
Lesson 3: Risk Management

Risk Assessment

Assets : valuable resources you are trying to protect.

Risks: the potential that a chosen action or activity will lead to a loss.

Threats: a negative action that may harm a system.

Vulnerabilities: a weakness that allows a threat to cause harm.

Impact: the severity of the damage, sometimes expressed in dollars.

TCO – Total Cost of Ownership

ROI - Return on Investment

Threats, Vulnerabilities, and Risks

Threat	Vulnerability	Risk
Intruder	No security guard or controlled entrance	Theft
Hacker	Misconfigured firewall	Stolen credit card information
Current employee	Poor accountability; no audit policy	Loss of integrity; altered data
Fire	Insufficient fire control	Damage or loss of life
Hurricane	Insufficient preparation	Damage or loss of life
Virus	Out-of-date antivirus software	Virus infection and loss of productivity
Hard drive failure	No data backup	Data loss and unrecoverable downtime

- Threat—a potentially negative occurrence
- • Vulnerability—a weakness in a system
- • Risk—a matched threat and vulnerability
- NOTE: Differentiating between the three is critical for the test.

SLE, ARO, & ALE

- **$SLE \times ARO = ALE$**
- Single Loss Expectancy (SLE)
Annualized Rate of Occurrence (ARO)
Annualized Loss Expectancy (ALE)

The Annualized Loss Expectancy (ALE) is the expected monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as: $ALE = SLE * ARO$ where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence

Computing Risk

- **Exposure Factor** The Exposure Factor (EF) is the percentage of value an asset lost due to an incident.
- **Single Loss Expectancy** The Single Loss Expectancy (SLE) is the cost of a single loss. $SLE = AV \times EF$ (SLE is the Asset Value (AV) times the Exposure Factor (EF)).
- **Annual Rate of Occurrence** The Annual Rate of Occurrence (ARO) is the number of losses you suffer per year.
- **Annualized Loss Expectancy**
 - The Annualized Loss Expectancy (ALE) is your yearly cost due to a risk. It is calculated by multiplying the Single Loss Expectancy (SLE) times the Annual Rate of Occurrence (ARO).

Basic formulas

$$\text{SLE} = \text{Asset Value (AV)} * \text{Exposure Factor (EF)}$$

$$\text{Risk} = \text{Probability of the Risk} * \text{Cost of the Eventuality}$$

$$\text{ALE} = \text{Single Loss Expectancy (SLE)} * \text{Annual Rate of Occurrence (ARO)}$$

Risk Management

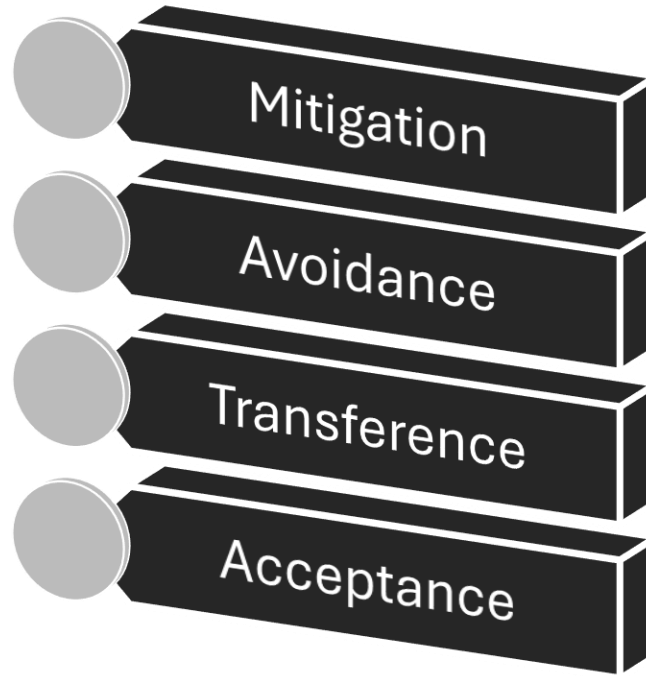


Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization's information systems



The primary deliverable from risk assessment was a list of documented vulnerabilities, ranked by criticality of impact

