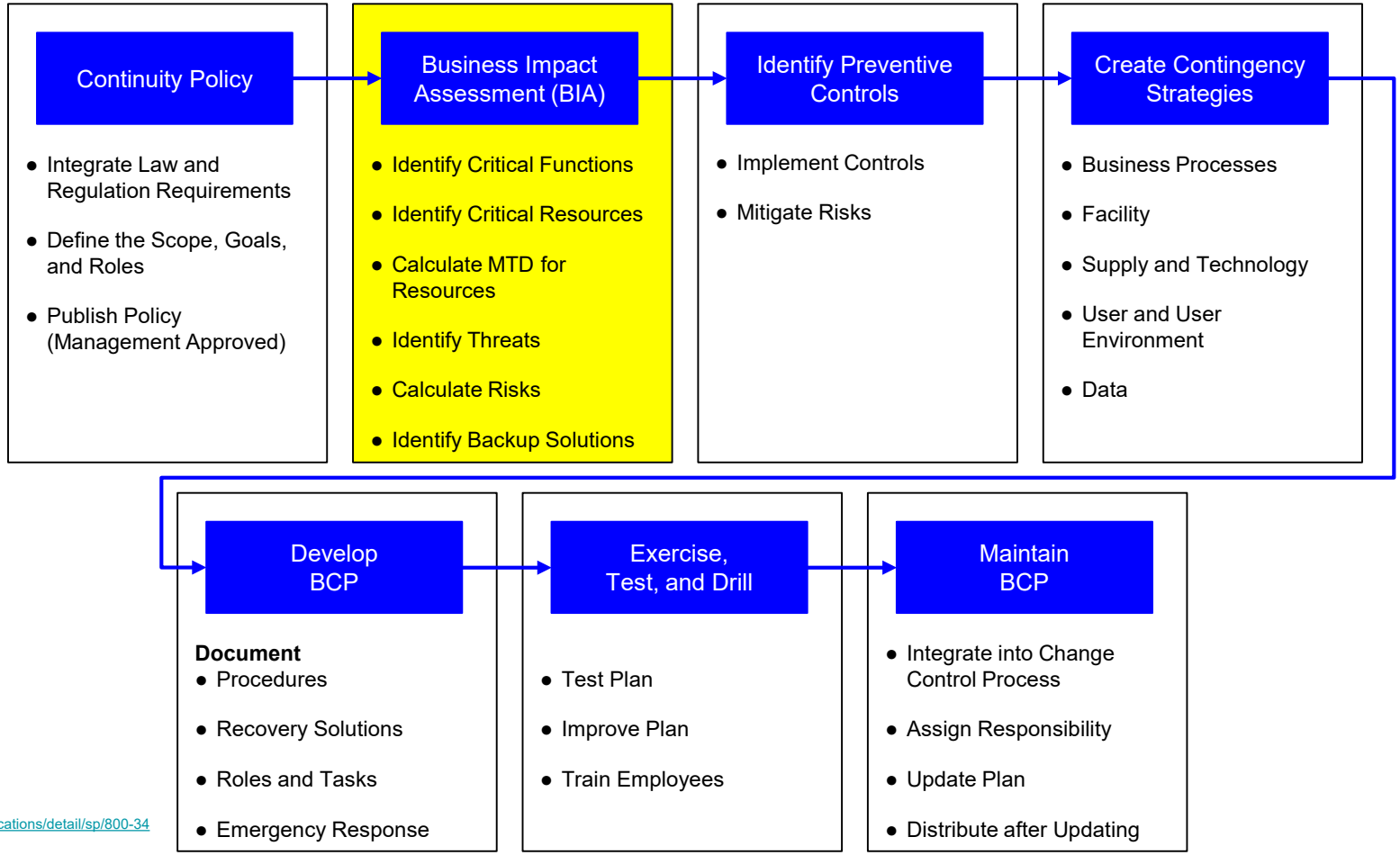
Risk Management

Agenda

- Business Continuity Planning
- Risk Management

Business Continuity Planning (BCP)



https://csrc.nist.gov/publications/detail/sp/800-34

Business Continuity Planning (BCP)

