CultureLink

CSX – Cybersecurity Fundamentals

Section 2 : Cybersecurity Concepts

Course Plan

Module Titles
Section 1 – Cybersecurity Introduction and Overview
Section 2 – Domain 1: Cybersecurity Concepts
Section 3 – Domain 2: Security Architecture Principles
Section 4 – Domain 3: Security of Networks, Systems, Applications and Data
Section 5 – Domain 4: Incident Response
Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology
Section 7 – Course Review
Section 8 – Practice Exam

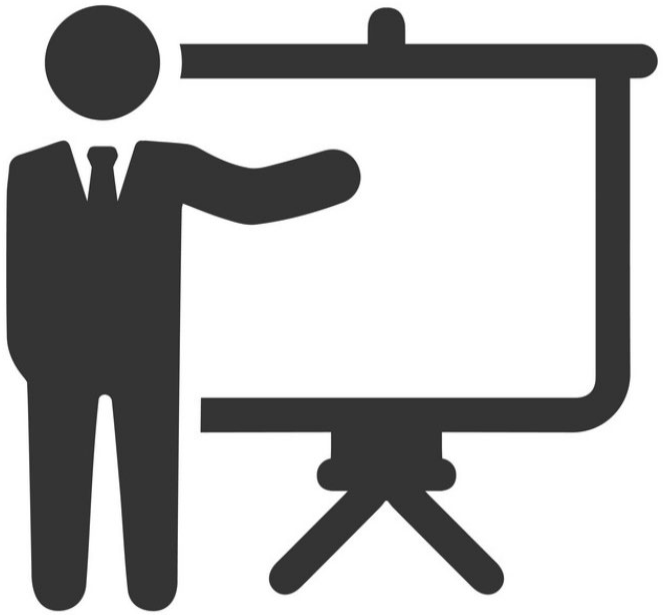
Learning Outcomes for this Module

- Knowledge of cybersecurity principles used to manage risk related to the use, processing, storage and transmission of information or data
- Knowledge of security management
- Knowledge of risk management processes, including steps and methods for assessing risk
- Knowledge of threat actors (e.g., script kiddies, non-nation state sponsored, and nation state sponsored)
- Knowledge of cybersecurity roles
- Knowledge of common adversary tactics, techniques, and procedures (TTPs)
- Knowledge of relevant laws, policies, procedures and governance requirements
- Knowledge of cybersecurity controls

Topics for this Module

- **2.1** Risk
- **2.2** Common attack types and vectors
- **2.2** Policies
- **2.3** Cybersecurity controls

Current Events



CultureLink

Section 2.1

Risk

Question

What is Risk?

Wikipedia Definition of Risk

*"is potential of **losing something of value**. Values (such as physical health, social status, emotional well-being or financial wealth) can be gained or lost when taking risk resulting from a given action, activity and/or inaction, foreseen or unforeseen. Risk can also be defined as the **intentional interaction with uncertainty.** Uncertainty is a potential, **unpredictable,** unmeasurable and uncontrollable outcome; risk is a **consequence of action** taken in spite of uncertainty"*

- Wikipedia

Definition of risk

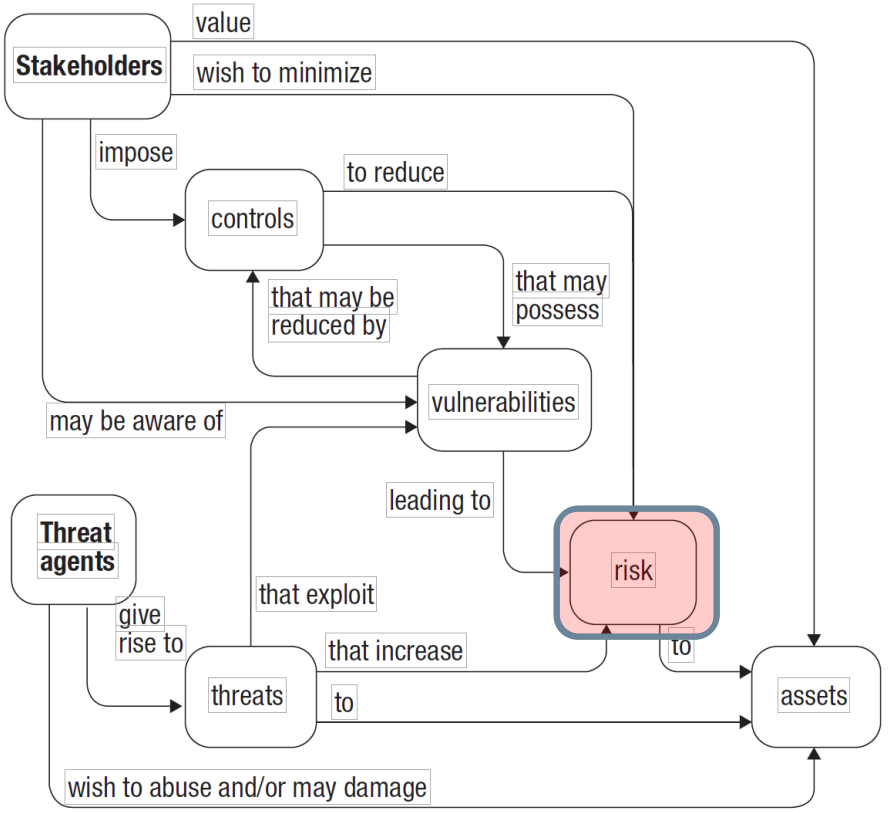
"The chance of something happening that will have **impact** upon objectives"

"**Possibility** that a particular threat will adversely impact an information system by exploiting a particular **vulnerability**"

