Module 1
Security Fundamentals

Submodule 2: Security Management

Submodule Learning Outcomes:

List types of security control and their functionalities

Demonstrate knowledge and understanding of security related frameworks

Discuss risk management in the context of cybersecurity

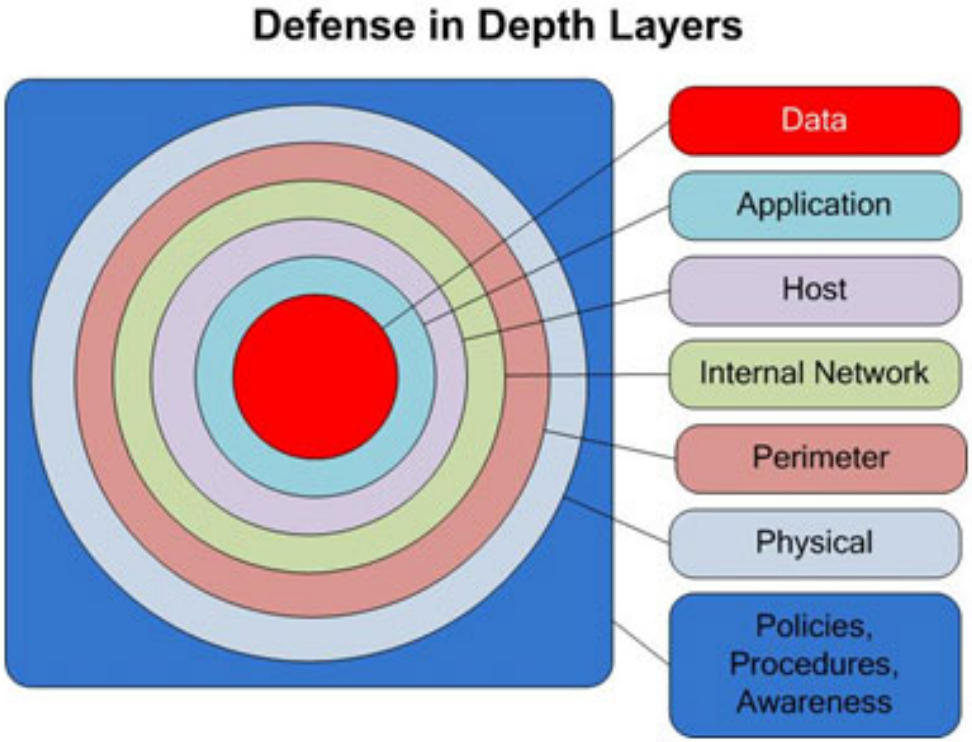
Discuss legal and ethical aspects of cybersecurity

Importance of Control

- Controls are put into place to reduce the risk an organization faces.
- There are three general types of control:
  - Administrative: soft control
    - Examples: security documentation, risk management, personnel security, and training.
  - Technical: logical control
    - Examples: software and hardware such as firewall, identification and authentication mechanisms.
  - Physical: items put into place to protect facility, personnel and resources.

Defense-in-depth

- Different types of control need to be coordinated in a layered approach to provide best protection.



Defense-in-Depth for Network

Basic network security models consist of: crypto systems, firewalls, anti-malware software, IDS

Security Control Functionalities

- There are six different control functionalities:
  - Preventive
  - Detective
  - Corrective
  - Deterrent
  - Recovery
  - Compensating
- Use preventative model, then detective, corrective, and recovery mechanisms to help support the model.

Security Control Functionalities-I

- Preventive control:
  - Try to prevent security violations and enforce access control.
  - Examples: Doors, Authentication requirements.
- Preventive control could be:
  - Administrative
    - Examples: policies and procedures, pre-employment background checks, security awareness
  - Physical
    - Examples: badges, guards, fences, locks
  - Technical
    - Examples: passwords, biometrics, encryption, antimalware software

Security Control Functionalities-II

- Detective control:
  - To detect security violations and alert the defenders.
  - Come into play when preventive controls have failed or have been circumvented.
  - Examples: cryptographic checksums, audit trails and logs.

Security Control Functionalities-III

- Compensating control:
  - Intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.
  - For example, a second of controls addresses the same threats that are addressed by another set of controls.
- Corrective control:
  - Correct the situation after a security violation has occurred.
  - “Damage control”—can be technical or administrative

Security Control Functionalities-IV

- Deterrent control:
  - To discourage potential attackers and send the message that it is better not to attack.
  - Example: notices of monitoring and logging.
- Recovery control:
  - Similar to corrective control buy applied in more severe situations.
  - Recover from security violations and restore information and information processing resources.
  - Example: disaster recovery and business continuity plan, backup systems and data.

Security Management

- Security management focuses on “how to select and implement technical and administrative measures to fulfill an organization’s security requirements?” by providing answers to the following questions:
  - What are the organization’s security objectives and general risk profile?
  - What types of controls can be used to deal with the identified risks:
    - Either reduce them to an acceptable level
    - Or accept the resultant risk

IT Security Management

- It is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, authenticity, and reliability.
- It contains following functions:
  - Determining organizational IT security objectives, strategies, and policies.
  - Determining organizational IT security requirements
  - Identifying and analyzing security threats to IT assets within the organization.
  - Identifying and analyzing risks.

IT Security Management (cont.)

- Specifying appropriate safeguards.
- Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization.
- Developing and implementing a security awareness program.
- Detecting and reacting to incidents.

Security Standards & Frameworks

- For security program development
  - ISO/IEC 27000 series
- For enterprise architecture development
  - Zachman Framework
  - TOGAF
- For security controls development
  - NIST SP800-53
  - COBIT
  - COSO
- For process management development
  - ITIL
  - Capability Maturity Model Integration (CMMI)

ISO/IEC 27000 Series

- The names:
  - ISO (International Standards Organization)
  - IEC (International Electrotechnical Commission)
- ISO is the world's largest developer and publisher of international standards.
- The ISO/IEC 27000 series serves as industry best practices for the management of security controls. Each standard has a specific focus.
  - This family of standards help organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to the organization by third parties.

ISO/IEC 27000:2018 Content

- An overview of information security management systems (ISMS)
- Terms and definitions commonly used in the series.
- The ISMS family of standards:
  - Standards specifying requirements such as ISO/IEC 27001.
  - Standards describing general guidelines such as ISO/IEC 27002.
  - Standards describing sector-specific guidelines such as ISO/IEC 27010.

Sample Synopsis of the Standards

Standard	Covers
27001	Information security management systems-Requirements: specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System.
27002	Code of practice for information security management: provides guidelines for information security management in an organization and contains a list of best-practice security controls.
27003	Information security management system implementation guidance: details the process from inception to the production of implementation plans of an Information Security Management System specification and design
27005	Information security risk management: provides guidelines on the information security risk management process.

