CYBER SECURITY ESSENTIAL

OBJECTIVE

By the completion of this course, successful learners will be able to:

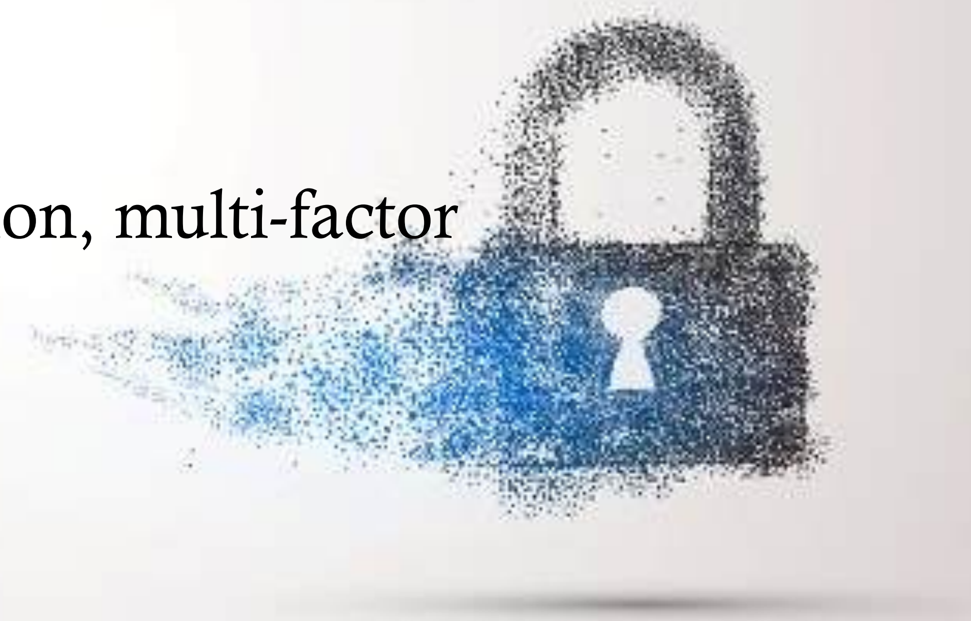
- □ Understand security principles, including the risk management process, security controls, governance processes and the Professional Code of Ethics
- □ Understand business continuity, disaster recovery and incident response concepts
- □ Understand access control concepts, including physical and logical access controls
- □ Understand Network Security, including network threats and attacks, and network security infrastructure
- □ Understand Security Operations, including data security, system hardening, security policies and security awareness training

DOMAINS

Domain One: Security Principles

1.1 - Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy



1.2 - Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment and treatment

DOMAINS

Domain One: Security Principles

1.3 - Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4 - Understand Professional Code of Ethics

- Professional code of conduct

1.5 - Understand governance processes

- Policies
- Procedures
- Standards
- Regulations and laws

DOMAINS

Domain Two: Business Continuity (BC), Disaster Recovery (DR) and Incident Response Concepts

2.1 - Understand business continuity (BC)