Risk



residual risk

What is left after mitigation

Is it below acceptable levels

If not then take further steps

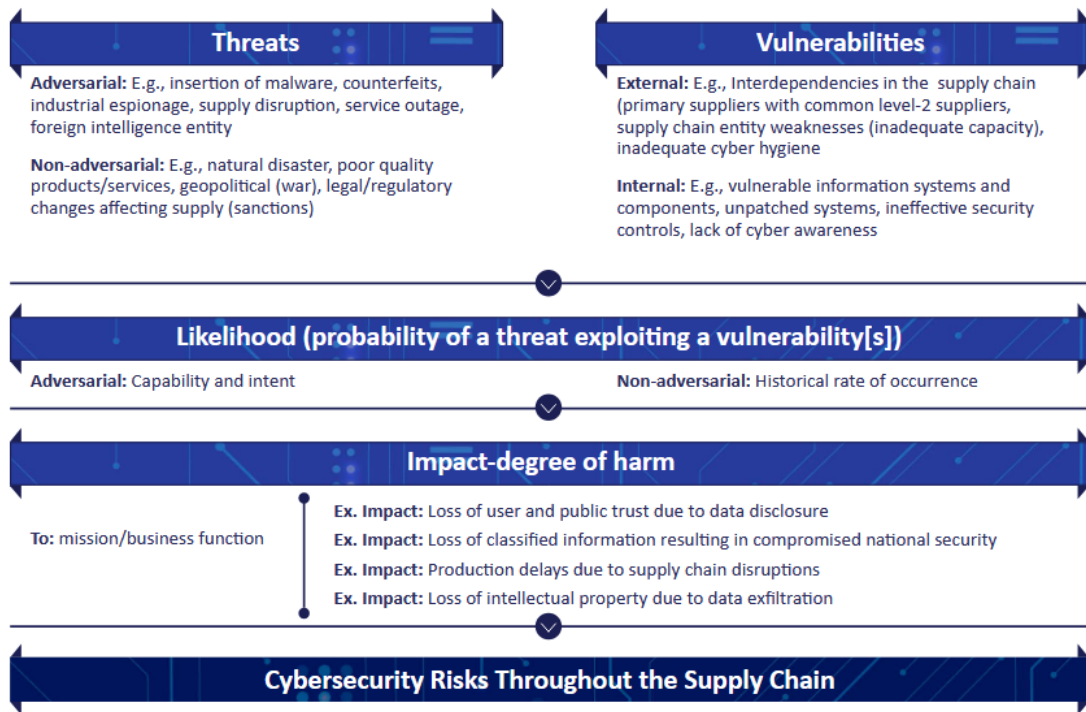


Figure 6: Cybersecurity Risks in the Supply Chain

Supply Chain Risk

The Cyber Resilience Engineering Framework Process

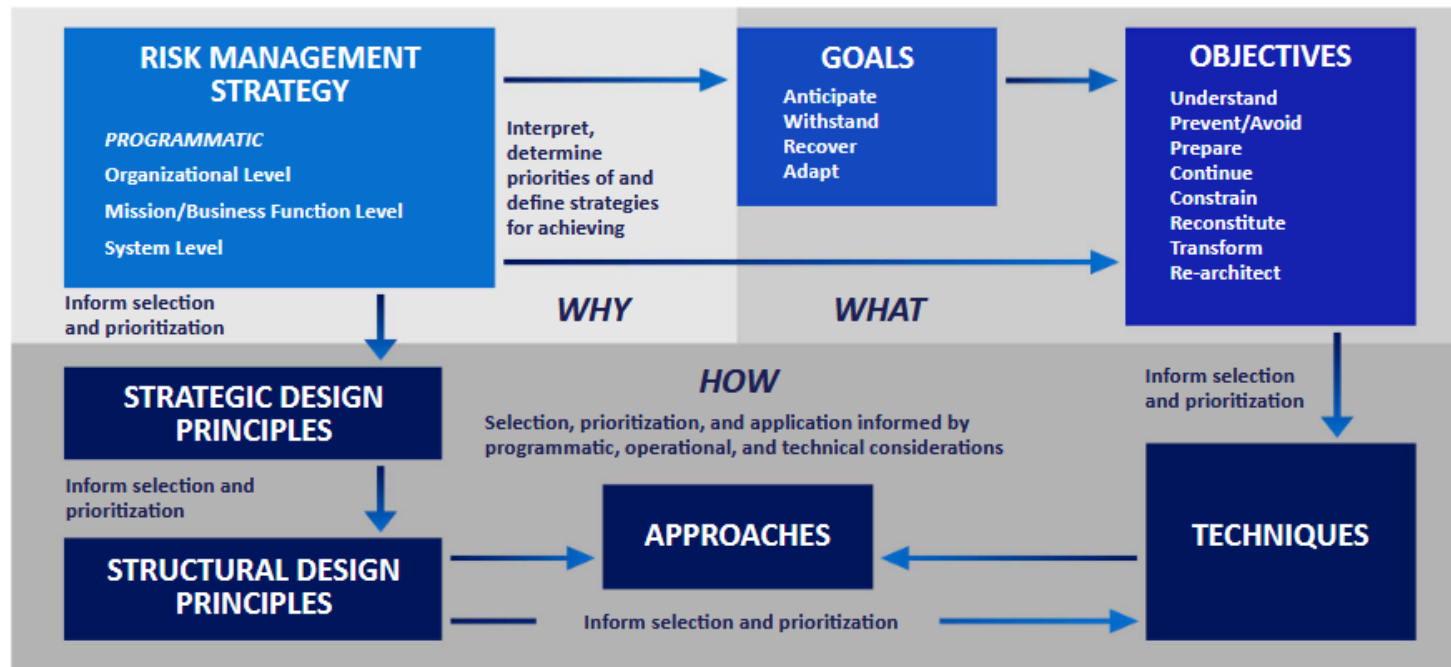
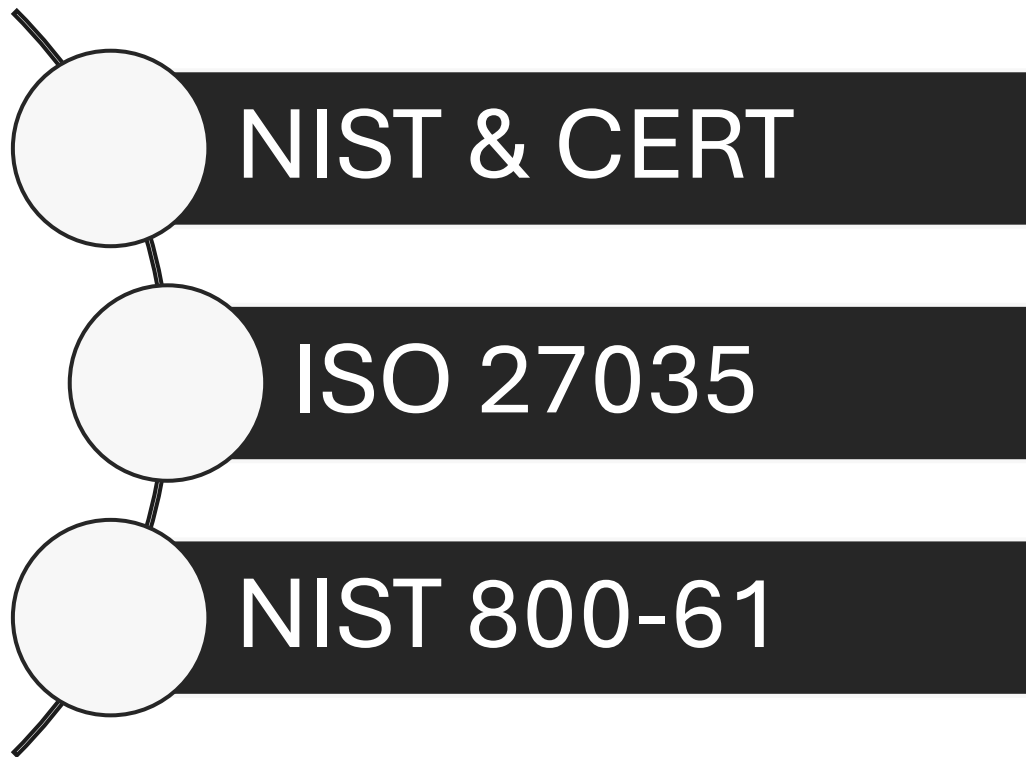


Figure 8: The Cyber Resilience Engineering Framework Process

Incident Response



ISO 27035

- **ISO/IEC 27035** is the international standard for **information security incident management**, published by the **International Organization for Standardization (ISO)** and the **International Electrotechnical Commission (IEC)**.
- It provides a structured framework for **detecting, reporting, assessing, and responding to information security incidents** in a consistent and effective manner.