Source: Information Assurance Handbook Corey Schou & Steven Hernandez

Key Terms and Definitions

Figure 1.3—Security Concepts and Relationships

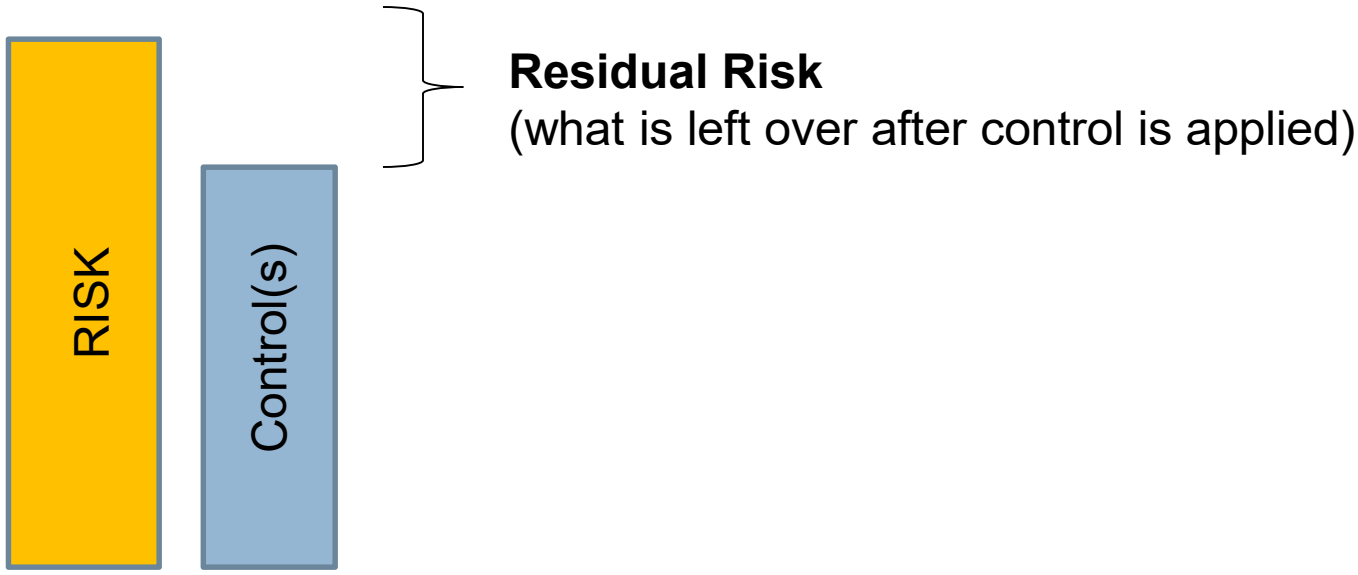


Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

Source: CSX Fundamentals Guide - ISACA

Key Terms and Definitions

- **Risk**—The combination of the probability of an event and its consequence (ISO/IEC 73). Risk is mitigated through the use of **controls or safeguards**



Key Terms and Definitions

- **Threat**—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm

- **Asset**—Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

Key Terms and Definitions

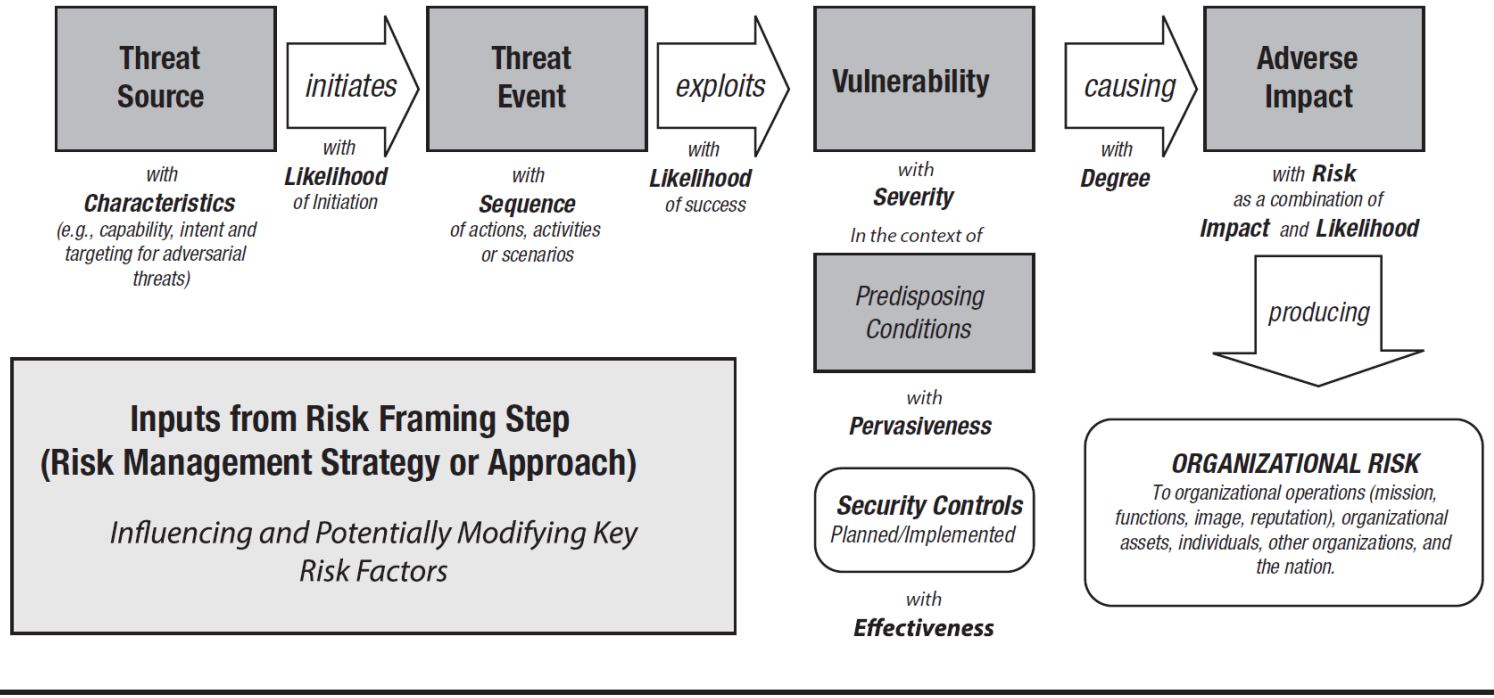
- **Vulnerability**—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

- **Inherent risk**—The risk level or exposure **without taking into account the actions** that management has taken or might take (e.g., implementing controls)

- **Residual risk**—Even after safeguards are in place, there will always be residual risk, defined as the **remaining risk after management has implemented a risk response**.