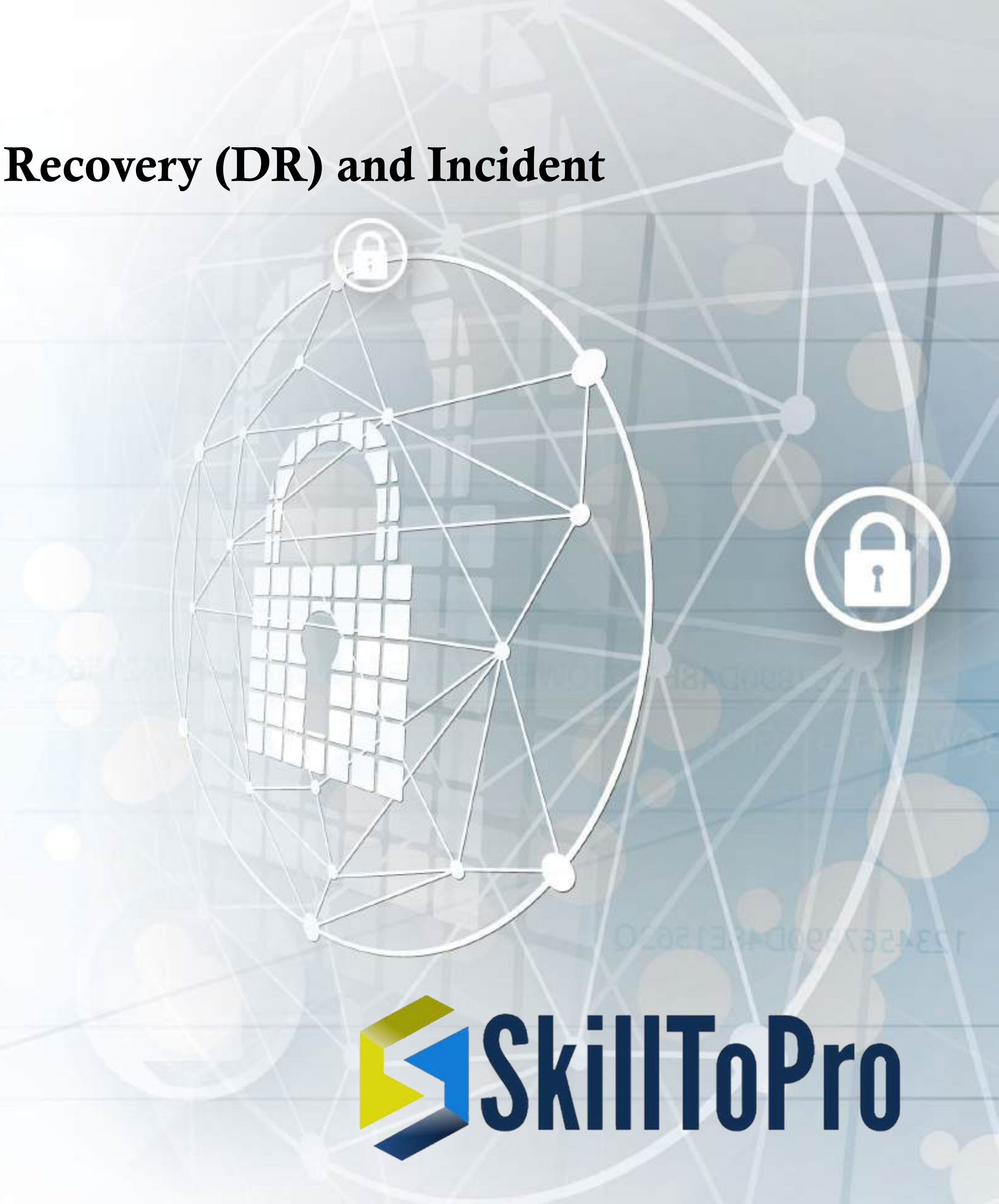
- Purpose
- Importance
- Components

2.2 - Understand disaster recovery (DR)

- Purpose
- Importance
- Components

2.3 - Understand incident response

- Purpose
- Importance
- Components



SkillToPro

DOMAINS

Domain Three: Access Controls Concepts

3.1 - Understand physical access controls

- Physical security controls (e.g., badge systems, gate entry, environmental design)
- Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
- Authorized versus unauthorized personnel

3.2 - Understand logical access controls

- Principle of least privilege
- Segregation of duties
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

DOMAINS

Domain Four: Network Security

4.1 - Understand computer networking

- Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
- Ports
- Applications

4.2 - Understand network threats and attacks

- Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
- Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
- Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

DOMAINS

4.3 - Understand network security infrastructure

- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

Domains

Domain Five: Security Operations

5.1 - Understand data security

- Encryption (e.g., symmetric, asymmetric, hashing)
- Data handling (e.g., destruction, retention, classification, labelling)
- Logging and monitoring security events

5.2 - Understand system hardening

- Configuration management (e.g., baselines, updat patches)

DOMAINS

5.3 - Understand best practice security policies

- Data handling policy
- Password policy
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policy
- Change management policy (e.g., documentation, approval, rollback)
- Privacy policy

5.4 - Understand security awareness training

- Purpose/concepts (e.g., social engineering, password protection)

Prerequisites

- There are no prerequisites for this course.