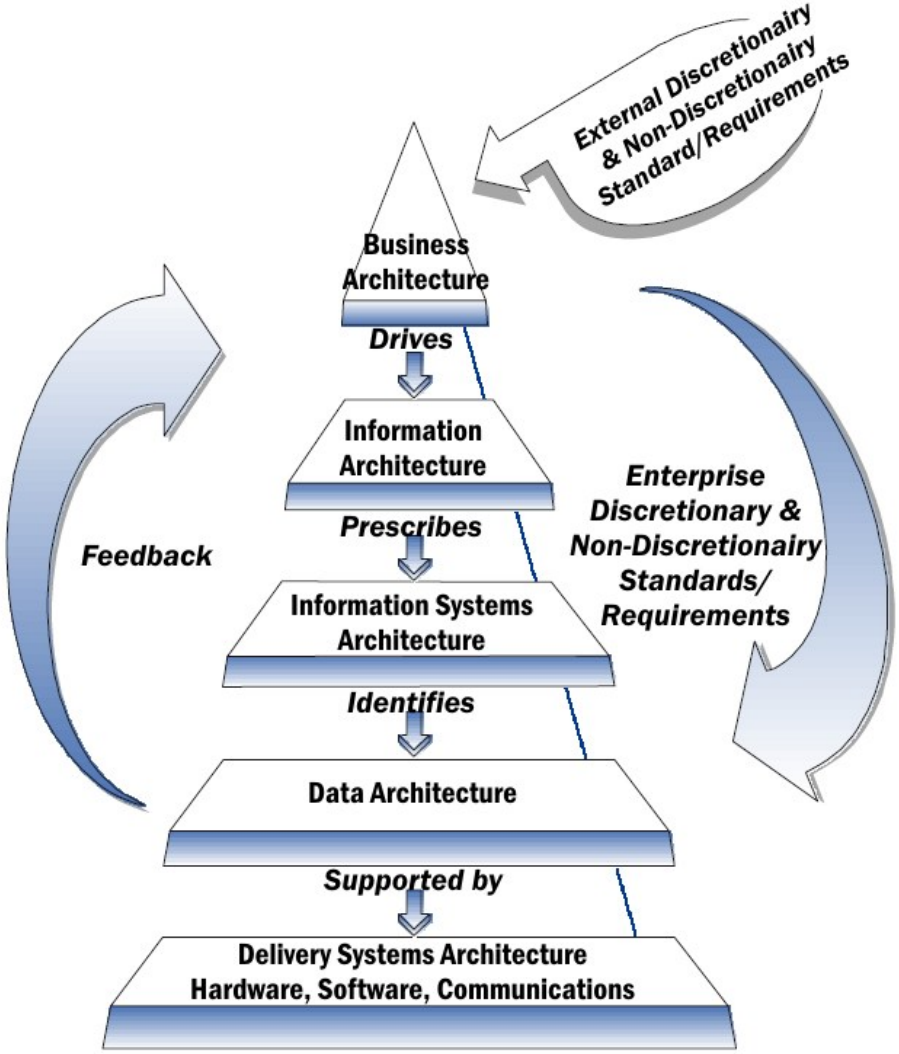
Enterprise Architecture

- An enterprise architecture:
  - Encompasses the essential
  - Unify components
  - Express the enterprise structure and behavior
  - Embodies the components and their relationships
- An enterprise security architecture:
  - Guide the implementation of solutions to ensure business needs
  - Provide standard protection across the environment
  - Reduce the amount of security surprises

NIST Enterprise Architecture Framework

- NIST: National Institute of Standards and Technology

- An enterprise architecture framework provides different views of the same thing.



Zachman Architecture Framework

- The framework is generic, but can be applied in information systems security.
- It is a two-dimensional model that uses:
  - Six basic communication interrogatives: what, how, where, who, when, and why
  - Different perspectives: executives, business managers, system architects, engineers etc.

	What	How	Where	Who	When	Why
Contextual (Executives)	Assets and Liabilities	Business Lines	Business Locales	Partners, Clients, and Employees	Milestones and Major events	Business Strategy
Conceptual (Business Mgrs.)	Products	Business Processes	Logistics and Communications	Workflows	Master Calendar	Business Plan
Architectural (System Architects)	Data Models	System Architectures	Distributed Systems Architectures	Use Cases	Project Schedules	Business Rule Models
Technological (Engineers)	Data Management	Systems Designs	System Interfaces	Human Interfaces	Process Controls	Process Outputs
Implementation (Technicians)	Data Stores	Programs	Network Nodes and Links	Access Controls	Network & Security Operations	Performance Metrics
Enterprise	Information	Functions	Networks	Organizations	Schedules	Strategies

TOGAF

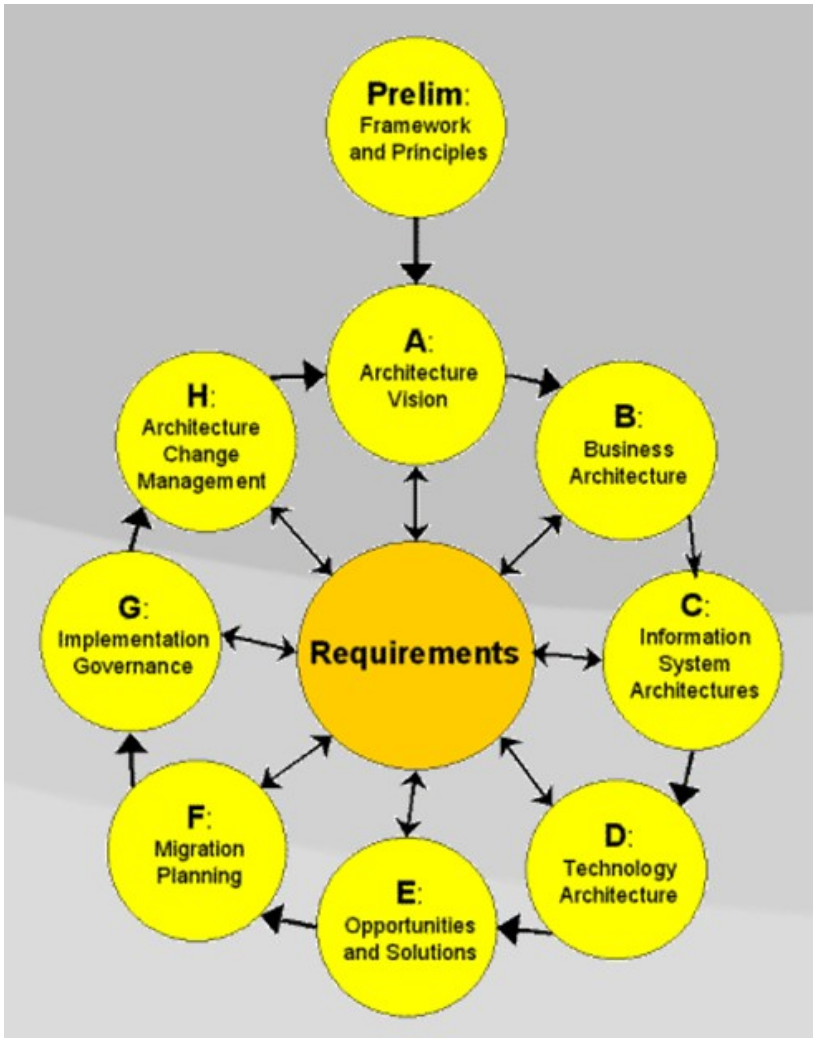
- The Open Group Architecture Framework
- Originated from U.S. DOD, provides an approach to design, implement, and govern an enterprise information architecture.
- TOGAF provides the methods and tools for assisting in the acceptance, production, use, and maintenance of an enterprise architecture.
- It is based on an iterative process model supported by best practices and a re-usable set of existing architecture assets.