Risk Management

Figure 2.2—Framing Risk Management



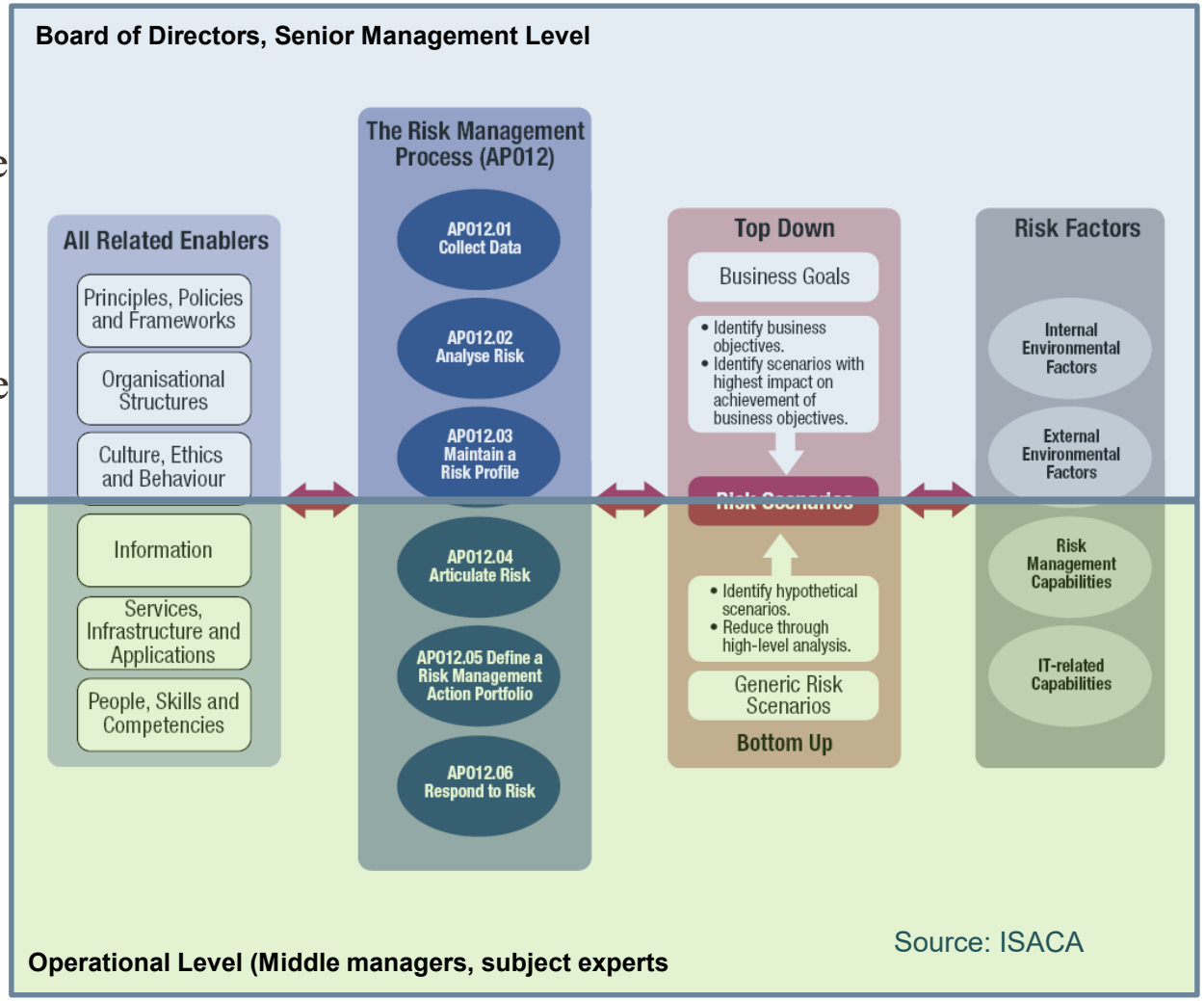
Source: National Institute of Standards and Technology, "Generic Risk Model with Key Risk Factors," NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, USA, Sept 2012

Risk Identification and Classification & Frameworks

- ISO 31000:2009 Risk Management – Principals and Guidelines
- COBIT 5 for Risk
- COBIT 2019 (new)
- IEC 31010:2009 Risk Management – Risk Assessment Techniques
- ISO/IEC 27001:21013
- ISO/IEC 27005:2011
- NIST 800-30 Rev1 – Guide for conducting Risk Assessment
- NIST 800-39 – Managing Information Security

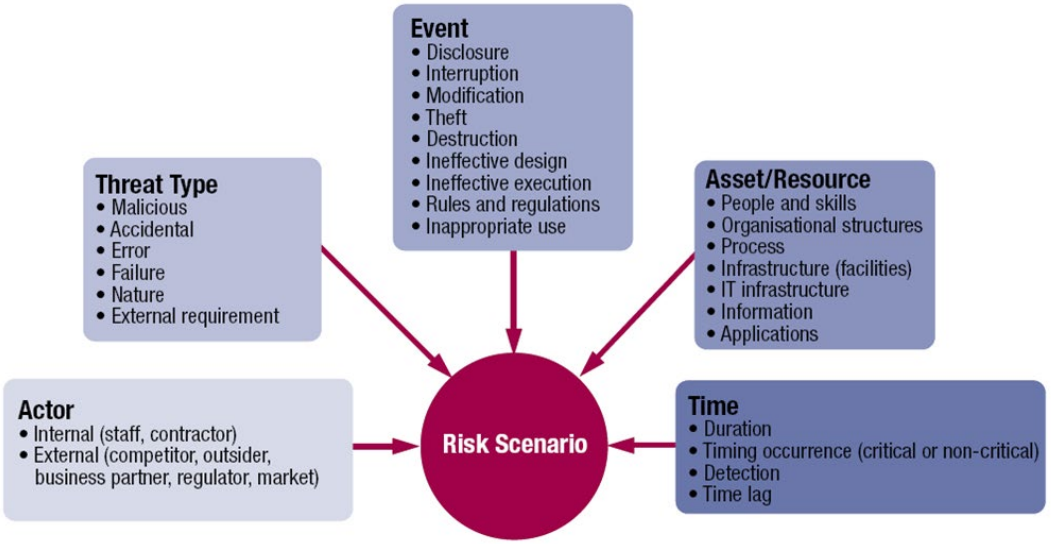
Approaches to Risk Scenarios

- **Top-down approach—** Use the overall enterprise objectives and consider the most relevant and probable IT risk scenarios impacting these
- **Bottom-up approach—** Use a list of generic scenarios to define a set of more relevant and customized scenarios, applied to the individual enterprise



