J. A. “Drew” Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Risk Analysis

Reference:

Drew Hamilton Lecture Notes

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Domain Outline

- Policies, Plans, and Procedures
- Risk Management and Business Impact Analysis
- Incident Response, Disaster Recovery, Continuity of Operations
- Digital Forensics
- Data Security and Privacy Practices

Standard Operating Procedures

- A standard operating procedure, or SOP, is a set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations.
- SOPs aim to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with industry regulations.

Types of Agreements

- BPA – Business Partnership Agreement
  - work on a project (e.g. industrial or research project) which would be too heavy or too risky for a single entity
  - join forces to have a stronger position on the market
  - comply with specific regulation (e.g. in some emerging countries, foreigners can only invest in the form of partnerships with local entrepreneurs.
- SLA – Service Level Agreement
  - is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.
- ISA – Interconnection Service Agreement
  - See NIST Special Publication 800-47\
  - ISAs are typically part of a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU).

MOA/MOU

- A memorandum of agreement (MOA) is a written document describing a cooperative relationship between two parties wishing to work together on a project or to meet an agreed upon objective.
  - An MOA serves as a legal document and describes the terms and details of the partnership agreement.
- A memorandum of understanding (MOU) is a type of agreement between two (bilateral) or more (multilateral) parties.
  - It expresses a convergence of will between the parties, indicating an intended common line of action.
  - It is a more formal alternative to a gentlemen's agreement.

Information Classification

- Control for the protection of information
- Important facet of policy
- Least
  - “for internal use only”
- Clean desk policy
  - Information is classified based on the amount of damage it could cause if disclosed to the wrong parties.

Administrative Management Responsibilities

- Job rotation means that, over time, more than one person fulfills the tasks of one position within the company
- Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more
- Mandatory vacations are used to force individuals to leave the office for some period of time in order to allow for the identification of fraudulent activity and to facilitate job rotation

Administrative Management Responsibilities

- The objective of separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way
- Separation of duties also helps prevent mistakes and minimize conflicts of interest that may take place if one person is performing a task from beginning to end.

Background Investigation

- Background checks by employers have proved to be a valuable investment for government agencies and corporations due to the repercussions costs, such as law suits or liability insurance.
- Corporations are reassuring themselves the hired individual is worthy of the effort and cost by conducting background check as part of the initial application process.

Layers of Responsibility

- Who's Involved?
- List of Roles
- Why So Many Roles?
- Personnel
- Structure
- Hiring Practices
- Employee Controls
- Termination

Layers of Responsibility

Players involved

- Board of directors - ensure the shareholders' interests are being protected and the organization is being run properly
- Chief Executive Officer (CEO) - day-to-day management responsibilities, highest ranking officer
- Chief Financial Officer (CFO) - responsible for financial activities
- Chief Information Officer (CIO) - bridges the gap between IT and upper management, usually pretty technical
- Chief Privacy Officer (CPO) - usually an attorney responsible for ensuring data is kept safe
- Chief Security Officer (CSO) - creates and maintains a security program that facilitates business drivers and provides security and compliance

Layers of Responsibility

Players involved (cont'd)

- Security steering committee - makes decisions on tactical and strategic security issues, not tied to any business unit
- Audit committee - provide independent and open communications among the board, management, internal, and external auditors
- Data owner - due care responsibilities for protecting data
- Data custodian - maintains and protects the data
- System owner - integrates security considerations into application and system purchasing decisions and development projects
- Security administrator - executes security-related tasks
- Security analyst - develops policies, standards, guidelines, and baselines

Layers of Responsibility

Players involved (cont'd)

- Application owner - dictates who can and cannot access their applications
- Supervisor - responsible for all user activity
- Change control analyst - approves or rejects requests to make changes to the network, systems, or software
- Data analyst - ensures that data is stored in a reasonable manner and those who require access have access
- Process owner - responsible for properly defining, improving, and monitoring processes
- Solution provider - works with management and data owners to deploy solutions that reduce pain points

Layers of Responsibility

Players involved (cont'd)

- The User - routinely uses the data, must have necessary level of access to perform their duties
- Product Line Manager - evaluates products in the market, works with vendors
- Auditor - brought in to determine if the controls have reached and comply with the security objectives identified by the organization or legislation

Most environments won't contain all these roles, but the responsibilities still must be carried out.

Layers of Responsibility

Personnel

Definition:
Separation of duties - makes sure one individual cannot complete a critical task by themselves

In an organization with good separation of duties, collusion must occur in order for fraud to be committed.

Hiring Practices

- **NDAs should be used to protect company information.**
- **References should be checked, military records reviewed, education verified, and if necessary, a drug test should be given.**

You want to mitigate risk, lower hiring costs, and lower turnover rates.

Layers of Responsibility

Employee Controls

Rotation of duties - no person should stay in one position too long (they may gain too much control)

Mandatory vacation - allows time for other individuals to come in and detect any errors or fraudulent activities

Separation of duties - split knowledge, dual control

Layers of Responsibility

Termination

When terminating an employee, follow the following rules:

- The employee must leave immediately under supervision of a manager or security guard.
- The employee must surrender any ID badges or keys, complete an exit interview, and return company supplies.
- That user's accounts and passwords should be disabled or change immediately.

Section Conclusion

- Understand the importance of policies, plans, and procedures related to organizational security
- Distinguish between the standard types of agreements
- Be introduced to personnel management policies and procedures
- Examine some general security policies

Policies, Plans, and Procedures
Risk Analysis

Reference:

Drew Hamilton Lecture Notes

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Security+

Business Continuity Planning

- a “disaster” is:
  - Trying to make red chili ribs in a crock pot
  - He lost a laptop with the only copy of his thesis
  - She lost her research and papers in the lab fire
  - Payroll system failed the day before payday
  - Asbestos released in a dorm renovation
  - The death of a student
  - The Northeast blackout
  - Hurricane Katrina

Business Continuity Planning

- Disaster
  - is an event, often unexpected, that seriously disrupts your usual operations or processes and can have long term impact on your normal way of life or that of your organization.
- RTO [Recovery Time Objective]
  - the point in time when you must have at least the critical aspects of your business operational again.
- RPO [Recovery Point Objective]
  - The last copy of your data that is out of harm' s way – hopefully it is recently current.

Business Continuity Planning

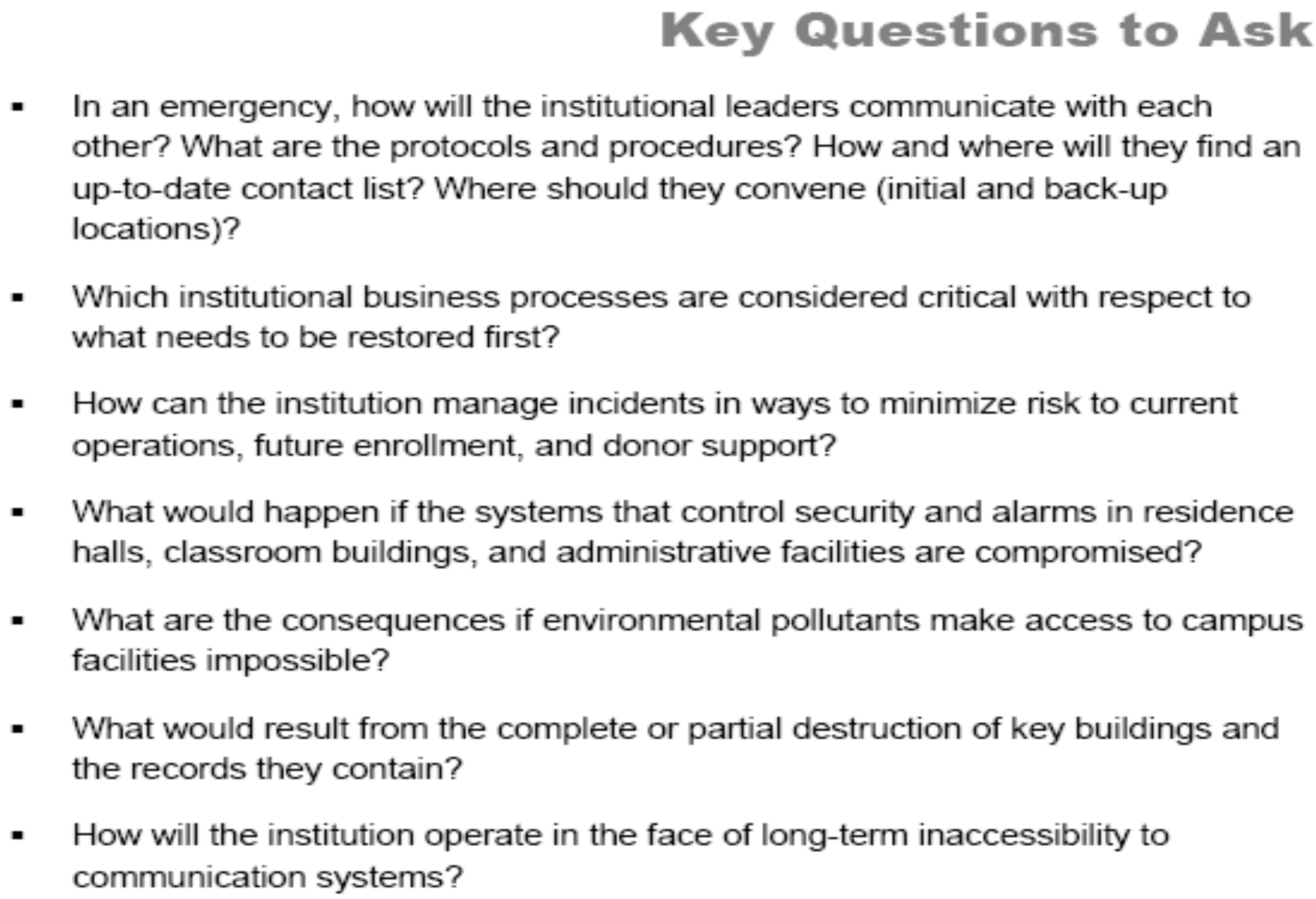
is:

- a process to minimize the impact of a major disruption to normal operations
- a process to enable restoration of critical assets
- a process to restore normalcy as soon as possible after a crisis.

not just:

- recovery of information technology resources
  - and it is the phase of crisis management that follows the immediate actions taken to protect life and property and contain the event
  - it begins when the situation has been stabilized.

Business Continuity Planning

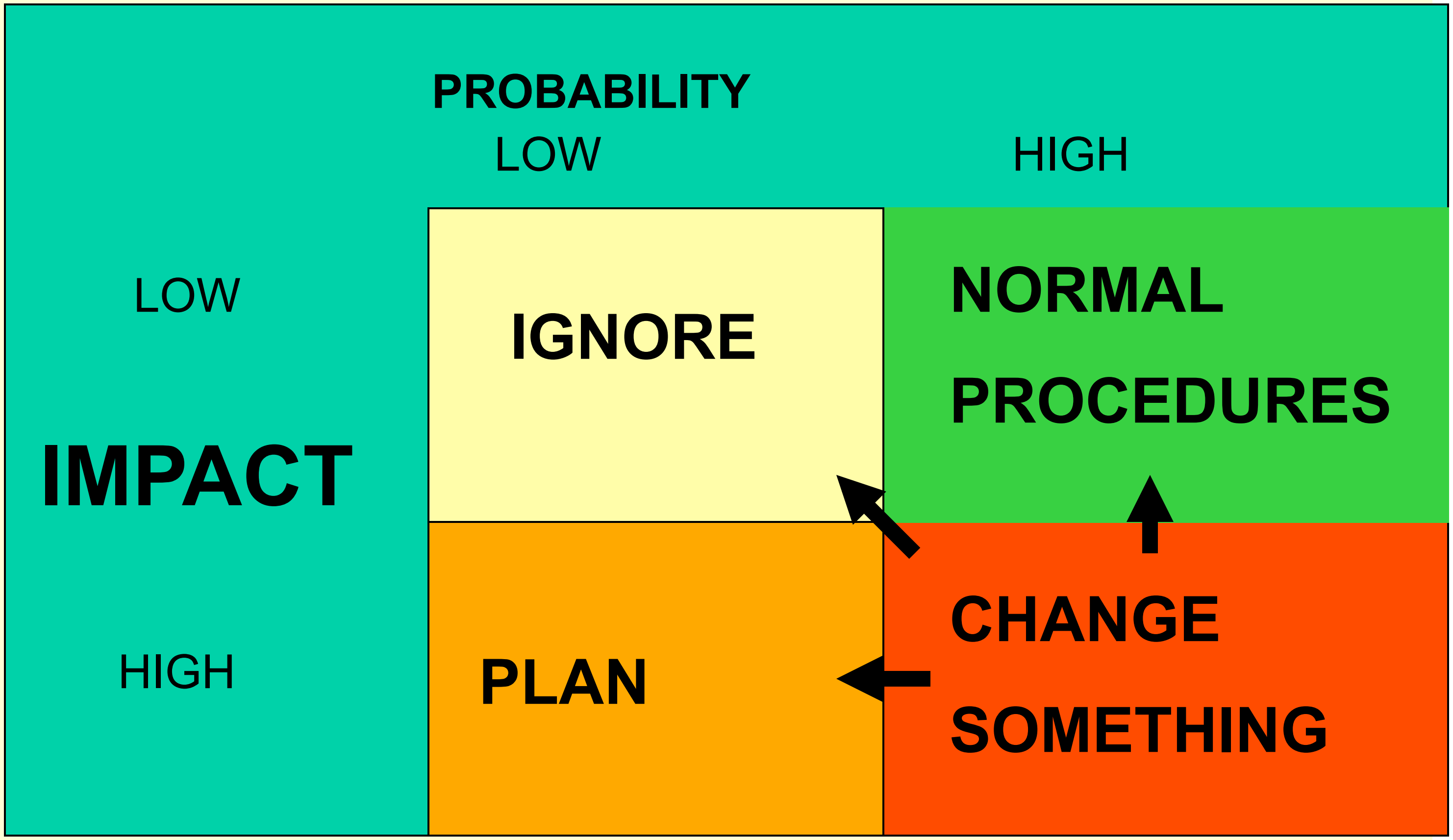


Key Questions to Ask

- In an emergency, how will the institutional leaders communicate with each other? What are the protocols and procedures? How and where will they find an up-to-date contact list? Where should they convene (initial and back-up locations)?
- Which institutional business processes are considered critical with respect to what needs to be restored first?
- How can the institution manage incidents in ways to minimize risk to current operations, future enrollment, and donor support?
- What would happen if the systems that control security and alarms in residence halls, classroom buildings, and administrative facilities are compromised?
- What are the consequences if environmental pollutants make access to campus facilities impossible?
- What would result from the complete or partial destruction of key buildings and the records they contain?
- How will the institution operate in the face of long-term inaccessibility to communication systems?