Architecture Domains TOGAF Supports

- TOGAF can be used to develop different architecture types:
  - Business architecture: defines the business strategy, governance, organization, and key business processes.
  - Data architecture: describes the structure of an organization's logical and physical data assets and data management resources.
  - Applications architecture: provides a blueprint for the individual application systems to be deployed, their interactions, and their relationships to the core business processes of the organization.
  - Technology architecture: describes the logical software and hardware capabilities that are required to support the deployment of business, data, and application services. This includes IT infrastructure, middleware, networks, communications, processing, standards etc.

TOGAF Architecture Development Method (ADM)

- ADM is applied to develop an enterprise architecture which will meet the business and IT needs of an organization.
- The process is iterative and cyclic.
- Each step checks with Requirements.



Enterprise Security Architecture

- It is needed to ensure that security efforts align with business practices in a standardized and cost-effective manner.
- It defines the information security strategy that consists of:
  - Layers of solutions, processes, and procedures and
  - The way they are linked across an enterprise strategically, tactically, and operationally.
- Sherwood Applied Business Security Architecture (SABSA) is a framework for enterprise security architecture and service management.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

SABSA Architecture Framework

Security Control Development

- The core question: what are the objectives of the controls in order to accomplish the goals outlined in security program and enterprise architecture.
  - COBIT
  - NIST SP 800-53
  - COSO

COBIT

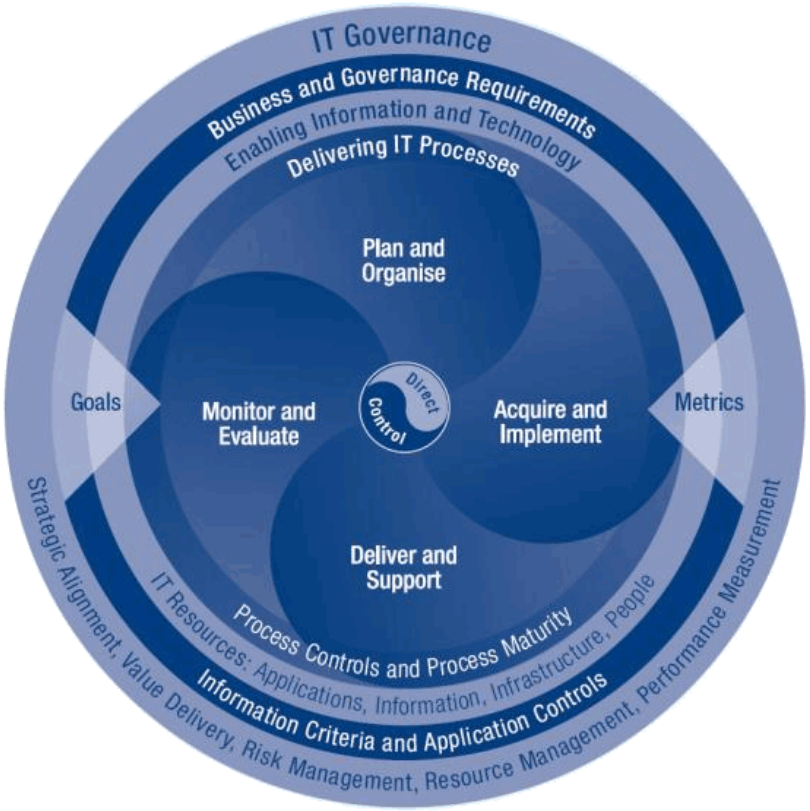
- The Control Objectives for Information and related Technology
  - Is a framework for governance and management
  - Developed by ISACA (Information Systems Audit and Control Association)
  - Helps organizations optimize the value of IT by balancing resource utilization, risk levels, and realization of benefits.
  - Tie together the following:
    - Stakeholder drivers
    - Stakeholder needs
    - Organization goals
    - IT goals

COBIT Key Principles

- Meeting stakeholder needs
- Covering the enterprise end to end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

COBIT (cont.)

- It is an IT governance framework and supporting toolset that:
  - Bridge the gap between control requirements, technical issues and business risks
  - Enable clear policy development and good practice for IT control throughout organizations
  - Emphasizes regulatory compliance



NIST SP 800-53

- "Security and Privacy Controls for Federal Information Systems and Organizations"
  - It is a checklist that outlines controls that agencies need to put into place to be compliant with the Federal Information Security Management Act.
  - The control categories are: management, operational, technical.
  - The controls are to project the availability, integrity, and confidentiality of the system and its information.

COSO

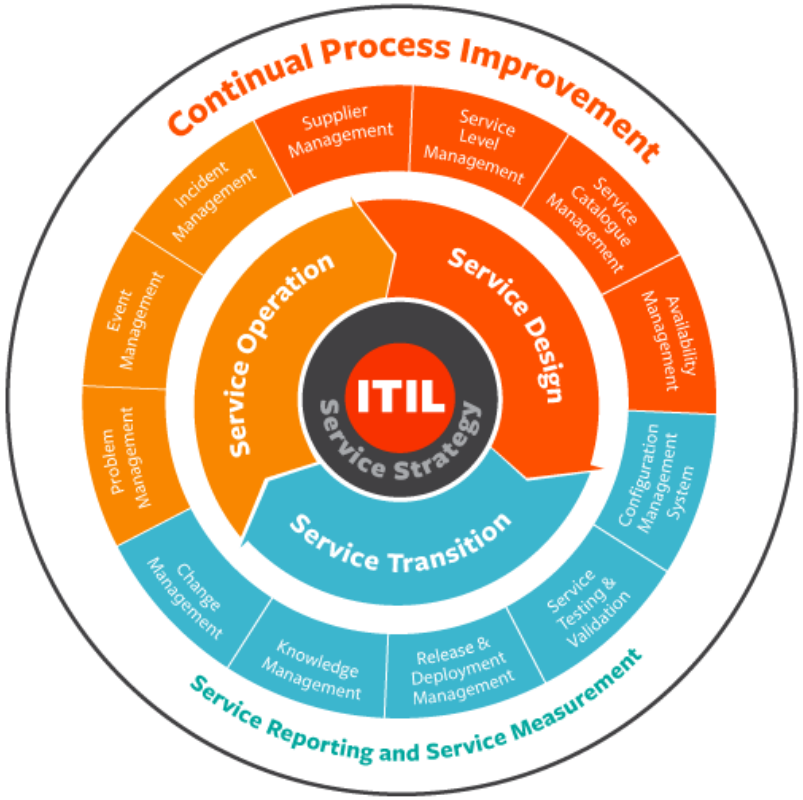
- The Committee of Sponsoring Organizations (COSO) Internal Control (IC) framework identified 17 internal control principles that are grouped into the following five components:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring activities
- It is a model for corporate governance.
- COBIT can be considered as a way to meet many of the COSO objectives, from IT perspective.