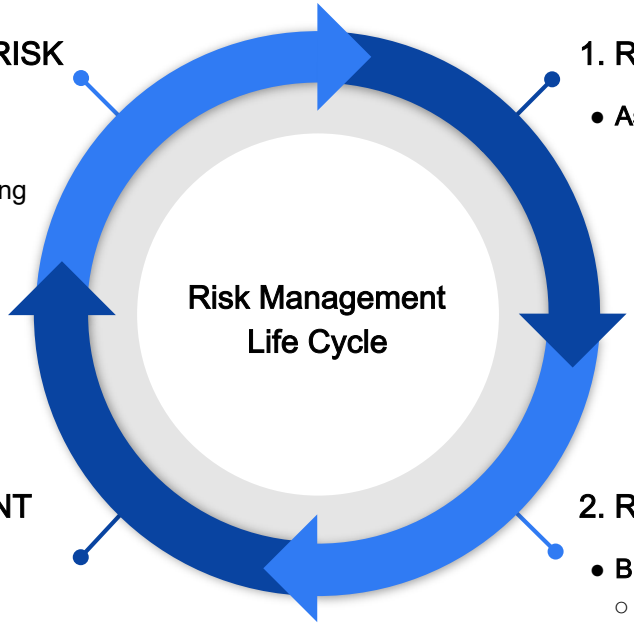
- Establish a BCP Committee
  - Business Unit Managers
  - Senior Management
  - IT Department
  - Legal/Communications
- Establish Risk Management Process
- Conduct the Business Impact Assessment (BIA) (i.e. Risk Assessment)
  - Identify Threats and Map them to:
    - Maximum Tolerable Downtime (MTD) and Disruption for Activities
    - Operational Disruption and Productivity
    - Financial Considerations
    - Regulatory Responsibilities
    - Reputation

Risk Management - Principles

Duty of Care Risk Analysis Standard

1. Risk analysis must consider the interests of all parties that may be harmed by the risk.
2. Risks must be reduced to a level that authorities and potentially affected parties would find appropriate.
3. Safeguards must not be more burdensome than the risks they protect against.

Risk Management



1. RISK IDENTIFICATION

- **Asset Identification**

2. RISK ANALYSIS & EVALUATION

- **Business Impact Analysis (BIA)**
  - Assess Threats
  - Analyze Vulnerabilities
  - Calculate Risk = Impact * Likelihood

3. RISK TREATMENT

- **Accept**
- **Mitigate (or Reduce)**
- **Transfer (or Share)**
- **Avoid**

- ***Identify Safeguard***
  - *Calculate Risk = Impact * Likelihood*

4. MANAGE RESIDUAL RISK

- **Risk Baseline**
  - Internal Audit
  - Pen Test & Threat Modeling
- **Reassess Risk**
  - Acquisitions
  - New Systems
  - Business Changes
  - New Laws or Regulations

1. Risk Identification

Asset Identification

Any item that has a value to the organization

- Information or Data
- Network Equipment
- Servers/Computers
- Software
- Personnel
- Processes

Asset Identification

EXAMPLES

- Buildings and Property
- Equipment (machinery, office eq, etc..)
- IT Equipment
- Supplies and Materials
- Records (any physical data)
- Information (any electronic data)
- Intellectual Property (Trade Secrets, etc.)
- Personnel
- Reputation (Customer Opinion)
- Brand Equity (Market Value)

2. Risk Analysis & Evaluation

Threats

Any condition that can cause harm, loss, damage, or compromise of an asset

- Natural Disasters
- Cyber Attacks
- Breach of integrity of data
- Disclosure of confidential data
- Malware

Types

- Adversarial Threats
- Accidental Threats
- Structural Threats
- Environmental Threats

Threats

Adversarial Threats

Consider their capability, intent, and likelihood

- Trusted insiders
- Competitors
- Suppliers
- Customers
- Business partners
- Nation states

Accidental Threats

Occur when someone makes a mistake that hurts the security of the system

- System administrator accidently takes servers offline causing loss of availability

2. Risk Analysis & Evaluation

Threats

Structural Threats

Occur when equipment, software, or environmental controls fail

- IT server fails due to hard drive failure
- Servers fail due to overheating (HVAC fail)
- Software failure (OS bug or crash)

Environmental Threats

Occur when natural or man-made disasters happen

- Fires
- Flooding
- Severe storms
- Loss of power from the city power grid
- Fiber or telecommunication lines cut

Threats

- Threats come from both external and internal sources
- Not only hackers, but trusted insiders too
- Security controls must consider disgruntled employees, inept administrators, and insider threats!