Business Continuity Planning

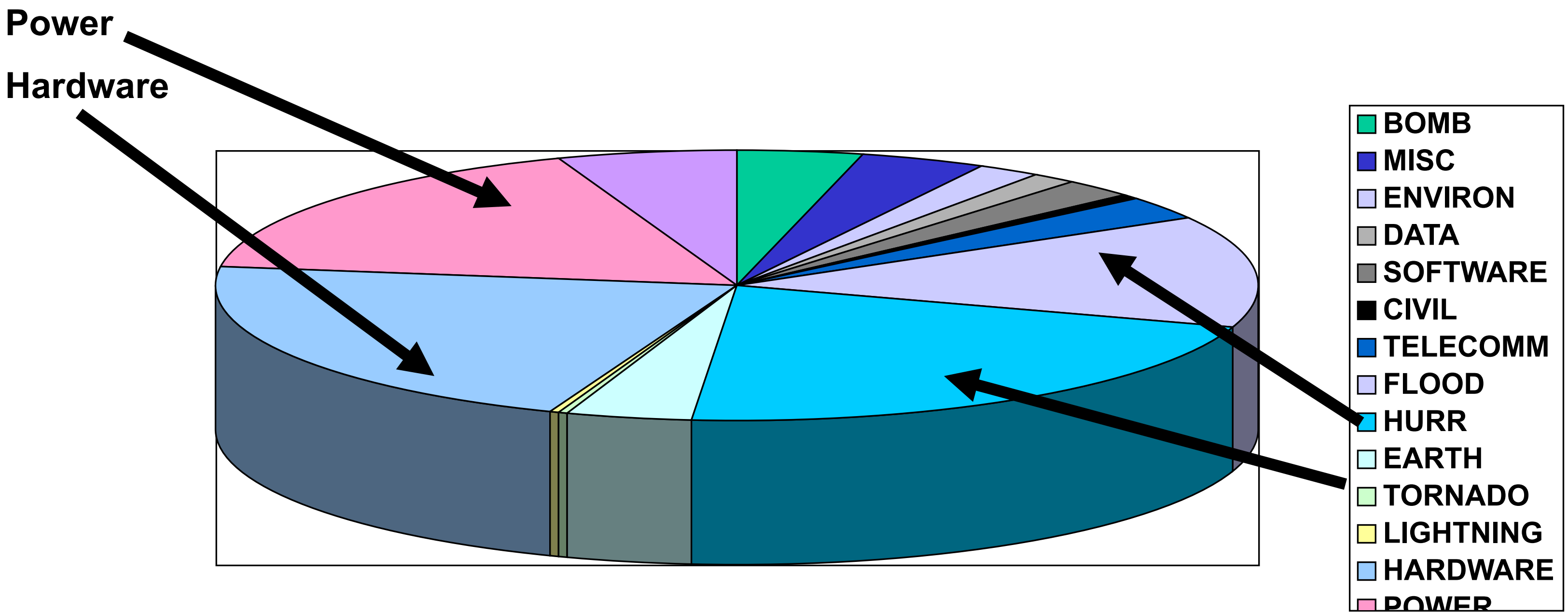
The Risk Matrix



	PROBABILITY LOW	HIGH
LOW IMPACT	IGNORE	NORMAL PROCEDURES
HIGH	PLAN	CHANGE SOMETHING

Business Continuity Planning

Network Operations Disruptions



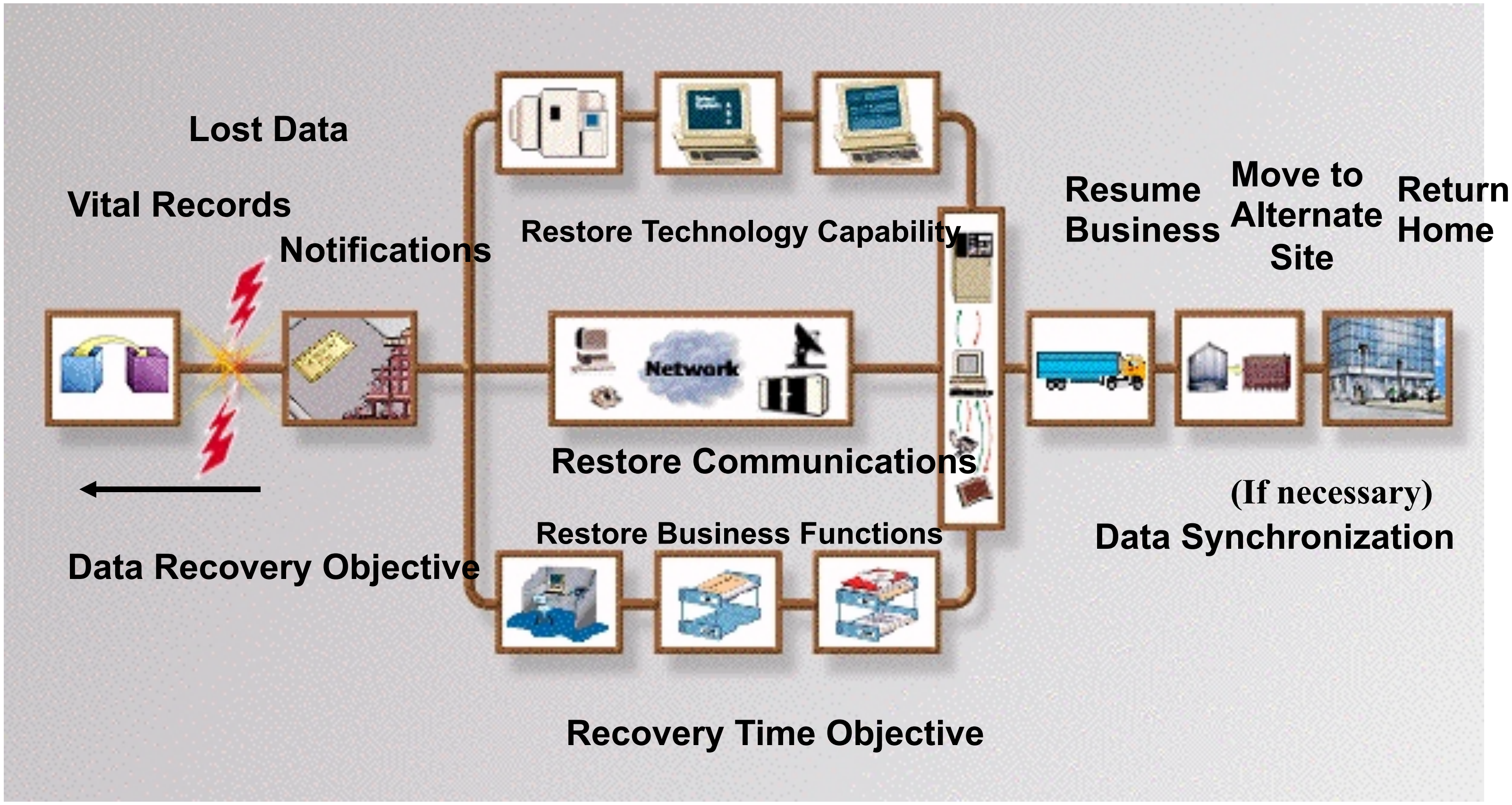
Source: Gartner Group and Comdisco

Business Continuity Planning

Mt. St. Helens – May 1980 – new threats arise

Business Continuity Planning

High Level Look at a Recovery Effort



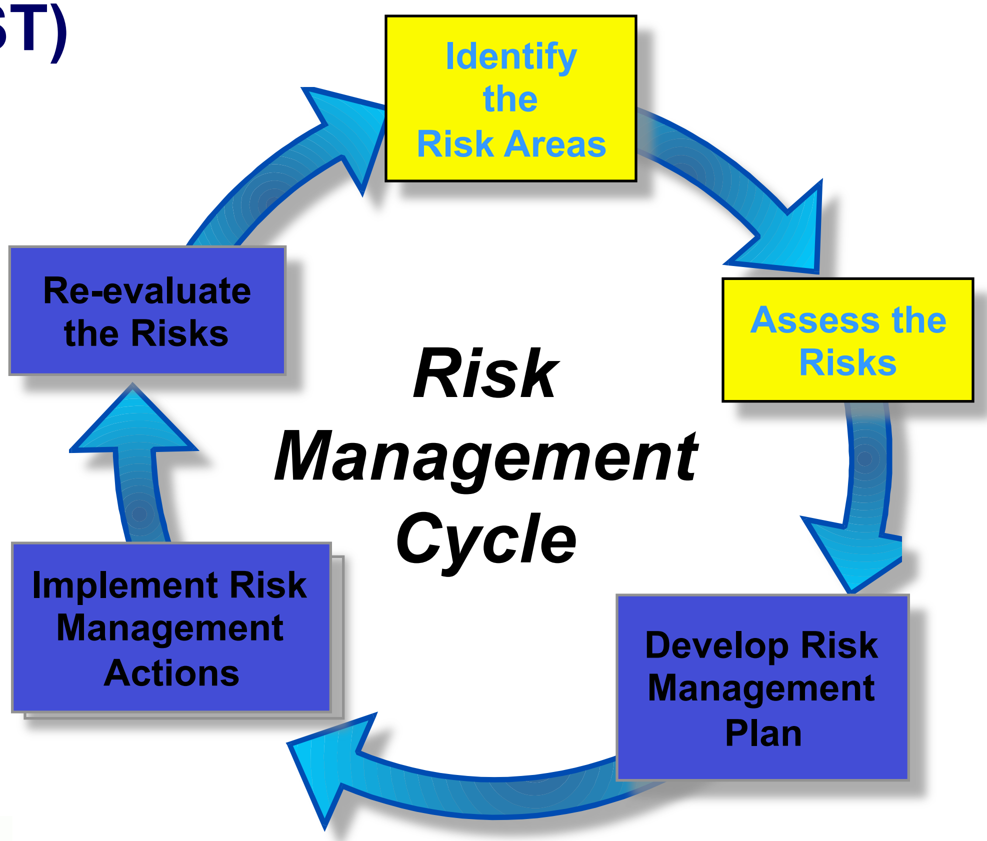
© Lucent technologies

MTBF, MTTR, Availability, Reliability

- **Mean Time Between Failures (MTBF) is the estimated lifespan of a piece of equipment.**
  - MTBF = sum(start of downtime – start of uptime) / number of failures
- **Mean Time to Repair (MTTR) is the amount of time expected to get a device repaired and back into production**
  - MTTR = (total downtime) / (number of breakdowns)
- **Availability is the time a systems performs its intended function.**
  - Availability = MTBF / (MTBF + MTTR)
- **Reliability is a measure of the frequency of system failures.**

Risk Management

- **The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)**



Identify the Risk Areas

Assess the Risks

Develop Risk Management Plan

Implement Risk Management Actions

Re-evaluate the Risks

Risk Management Cycle

🟨 Risk Assessment

🟦 Risk Control (Mitigation)

Risk Identification Process

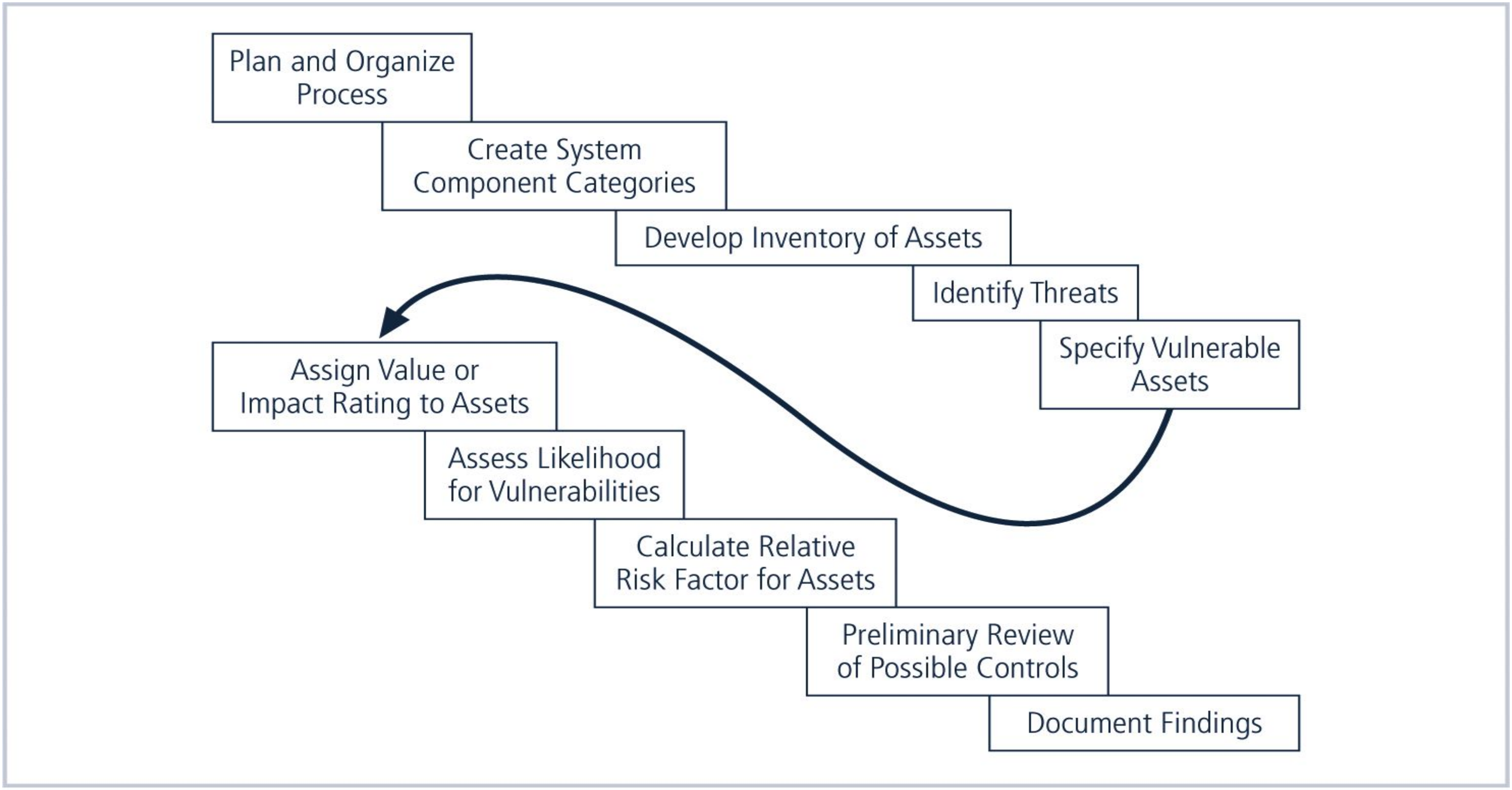

Plan and Organize Process
Create System Component Categories
Develop Inventory of Assets
Identify Threats
Specify Vulnerable Assets
Assign Value or Impact Rating to Assets
Assess Likelihood for Vulnerabilities
Calculate Relative Risk Factor for Assets
Preliminary Review of Possible Controls
Document Findings

FIGURE 7-1 Risk Identification Process

Risk Identification

- Risk identification
  - begins with the process of self-examination
- Managers
  - identify the organization's information assets,
  - classify them into useful groups, and
  - prioritize them by their overall importance

Inventorying Information Assets

- Identify information assets, including
  - people, procedures, data and information, software, hardware, and networking elements
- Should be done without pre-judging value of each asset
  - Values will be assigned later in the process

Organizational Assets

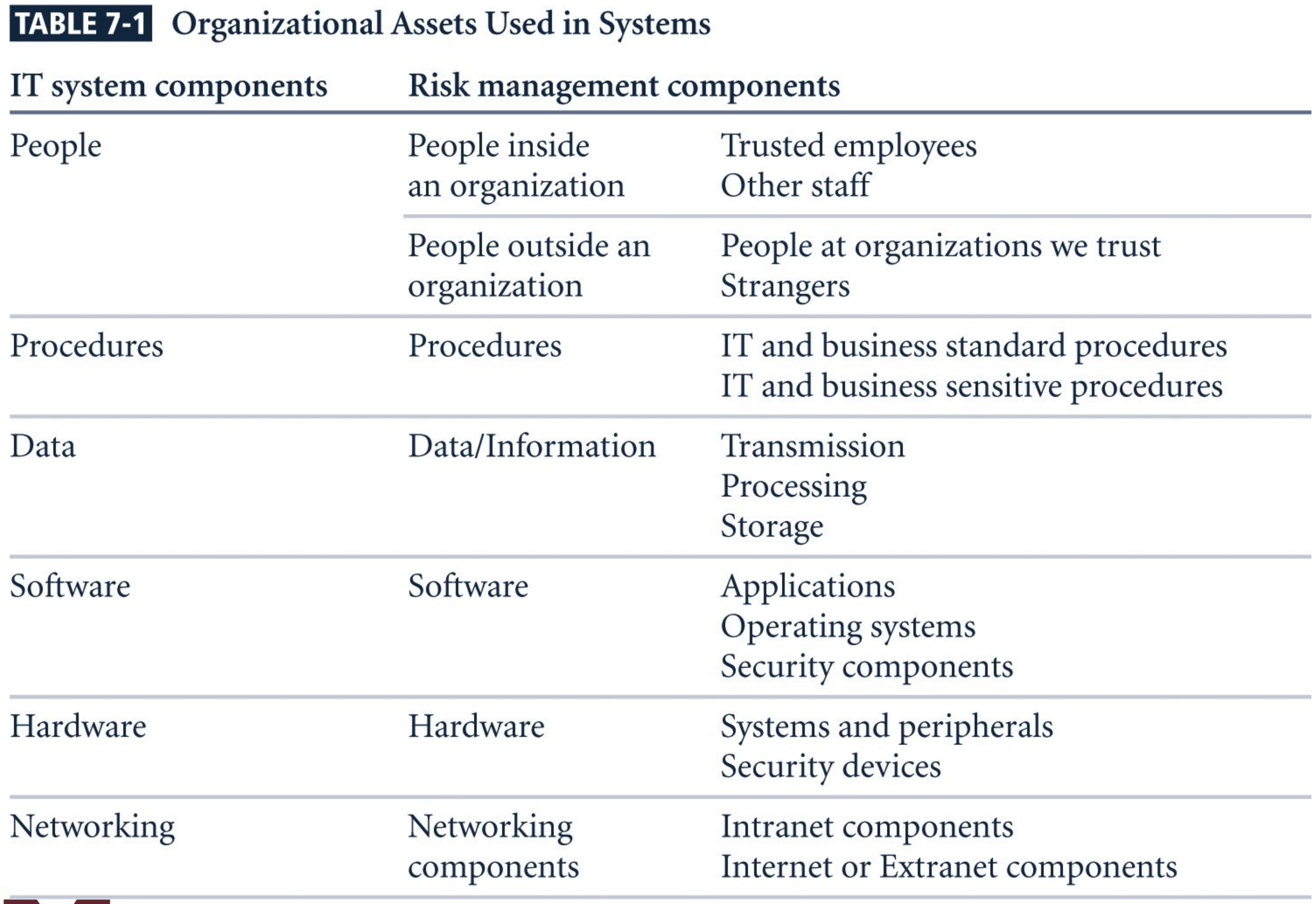


TABLE 7-1 Organizational Assets Used in Systems

IT system components	Risk management components	
People	People inside an organization	Trusted employees Other staff
	People outside an organization	People at organizations we trust Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking components	Intranet components Internet or Extranet components

Attributes for Assets

- **Potential attributes:**
  - Name
  - IP address
  - MAC address
  - Asset type
  - Manufacturer name
  - Manufacturer's model or part number
    - Software version, update revision,
  - Physical location
  - Logical location
  - Controlling entity

Identifying People, Procedures, and Data Assets

- Whose Responsibility ?
  - managers who possess the necessary knowledge, experience, and judgment
- Recording
  - use reliable data-handling process