Risk Scenario Breakdown

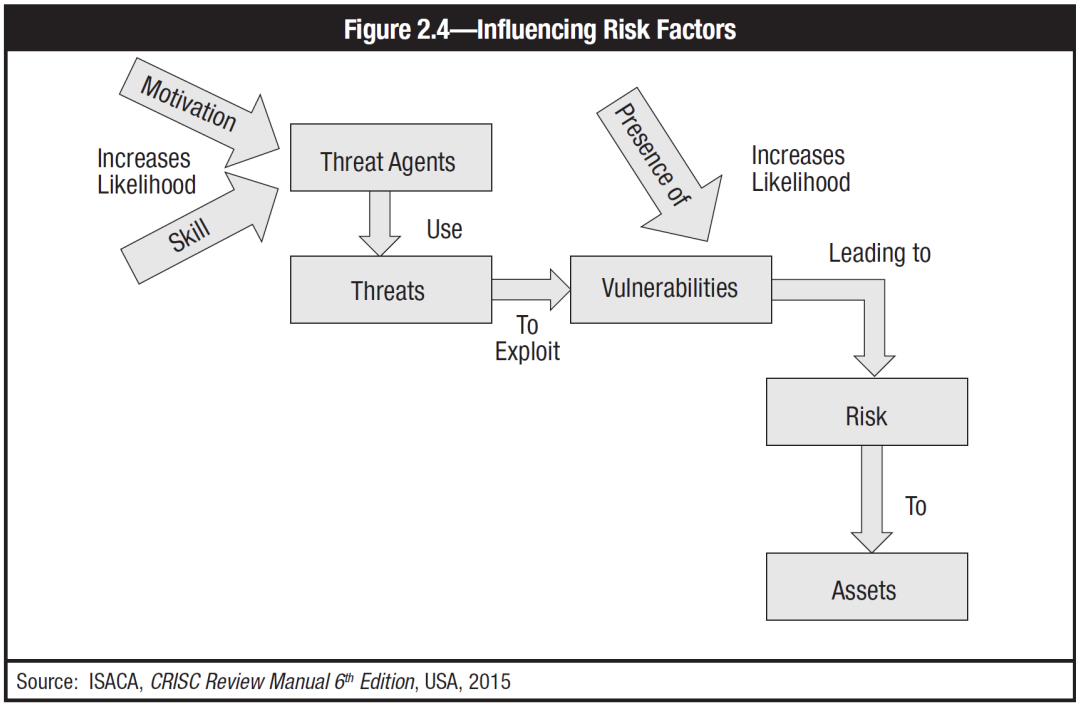
- When a risk scenario materializes, a loss event occurs. The loss event has been triggered by a threat event (Threat type + Event).
- The frequency of the threat event is influenced by a vulnerability. The vulnerability is usually a state; it can be increased/ decreased by vulnerability events, e.g., controls strength or by the threat strength.



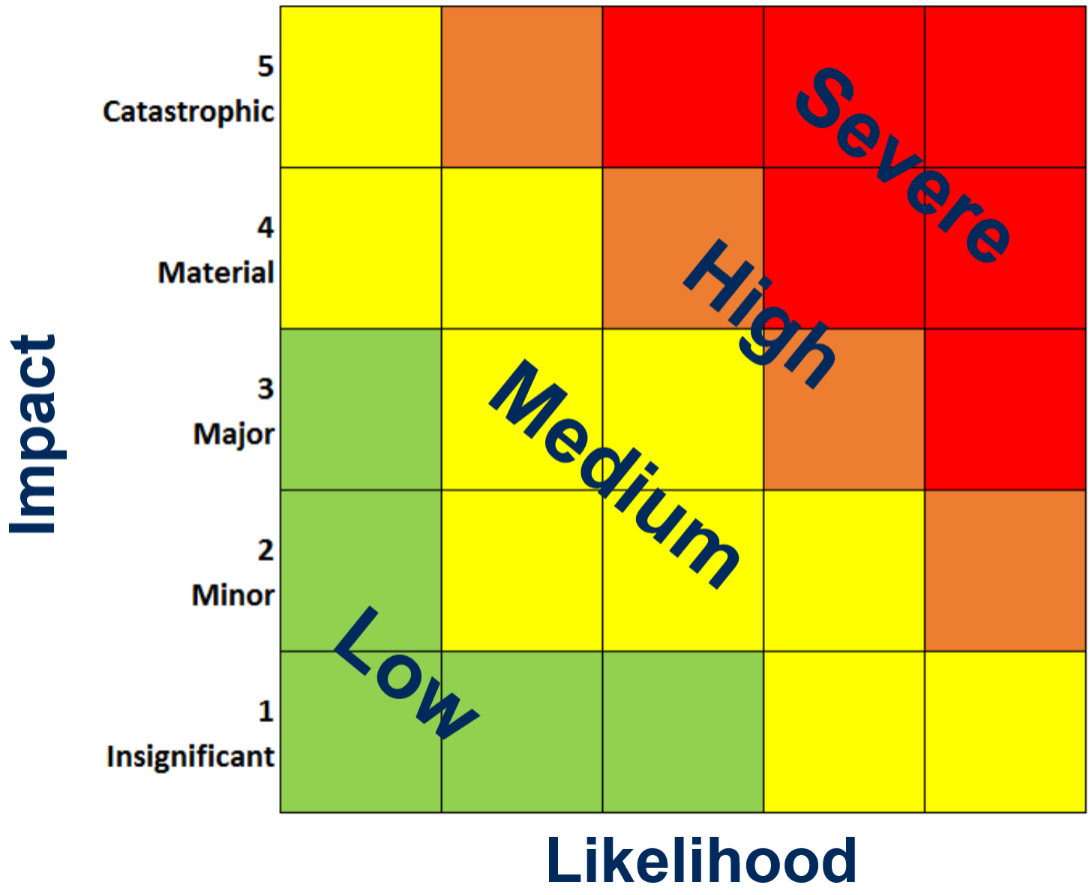
Source: ISACA

Likelihood and Impact

- Likelihood (also called probability) is the measure of frequency of which and event may occur
- Calculation : Likelihood x Frequency = Risk



