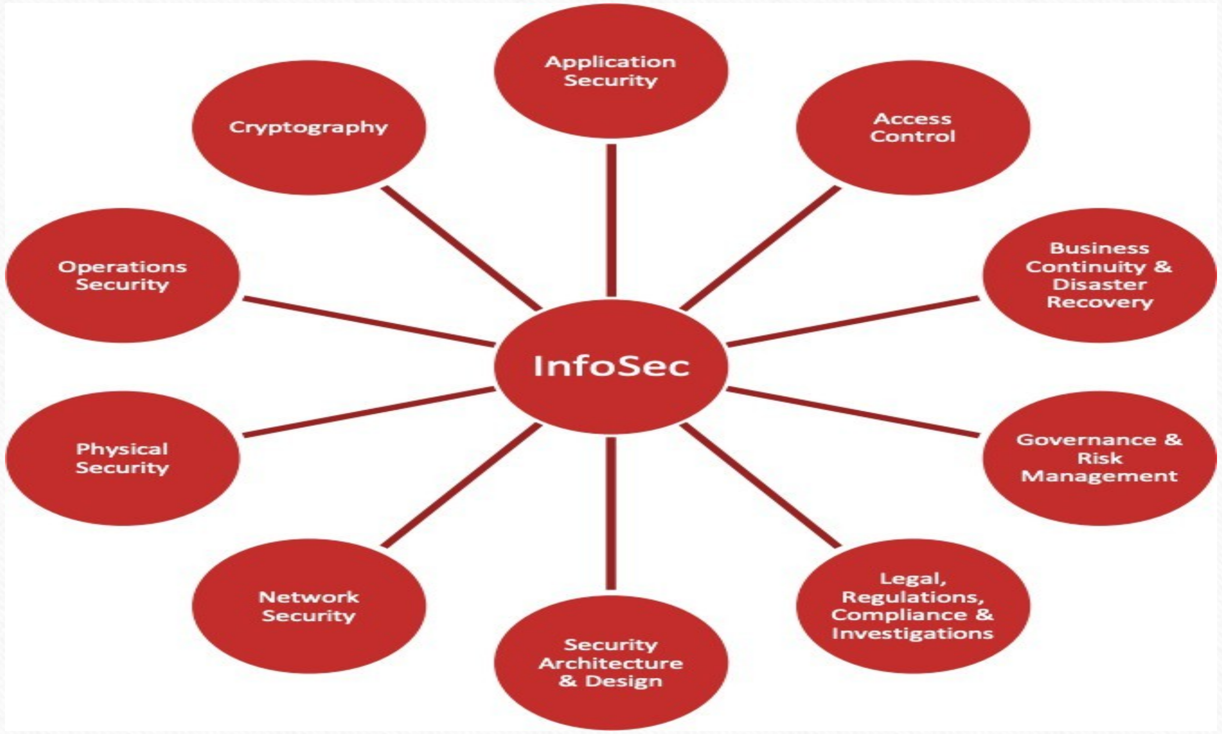
- Information security (InfoSec) is the protection of important information against unauthorized access, disclosure, use, alteration or disruption.
- It helps ensure that sensitive organizational data is available to authorized users, remains confidential and maintains its integrity.
- Information security is an umbrella term that covers an organization's efforts to protect information. It includes physical IT **asset security, endpoint security, data encryption, network security and more.**

- IT security is also concerned with protecting physical and digital IT assets and data centers but does not include protection for the storage of paper files and other media.
- It focuses on the technology assets rather than the information itself.

- Cybersecurity focuses on securing digital information systems. The goal is to help protect digital data and assets from cyberthreats.
- While an enormous undertaking, cybersecurity has a narrow scope, as it is not **concerned with protecting paper or analog data.**

- Data security is the practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle.
- It includes the **physical security of hardware and storage devices**, along with administrative and access controls. It also covers the logical security of software applications and organizational policies and procedures.

The Many Areas of Information Security


InfoSec
Application Security
Access Control
Business Continuity & Disaster Recovery
Governance & Risk Management
Legal, Regulations, Compliance & Investigations
Security Architecture & Design
Network Security
Physical Security
Operations Security
Cryptography