Suggested Attributes

- People
  - Position name/ number/ID
  - Supervisor name/ number/ID
  - Security clearance level
  - Special skills
- Procedures
  - Description
  - Intended purpose
  - Software/hardware/ networking elements to which it is tied
  - Location where it is stored for reference
  - Location where it is stored for update purposes
- Data
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used
  - Online or offline
  - Location
  - Backup procedures

Classifying and Categorizing Assets

- Determine whether its asset categories are meaningful
  - After initial inventory is assembled,
- Inventory should also reflect sensitivity and security priority assigned to each asset
- A classification scheme categorizes these information assets based on their sensitivity and security needs

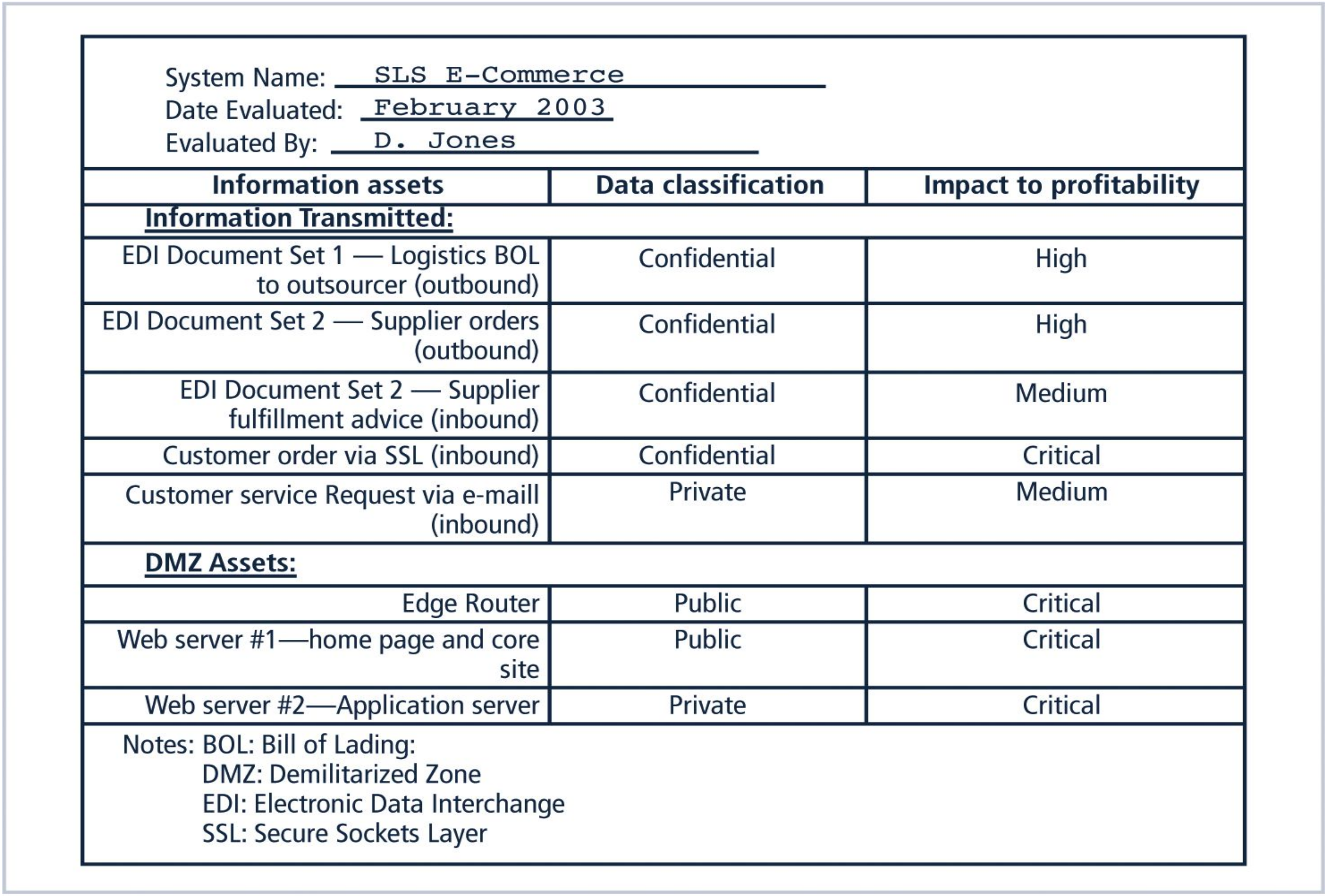
Classifying and Categorizing Assets (Continued)

- Categories
  - designates level of protection needed for a particular information asset
- Classification categories must be comprehensive and mutually exclusive
- Some asset types, such as personnel,
  - may require an alternative classification scheme that would identify the clearance needed to use the asset type

Assessing Values for Information Assets

- Assign a relative value
  - to ensure that the most valuable information assets are given the highest priority, for example:
    - Which is the most critical to the success of the organization?
    - Which generates the most revenue?
    - Which generates the highest profitability?
    - Which is the most expensive to replace?
    - Which is the most expensive to protect?
    - Whose loss or compromise would be the most embarrassing or cause the greatest liability?
- Final step in the RI process is to list the assets in order of importance
  - Can use a weighted factor analysis worksheet

Asset Classification Worksheet



System Name: SLS E-Commerce

Date Evaluated: February 2003

Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-maill (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Weighted Factor Analysis Worksheet (NIST SP 800-30)

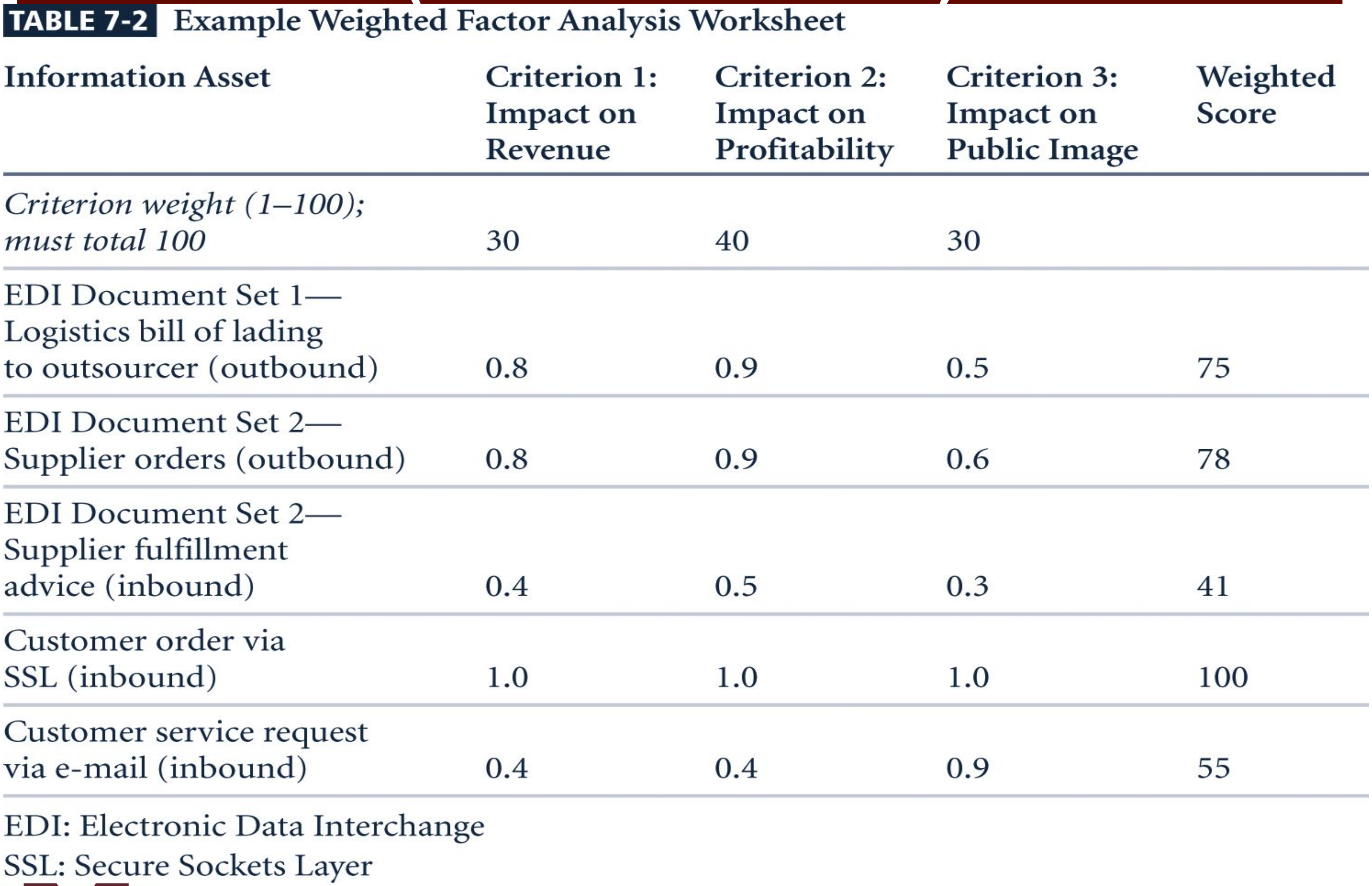


TABLE 7-2 Example Weighted Factor Analysis Worksheet

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

EDI: Electronic Data Interchange

SSL: Secure Sockets Layer

Threat Identification

- Any organization typically faces a wide variety of threats
- If you assume that every threat can and will attack every information asset, then the project scope becomes too complex
- To make the process less unwieldy, manage separately
  - each step in the threat identification and
  - vulnerability identification processes

  then coordinate them at the end

Identify And Prioritize Threats and Threat Agents

- Each threat presents a unique challenge to information security
  - Must be handled with specific controls that directly address particular threat and threat agent's attack strategy
- Threat assessment
  - Before threats can be assessed in risk identification process, each threat must be further examined to determine its potential to affect targeted information asset

Threats to Information Security

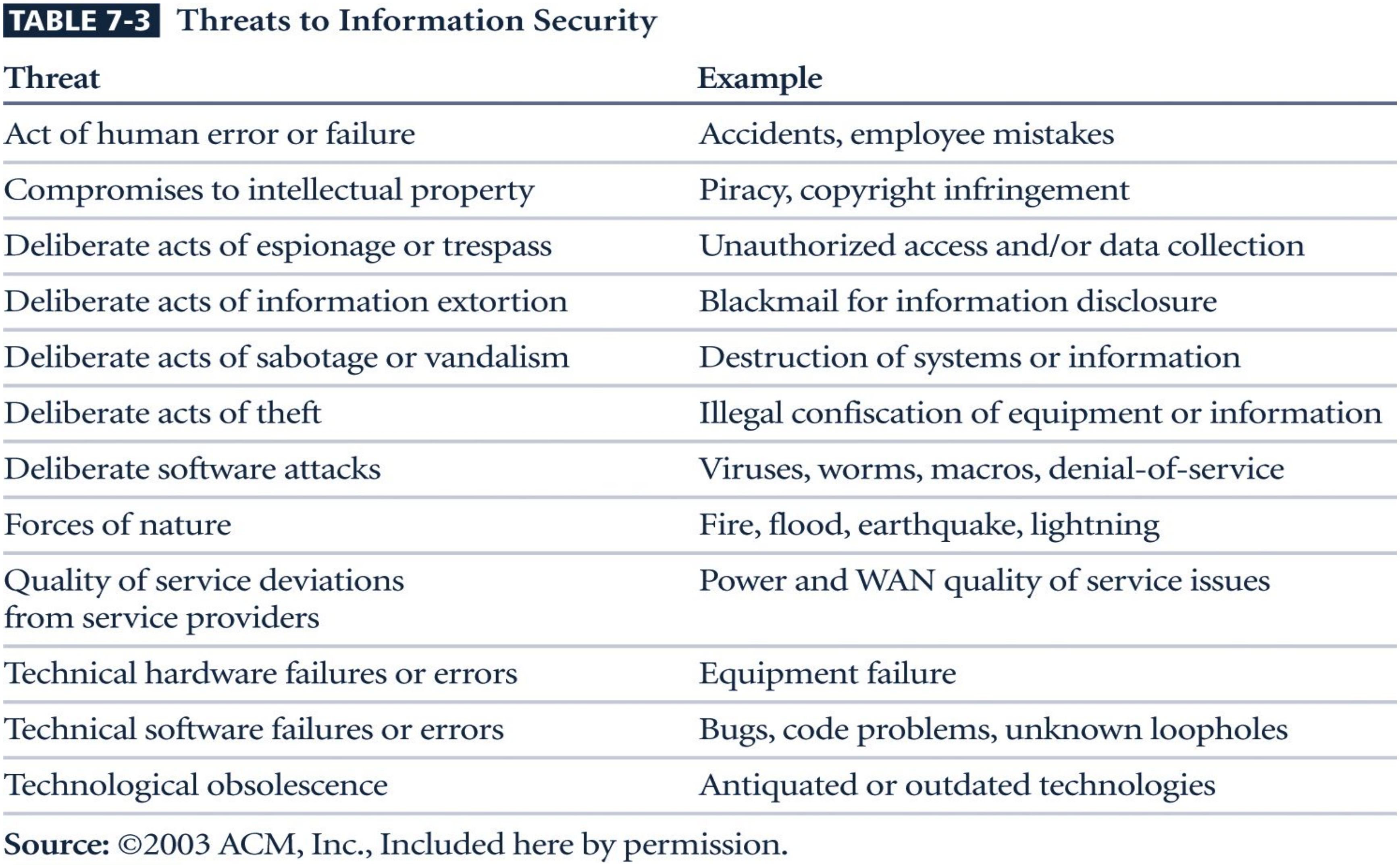
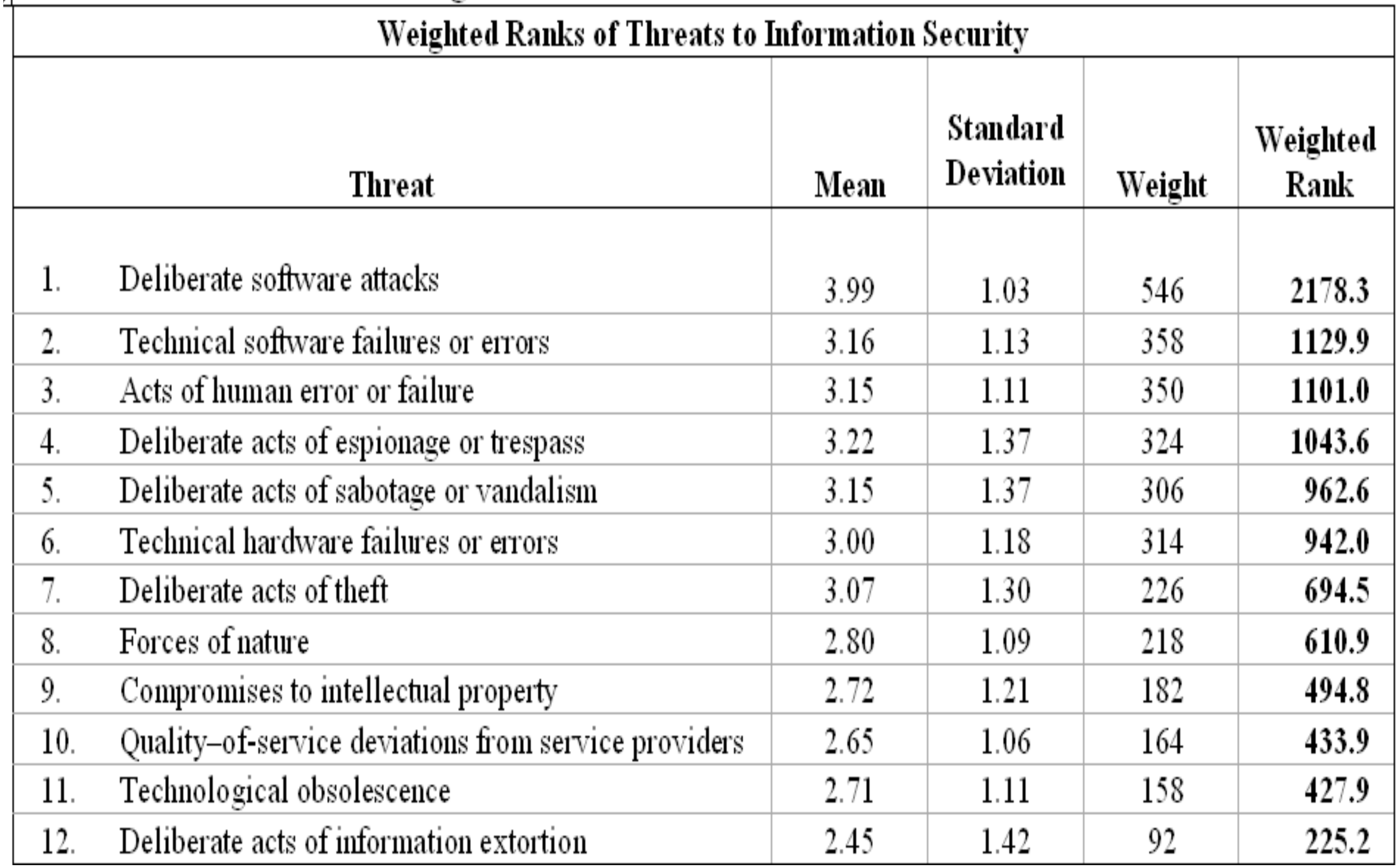


TABLE 7-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Source: ©2003 ACM, Inc., Included here by permission.