Risk Qualitative Measurement



Threats

- Threats to information assets must be assessed as well
- Threats are any circumstance or event with the potential to harm an asset through a specific vulnerability (or a set of them)

They are categorized as:

- Natural
- Unintentional
- Intentional physical
- Intentional nonphysical

Vulnerabilities

- Weaknesses in our environment
- Not necessarily binary
- Estimating the degree of vulnerability requires experience
- Control effectiveness will affect any existing vulnerability
- While automatic scanning equipment is used to identify
- technical vulnerabilities, this cannot be done for physical,
- process or performance vulnerabilities

Vulnerabilities (cont.)

- Examples are:
- Defective software
- Improperly configured equipment
- Inadequate compliance enforcement
- Poor network design
- Uncontrolled or defective process
- Inadequate management
- Insufficient staff
- Lack of knowledge to support users or running the process
- Lack of security functionality
- Lack of proper maintenance
- Poor choice of passwords
- Untested technology
- Transmission of unprotected communications
- Lack of redundancy
- Poor management communications

Vulnerabilities

Can you think of other examples?

Approaches to Cybersecurity Risk

- ***Ad hoc***—An *ad hoc* approach simply implements security with no particular rationale or criteria

- **Compliance-based**—Also known as standards-based security, this approach relies on regulations or standards to determine security implementations

- **Risk-based**—Risk-based security relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity's risk tolerance and business needs

CultureLink

Any questions?

CultureLink

Section 2.2

Common attack types and vectors

Common attacks types and vectors

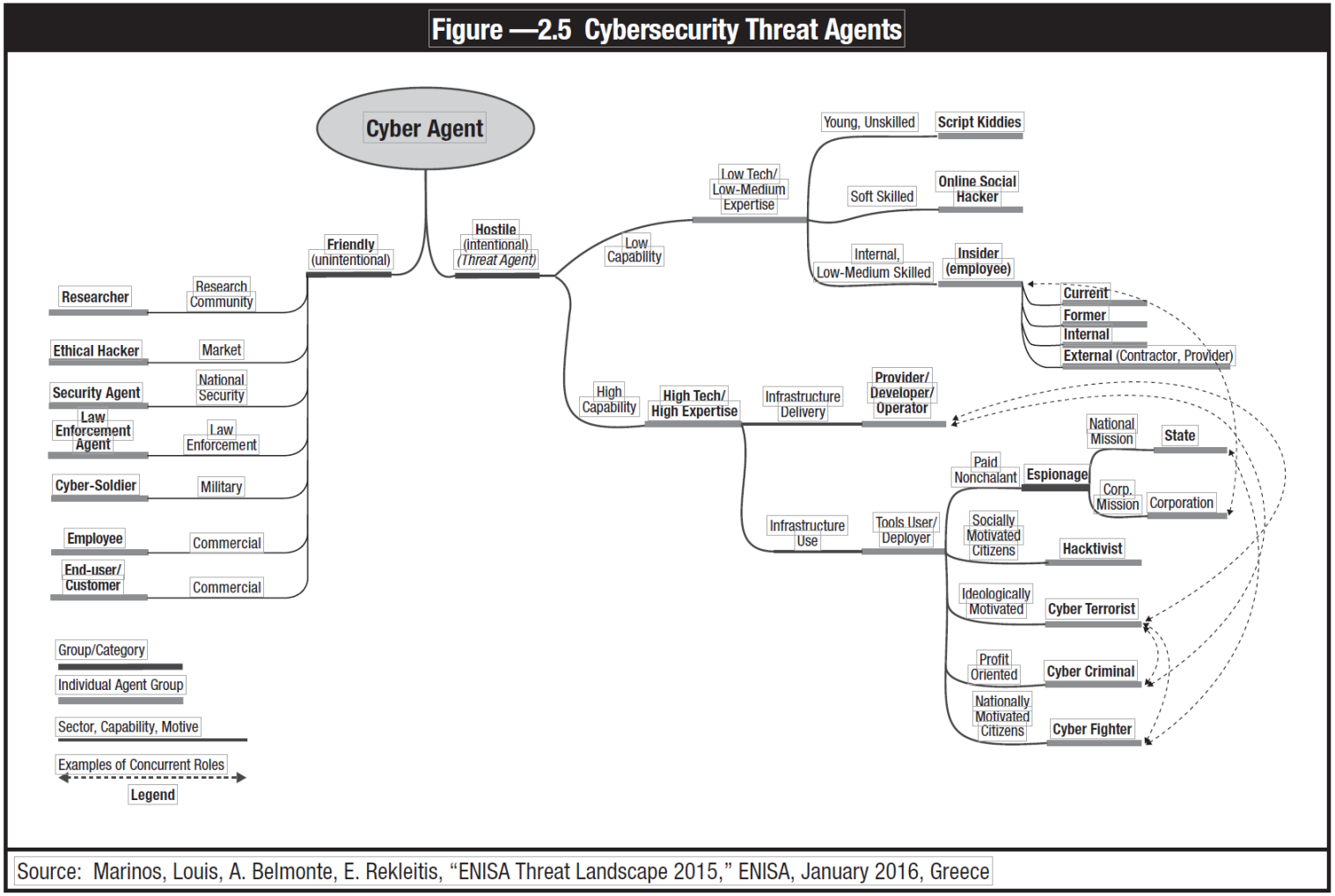
Attack vectors and methodologies **keep evolving**:

Attack vector: is the path or route used to gain access to the target (asset)

Example of paths used:

- Phishing
- Social engineering
- Supply chain
- Crimeware (Ransomware)

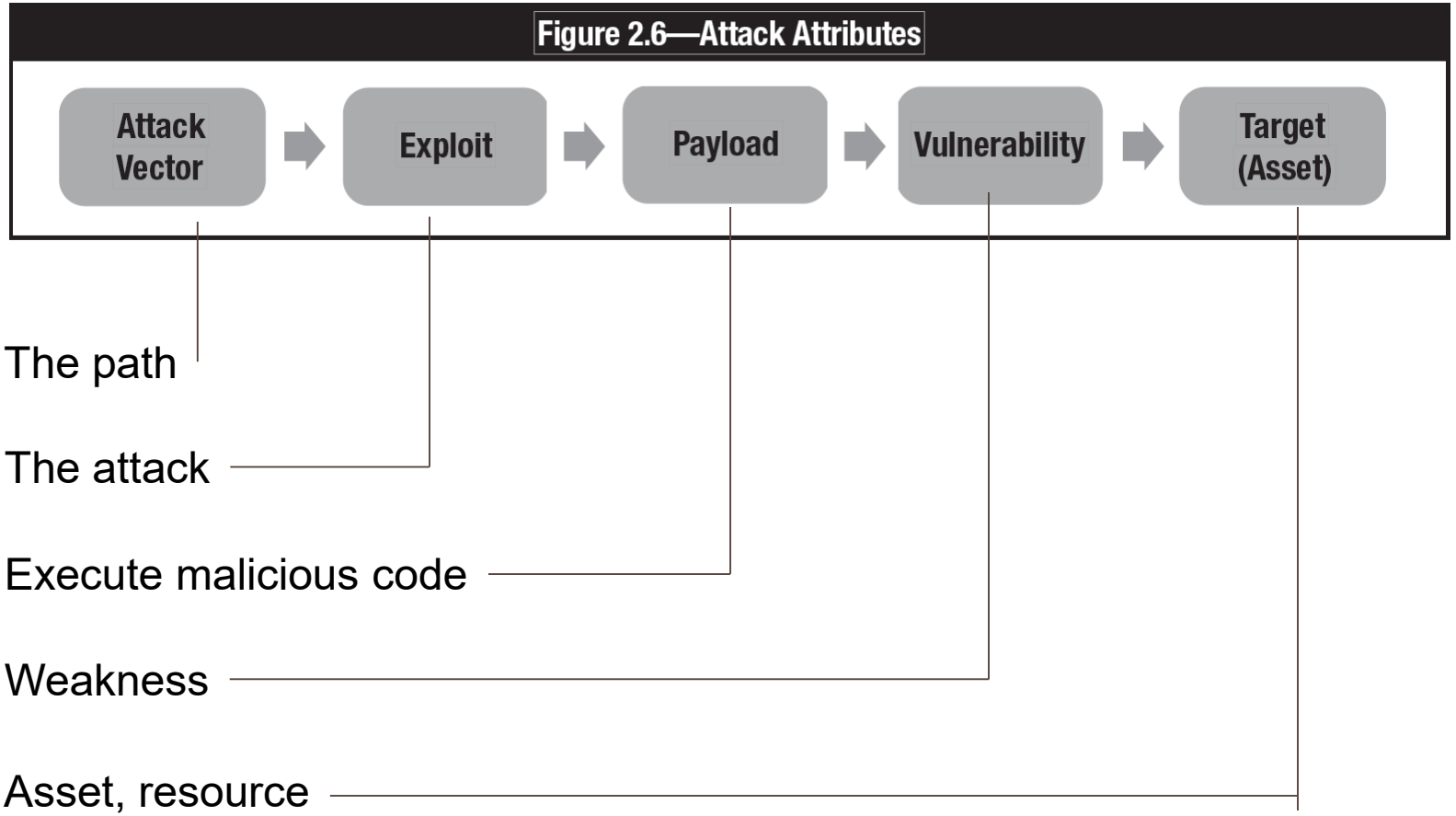
Threat agent breakdown



Source: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, January 2016, Greece

CultureLink

Attack Attributes



Attack attributes

- In order to understand and analyze the attack attributes, it is important to work with the business
- Require technical and subject matter experts input

- Attacks can be categorized in **adversarial** threat event and **nonadverserial** threat event

Adversarial: is a adversary (opponent)

Nonadverserial: human error, mistakes, flood, setting incorrect privileged settings, fire, aged equipment

Malware, ransomware and attack types

- **Malware,** also called **malicious code**, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations. There are several types of malware, the most important being **computer viruses, network worms and Trojan horses**, which are differentiated by the way in which they operate or spread.
- **Viruses** - A computer virus is a piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage.
- **Network worm** - A variant of the computer virus, which is essentially a piece of self-replicating code designed to spread itself across computer networks. It does not require intervention or execution to replicate.

Malware, ransomware and attack types (cont.)

- **Trojan horses**—A piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes.
- **Botnets**—Derived from "robot network," a large, automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as DoS.