2. Risk Analysis & Evaluation

Vulnerabilities

Any weakness in the system design, implementation, software code, or lack of preventative mechanisms

- Software bugs
- Misconfigured software
- Misconfigured network devices
- Improper physical security

Cybersecurity professionals control vulnerabilities

Vulnerabilities are internal factors

Vulnerabilities (in Countermeasures)

EXAMPLES

- Unpatched Computer Systems
- Weak/Reused/Shared Passwords
- Inadequate Audit Logging
- Insufficient Video Surveillance

2. Business Impact Analysis (BIA)

Likelihood and Impact

Measurement of the risk that the combined threat and vulnerability pose is based on the likelihood and impact

- **Likelihood** is the chance that the risk will be realized
- **Impact** is the severity of damage that occurs if the risk is realized

Likelihood Factors

What is the likelihood that the threat will initiate the risk?

- Example: How likely is it that the hacker attacks us?

Likelihood Factors

What is the likelihood that if the risk occurs it will have a bad impact for us?

- Example: If the organization has proper security controls, the threat may be mitigated with no adverse effects to the organization.

Likelihood is qualitative

- 1 (not foreseeable) thru
  5 (current/happening now)

  OR more simply:

- Low, Medium, High

2. Business Impact Analysis (BIA)

Impact

- Always assume the threat takes place and the risk is realized when measuring
- Identify the severity of the impact
- Consider each of the pieces of CIA triad: Confidentiality, Integrity, and Availability

Impact is qualitative

- 1 (negligible) thru 5 (catastrophic)

OR more simply:

- Low, Medium, High

2. Business Impact Analysis (BIA)

Risk Assessment Criteria

Impact Score	
1. Negligible	No Consequences
2. Acceptable	Acceptable Consequences
3. Unacceptable	Unacceptable **but** recoverable with little effort
4. High	Unacceptable **but** recoverable with **significant** effort
5. Catastrophic	**Unrecoverable**

Likelihood Score	
1	**Not foreseeable.** This is not plausible in the environment.
2	**Foreseeable.** This is plausible, but not expected.
3	**Expected.** We are certain this will eventually occur.
4	**Common.** This happens repeatedly.
5	**Current.** This may be happening now.

2. Business Impact Analysis (BIA)

Risk Analysis

Asset	Threat	Impact Threshold	X	Likelihood Threshold	=	Risk Score
Email Server	Phishing Campaign	4	X	3	=	12
… therefore …						
				Acceptable Risk	<	9

3. Risk Treatment

- **Accept**: Accept risk “As Is”
- **Mitigate** (or Reduce): Implement safeguard (countermeasure) to reduce level of risk
- **Transfer** (or Share): Share risk with another entity (i.e. insurance company)
- **Avoid**: Discontinue activity associated with the risk

- Countermeasure Decisions
  - Cost/Benefit Analysis (**Countermeasure shouldn’t cost more than the asset it’s protecting**)
  - Accountability (Who’s responsible for the safeguard)
  - Security Controls are acceptable to the business
  - Defense in Depth
  - Minimize Human Intervention (AUTOMATION)

3. Risk Treatment

- Control Types
  - Physical (Locks, Fences, etc…)
  - Technology/Logical Controls (Hardware & Software)
  - Administrative/Management (Policies & Procedures)
- Control Categories
  - Directive (Management)
  - Compensating (Alternatives)
  - Deterrent (Consequences)
  - Preventive (Stop unwanted activity or behaviour)
  - Detective (Identify and Monitor)
  - Corrective (Mitigate)
  - Recovery (Restoration)

3. Risk Treatment

Examples

	TYPES		
CATEGORIES	**Administrative**	**Technical**	**Physical**
Directive	Written Policies	Encryption	Phishing Training
Compensating	Mandatory Vacation	2FA	Dual Control
Deterrent	Disciplinary Policy	Notification on Login	Cameras
Detective	Personnel Audit	Logging/SIEM	Alarm Systems
Preventive	Due Diligence Hiring	Screen Lock / URL Filtering	Locks/Fences
Corrective	Access Review	VLAN / Net. Seg.	Fire Suppression
Recovery	DR Plan	Failover to Alt Site	Off Site Media

3. Risk Treatment

Model Safeguard (Countermeasure) Analysis: Reduce (or Mitigate)

Asset	Threat	Impact Threshold	X	Likelihood Threshold	=	Risk Score
Email Server	Phishing Campaign	**Safeguard Risks**				
Reduce	Email Filtering, Web URL Filtering, Security Awareness Training	4	X	2	=	8
… therefore …						
				Acceptable Risk	<	9

4. Manage Residual Risk

Risk Baseline (Evaluation & Assurance)

Level of Confidence that security requirements are Achieved:

- Auditing
- Pen Testing & Threat Modeling

Reassess Risk (Periodic Review of Risk Management Program)

- Acquisitions
- New Systems
- Business Changes
- New Laws or Regulations

Questions & Answers