Threats to Information Security



Weighted Ranks of Threats to Information Security				
Threat	**Mean**	**Standard Deviation**	**Weight**	**Weighted Rank**
1. Deliberate software attacks	3.99	1.03	546	**2178.3**
2. Technical software failures or errors	3.16	1.13	358	**1129.9**
3. Acts of human error or failure	3.15	1.11	350	**1101.0**
4. Deliberate acts of espionage or trespass	3.22	1.37	324	**1043.6**
5. Deliberate acts of sabotage or vandalism	3.15	1.37	306	**962.6**
6. Technical hardware failures or errors	3.00	1.18	314	**942.0**
7. Deliberate acts of theft	3.07	1.30	226	**694.5**
8. Forces of nature	2.80	1.09	218	**610.9**
9. Compromises to intellectual property	2.72	1.21	182	**494.8**
10. Quality–of-service deviations from service providers	2.65	1.06	164	**433.9**
11. Technological obsolescence	2.71	1.11	158	**427.9**
12. Deliberate acts of information extortion	2.45	1.42	92	**225.2**

Vulnerability Assessment

- **Steps revisited**
  - **Identify the information assets of the organization and**
  - **Document some threat assessment criteria,**
  - **Begin to review every information asset for each threat**
    - **Leads to creation of list of vulnerabilities that remain potential risks to organization**
- **Vulnerabilities**
  - **specific avenues that threat agents can exploit to attack an information asset**
- **At the end of the risk identification process,**
  - **a list of assets and their vulnerabilities has been developed**

Weighted Ranking of Threat-Driven Expenditures

Top Threat-Driven Expenses	Rating
Deliberate software attacks	12.7
Acts of human error or failure	7.6
Technical software failures or errors	7.0
Technical hardware failures or errors	6.0
QoS deviations from service providers	4.9
Deliberate acts of espionage or trespass	4.7
Deliberate acts of theft	4.1
Deliberate acts of sabotage or vandalism	4.0
Technological obsolescence	3.3
Forces of nature	3.0
Compromises to intellectual property	2.2
Deliberate acts of information extortion	1.0

Risk Identification Estimate Factors

Risk is:

The likelihood of the occurrence of a vulnerability

Multiplied by

The value of the information asset

Minus

The percentage of risk mitigated by current controls

Plus

The uncertainty of current knowledge of the vulnerability

Likelihood

- Likelihood
  - /of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event
  - is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited
- Using the information documented during the risk identification process,
  - assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc

Assessing Potential Loss

- To be effective, the likelihood values must be assigned by asking:
  - Which threats present a danger to this organization's assets in the given environment?
  - Which threats represent the most danger to the organization's information?
  - How much would it cost to recover from a successful attack?
  - Which threats would require the greatest expenditure to prevent?
  - Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

Mitigated Risk / Uncertainty

- If it is partially controlled,
  - Estimate what percentage of the vulnerability has been controlled
- Uncertainty
  - is an estimate made by the manager using judgment and experience
  - It is not possible to know everything about every vulnerability
  - The degree to which a current control can reduce risk is also subject to estimation error

Risk Determination Example

- Asset A has a value of 50 and has vulnerability #1,
  - likelihood of 1.0 with no current controls
  - assumptions and data are 90% accurate
- Asset B has a value of 100 and has two vulnerabilities
  - Vulnerability #2
    - likelihood of 0.5 with a current control that addresses 50% of its risk
  - Vulnerability # 3
    - likelihood of 0.1 with no current controls
    - assumptions and data are 80% accurate

Risk Determination Example

- **Resulting ranked list of risk ratings for the three vulnerabilities is as follows:**
  - **Asset A: Vulnerability 1 rated as 55 =**
    - **(50 × 1.0) – 0% + 10%**
  - **Asset B: Vulnerability 2 rated as 35 =**
    - **(100 × 0.5) – 50% + 20%**
  - **Asset B: Vulnerability 3 rated as 12 =**
    - **(100 × 0.1) – 0 % + 20%**

Risk Analysis

Quantitative Risk Analysis

This attempts to assign real and meaningful numbers to all elements of the risk analysis process.

Purely quantitative risk analysis is not possible because the method attempts to quantify qualitative items.

Most automated systems store base data in a database and then can run scenarios with that data with different parameters to give a view of the outcomes for different exposures.

Risk Analysis

Steps of a Quantitative Risk Analysis

1. Assign Value to Assets
2. Estimate Potential Loss per Threat
3. Perform a Threat Analysis
4. Derive the Overall Annual Loss Potential per Threat
5. Reduce, Transfer, Avoid, or Accept the Risk

Definitions:

exposure factor (EF): percentage loss of an asset
single loss expectancy (SLE) = asset value * EF
annualized rate of occurrence (ARO): frequency of exposure
annualized loss expectancy (ALE) = SLE * ARO

Risk Analysis

Results of a Risk Analysis

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures, and actions

Risk Analysis

Qualitative Risk Analysis

Techniques include judgement, best practices, intuition, and experience

1. A risk analysis team is built consisting of members from across many departments with experience and education on the threats being evaluated
2. A scenario is written for each major threat
3. Safeguards that diminish the damage of the threat are evaluated and the scenario is played out for each

Risk Analysis

Qualitative Risk Analysis

Benefits

- communication must happen among team members
- risks and safeguards are ranked
- strengths and weaknesses are identified
- those who know the subjects best provide their opinions to management

Risk Analysis

Countermeasure Selection

Again, you need to do a cost/benefit analysis.

Example:
If the ALE of a threat is $12,000 before applying the safeguard, and $3,000 after applying it, and the annual cost of the safeguard is $650, then the value of the safeguard is $8,350/year.

Remember that the cost of a countermeasure is more that just the purchase price. Also, note that you will likely never reduce the ALE to $0. This is due to residual risk.

Risk Analysis

Total Risk vs. Residual Risk

No system or environment is 100% secure, which means there is always some risk left over to deal with.

Total risk is the risk a company faces if it chooses not to implement a certain safeguard. Residual risk is the risk left over after implementing that safeguard.

threats * vulnerability * asset value = *total risk*
total risk * controls gap = *residual risk*

Risk Analysis

Handling Risk

Risk can be dealt with by:

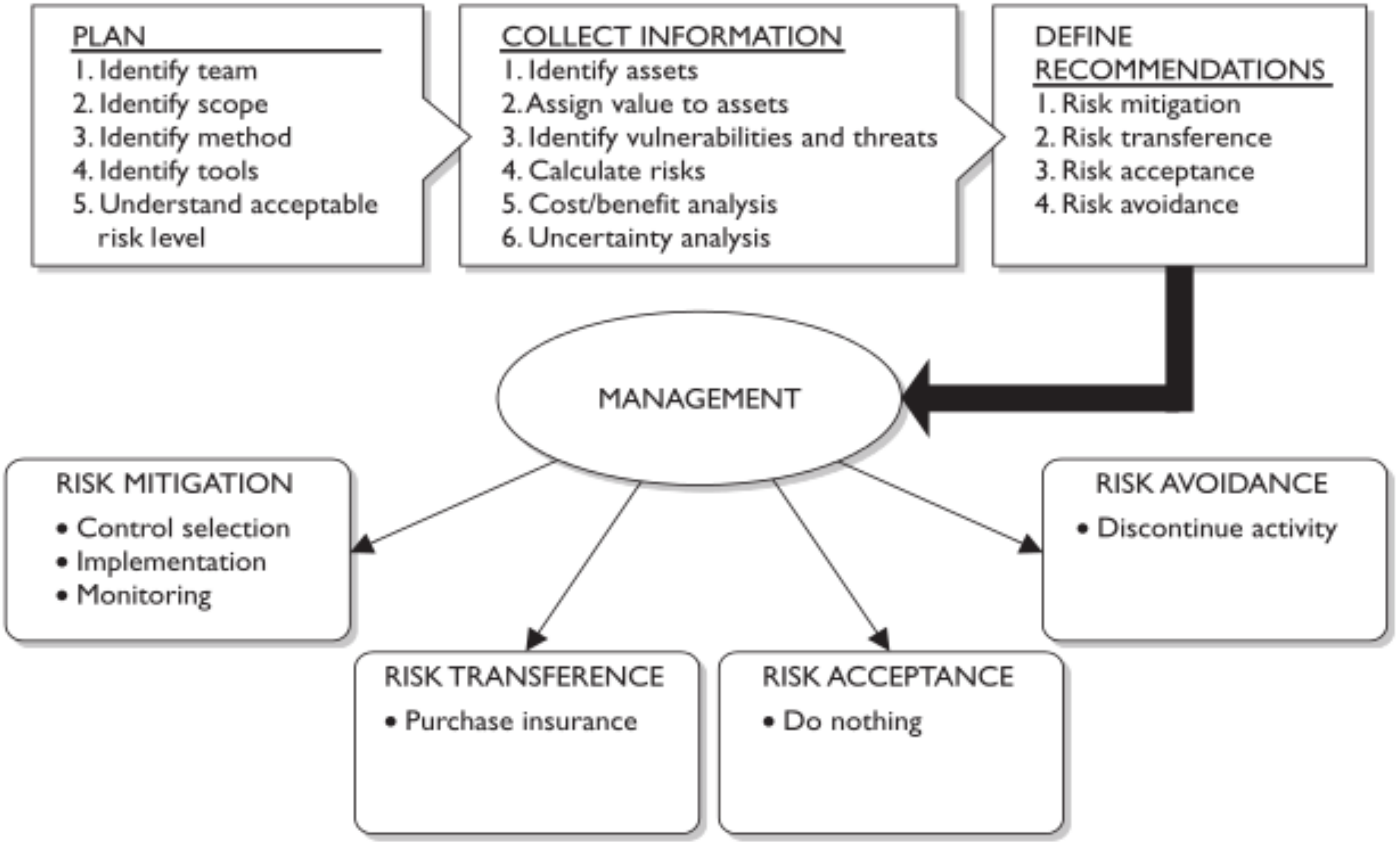
- transferring it - through insurance or delegating
- rejecting it - also called risk avoidance, you do this by terminating the activity that is introducing the risk
- reducing it - also called risk mitigation
- accepting it

Risk acceptance:

- Is the potential loss lower than the countermeasure?
- Can the organization deal with the "pain" that will come with accepting the risk?

This "pain" can be more than just financial

Risk Analysis



PLAN
1. Identify team
2. Identify scope
3. Identify method
4. Identify tools
5. Understand acceptable risk level

COLLECT INFORMATION
1. Identify assets
2. Assign value to assets
3. Identify vulnerabilities and threats
4. Calculate risks
5. Cost/benefit analysis
6. Uncertainty analysis

DEFINE RECOMMENDATIONS
1. Risk mitigation
2. Risk transference
3. Risk acceptance
4. Risk avoidance

MANAGEMENT

RISK MITIGATION
- Control selection
- Implementation
- Monitoring

RISK TRANSFERENCE
- Purchase insurance

RISK ACCEPTANCE
- Do nothing

RISK AVOIDANCE
- Discontinue activity

Figure 3-10 How a risk management program can be set up

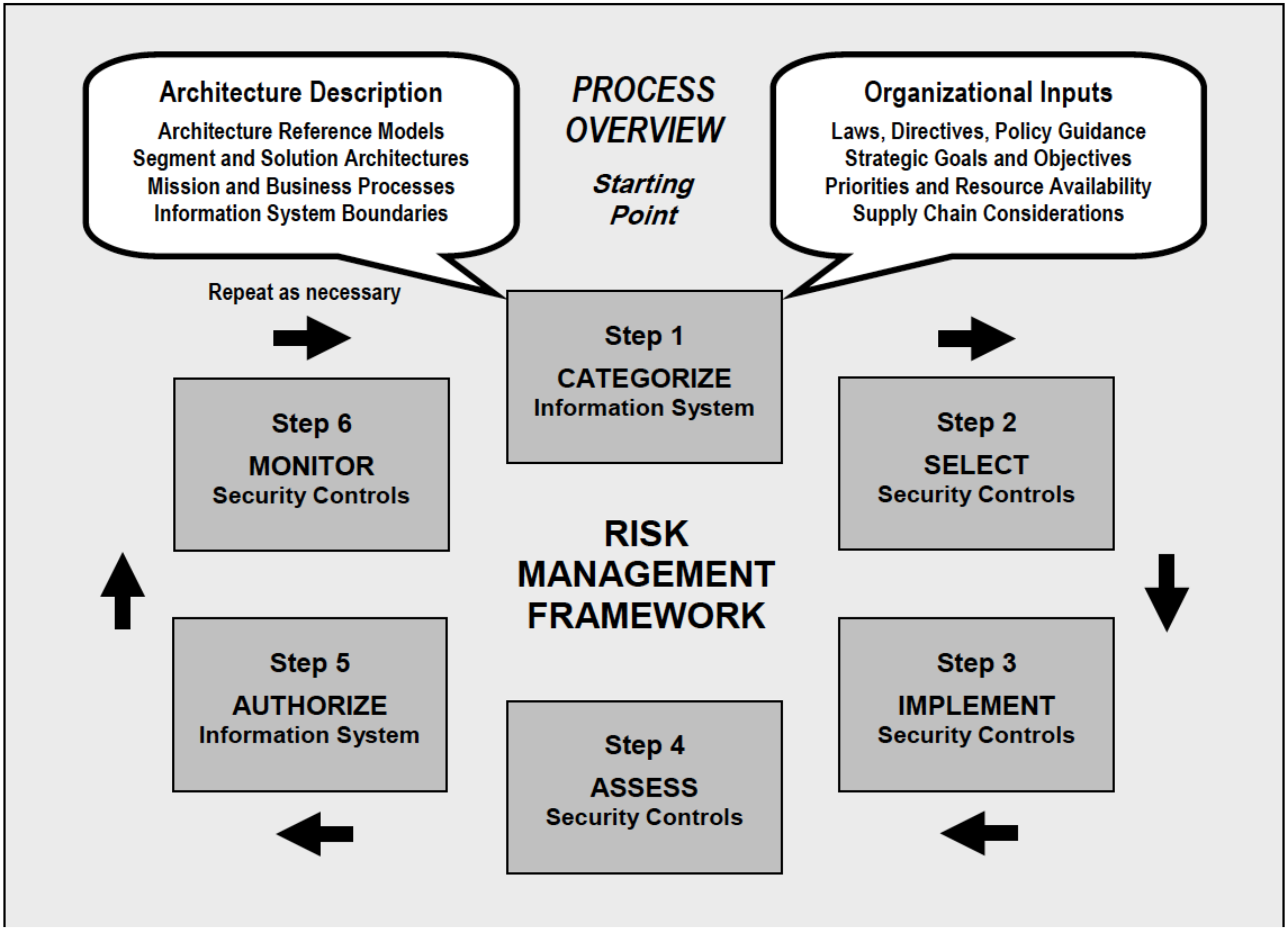
ISC2 continuum of controls relative to the timeline of a security incident

- **Directive**
  - Controls designed to specify acceptable rules of behavior within an organization
- **Deterrent**
  - Controls designed to discourage people from violating security
- **Preventive**
  - Controls implemented to prevent a security incident or information breach
- **Compensating**
  - Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
- **Detective**
  - Controls designed to signal a warning when a security control has been breached
- **Corrective**
  - Controls implemented to remedy circumstance, mitigate damage, or restore controls
- **Recovery**
  - Controls implemented to restore conditions to normal after a security incident

NIST 800-137 RMF & Controls

- ***Categorize***
  - the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- ***Select***
  - an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- ***Implement***
  - the security controls and describe how the controls are employed within the information system and its environment of operation.
- ***Assess***
  - the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize***
  - information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- ***Monitor***
  - the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

NIST 800-137 RMF



Architecture Description

Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

RISK MANAGEMENT FRAMEWORK

Section Conclusion

- Understand concepts of business impact analysis
- Understand concepts of risk management
- Explore risk management processes
- Compare and contrast various types of controls
- Learn the categories of security controls

Risk Management and Business Impact Analysis
Risk Analysis

Reference:

Drew Hamilton Lecture Notes

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Key References

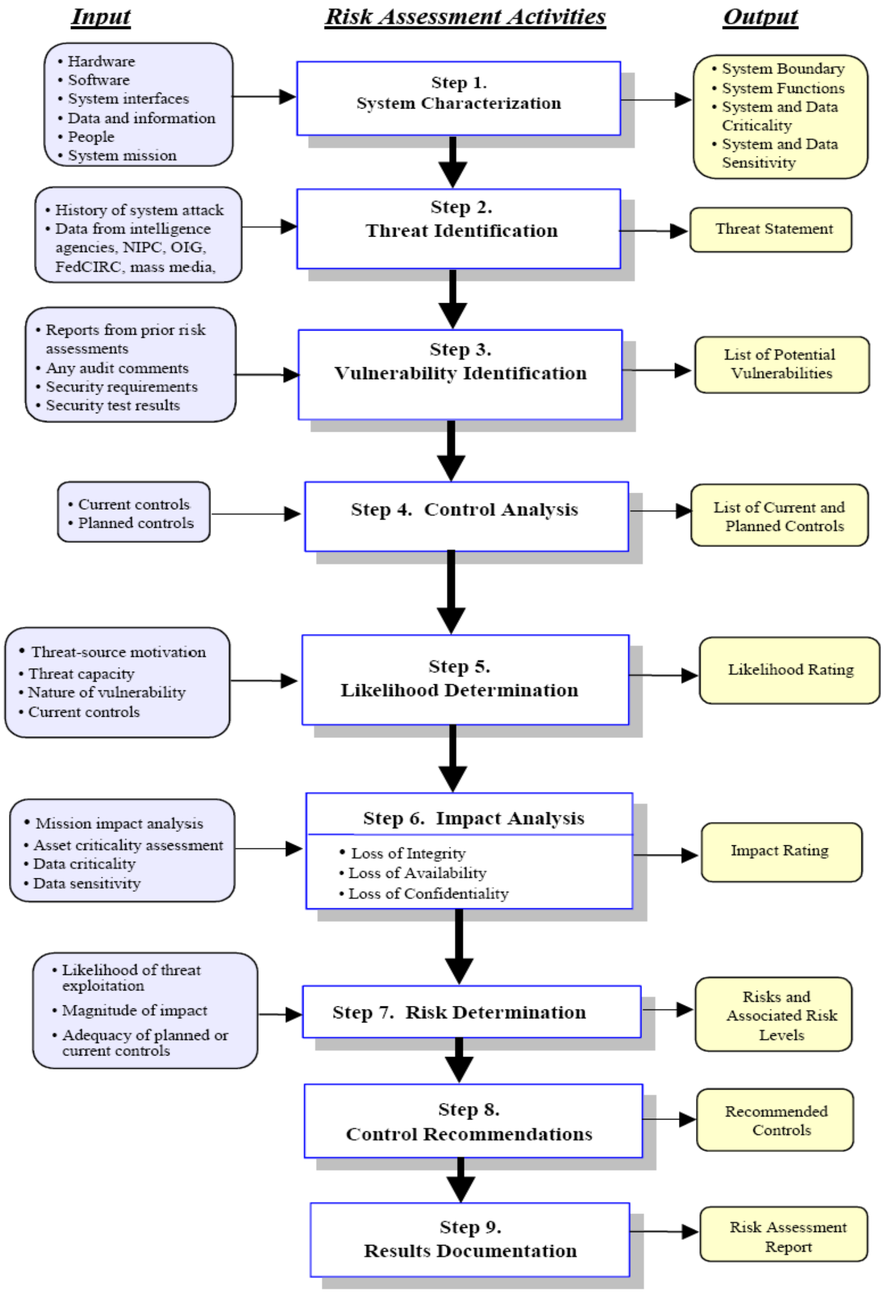
- NIST SP800-30: Risk Management Guide for IT
- NIST SP800-42: Guideline on Network Security Testing
- NIST SP800-53: Recommended Security Controls for Federal Information Systems
- SP800-61: Computer Security Incident Handling Guide
- FIPS-PUB-199: Standards for Security Categorization of Federal Information and Information Systems

Section A - E: Risk Assessments, Avenues of Attack, and Vulnerabilities

- **Risk assessment is the first process in the risk management methodology.**
- **Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC.**
- **The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed later.**
- ***Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.**
- **To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.**
- **Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability.**
- **The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the IT system components and data).**

- **The risk assessment methodology encompasses nine primary steps:**

  Step 1:
  System Characterization
  Step 2:
  Threat Identification
  Step 3:
  Vulnerability Identification
  Step 4:
  Control Analysis
  Step 5:
  Likelihood Determination
  Step 6:
  Impact Analysis
  Step 7:
  Risk Determination
  Step 8:
  Control Recommendations
  Step 9:
  Results Documentation



Input | ***Risk Assessment Activities*** | ***Output***

- Hardware
- Software
- System interfaces
- Data and information
- People
- System mission

Step 1.
System Characterization

- System Boundary
- System Functions
- System and Data Criticality
- System and Data Sensitivity

- History of system attack
- Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,

Step 2.
Threat Identification

Threat Statement

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test results

Step 3.
Vulnerability Identification

List of Potential Vulnerabilities

- Current controls
- Planned controls

Step 4. Control Analysis

List of Current and Planned Controls

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Step 5.
Likelihood Determination

Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Step 6. Impact Analysis
- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

Impact Rating

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Step 7. Risk Determination

Risks and Associated Risk Levels

Step 8.
Control Recommendations

Recommended Controls

Step 9.
Results Documentation

Risk Assessment Report

Figure 3-1. Risk Assessment Methodology Flowchart

Risk Assessment/Boundary Definition

- **In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system.**

- **Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.**

- **The methodology described can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.**

Risk Assessment

- Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:
  - Hardware
  - Software
  - System interfaces
    - (e.g., internal and external connectivity)
  - Data and information
  - Persons who support and use the IT system
  - System mission
    - (e.g., the processes performed by the IT system)
  - System and data criticality
    - (e.g., the system's value or importance to an organization)
  - System and data sensitivity.

Risk Assessment

- Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:
- The functional requirements of the IT system
- Users of the system (system users providing technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)

Risk Assessment

- Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- Management controls used for the IT system (e.g., rules of behavior, security planning)Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

IT System Security

- For a system that is in the initiation or design phase, system information can be derived from the design or requirements document.

- For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system.

- System design documents and the system security plan can provide useful information about the security of an IT system that is in development.

- For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices.

- Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

IT Information-Gathering Techniques

- Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:
- Questionnaire. To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system.
  - This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.
- On-site Interviews. Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed).
  - On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system

IT Information-Gathering Techniques (2)

- **Document Review.** Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan5, security policies) can provide good information about the security controls used by and planned for the IT system.
  - An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.
- **Use of Automated Scanning Tool.** Proactive technical methods can be used to collect system information efficiently.
  - For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Threat Identification

- **Threat: The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.**

- **Threat-Source: Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.**

- **The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the IT system being evaluated.**

Threat-Source Identification (2)

- In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. For example, although the threat statement for an IT system located in a desert may not include “natural flood” because of the low likelihood of such an event’s occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization’s IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors.
- A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer’s writing a Trojan horse program to bypass system security in order to “get the job done.”

Threat Sources

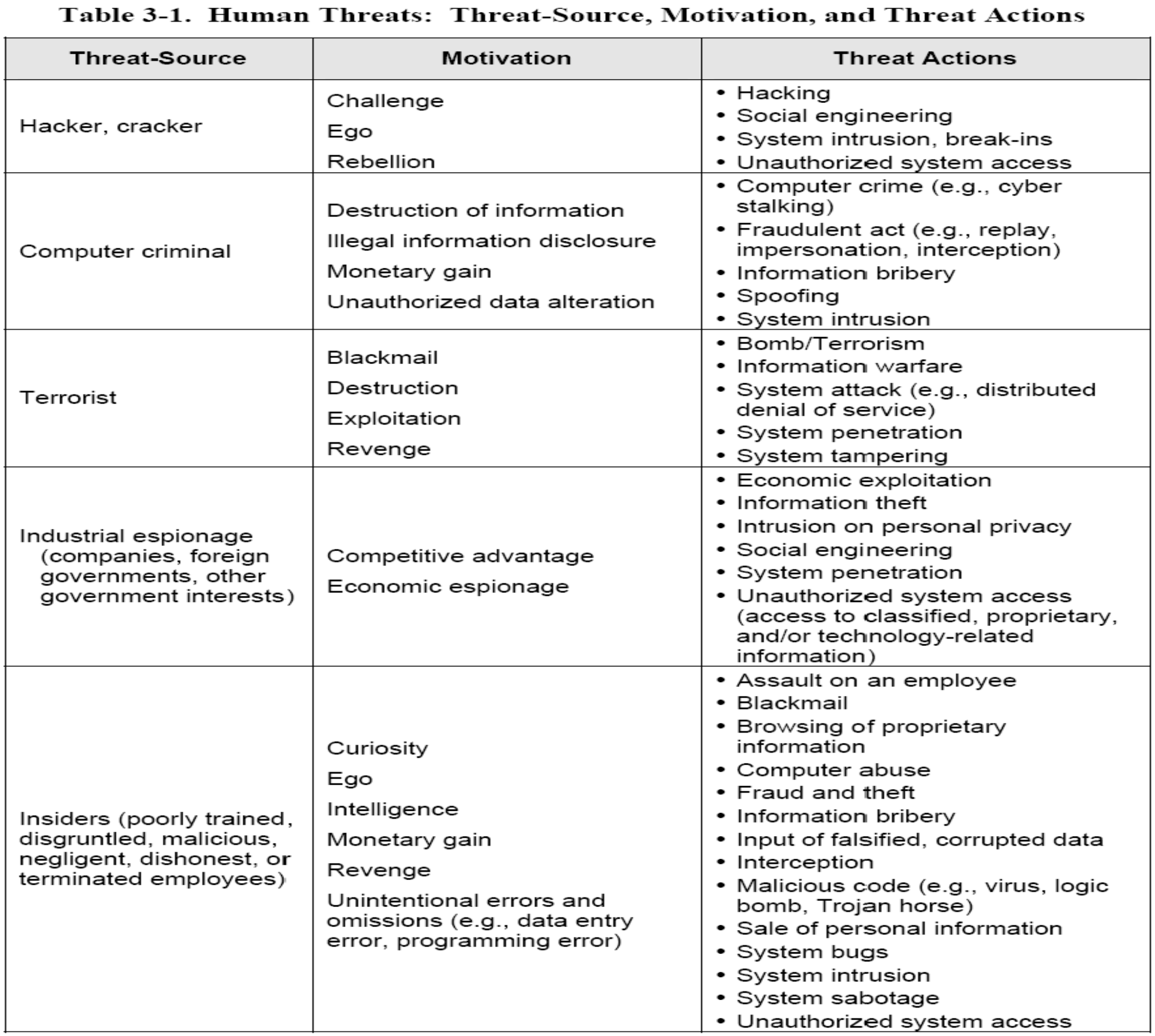


Table 3-1. Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Threat-Sources (2)

- An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat’s exercising a system vulnerability, as described later.
- The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits).
- In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.
- Known threats have been identified by many government and private sector organizations.

Threat-sources (3)

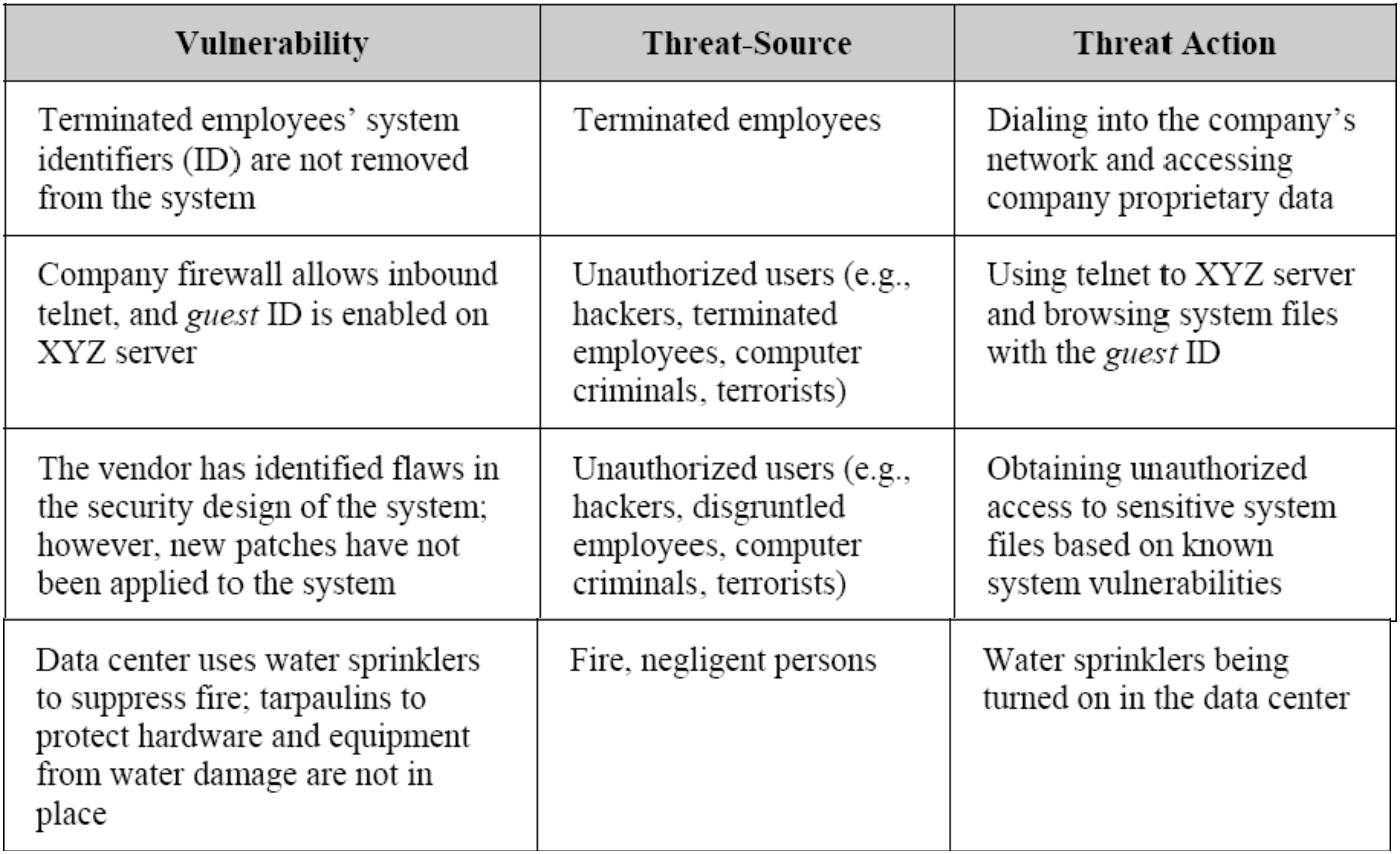
- Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:
- Intelligence agencies (for example, the Federal Bureau of Investigation’s National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

Output from Step 2: A threat statement containing a list of threat-sources that could exploit system vulnerabilities

Vulnerabilities

- Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- The analysis of the threat to an IT system must include an analysis of the vulnerabilities associated with the system environment.
- The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

Vulnerabilities (2)



Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Vulnerabilities (3)

- Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.
- It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the IT system and the phase it is in, in the SDLC:
- If the IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers).
- If the IT system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the IT system is operational, the process of identifying vulnerabilities should include an analysis of the IT system security features and the security controls, technical and procedural, used to protect the system.

Vulnerability Sources

- The technical and nontechnical vulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques.
- A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system).
- The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities.
- Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following (next slide):

Vulnerability Sources (2)

- Previous risk assessment documentation of the IT system assessed the IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

System Security Testing

- Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include
    1. Automated vulnerability scanning tool
    2. Security test and evaluation (ST&E)
    3. Penetration testing.
- The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying).
- However, it should be noted that some of the *potential* vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment.
- For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements.
- Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it.
- Thus, this test method may produce false positives.

System Security Testing (2)

- ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results).
- The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment.
- The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.
- Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured.
- Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.
- The results of these types of optional security testing will help identify a system's vulnerabilities.

(Note: SP800-42 provides additional information on vulnerability testing using automated tools).

Development of Security Requirements Checklist

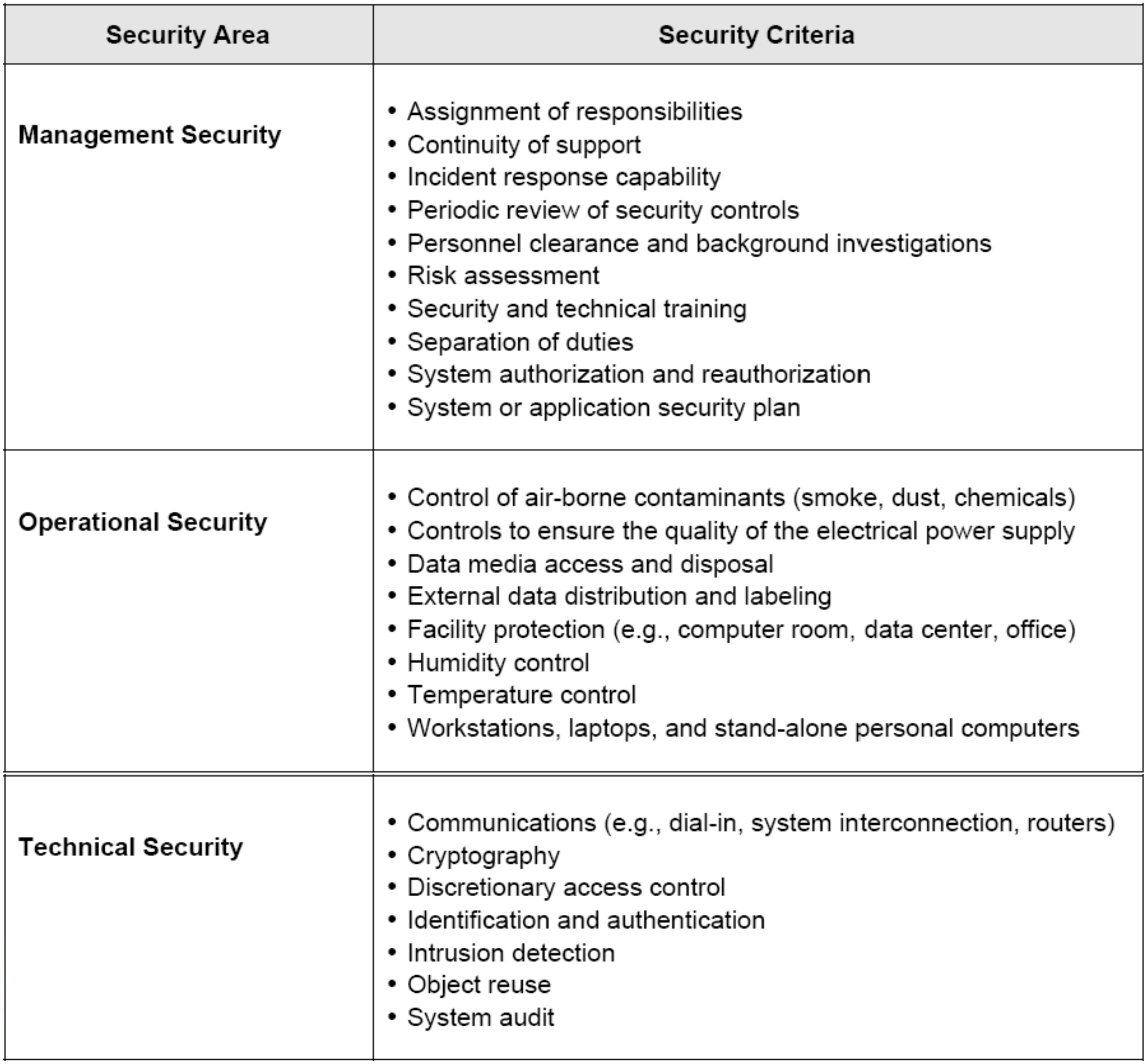
Step 3:

- During this step, the risk assessment personnel determine whether the security requirements stipulated for the IT system and collected during system characterization are being met by existing or planned security controls.
- Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.
- A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, information), non-automated procedures, processes, and information transfers associated with a given IT system in the following security areas:
  - Management
  - Operational
  - Technical.