The Many Areas of Information Security

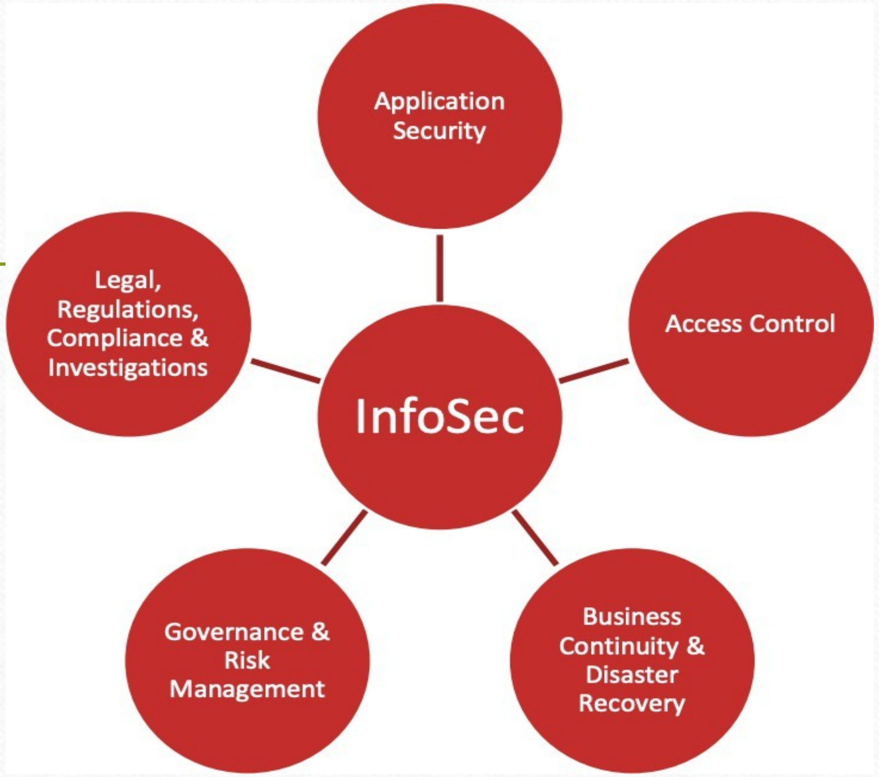
Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

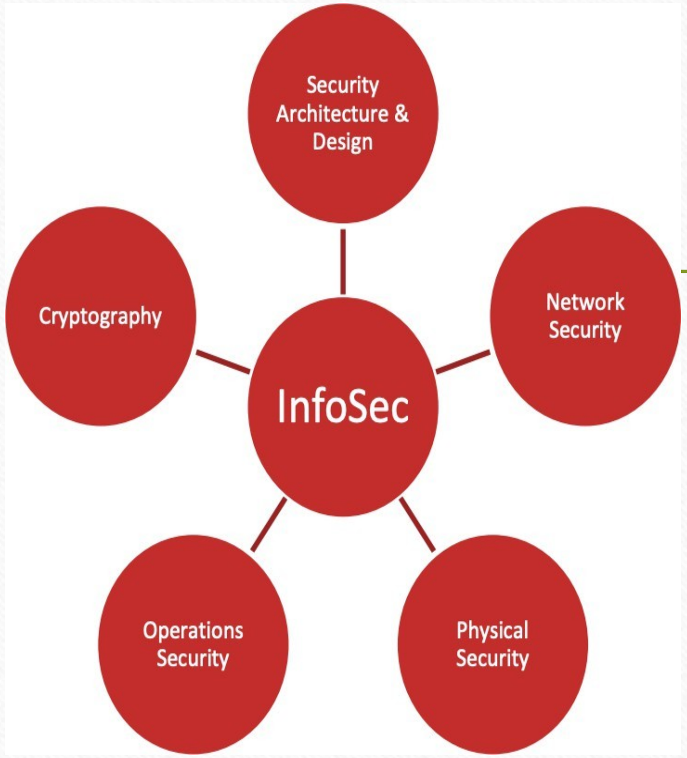
Business continuity and disaster recovery (BCDR or BC/DR) is a set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations.

Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations.

Legal, Regulations, Investigations and Compliance domain addresses ethical behavior
and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed, and methods used to gather evidence.


Application Security
Legal, Regulations, Compliance & Investigations
Access Control
InfoSec
Governance & Risk Management
Business Continuity & Disaster Recovery

The Many Areas of Information Security



Security architecture and design looks at how information security controls and safeguards are implemented in IT systems in order to protect the **C**onfidentiality, **I**ntegrity, and **A**vailability of the data that are used, processed, and stored in those systems.

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible

Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm.

Operations security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by enemy intelligence, determines if information obtained by adversaries could be interpreted to be useful to them.

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. ... When transmitting electronic data, the most common use of cryptography is to encrypt and decrypt email and other plain-text messages.

NIST SP 800-100 OVERVIEW

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100: Information Security:

- **Overview:**

Provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

- **Purpose:**

Inform members of the information security management team about various aspects of information security that they will be expected to implement and oversee in their respective organizations. In addition, the handbook provides guidance for facilitating a more consistent approach to information security programs across the federal government. Even though the terminology in this document is geared toward the federal sector, the handbook can also be used to provide guidance on a variety of other governmental, organizational, or institutional security requirements.

- **Audience:**

The intended audience includes agency heads, CIOs, CISOs, and security managers. The handbook provides information that the audience can use in building their information security program strategy. The handbook is useful to any manager who requires a broad overview of information security practices.

NIST SP 800-100 PROGRAM ELEMENT

- Information Security Governance
- System Development Life Cycle
- Awareness and Training
- Capital Planning and Investment Control
- Interconnecting Systems
- Performance Measures
- Security Planning
- IT Contingency Planning
- Risk Management
- Certification, Accreditation, and Security Assessments
- Security Services and Products Acquisition
- Incident Response
- Configuration Management

References

- https://www.vmware.com/topics/glossary/content/application-security
- https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html https://www.cio.com/article/3206607/what-is-grc-and-why-you-need-it.html
- https://nvlpubs.nist.gov/