SkillToPro

INFORMATION TECHNOLOGY & THE RISE CYBERSECURITY

INFORMATION TECHNOLOGY

- □ **Information technology (IT)** is the hardware and software used to create, store, transmit, manipulate, and display information and data. Metaphorically, it is the lifeblood of the Information Age. On a high level, it is anything and everything that has to do with computing and communications.

Common information technology types:

- □ Internet and web technologies
- □ Cloud computing
- □ Databases
- □ Artificial intelligence and machine learning
- □ Cybersecurity
- □ Internet of things
- □ IT governance
- □ Data analytics and business intelligence
- □ Disruptive Technology

DISRUPTIVE TECHNOLOGY

- Harvard Business School professor and business consultant, **Clayton Christensen**, coined the term **“disruptive innovation”** in the magazine Harvard Business Review back in 1995.

- For Christensen, technology that causes a relevant change and abruptly interrupts the way in which industries, companies, and consumers operate constitutes a disruptive innovation.

- **Disruptive technology** is an innovation that significantly alters established industries and markets, creating new sectors and business models. An innovation that radically changes the way the market is structured and how products and services are consumed.

DISRUPTIVE TECHNOLOGY - EXAMPLES

- □ Blockchain
- □ Robotics
- □ Green Tech
- □ 3D Printing
- □ 5G technology
- □ Internet of Things
- □ Quantum Computing

- □ Nanotechnology
- □ Biotechnology
- □ Cloud computing (As-a-service Models)
- □ Artificial Intelligence and Machine Learning
- □ Virtual, Augmented and Mixed Reality

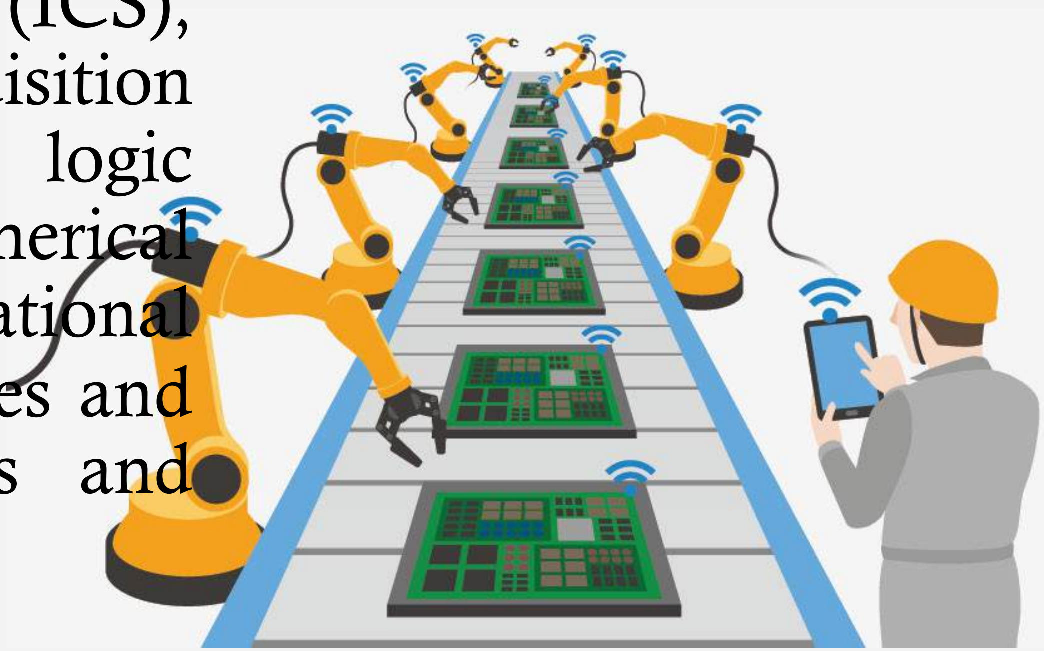
SkillToPro

OPERATIONAL TECHNOLOGY

Operational Technology Defined

- ❑ Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.