Table 3-3 lists security criteria suggested for use in identifying an IT system's vulnerabilities in each security area.

Additional Security Guidance can be obtained from NIST-SP-800-53.

Table 3-3. Security Criteria



Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

Development of Security Requirements Checklist (2)

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the IT system processing environment:

- CSA of 1987
- Federal Information Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the IT system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

The NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured.

The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

Output from Step 3: A list of the system vulnerabilities (observations)7 that could be exercised by the potential threat-sources.

Control Analysis

Step 4:

- The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

- To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered.

- For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Control Analysis (2)

- Control Methods
  - Security controls encompass the use of technical and non-technical methods.
  - Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software).
  - Non-technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.
- Control Categories

The control categories for both technical and non-technical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

Control Analysis (3)

Control Analysis Technique

- **As discussed, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner.**
- **The security requirements checklist can be used to validate security noncompliance as well as compliance.**
- **Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.**

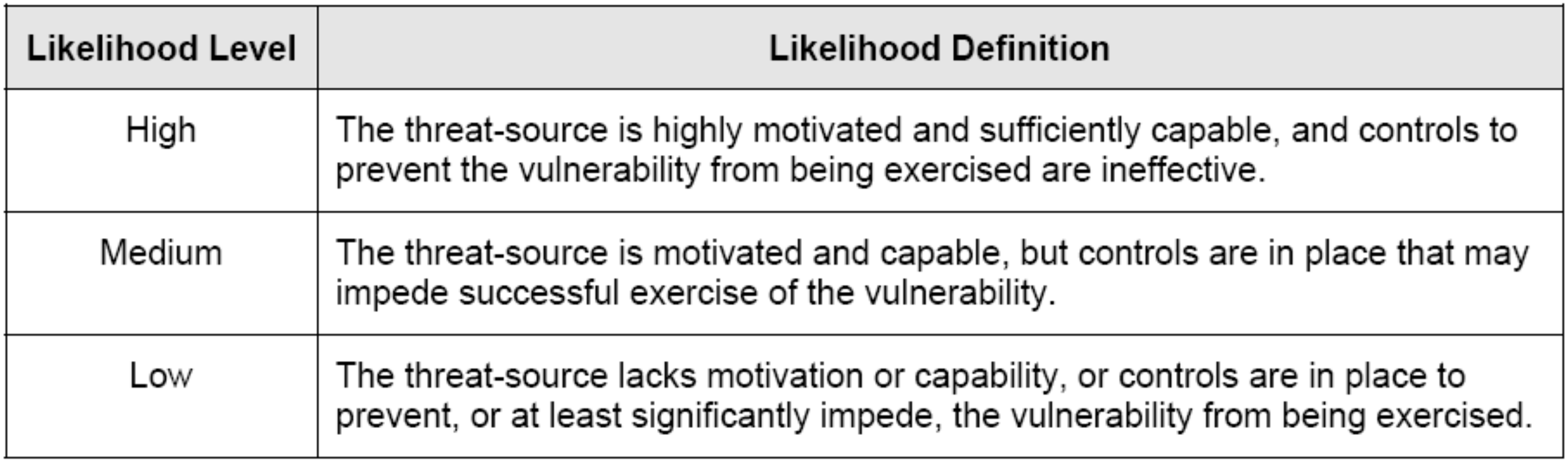
Output from Step 4: List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event.

Likelihood Determination

Step 5:

- **To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:**
  - **Threat-source motivation and capability**
  - **Nature of the vulnerability**
  - **Existence and effectiveness of current controls.**
- **The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low.**

Output from Step 5: Likelihood rating (High, Medium, Low)



Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis

Step 6:

- The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability. Before beginning the impact analysis, it is necessary to obtain the following information as discussed previously:
    - 1. System mission (e.g., the processes performed by the IT system)
    - 2. System and data criticality (e.g., the system's value or importance to an organization)
    - 3. System and data sensitivity.
- This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets.
- An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

Impact Analysis (2)

- If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality.
- Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).
- Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

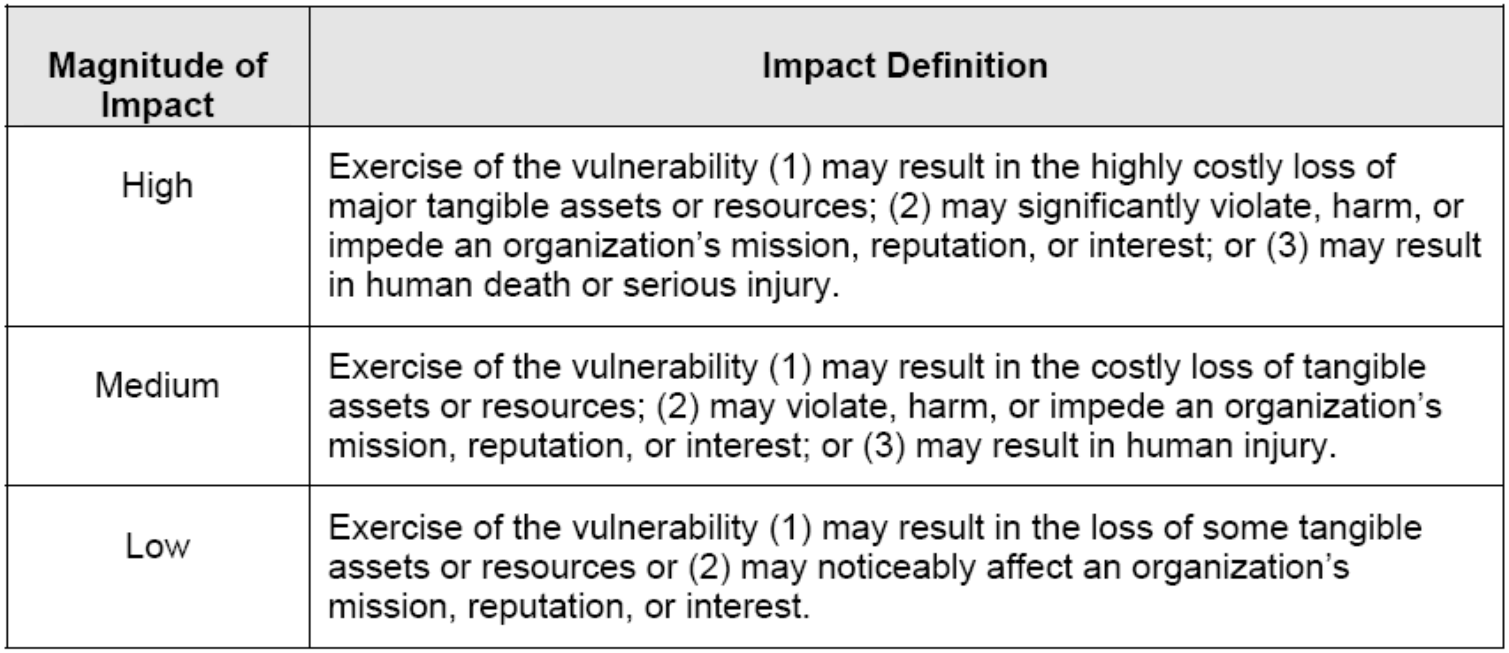
1. Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
2. Loss of Availability. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
3. Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Impact Analysis (3)

- **Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action.**

- **Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts.**

Table 3-5. Magnitude of Impact Definitions



Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Impact Analysis (4)

Quantitative versus Qualitative Assessment

- In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments.
- The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
- The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.
- The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls.
- The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner.
- Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to— An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

Output from Step 6: Magnitude of impact (High, Medium, or Low)

Risk Determination

Step 7:

The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

• The likelihood of a given threat-source's attempting to exercise a given vulnerability

• The magnitude of the impact should a threat-source successfully exercise the vulnerability

• The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed.

Risk Determination (2)

- **The sample matrix in Table 3-6 shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example, The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.**

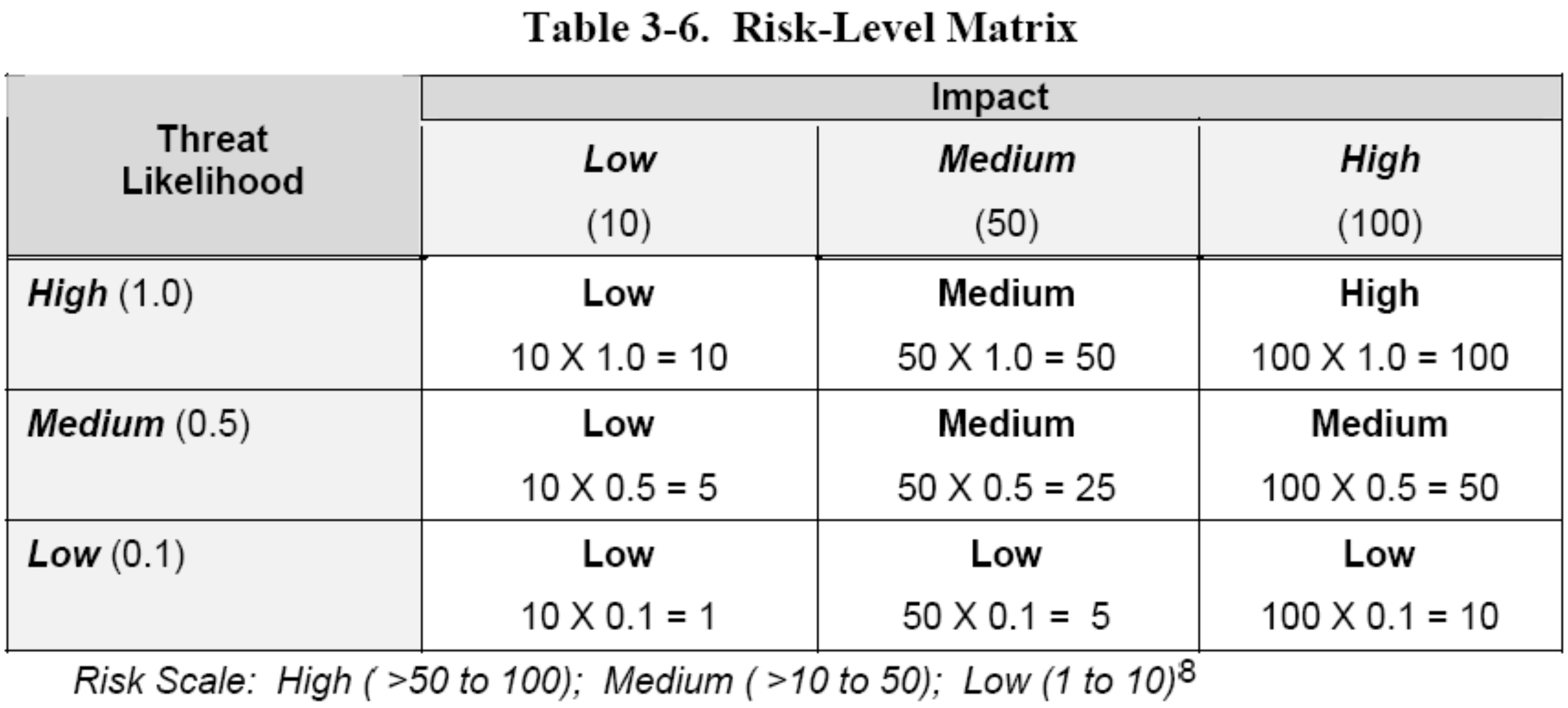


Table 3-6. Risk-Level Matrix

Threat Likelihood	**Impact**		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

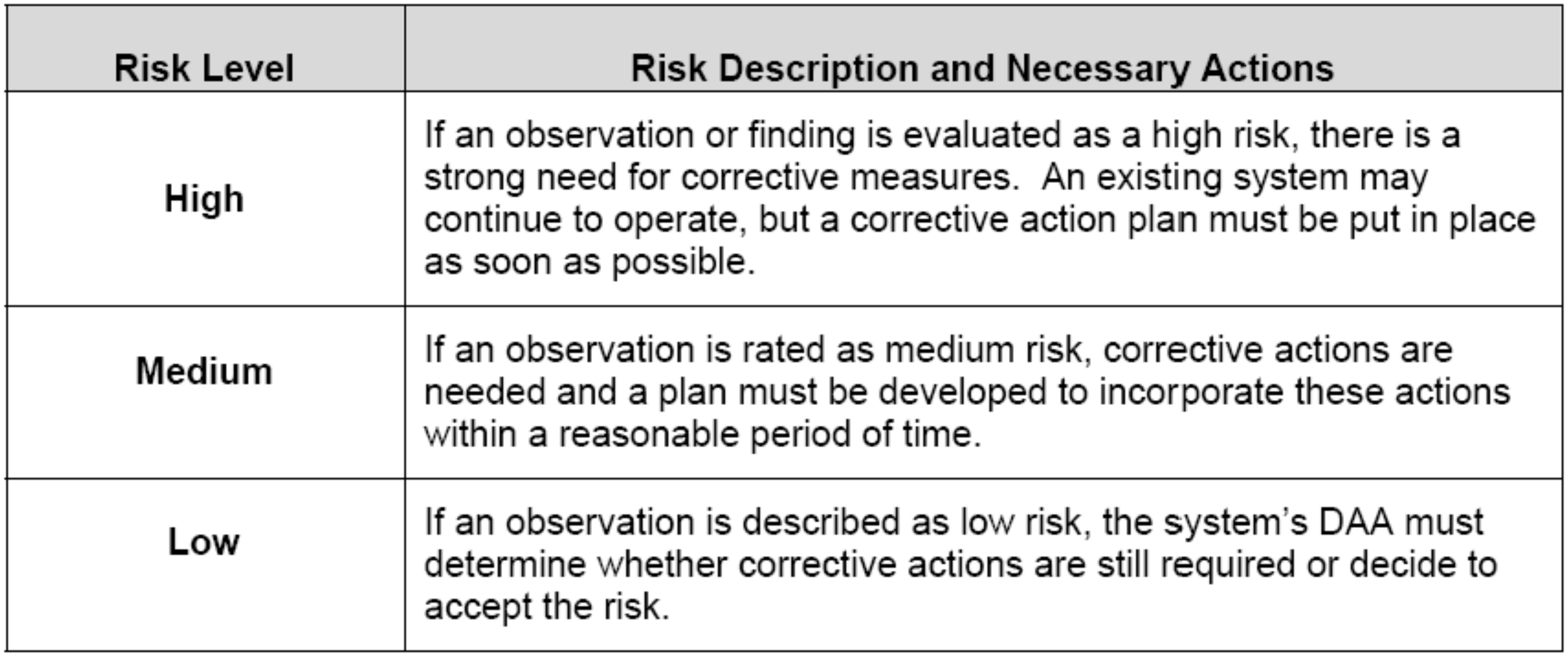
Risk Determination (3)

Description of Risk Level

Table 3-7 describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Output from Step 7: Risk level (High, Medium, Low)

Table 3-7. Risk Scale and Necessary Actions



Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk.

Control Recommendations

Step 8:

- During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:
- ➢ Effectiveness of recommended options (e.g., system compatibility)
- ➢ Legislation and regulation
- ➢ Organizational policy
- ➢ Operational impact
- ➢ Safety and reliability
- The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
- It should be noted that not all possible recommended controls can be implemented to reduce loss.
- To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed later, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.
- *Output from Step 8: Recommendation of control(s) and alternative solutions to mitigate risk*

Results Documentation

Step 9:

- **Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.**
- **A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.**
- **Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.**
- **Appendix B provides a suggested outline for the risk assessment report.**
- ***Output from Step 9*: *Risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation***

Cost/Benefit Analysis

- Cost analysis of data protection versus cost of data loss or compromise
- SP800-30: Risk Management Guide for IT Systems, pgs. 37-39

- Annualized Rate of Occurrence (ARO)
- Single Loss Expectancy (SLE) =
  SLE = Asset Value in $ X Exposure Factor
- Annualize Loss Expectancy (ALE) =
  ALE = SLE X ARO

Security Objectives

- **The FISMA defines three security objectives for information and information systems:**

1. **CONFIDENTIALITY**

   "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

   A loss of *confidentiality* is the unauthorized disclosure of information.