- ** Review other attack types on page 37 of study guide

CultureLink

Section 2.3

Policies

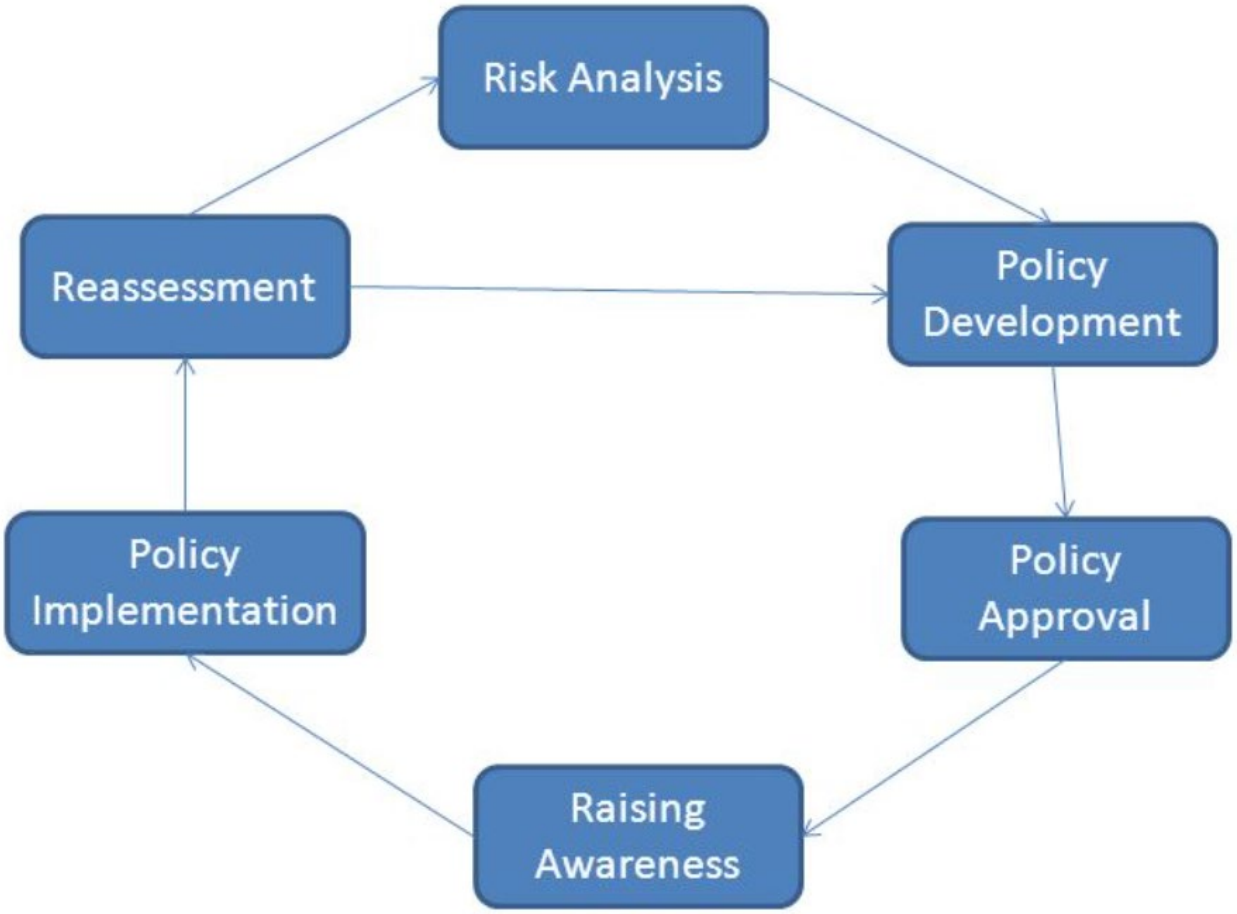
Discussion questions

- What is a policy?
- What is its purpose?
- Who is responsible for writing policies?

Discussion questions

- What is a policy?
  - Outline expected behaviours expected from the organization
  - Specify the roles and responsibilities
- What is its purpose?
  - Guide staff, to uphold the strategic direction of the company
  - Uphold values, principles and mission
- Who is responsible for writing policies?
  - Management is responsible
  - Validated by the Board of Directors and senior management

Policy lifecycle



Policy guidelines

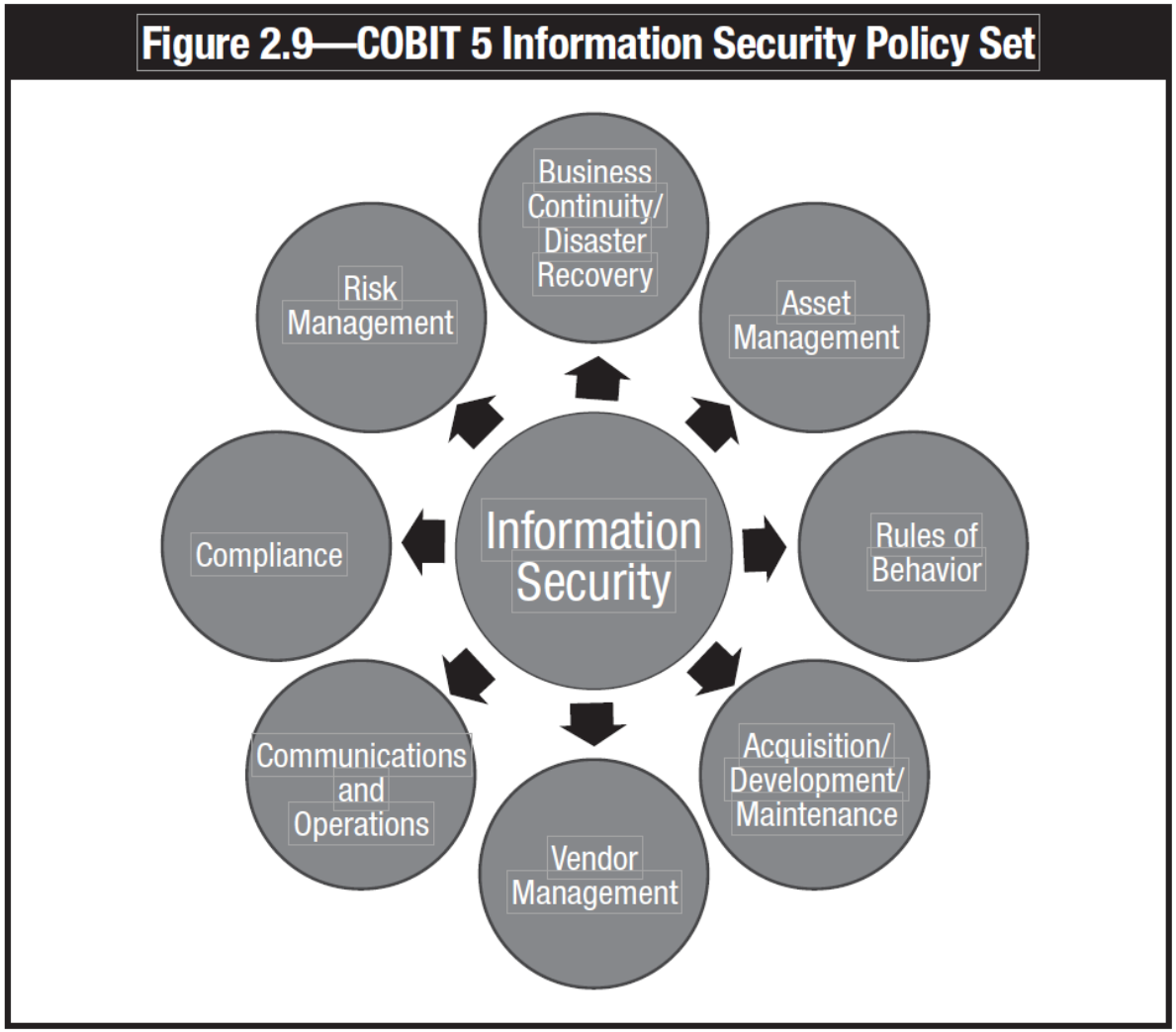
- Security policies should be an articulation of a well-defined information security strategy that **captures the intent, expectations and direction of management.**
- Policies **must be clear and easily understood** by all affected parties.
- Policies should be **short and concise**, written in plain language.
- See example