- ❑ Robots, industrial control systems (ICS), Supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and computer numerical control (CNC) are examples of OT. Operational technology can also be found in warehouses and in outdoor areas such as parking lots and highways.



WHAT IS CYBERSECURITY

- ❑ The protection of software, hardware, and data resources connected and stored on the Internet is known as the cybersecurity”.
- ❑ The protection of the personal, financial data, commercial data, business-critical information, operational continuity, data integrity, and availability of online software services fall in the cybersecurity domain.
- ❑ Regulating the physical access and controlling the malicious intrusion, allowing the authorized access, encrypting the valuable information, and safeguarding the privacy are the components of cybersecurity.

CYBERSECURITY DOMAINS

Cybersecurity can be classified into multiple elements as mentioned below:

❑ **Network security (NS)**

❑ **Information security (IS)**

❑ **Application security (AS)**

❑ **Business continuity planning (BCP)/disaster recovery**

❑ **Leadership commitment**

❑ **Operational security (OPSEC)**

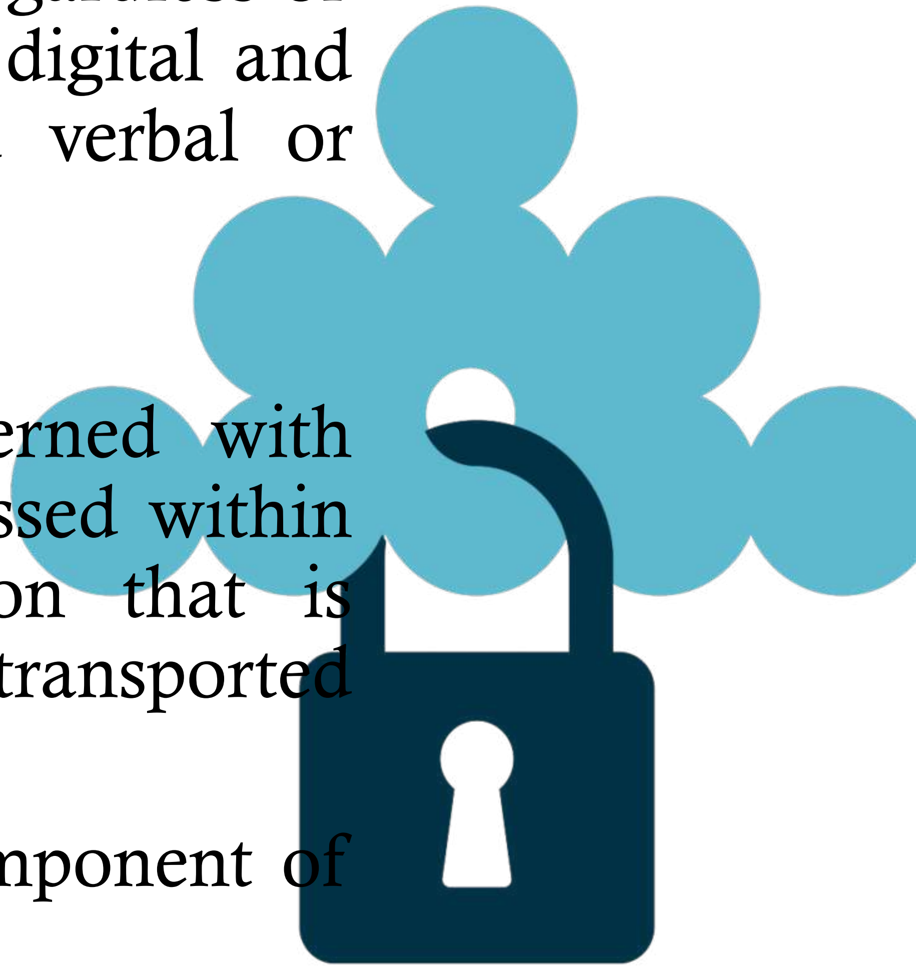
❑ **End-user education**

Information Security and Cybersecurity

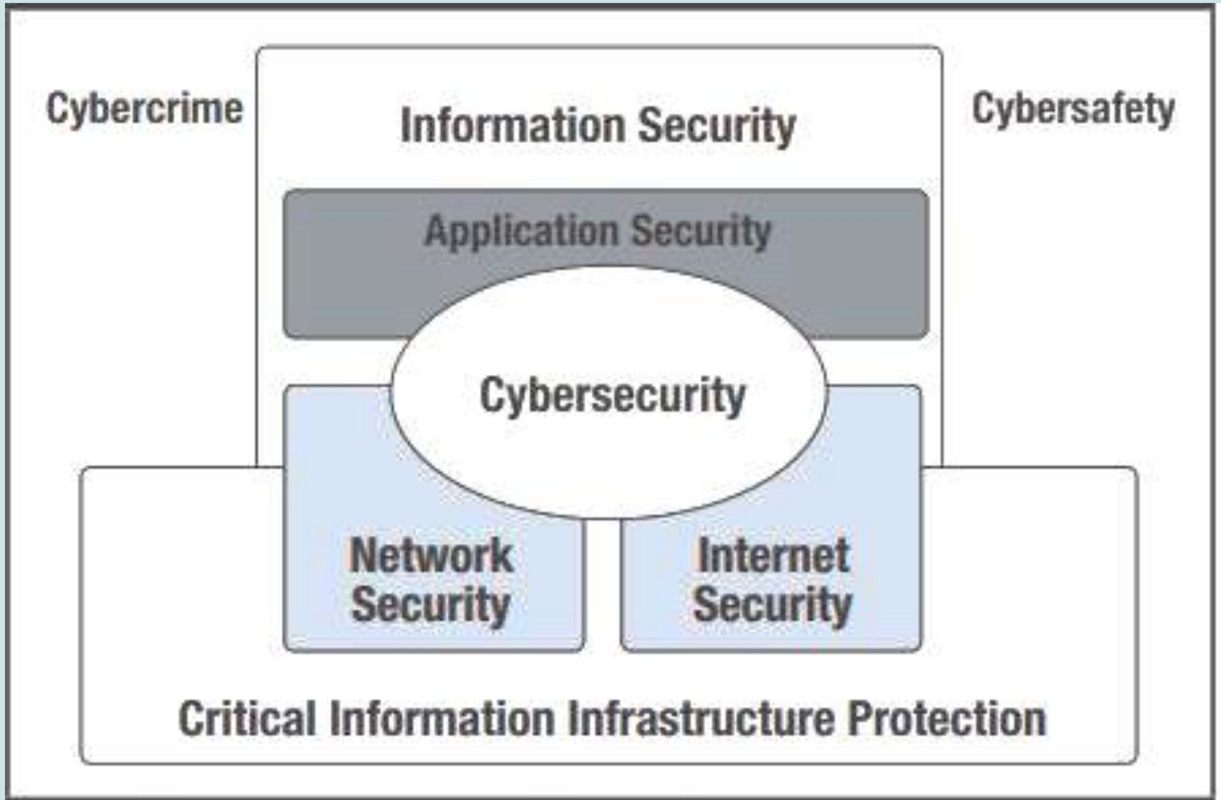
❑ Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.

❑ Cybersecurity, on the other hand, is concerned with protecting digital assets—everything encompassed within network hardware, software and information that is processed, stored within isolated systems or transported by internetworked information environments.

❑ It is helpful to think of cybersecurity as a component of information security.