2. **INTEGRITY**

   "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

   A loss of *integrity* is the unauthorized modification or destruction of information.

3. **AVAILABILITY**

   "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

   A loss of *availability* is the disruption of access to or use of information or an information system. [FIPS-PUB-199]

Potential Impact (Low)

FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The *potential impact* is LOW if—

− The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.2

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Potential Impact (Moderate)

The *potential impact* is MODERATE if—

− The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

[FIPS-PUB-199]

Potential Impact (High)

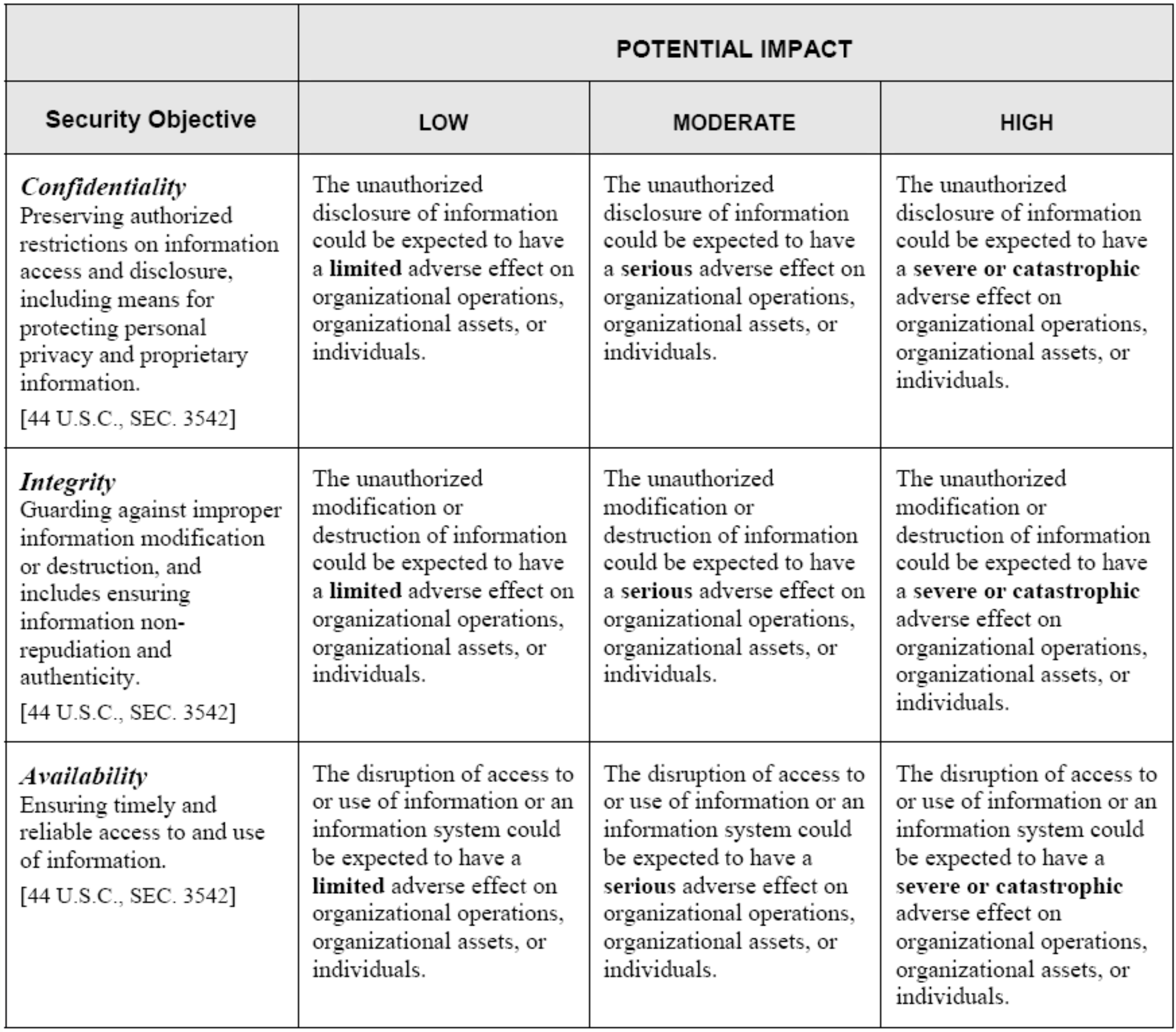
The *potential impact* is HIGH if—

− The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

[FIPS-PUB-199]

Potential Impact Definitions for Security Objectives



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Redundancy and Fault-Tolerant Systems

- Backup and availability solutions
  - Redundant hardware ready for “hot swapping”
  - Fault-tolerant technologies
  - Service Level Agreements
  - Solid Operational Procedures
- Mean Time Between Failures (MTBF) is the estimated lifespan of a piece of equipment.
- Mean Time to Repair (MTTR) is the amount of time expected to get a device repaired and back into production

Incident Response, Disaster Recovery, Continuity of Operations Risk Analysis

Reference:

Drew Hamilton Lecture Notes

C.W. Perr, Sandia Labs

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

What we will cover…

- Project initiation steps
- Recovery and continuity planning requirements
- Business impact analysis
- Selecting, developing, and implementing disaster and continuity plans
- Backup and offsite facilities
- Types of drills and tests

What do we do if everything blows up?

- The goal of ***disaster recovery*** is to minimize the effects of a disaster and to take the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner. (Usually very IT focused).

- The short: make it not hurt so bad, and get it fixed right away.

Business Continuity Plan

- ***Availability, integrity, and confidentiality*…a running theme through the ISC2 materials.**
- **↑ These items need to be considered just as important during and after an emergency.**
- **Might be more vulnerable after a disaster.**
- **The plan for this is the Business Continuity Plan (BCP).**

Business Continuity Planning

- This is a preplanned activity which allows us to…
  - Provide and immediate and appropriate response to an emergency
  - Protect lives and ensure safety
  - Reduce business impact
  - Resume critical business functions
  - Work with outside vendors during the recovery period
  - Reduce confusion during a crisis
  - Ensure survivability of the business
  - Get "up and running" quickly after a disaster

Business Continuity Planning (continued)

- Part of business decisions today should include the following:
  - Letting business partners know your company is prepared
  - Reassuring shareholders and boards of trustees about your company's readiness
  - Making sure a BCP is in place if industry regulations require it

7 Steps for Business Continuity

1. **Develop the continuity planning policy statement.**
   - Write a policy that provides the guidance necessary to develop a BCP and that assigns authority to the necessary roles to carry out these tasks.
2. **Conduct the business impact analysis (BIA).**
   - Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities, threats, and calculate risks.
3. **Identify preventive controls.**
   - Once threats are recognized, identify and implement controls and countermeasures to reduce the organization's risk level in an economical manner.

*best practices are developed by the National Institute of Standards and Technology(NIST).

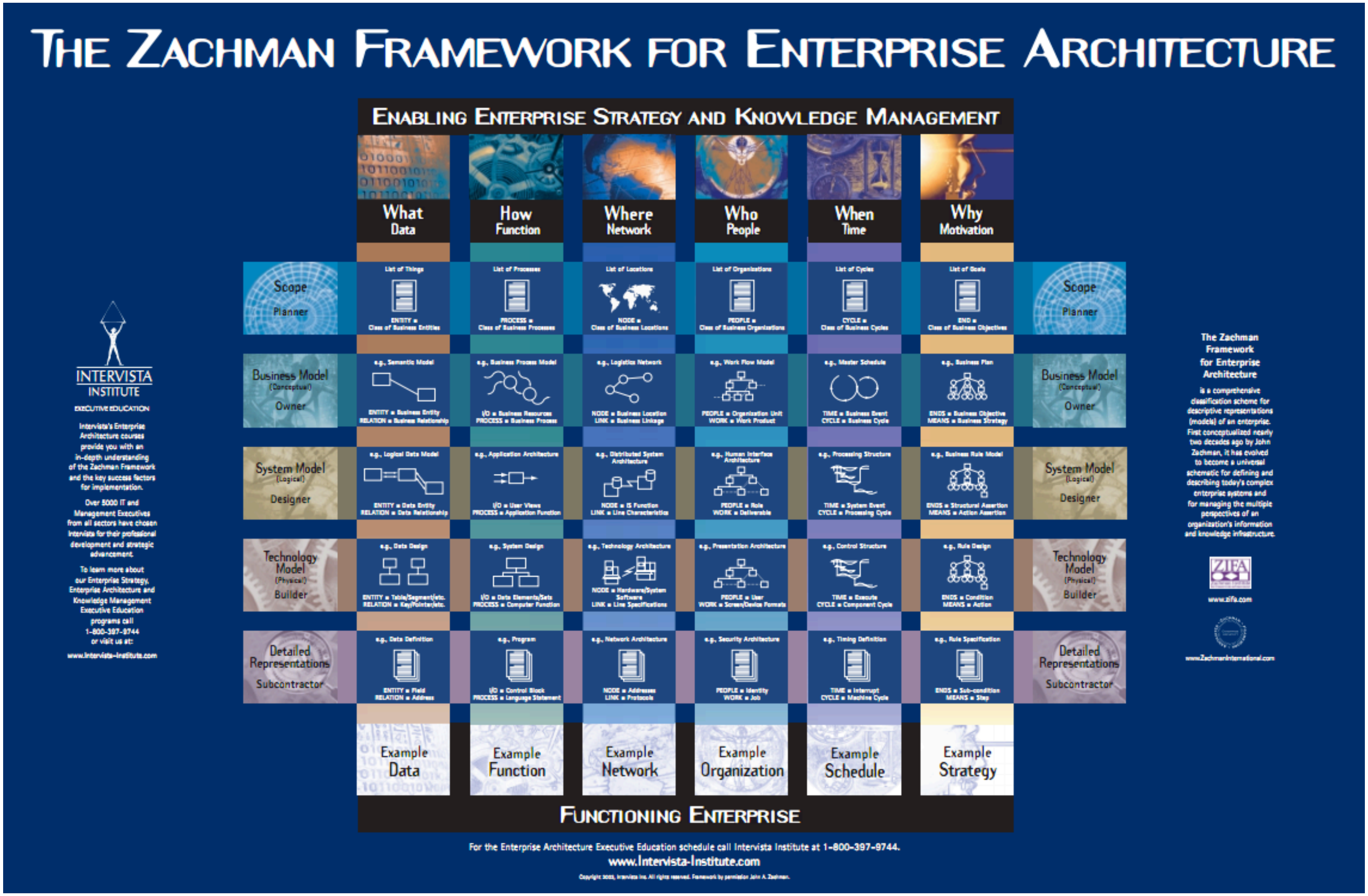
7 Steps for Business Continuity

4. Develop recovery strategies
   - Formulate methods to ensure systems and critical functions can be brought online quickly.
5. Develop the contingency plan.
   - Write the procedures and guidelines for how the organization can still stay functional in a crippled state.
6. Test the plan and conduct training and exercises.
   - Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.
7. Maintain the plan.
   - Put in place steps to ensure the BCP is a living document that is updated regularly.

…another Company's version

- (ISC)^2
  1. Project initiation
  2. BIA (business impact analysis)
  3. Recovery strategy
  4. Plan design and development
  5. Implementation
  6. Testing
  7. Continual maintenance

Understand the Organization First



THE ZACHMAN FRAMEWORK FOR ENTERPRISE ARCHITECTURE

ENABLING ENTERPRISE STRATEGY AND KNOWLEDGE MANAGEMENT

	What Data	How Function	Where Network	Who People	When Time	Why Motivation	
Scope Planner	List of Things ENTITY = Class of Business Entities	List of Processes PROCESS = Class of Business Processes	List of Locations NODE = Class of Business Locations	List of Organizations PEOPLE = Class of Business Organizations	List of Cycles CYCLE = Class of Business Cycles	List of Goals END = Class of Business Objectives	Scope Planner
Business Model (Conceptual) Owner	e.g., Semantic Model ENTITY = Business Entity RELATION = Business Relationship	e.g., Business Process Model I/O = Business Resources PROCESS = Business Process	e.g., Logistics Network NODE = Business Location LINK = Business Linkage	e.g., Work Flow Model PEOPLE = Organization Unit WORK = Work Product	e.g., Master Schedule TIME = Business Event CYCLE = Business Cycle	e.g., Business Plan ENDS = Business Objective MEANS = Business Strategy	Business Model (Conceptual) Owner
System Model (Logical) Designer	e.g., Logical Data Model ENTITY = Data Entity RELATION = Data Relationship	e.g., Application Architecture I/O = User Views PROCESS = Application Function	e.g., Distributed System Architecture NODE = IS Function LINK = Line Characteristics	e.g., Human Interface Architecture PEOPLE = Role WORK = Deliverable	e.g., Processing Structure TIME = System Event CYCLE = Processing Cycle	e.g., Business Rule Model ENDS = Structural Assertion MEANS = Action Assertion	System Model (Logical) Designer
Technology Model (Physical) Builder	e.g., Data Design ENTITY = Table/Segment/etc. RELATION = Key/Pointer/etc.	e.g., System Design I/O = Data Elements/Sets PROCESS = Computer Function	e.g., Technology Architecture NODE = Hardware/System Software LINK = Line Specifications	e.g., Presentation Architecture PEOPLE = User WORK = Screen/Device Formats	e.g., Control Structure TIME = Execute CYCLE = Component Cycle	e.g., Rule Design ENDS = Condition MEANS = Action	Technology Model (Physical) Builder
Detailed Representations Subcontractor	e.g., Data Definition ENTITY = Field RELATION = Address	e.g., Program I/O = Control Block PROCESS = Language Statement	e.g., Network Architecture NODE = Addresses LINK = Protocols	e.g., Security Architecture PEOPLE = Identity WORK = Job	e.g., Timing Definition TIME = Interrupt CYCLE = Machine Cycle	e.g., Rule Specification ENDS = Sub-condition MEANS = Step	Detailed Representations Subcontractor
	Example Data	Example Function	Example Network	Example Organization	Example Schedule	Example Strategy	

FUNCTIONING ENTERPRISE

INTERVISTA
INSTITUTE
EXECUTIVE EDUCATION

Intervista's Enterprise Architecture courses provide you with an in-depth understanding of the Zachman Framework and the key success factors for implementation.

Over 5000 IT and Management Executives from all sectors have chosen Intervista for their professional development and strategic advancement.

To learn more about our Enterprise Strategy, Enterprise Architecture and Knowledge Management Executive Education programs call 1-800-397-9744 or visit us at:

www.Intervista-Institute.com

The Zachman Framework for Enterprise Architecture is a comprehensive classification scheme for descriptive representations (models) of an enterprise. First conceptualized nearly two decades ago by John Zachman, it has evolved to become a universal schematic for defining and describing today's complex enterprise systems and for managing the multiple perspectives of an organization's information and knowledge infrastructure.

ZIFA

www.zifa.com

www.ZachmanInternational.com

For the Enterprise Architecture Executive Education schedule call Intervista Institute at 1-800-397-9744.

www.Intervista-Institute.com

Making BCP Part of the Security Policy and Program

- Why do we need to combine business continuity and security plans anyway?

- Response: They both protect the business, unenlightened one. (Their words…not mine).