ISO 27035



-
- ISO/IEC 27035-1: Principles of incident management
 - Introduces the concepts, principles, and processes of incident management.
 - Defines key terms (e.g., event vs. incident).
 - Provides a high-level incident management lifecycle.
 - ISO/IEC 27035-2: Guidelines to plan and prepare for incident response
 - Focuses on establishing an incident response capability (IRC).
 - Covers roles and responsibilities, policies, incident response plans, and communication channels.
 - Helps organizations build resilience and readiness.
 - ISO/IEC 27035-3: Guidelines for incident response operations
 - Provides detailed operational guidance for handling incidents.
 - Covers incident detection, analysis, containment, eradication, recovery, and post-incident learning.
 - Encourages using metrics and lessons learned to improve future responses.

ISO 27035

- The major points within the "Plan and Prepare" phase include the following:
 - information security incident management policy and commitment of top management;
 - information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels;
 - information security incident management plan;
 - incident response team (IRT) establishment;
 - establish relationships and connections with internal and external organizations;
 - technical and other support (including organizational and operational support);
 - information security incident management awareness briefings and training;
 - information security incident management plan testing.

NIST 800-61

- Establishing an incident response capability should include the following actions:
 - Creating an incident response policy and plan
 - Developing procedures for performing incident handling and reporting
 - Setting guidelines for communicating with outside parties regarding incidents
 - Selecting a team structure and staffing model
 - Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
 - Determining what services the incident response team should provide
 - Staffing and training the incident response team.

NIST 800-61



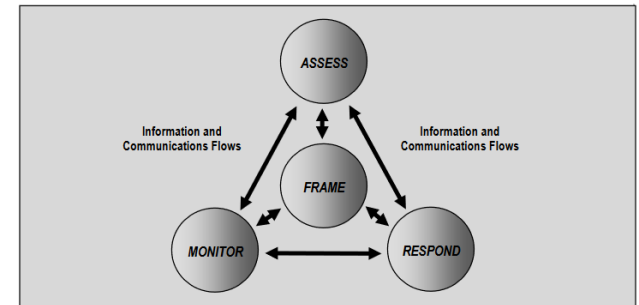
-
- Establishing an incident response capability should include the following actions:
 - Creating an incident response policy and plan
 - Developing procedures for performing incident handling and reporting
 - Setting guidelines for communicating with outside parties regarding incidents
 - Selecting a team structure and staffing model
 - Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
 - Determining what services the incident response team should provide
 - Staffing and training the incident response team.

NIST 800-30

- NIST 800-30 is the U.S. standard for how to conduct risk assessments. The standard is divided into three chapters. The first is just introductory information such as the target audience and purpose of the standard. Chapter 2 discusses the risk management process and concepts. Chapter 3 provides a process for conducting a risk assessment.
-

2.1 RISK MANAGEMENT PROCESS

Risk assessment is a key component of a holistic, organization-wide *risk management process* as defined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. Figure 1 illustrates the four steps in the risk management process—including the risk assessment step and the information and communications flows necessary to make the process work effectively.¹³