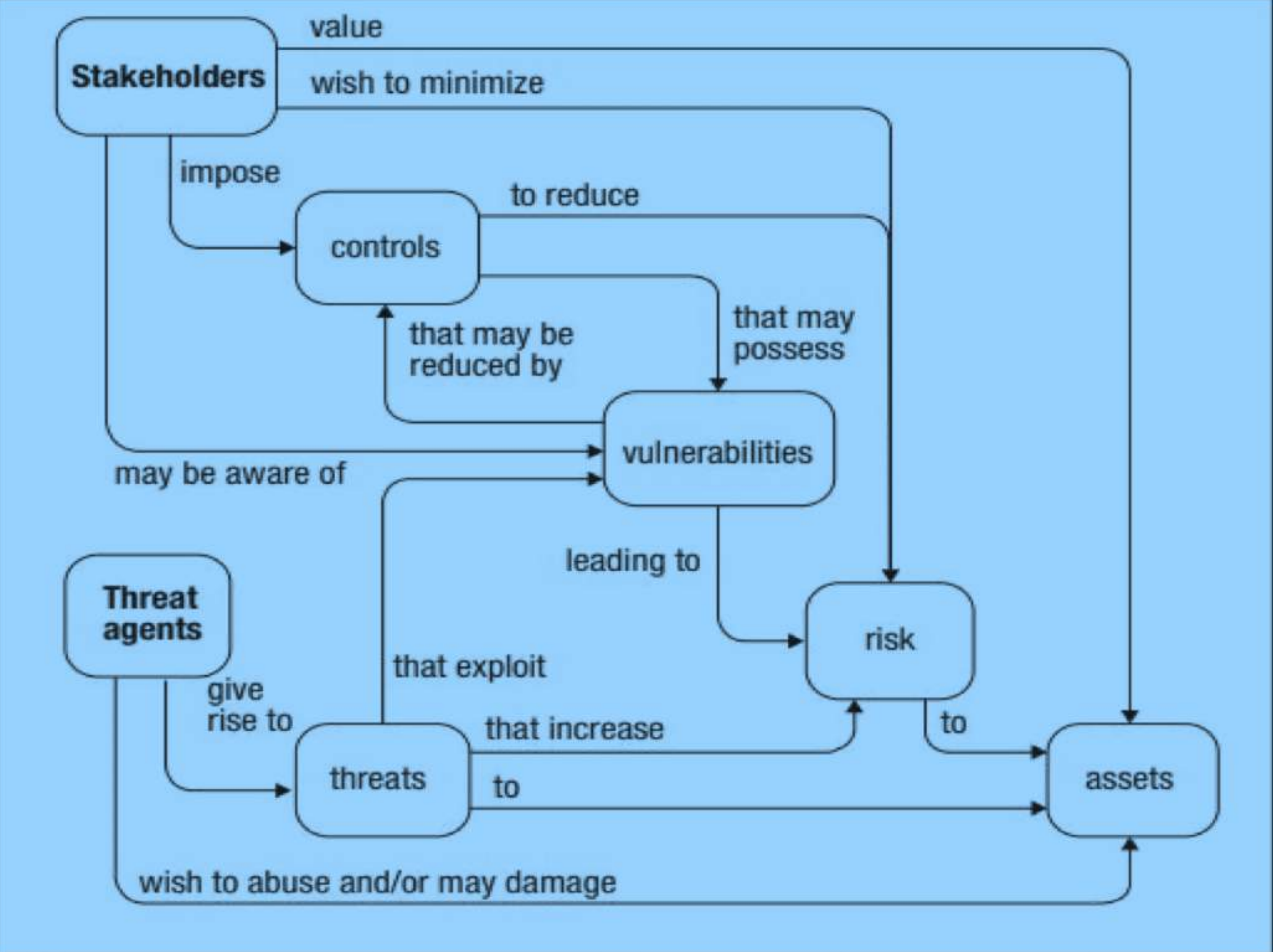


RELATIONSHIP AMONG CYBERSECURITY AND OTHER SECURITY DOMAINS



Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

SECURITY CONCEPTS AND RELATIONSHIPS



Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

PROTECTING DIGITAL ASSETS

In the core of its cybersecurity framework, the National Institute of Standards and Technology (NIST) identifies five key functions necessary for the protection of digital assets.

- ❑ **Identify—Use** organizational understanding to minimize risk to systems, assets, data and capabilities.
- ❑ **Protect—Design** safeguards to limit the impact of potential events on critical services and infrastructure.
- ❑ **Detect—Implement** activities to identify the occurrence of a cybersecurity event.
- ❑ **Respond—Take** appropriate action after learning of a security event.
- ❑ **Recover—Plan** for resilience and the timely repair of compromised capabilities and services.