Process Management Development

- ITIL (Information Technology Infrastructure Library)
- Capability Maturity Model Integration (CMMI)

ITIL

- ITIL framework provides: the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals.



CMMI

- It can be used to determine the maturity of an organization's processes.
- It develops structured steps to follow in order to evolve from one level to the next and constantly improve processes and security posture.

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Nonexistent management	Unpredictable processes	Repeatable processes	Defined processes	Managed processes	Optimized processes
No process	Ad hoc and disorganized	Immature and developing	Documented and communicated	Monitored and measured	Automated practices
No assessment	Reactive activities	Security assigned to IT	Defined procedures	Security and business objectives mapped	Structured and enterprise wide

Security Policies

- An organization's security policy (master security policy) describes what the security objectives and strategies are and how to achieve those.
- Security policy could also be issue-specific (functional policy), or system-specific.
- General types of organization security policies:
  - Regulatory: ensure compliance with industry specific regulations
  - Advisory: what behaviors should or should not happen
  - Informative: informs employees of certain topics

Risks Everywhere

TOP 10 RISKS IN THE USA

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 468

Responses: 586

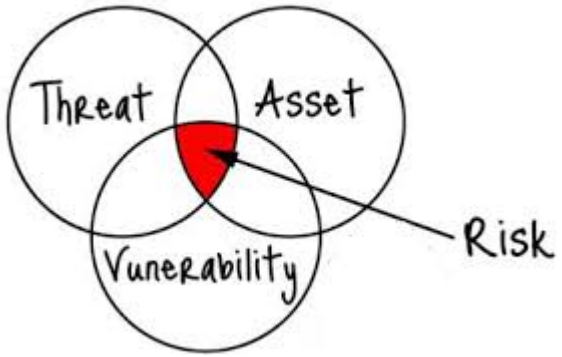
More than one risk and industry could be selected. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2017 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure, data breaches)**	**45%**	2 (34%)	▲
2	Business interruption (incl. supply chain disruption)	**39%**	1 (41%)	▼
3	Natural catastrophes (e.g. storm, flood, earthquake)	**38%**	3 (30%)	=
4	Market developments (e.g. volatility, intensified competition / new entrants, M&A, market stagnation, market fluctuation)	**23%**	4 (27%)	=
5	Fire, explosion	**19%**	6 (16%)	▲
6	Changes in legislation and regulation (e.g. government change, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**17%**	5 (20%)	▼
7	Loss of reputation or brand value	**14%**	7 (15%)	=
8	New technologies (e.g. impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones)	**13%**	8 (12%)	=
9	Climate change/increasing volatility of weather **NEW**	**11%**	-	▲
10	Talent shortage **NEW**	**11%**	-	▲

Source: Allianz Global Corporate & Specialty Allianz Risk Barometer 2018

Risk Assessment

- Risk assessment is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.
- Approaches to risk assessment of IT infrastructure:
  - Baseline approach
  - Informed approach
  - Detailed risk analysis
  - Combined approach

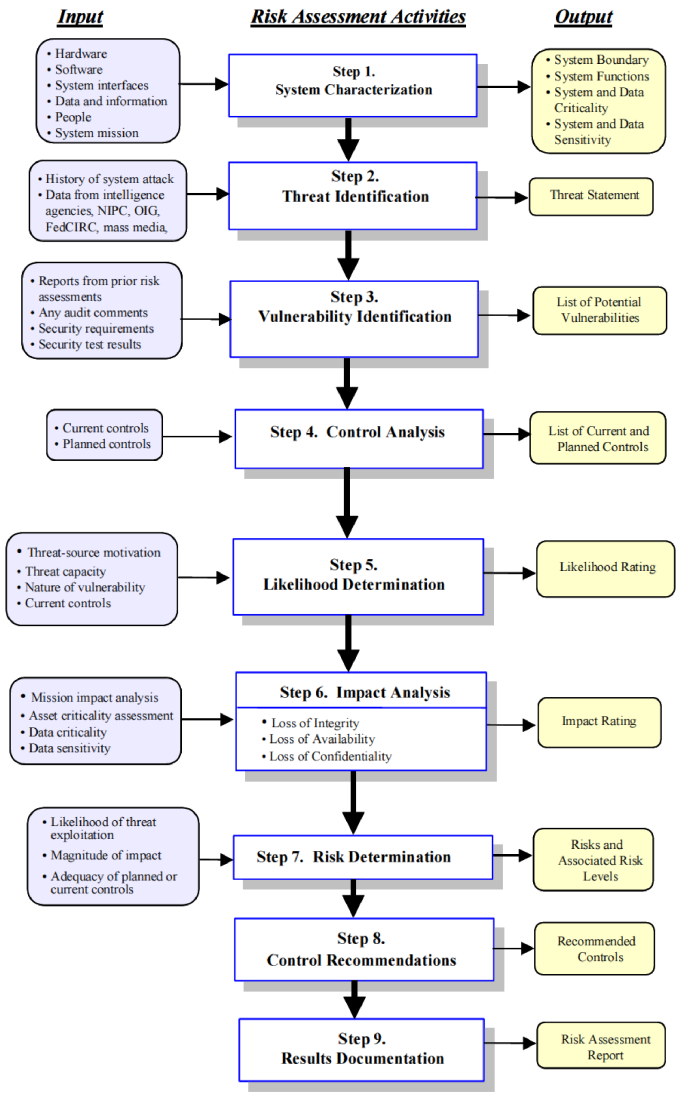


	What to do	Pros & Cons	Good for
Baseline Approach	Implement a basic general level of security controls using baseline documents, codes of practice, and industry best practice.	Pros: saving cost of formal risk assessment Cons: may not be accurate and precise	Only recommended for small organizations without the resources to implement more structured approaches
Informal Approach	Conducting some forms of informal, pragmatic risk analysis without using of a structured process.	Pros: can be done quickly and cheaply. Cons: Some risks may not be considered	Recommended for small to mid-sized organizations where IT systems are not essential.
Detailed Risk Analysis	Risk assessment using a formal structured process that contains multiple well-defined stages	Pros: detailed analysis results provide strong justification for expenditure on proposed controls. Cons: significant cost in time, resources, and expertise	This can be required for organizations and businesses at stake. Also can be choice to large organizations with IT critical to business processed.