NIST 800-30

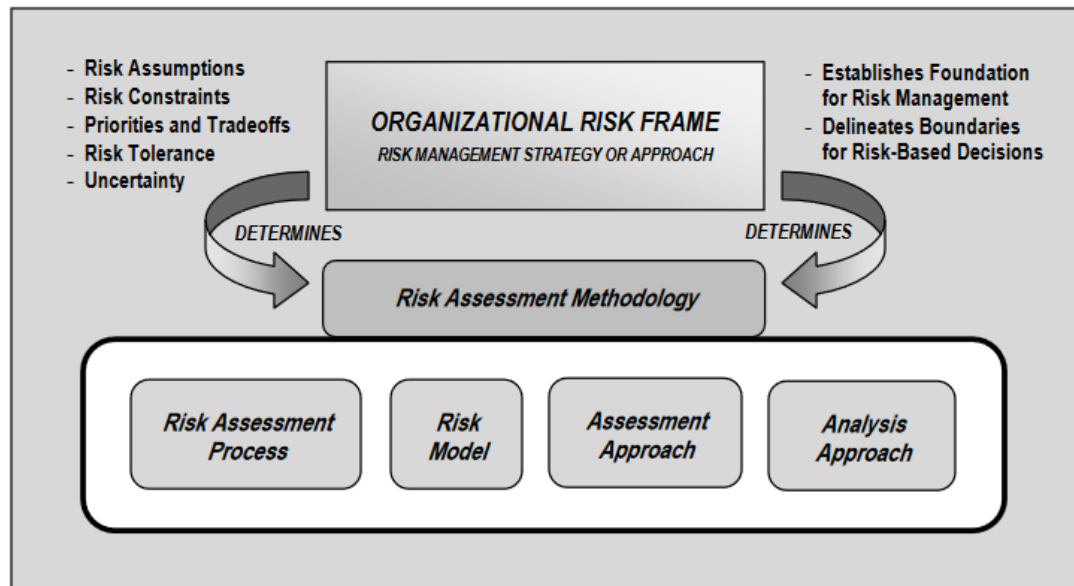


FIGURE 2: RELATIONSHIP AMONG RISK FRAMING COMPONENTS

NIST 800-30

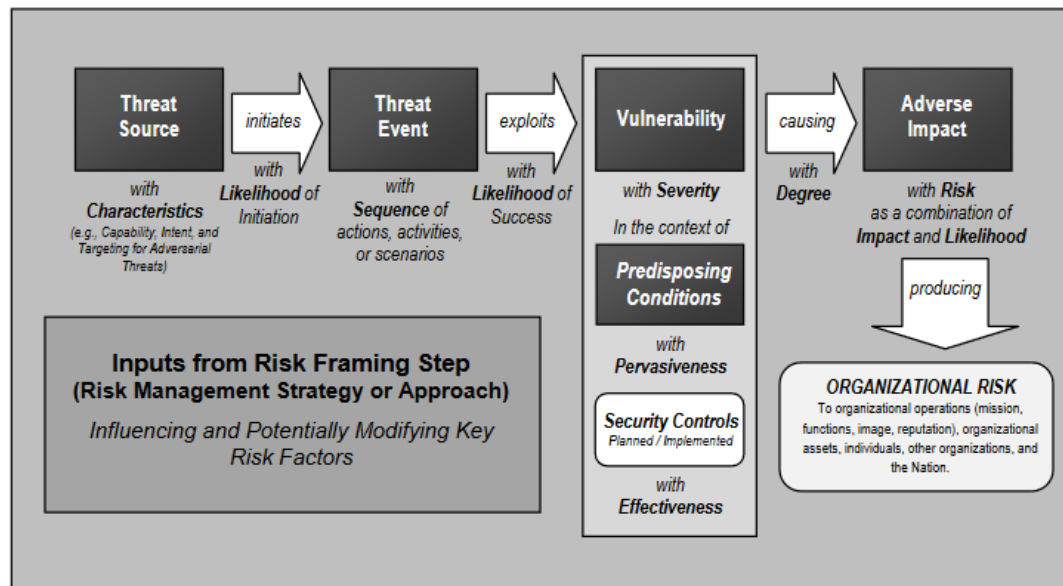
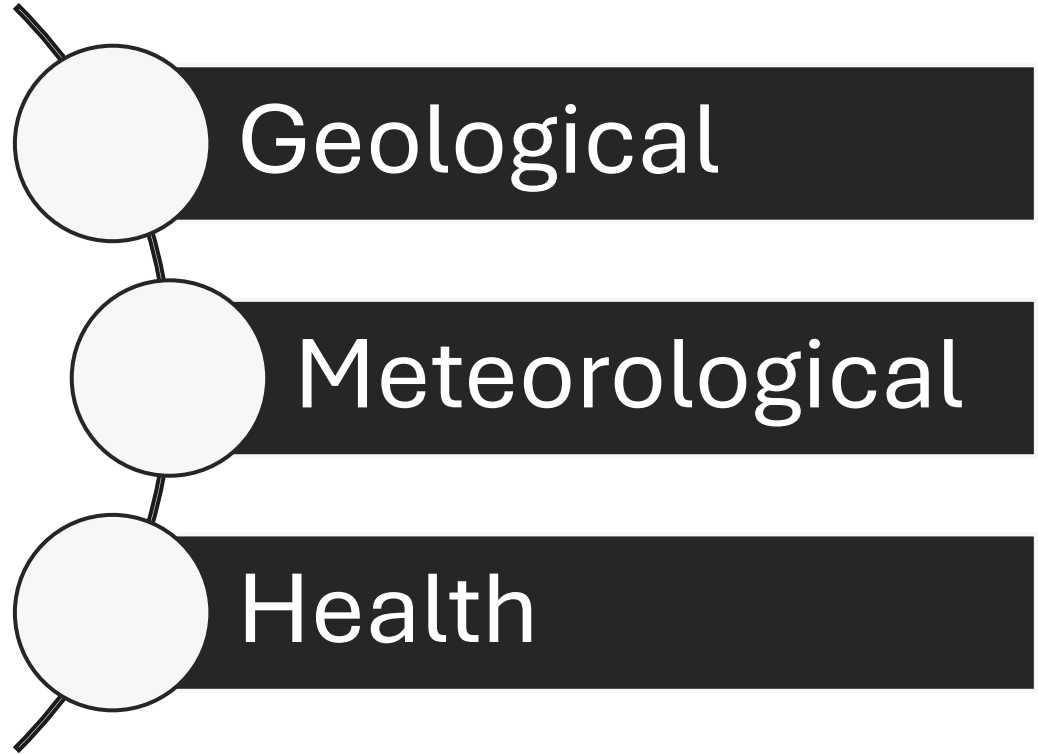


FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

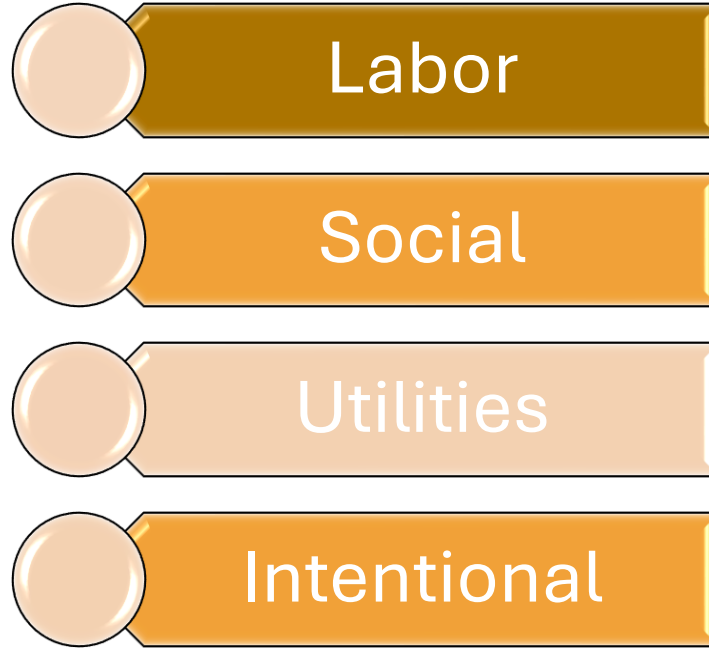
What Is a Disaster

Any natural or man-made event that disrupts the operations of a organizational in such a significant way that a considerable and coordinated effort is required to achieve a recovery.

Natural Disasters



Man-made Disasters



BCP and DRP Differences and Similarities



BCP

Critical systems
running until
full-recovery.



DRP

Full-recovery



ISO 27001

- Standard for Information Security Management System (ISMS)
- Plan-Do-Check-Act cycle
 - Plan = define requirements, assess risks, decide which controls are applicable
 - Do = implement and operate the ISMS
 - Check = monitor and review the ISMS
 - Act = maintain and continuously improve the ISMS
- Document the entire process
- NOTE: PDCA is NOT in ISO 27001:2014

ISO 27001

- ISO/IEC 27001 requires that management:
 - Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
 - Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
 - Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.
- Note that ISO27001 is designed to cover much more than just IT.

ISO 27001

- The ISO/IEC 27001 certification,[5] like other ISO management system certifications, usually involves a three-stage external audit process defined by the ISO/IEC 17021[6] and ISO/IEC 27006[7] standards:
 - Stage 1 is a preliminary, informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
 - Stage 2 is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation (for example by confirming that a security committee or similar management body meets regularly to oversee the ISMS). Certification audits are usually conducted by ISO/IEC 27001 Lead Auditors. Passing this stage results in the ISMS being certified compliant with ISO/IEC 27001.
- Ongoing involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently, particularly while the ISMS is still maturing.

Industry Standards Supporting BCP and DRP

- NIST 800-34
 - Contingency Planning Guide for Information Technology Systems.
 - Seven step process for BCP and DRP projects
 - From U.S. National Institute for Standards and Technology
- NFPA 1600
 - Standard on Disaster / Emergency Management and Business Continuity Programs
 - From U.S. National Fire Protection Association

5 phases of BCP

- Project management & initiation
- Business Impact Analysis (BIA)
- Recovery strategies
- Plan design & development
- Testing, maintenance, awareness, training

Performing a Business Impact Analysis

Asset Analysis

- Purchase cost, development cost, administrative cost, maintenance cost.