Compliance documents and policy frameworks

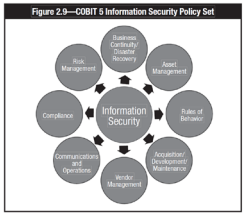
Figure 2.8—Compliance Document Types	
Type	**Description**
Policies	Communicate required and prohibited activities and behaviors
Standards	Interpret policies in specific situations
Procedures	Provide details on how to comply with policies and standards
Guidelines	Provide general guidance on issues such as "what to do in particular circumstances." These are not requirements to be met but are strongly recommended.

- Not all organization implement these types of documents or guidelines
- Smaller companies tend to do Ad-hoc, policies my be verbal
- Larger organizations more mature tend to have these documents types
- Depends on org. culture, compliance and regulations

General information security policies



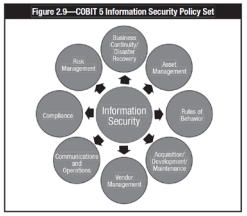
Information security policies



Business Continuity and Disaster Recovery:

- Business impact analysis (BIA)
- Business contingency plans with trusted recovery
- Recovery requirements for critical systems
- Defined thresholds and triggers for contingencies and escalation
- Disaster recovery plan (DRP)
- Training and Testing

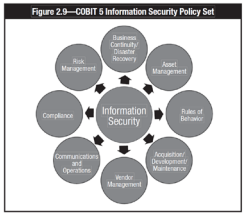
Information security policies



Asset Management:

- Data classification and ownership
- System classification and ownership
- Resource utilization and prioritization
- Asset life cycle management
- Asset protection

Information security policies



Rules of Behavior:

- At-work acceptable use and behavior, including privacy, Internet/email, mobile devices, BYOD, etc.
- Offsite acceptable use and behavior, including social media, blogs

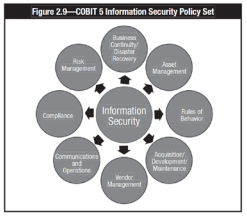
Acquisition/Development/Maintenance:

- Information security within the life cycle, requirements definition and procurement/acquisition processes
- Secure coding practices
- Integration of information security with change and configuration management

Vendor Management:

- Contract management

Information security policies



Communication and Operations:

- IT information security architecture and application design
- Service level agreements

Compliance:

- IT information security compliance assessment process
- Development of metrics
- Assessment repositories

Risk Management:

- Organizational risk management plan
- Information risk profile

Other policies

Access Control Policy:

- Are high-level requirements that specify how **access** is managed and who may **access** information under what circumstances

Personal Information Security Policy:

- Requirements assuring **personal information** is protected
- Personal information that is gathered about staff

Security Incident Response Policy:

- Management responsibilities and procedures should be established to **ensure a quick, effective, and orderly response to Security Incidents**. ... Security Events should be assessed and it should be decided if they are to be classified as Security Incidents.

CultureLink

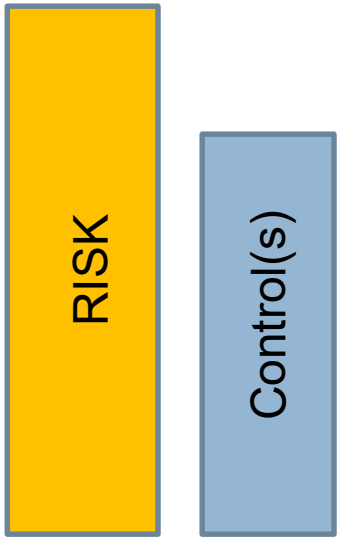
Section 2.4

Cybersecurity controls

Cybersecurity controls

- Controls are critical to maintaining security with the organisations IT infrastructure

- **Areas of controls:**
  - Identity Management
  - Provisioning and deprovisionning
  - Authorization
  - Access control lists
  - Access lists
  - Privileged user management
  - Change management
  - Configuration management
  - Patch management



Cybersecurity controls

- **Identity management:**
  - is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities.
- **Provisioning and deprovisioning:**
  - One of the key responsibilities of Identity Management is providing new users with access to the things they need, and removing this access when they depart. The industry calls this provisioning and deprovisioning.
- **Authorization:**
  - Access rules, specify who can access what
  - Often based on least privileged, which means users granted privileges to only do their work

Cybersecurity controls

- **Change management:**
  - Important to IT infrastructure
  - There are a lot of variables in a network
  - For example, network admin replaces a router, ACL are affected, applications, file storage access, etc…
- **Configuration management:**
  - Maintain devices, software configuration settings, etc.
  - Modification to device settings is critical
  - Ad-hoc changes can introduce risk or vulnerabilities
- **Patch management:**
  - Updating software bugs
  - Patch known vulnerabilities
  - Failure to do so, introduces holes which can be exploited

CultureLink

Any questions?

CultureLink

Thank You