Risk Analysis

- A risk analysis has four main goals:
  1. Identify assets and their value to the organization
  2. Identify vulnerabilities and threats
  3. Quantify the probability and business impact of these potential threats
  4. Provide an economic balance between the impact of the threat and the cost of the countermeasure

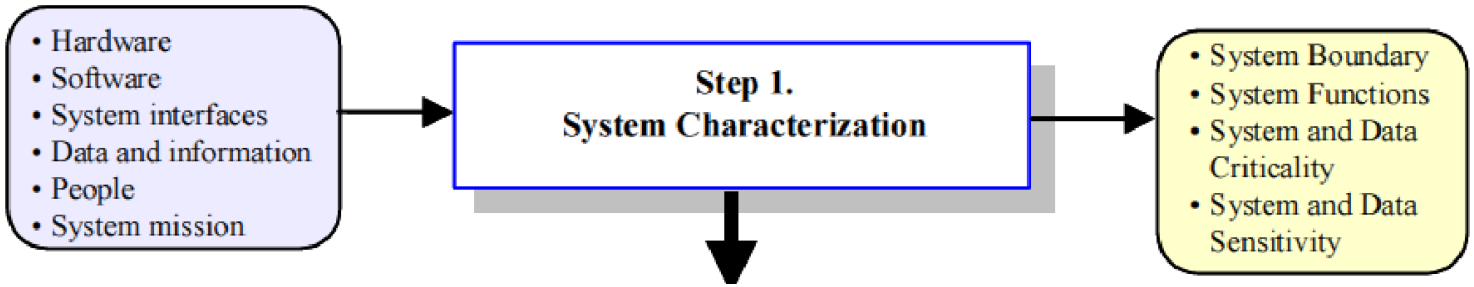
Risk Analysis Flowchart



Typical process used in formal risk analysis defined in many standards such as NIST02.

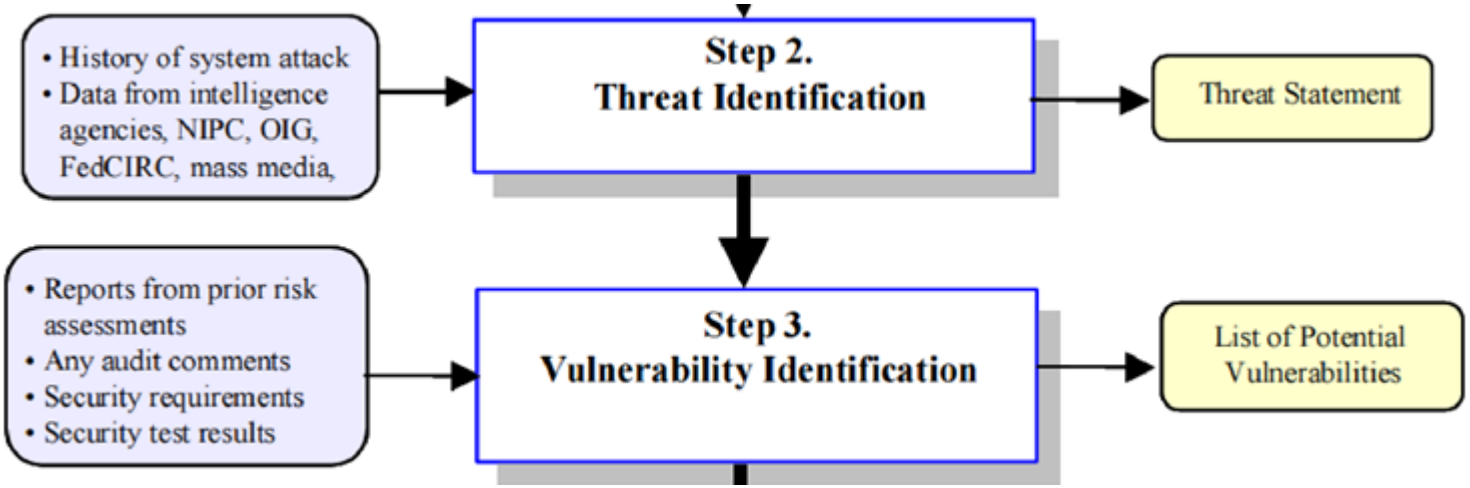
Context and System Characterization

- Determine an organization's broad risk exposure, taking into consideration of any relevant legal and regulatory constraints.
- Define the organization's risk appetite.
- Define the boundary of the analysis.
- Identify the assets to examine.