Survey critical processes

Perform risk analyses and threat assessment

Determine Maximum Tolerable Downtime (MTD)

Establish key recovery targets

Survey In-scope Business Processes

- Develop interview / intake template
- Interview a rep from each department
 - Identify all important processes
 - Identify dependencies on systems, people, equipment
- Collate data into database or spreadsheets
 - Gives a big picture, all-company view

Threat and Risk Analysis

- Identify threats, vulnerabilities, risks, for each key process
 - Rank according to probability, impact, cost
 - Identify mitigating controls

	A	B	C	D	E
	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Develop Statements of Impact

- For each process, describe the impact on the rest of the organization if the process is incapacitated
- Examples
 - Inability to process payments
 - Inability to produce invoices
 - Inability to access customer data for support purposes

Record Other Key Metrics

- Examples
 - Cost to operate the process
 - Cost of process downtime
 - Profit derived from the process
- Useful for upcoming **Criticality Analysis**

Determine Maximum Tolerable Downtime (MTD)



FOR EACH ORGANIZATION PROCESS

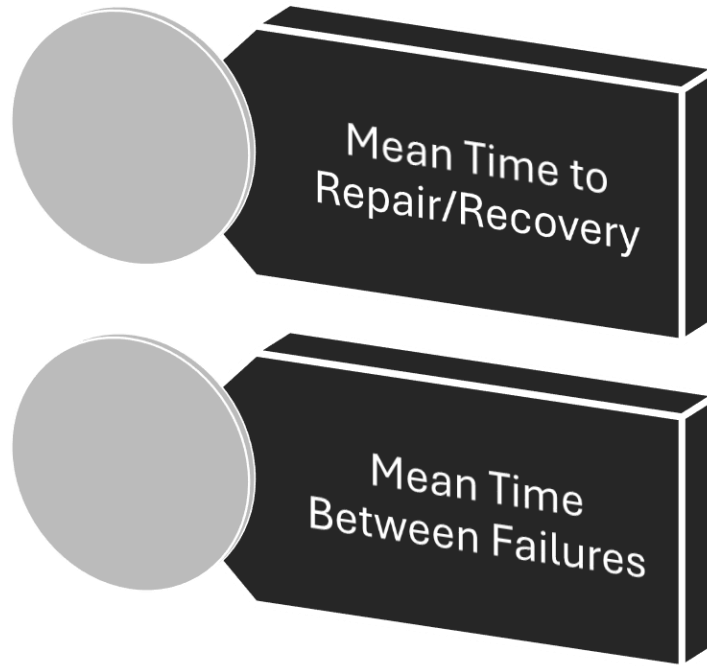


IDENTIFY THE MAXIMUM TIME THAT
EACH ORGANIZATIONAL PROCESS CAN
BE INOPERATIVE BEFORE SIGNIFICANT
DAMAGE OR LONG-TERM VIABILITY IS
THREATENED



PROBABLY AN EDUCATED GUESS FOR
MANY PROCESSES

MTTR & MTBF



Ascertain Current Continuity and Recovery Capabilities

- For each organizational process
 - Identify documented continuity capabilities
 - Identify documented recovery capabilities
 - Identify undocumented capabilities
 - *What if* the disaster happened tomorrow

Develop Key Recovery Targets



RECOVERY TIME
OBJECTIVE



RECOVERY POINT
OBJECTIVE

Criticality Analysis

- Rank processes by criticality criteria
 - MTD (maximum tolerable downtime)
 - MTTR(Mean Time to Repair/Mean Time to Recover)
 - MTBF (Mean Time Between/Before Failures)
 - RTO (recovery time objective)
 - RPO (recovery point objective)
 - Cost of downtime or other metrics
 - Qualitative criteria
 - Reputation, morale, etc.

Quantitative v Qualitative

Quantitative RA – Assigns objective dollar costs to assets

Qualitative RA – Intangible values of data loss and other issues that are not pure hard costs

Risk Assessment

- **Assets** : valuable resources you are trying to protect.
- **Risks**: the potential that **a** chosen action or activity will lead to a loss.
- **Threats**: a negative action that may harm a system.
- **Vulnerabilities**: a weakness that allows a threat to cause harm.
- **Impact**: the severity of the damage, sometimes expressed in dollars.
- **TCO** – Total Cost of Ownership
- **ROI** - Return on Investment

Logistics and Supplies



-
- Food and drinking water
 - Blankets and sleeping cots
 - Sanitation (toilets, showers, etc.)
 - Tools
 - Spare parts
 - Waste bins
 - Information
 - Communications
 - Fire protection (extinguishers, sprinklers, smoke alarms, fire alarms)