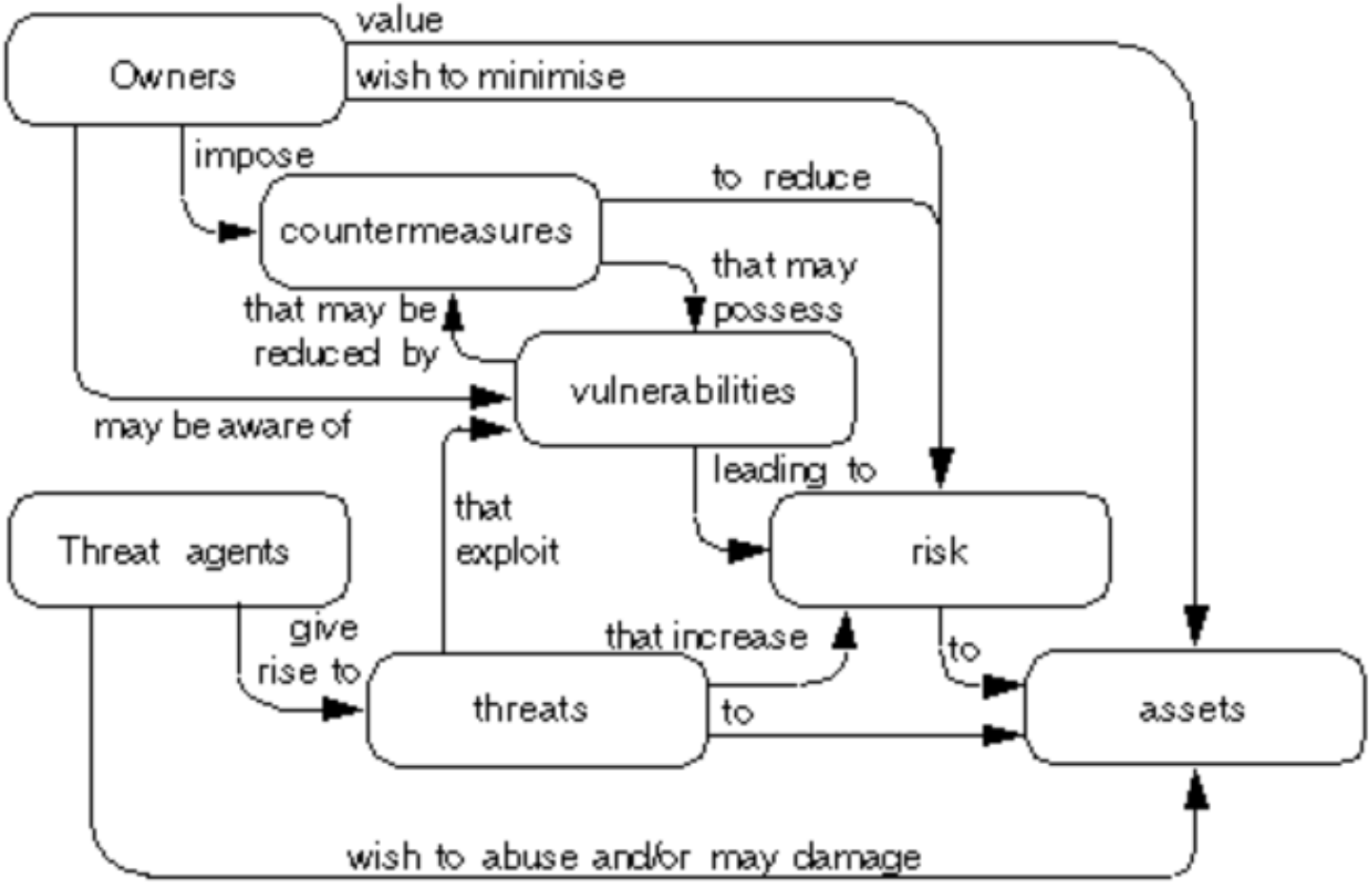


Identification of Threats/Risks/Vulnerabilities

- Who or what could cause assets harm?
  - Identify potential threats to assets
- How could this occur?
  - Identify flaws of weakness in the organization's IT systems or processes

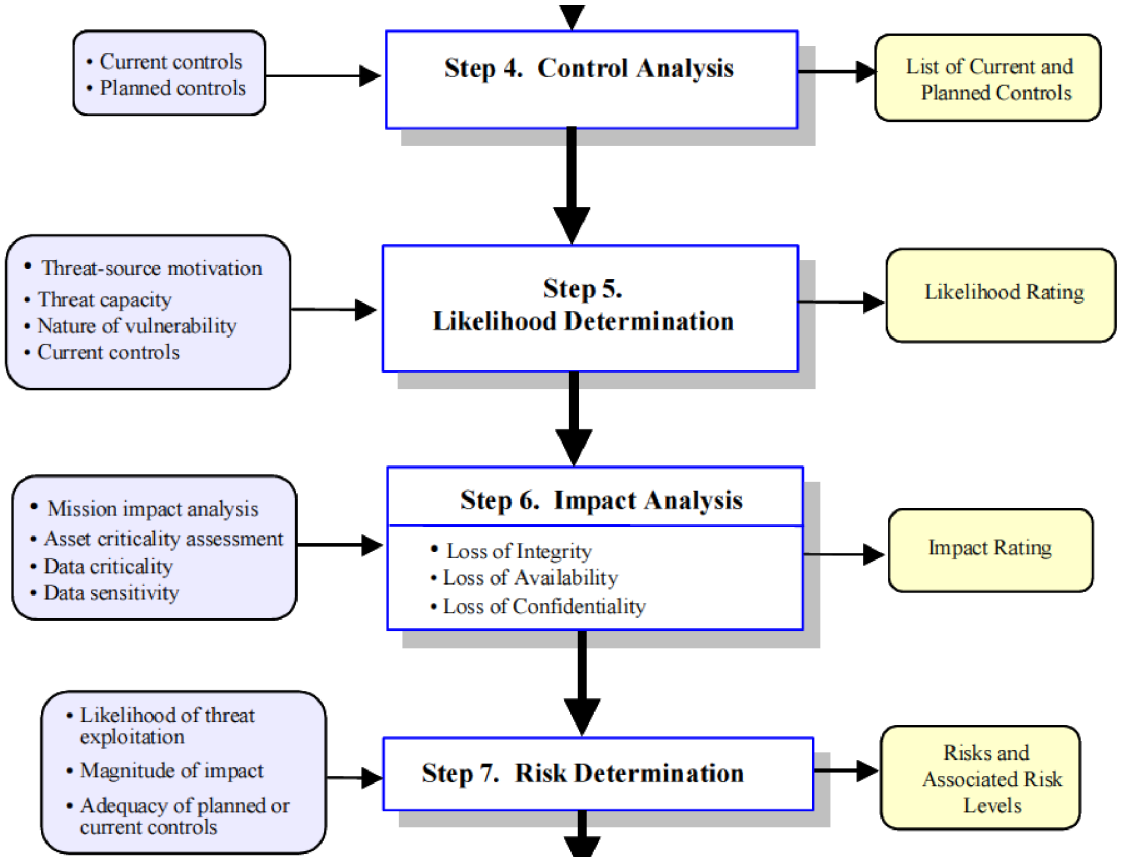


Relationships between Security Concepts



Analyze Risks

- Determine the level of risk posed by the identified threats/vulnerabilities



Risk =
Probability that threat occurs
X
Cost to organization

Analyze Risks (Cont.)

- Analyze existing control
- Determine likelihood
  - Rare, Unlikely, Possible, Likely, Almost Certain
- Determine consequence/impact on organization
  - Insignificant, Minor, Moderate, Major, Catastrophic, Doomsday
- Determine resulting level of risk
  - Extreme, High, Medium, Low
- Documenting the results in a risk register

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

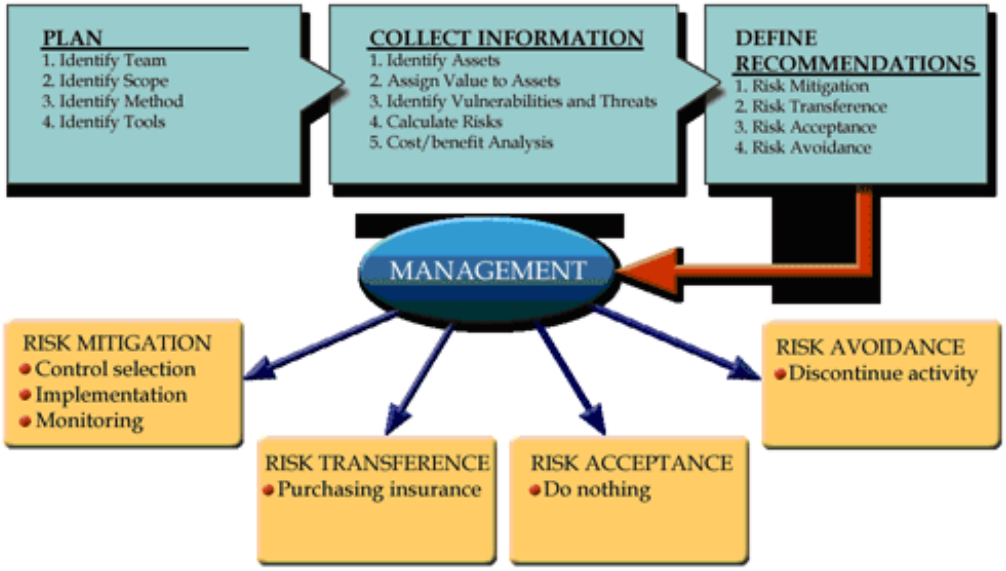
SYSTEM: IT Admin Laptop			
Threat Event	**Likelihood**	**Impact**	**Risk Level**
1. Loss of Confidentiality	Possible	Severe	**HIGH**
2. Loss of Integrity	Unlikely	Minor	**LOW**
3. Loss of Availability	Possible	Significant	**MODERATE**
		OVERALL RISK:	**HIGH**

SYSTEM: Employee Office Computer with UI institutional data			
Threat Event	**Likelihood**	**Impact**	**Risk Level**
1. Loss of Confidentiality	Possible	Significant	**MODERATE**
2. Loss of Integrity	Unlikely	Minor	**LOW**
3. Loss of Availability	Possible	Moderate	**MODERATE**
		OVERALL RISK:	**MODERATE**

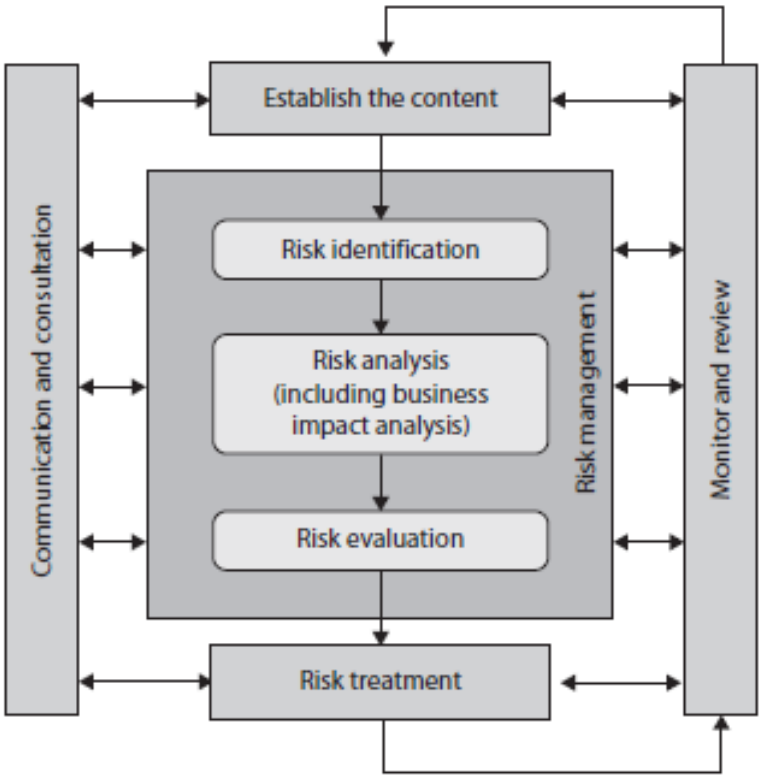
Risk Management

- Total risk = threats X vulnerability X asset value
- Residual risk = total risk X controls gap

  = total risk – countermeasures
- To handle residual risks:
  - Transfer it
  - Avoid it
  - Reduce it
  - Accept it



Risk Treatment



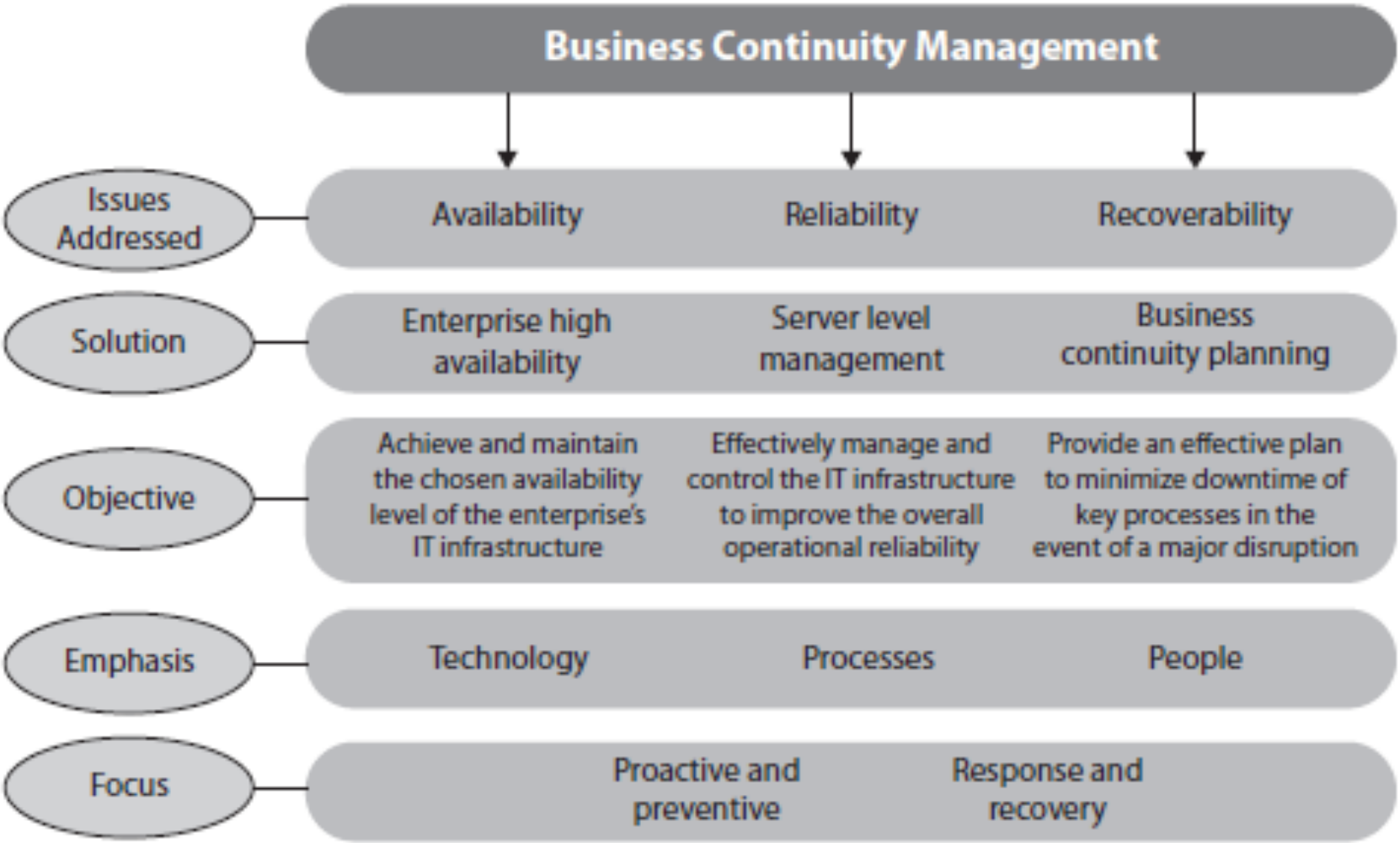
- Risks cannot be completely eliminated.
- Organizations need to prepare themselves for the possible negative impacts and losses caused by incidents.
- Organizations need to continue to operate at some minimum acceptable threshold capacity and return to normal activities.