Business Resumption Planning

- Alternate work locations
- Alternate personnel
- Communications
 - Emergency, support of organizational processes
- Standby assets and equipment
- Access to procedures, organizational records

Restoration and Recovery

Repairs to facilities, equipment

Replacement equipment

Restoration of utilities

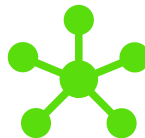
Resumption of organizational operations in primary business facilities

Improving System Resilience and Recovery



Off-site media storage

Assurance of data recovery



Server clusters

Improved availability
Geographic clusters:
members far apart



Data replication

Application, DMBS, OS, or
Hardware
Maintains current data on
multiple servers even in
remote places

Training Staff

Everyday operations

Recovery procedures

Emergency procedures

Resumption procedures

BCP/DRP Testing

Document Review/Checklist

Walkthrough/Tabletop

Simulation

Parallel

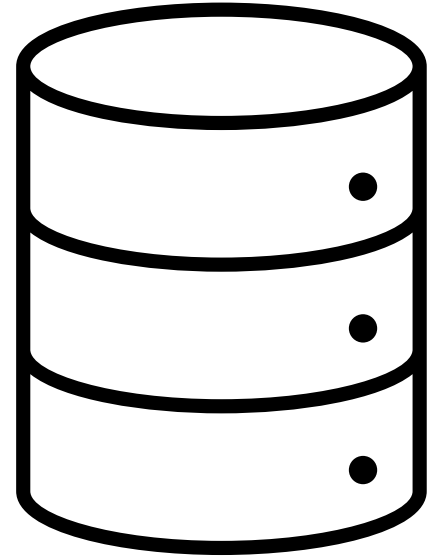
Cut-off/Full Interruption

Hot Sites, Warm Sites, Cold Sites

- Hot site- Fully configured sited ready to work at
- Cold Site -alternate location earmarked
- Warm site - site that can be converted
- Reciprocal Agreement also called “Mutual Aid” is when two companies agree to help each other out in the case of an emergency.
- Hot spare - fully configured hardware
- Cold spare - duplicate hardware that can be configured

HSM

- Hierarchical Storage Management (HSM).
HSM provides continuous on-line backup by using optical or tape 'jukeboxes,' similar to WORMs . It appears as an infinite disk to the system, and can be configured to provide the closest version of an available real-time backup



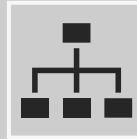
Business Continuity Terms



Contingency Plan – a document providing the procedures for recovering a major application or information system network in the event of an outage or disaster.



Crisis Communications Plan – A document that outlines the procedures for disseminating status reports to personnel and the public in the event of an outage or disaster.



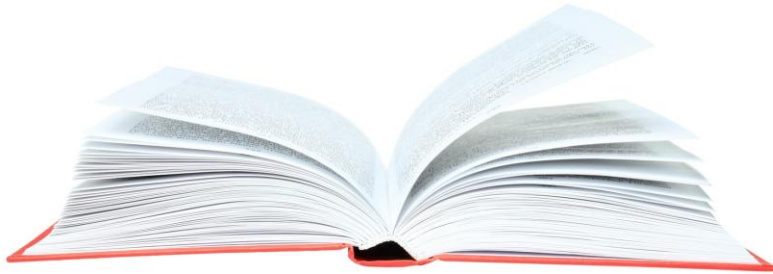
Continuity of Operations Plan – A document describing the procedures and capabilities to sustain an organizations essential strategic functions at an alternate site for up to 30 days

Business Continuity Terms- Continued

Critical System – The hardware and software necessary to ensure the viability of a business unit or organization during an interruption in normal data processing support.

Cyber Incident Response Plan – strategies to detect, respond and limit the consequences of cyber incidents.

General Terms/Acronyms



- Continuity Planning Project Team (CPPT)
- Crisis Management Plan (CMP)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)
- Business Impact Assessment or analysis (BIA)
- MTTD (Maximum Tolerable Downtime)
- MTTR (mean time to recover or mean time to repair)
- MSMT Mean Scheduled Maintenance Time
- MTBCF Mean Time Between Critical Failure
- MTBDE Mean Time Between Downing Event
- MTBF Mean Time Between Failures
- MTBFA Mean Time Between False Alarms
- MTBM Mean Time Between Maintenance
- MTBMA Mean Time Between Maintenance Actions
- MTBPM Mean Time Between Preventative Maintenance
- MTBSA Mean Time Between System Aborts
- MTBR Mean Time Between Removal
- MTBUM Mean Time Between Unscheduled Maintenance