Disaster Recovery

- The goal is to minimize the effects of a disaster or disruption.
- Needs to ensure the resources, personnel, and business processes are able to resume operation in a timely manner.
- A disaster recovery plan (DRP) handles the disaster and its ramifications right after the disaster hits.

Continuity Planning

- Provides methods and procedures for dealing with longer-term outages and disasters.
- Business continuity plan (BCP)—how to ensure organizations/businesses continue to function after incidents happen, before everything returns normal.
- Business continuity management (BCM) should cover both disaster recovery and continuity planning.


Business Continuity Management
Issues Addressed
Availability
Reliability
Recoverability
Solution
Enterprise high availability
Server level management
Business continuity planning
Objective
Achieve and maintain the chosen availability level of the enterprise's IT infrastructure
Effectively manage and control the IT infrastructure to improve the overall operational reliability
Provide an effective plan to minimize downtime of key processes in the event of a major disruption
Emphasis
Technology
Processes
People
Focus
Proactive and preventive
Response and recovery

Computer Crime Laws

- Computer Crime Laws (cyberlaw) deals with crimes that involve:
  - Unauthorized modification or destruction
  - Disclosure of sensitive information
  - Unauthorized access
  - Use of malware
- The crime could be
  - Computer assisted
  - Computer targeted
  - Computer is incidental

Cybercrimes Are Complex

- Fighting cybercrimes has its unique difficulties, which leads to low success rate:
  - Law enforcement agencies may not possess the sophisticated technologies needed to investigate the crime.
  - Investigations often consume large amount of technical resources, which may not always be available.
  - It is not always practical to have agencies allocated in different geographical locations to collaborate.
  - Victims of cybercrimes may fail to report the crimes.

Examples of Cybercrimes

- Illegal access
- Illegal interception
- Data interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Offenses related to child pornography
- Infringements of copyright and related rights

Examples of Cyberlaws

- 18 USC 1029: Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030: Fraud and Related Activity in Connection with Computers
- 18 USC 2510 et seq.: Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC 2701 et seq.: Stored Wire and Electronic Communications and Transactional Records Access
- Digital Millennium Copyright Act

Intellectual Property Basics

- Different from Real Property, Personal Property, Intellectual Property refers to:
  - Intangible asset that consists of human knowledge and ideas.
- Types of intellectual property:
  - Copyrights: tangible or fixed expression of an idea, not the idea itself.
  - Patents: grant the property right of an invention to the inventor.
  - Trademarks: indicate the source of the goods in trade and distinguish them from the rest.
  - Examples of each?

Intellectual Property and Security

- Intellectual property could be violated due to its forms:
  - Software—may need to protected by copyright or patent
  - Databases—both the data and the way the data is organized and managed may need to protected, probably using copyright
  - Digital content in various forms—need to be protected from illegal interception and distribution
  - Algorithms—some are patentable

- The protection of these needs to resort to:
  - Technical measures
  - Legal tools

Privacy

- With advancement of computing especially Internet technologies, protection of privacy has become a greater concern everyday.

- Personal information at various levels is collected, stored, processes, and analyzed for many purposes:
  - Personal convenience
  - Economic incentives
  - Law enforcement
  - National security

Personally Identifiable Information (PII)

- Data can be used to uniquely identify, contact, or locate a single person or can be sued with other sources to uniquely identify a single individual.
  - Examples of PII
- Balance in the protection of PII:
  - PII needs to be protected because it can be used in crimes against our citizens.
  - Government and businesses often need to collect and use PII for valid reasons.
- Definition and coverage of PII may vary from one sector to another.

Privacy Functions in Trusted Systems

- Anonymity
  - A user may use a resource or service without disclosing the user's identity—authorization is bound to IDs, not PII.
- Pseudonymity
  - A user may use a resource or service without disclosing its user identity, but can still be accountable for that use—use alias.
- Unlinkability
  - A user may make multiple uses of resources or services without others being able to link these uses together.
- Unovservability
  - A user may use a resource or service without others being able to observe that the resource or service is being used.

Source: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements

Fair Information Practice Principles

- Established by United States Federal Trade Commission.
- Represent widely accepted concepts concerning fair information practice in an electronic marketplace.

FIPPS Principles

- Notice/Awareness
  - Before any personal information is collected from them, consumers should be given notice of an entity's information practices including: what is being collected, how is it going to be used, who will have access to it, what protection is provided etc.
- Choice/Consent
  - Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used, or to whom the data is disclosed. They have the right not to have any sensitive information collected or used without express permission.

FIPPS Principles (Cont.)

- Access/Participation
  - A consumer should have the ability to view the data collected, also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.
- Integrity/Security
  - Information collectors should ensure that the data they collect is accurate and secure.
- Enforcement/Redress
  - Three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement that can include civil and criminal penalties levied by the government.

Privacy Related Laws

- Federal Privacy Act of 1974
- Federal Information Security Management Act of 2002
- Department of Veterans Affairs Information Security Protection Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- USA PATRIOT Act
- Gramm0Leach0Bliley Act (GLBA)

To Protect Privacy

- Laws on government
- Laws on corporations
- Self-regulation
  - PCI DSS—Payment Card Industry Data Security Standard, which applies to any entity that processes, transmits, stores, or accepts credit card data.
- Individual user
  - Passwords
  - Encryption
  - VPNs
  - Awareness

Ethics in Computing

- Ethics is a system of moral principles that separate right from wrong. It carefully examines the benefits and harms of a particular actions and consequences of those actions.

- Proliferation of computing at various levels poses new facets of ethical issues:
  - Computing technologies enable entities to have more opportunities to access and utilize PII to do harm
  - There is a lack of applicable and agreed-upon ethical rules

Ethical Issues with Information Systems

Issues	Examples
Technology Intrusion	Privacy internal to the firm, Privacy external to the firm, Computer surveillance, Employee monitoring, Hacking
Ownership Issues	Moonlighting, Proprietary rights, Conflicts of interest, Software copyrights, Use of company assets for personal benefit, Theft of data, software, or hardware
Legal Issues and Social Responsibilities	Embezzlement, fraud and abuse, Accuracy and timelines of data, Over-rated system capabilities and "smart" computers, Monopoly of data
Personnel Issues	Employee sabotage, Ergonomics and human factors, Training to avoid job obsolescence

Source: Harrington, S. and McCollum, R. "Lessons from Corporate America Applied to Training in Computer Ethics"

Code of Conduct

- Code of conduct provides professionals guidelines as to what are expected of them from employers and customers.
  - Provide positive stimulus for ethical conduct in the profession.
  - Educate professionals about their commitment to quality and responsibility for users of their products/ services.
  - Support professionals who may need face conflicts in professional setting.
  - Serve the purpose of deterrence and discipline.
  - Enhance the profession's public image.

Source: Gotterbarn, D. "How the New Software Engineering Code of Ethics Affects You".

Relevant Professional Code of Conduct

- ACM Code of Ethics and Professional Conduct
- IEEE Code of Ethics
- AITP Standard of Conduct
- $(ISC)^2$ Code of Ethics
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principals.
  - Advance and protect the profession.