- BCP = Business Continuity Planning

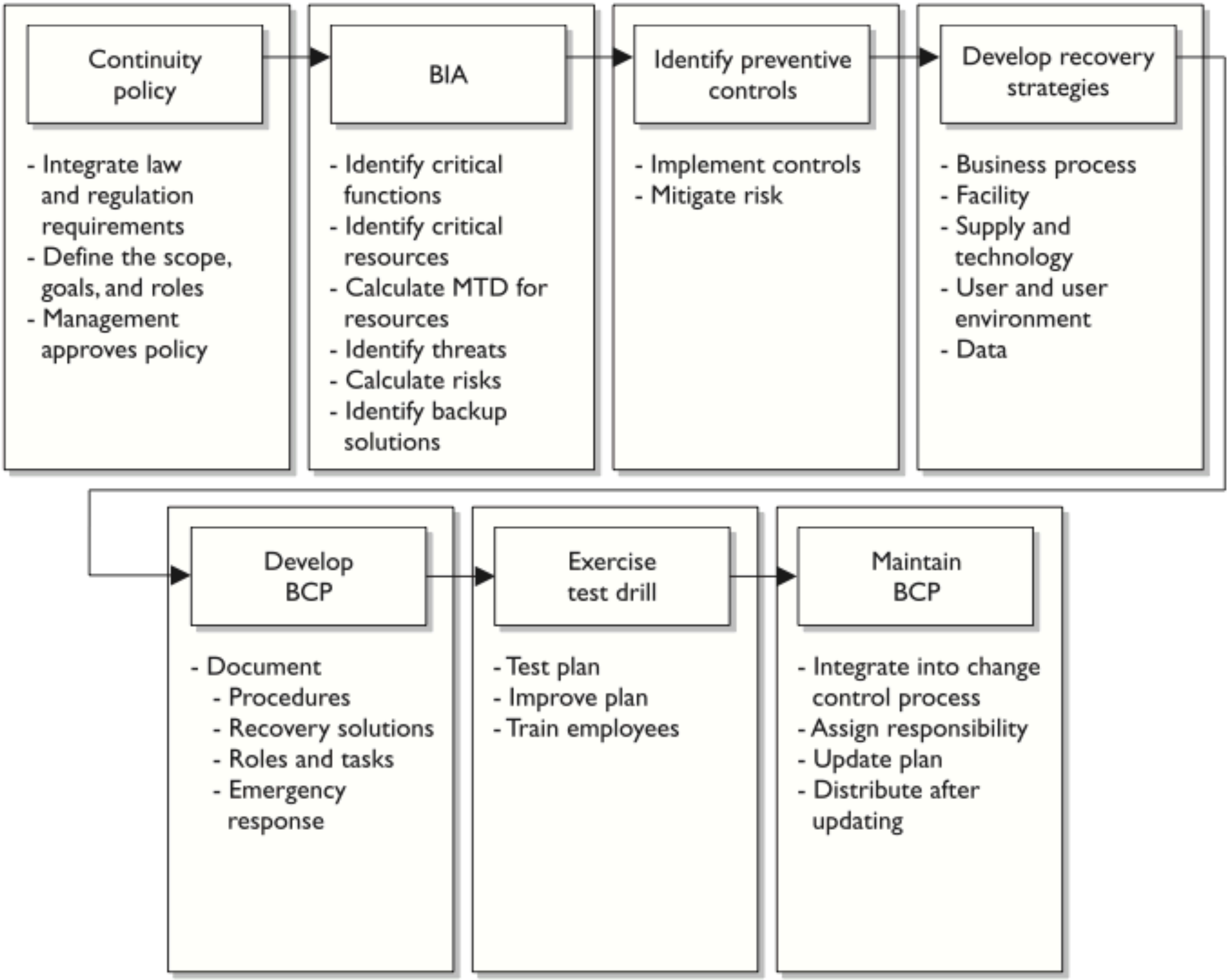

Continuity policy
- Integrate law and regulation requirements
- Define the scope, goals, and roles
- Management approves policy
BIA
- Identify critical functions
- Identify critical resources
- Calculate MTD for resources
- Identify threats
- Calculate risks
- Identify backup solutions
Identify preventive controls
- Implement controls
- Mitigate risk
Develop recovery strategies
- Business process
- Facility
- Supply and technology
- User and user environment
- Data
Develop BCP
- Document
- Procedures
- Recovery solutions
- Roles and tasks
- Emergency response
Exercise test drill
- Test plan
- Improve plan
- Train employees
Maintain BCP
- Integrate into change control process
- Assign responsibility
- Update plan
- Distribute after updating

Figure 9-1 The process components of developing a business continuity plan

Why are we doing this? (Warning: Busy Slide)

A very important question to ask when first developing a BCP is why it is being developed.

This may seem silly and the answer may at first appear obvious, but that is not always the case.

You might think that the reason to have these plans is to deal with an unexpected disaster and to get people back to their tasks as quickly and as safely as possible, but the full story is often a bit different. Why are most companies in business?

To make money and be profitable. If these are usually the main goals of businesses, then any BCP needs to be developed to help achieve and, more importantly, maintain these goals.

The main reason to develop these plans in the first place is to reduce the risk of financial loss by improving the company's ability to recover and restore operations.

This encompasses the goals of mitigating the effects of the disaster.

1. Project Initiation

- **After the coffee and donuts have been fetched it is time to get down to business.**
  - Solidify management support
  - Select a *business continuity coordinator* (needs to have direct access to management, and the ability to carry out decisions)
  - Bring all issues and threats to the table (representatives from Business units, Senior management, IT department, Security department, Communications department, and the Legal department) –give a sense of ownership here…

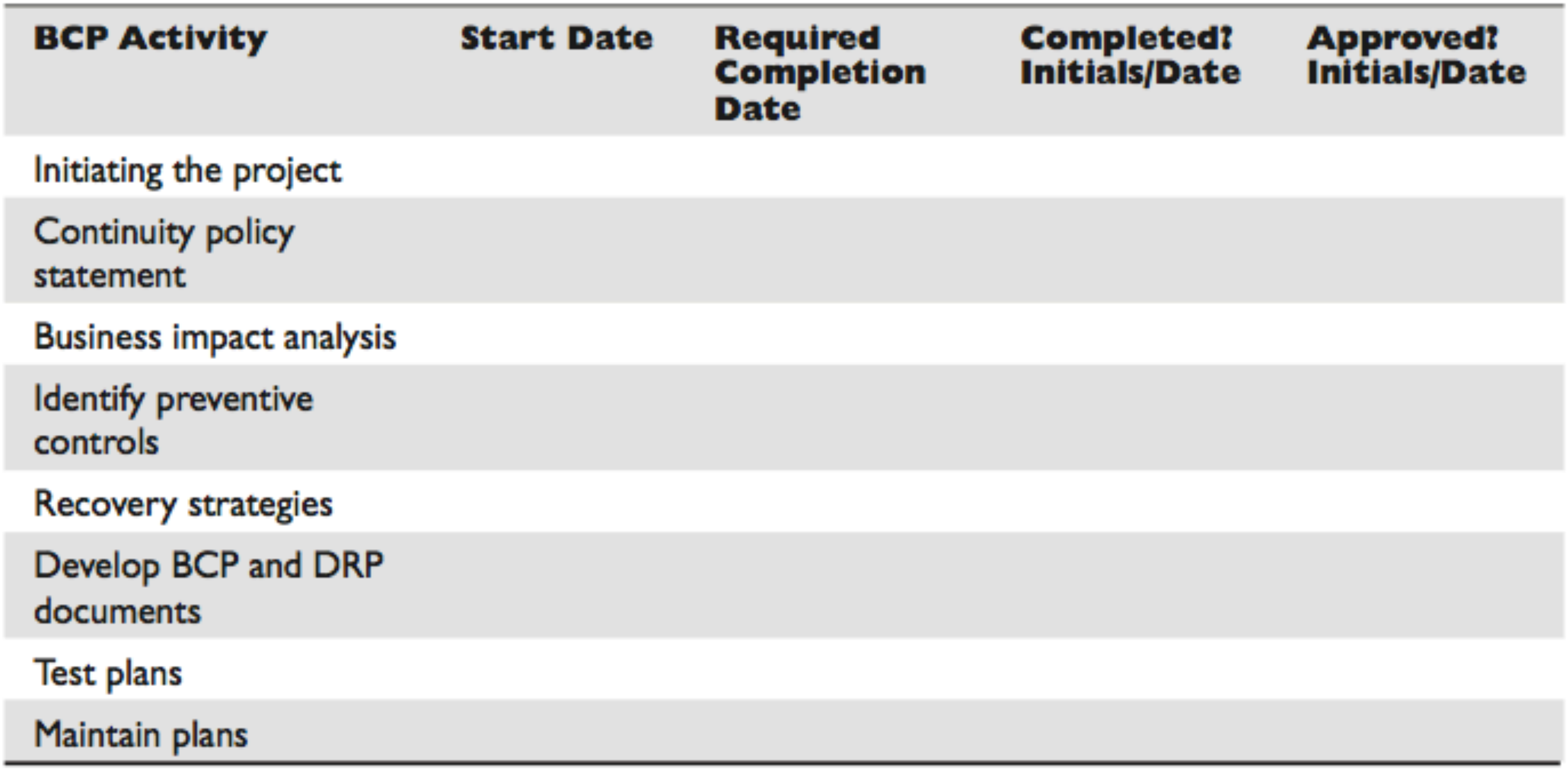
Project Initiation (continued)

- The people who develop the BCP should be the ones to execute it.
- Work with management to develop goals.
- What should the plan address? (natural disaster, terrorist attack, communication outage, etc?)

Continuity planning statement – the scope of the business continuity plan, roles of team members, and goals. [like a mission statement for everything else]

Most companies outline the scope of their BCP to encompass only the larger threats. The smaller threats are then covered by independent departmental contingency plans.

The BCP Coordinators product



BCP Activity	Start Date	Required Completion Date	Completed? Initials/Date	Approved? Initials/Date
Initiating the project				
Continuity policy statement				
Business impact analysis				
Identify preventive controls				
Recovery strategies				
Develop BCP and DRP documents				
Test plans				
Maintain plans				

Table 9-1 Steps to Be Documented and Approved

Project Plan Components

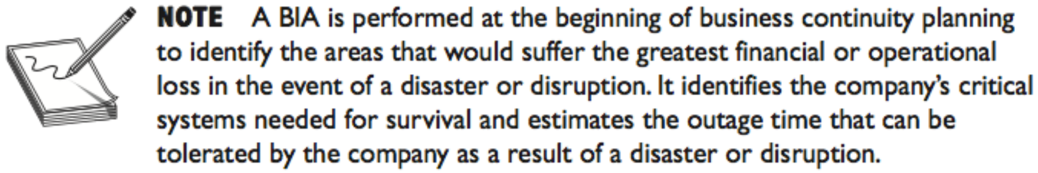
- Objective-to-task mapping
- Resource-to-task mapping
- Milestones
- Budget estimates
- Success factors
- Deadlines

Convince them of value…

- Documents potential loss for the threats involved
- Lip service equals false sense of security…bad
- Legal obligation to due diligence
- Business is the drive to deliver a product, and the sense to anticipate disaster
- Management sets the goals and is responsible for follow up

2. Business Impact Analysis

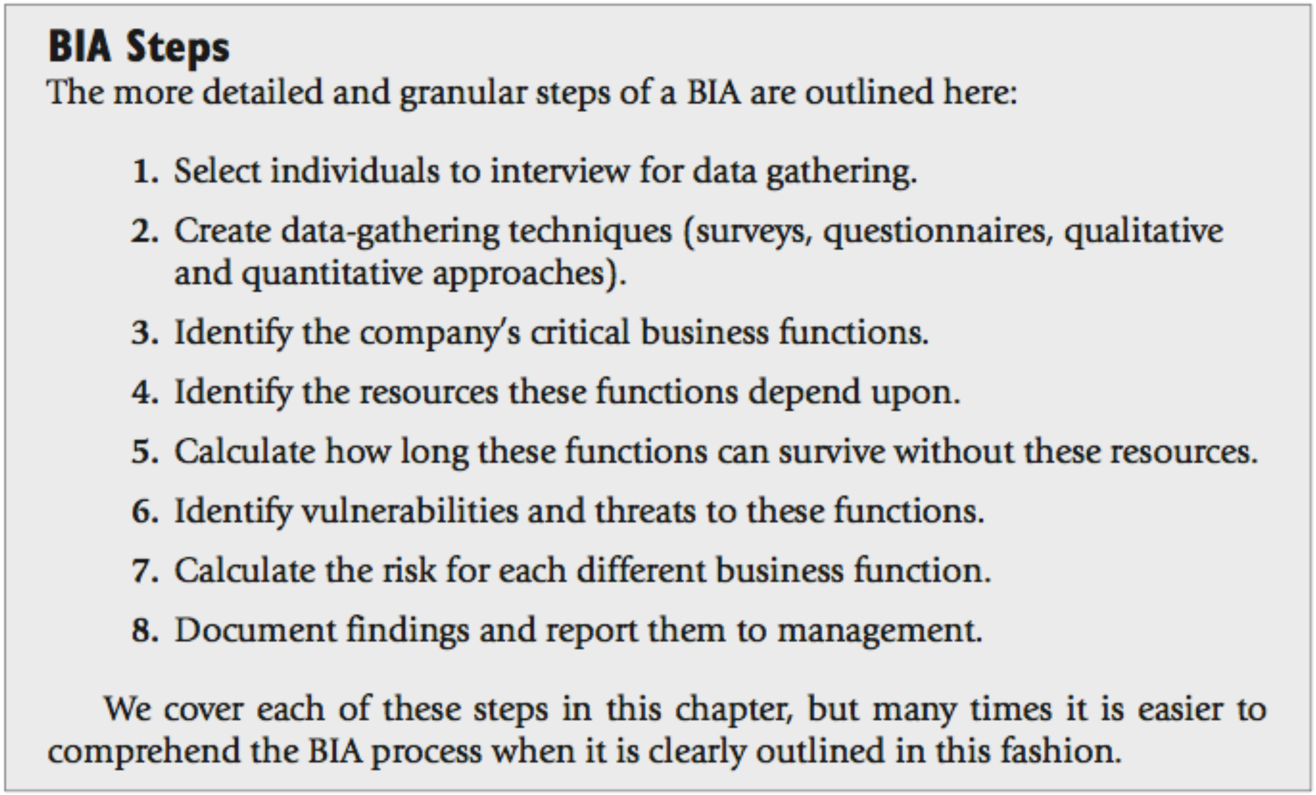
- ***How bad will this hurt and how long can we deal with this level of pain?***
- **Business impact analysis answers this.**
  - **Functional analysis: based on business, functions, activities, and transactions.**
  - **Threats are mapped based on:**
    - **Maximum tolerable downtime**
    - **Operational disruption and productivity**
    - **Financial considerations**
    - **Regulatory responsibilities**
    - **Reputation**



NOTE A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company's critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.

Business Impact Analysis (continued)

- Data collection comes from asking the committee what they think the threats are



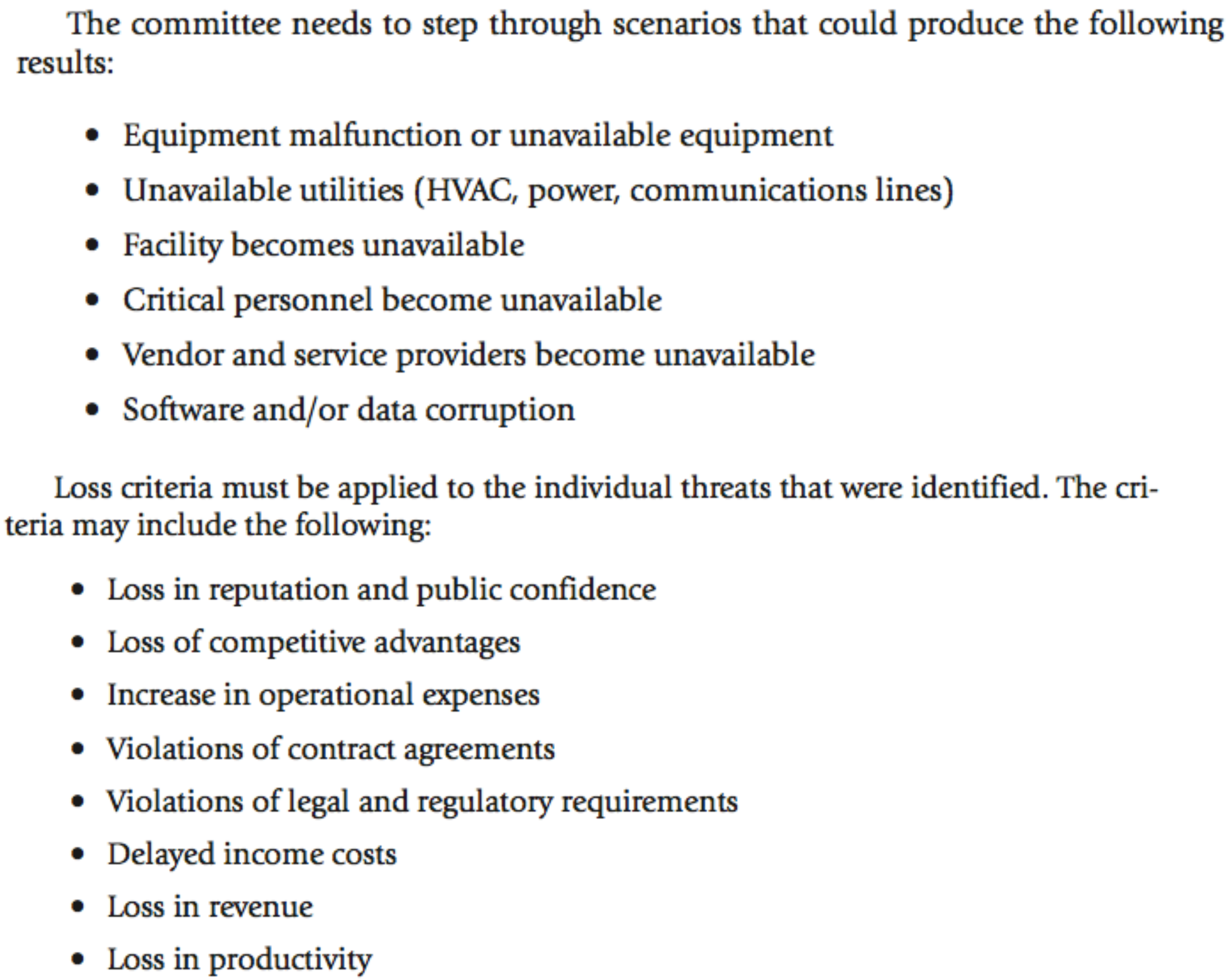
BIA Steps

The more detailed and granular steps of a BIA are outlined here:

1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

We cover each of these steps in this chapter, but many times it is easier to comprehend the BIA process when it is clearly outlined in this fashion.

Loss Criteria



The committee needs to step through scenarios that could produce the following results:

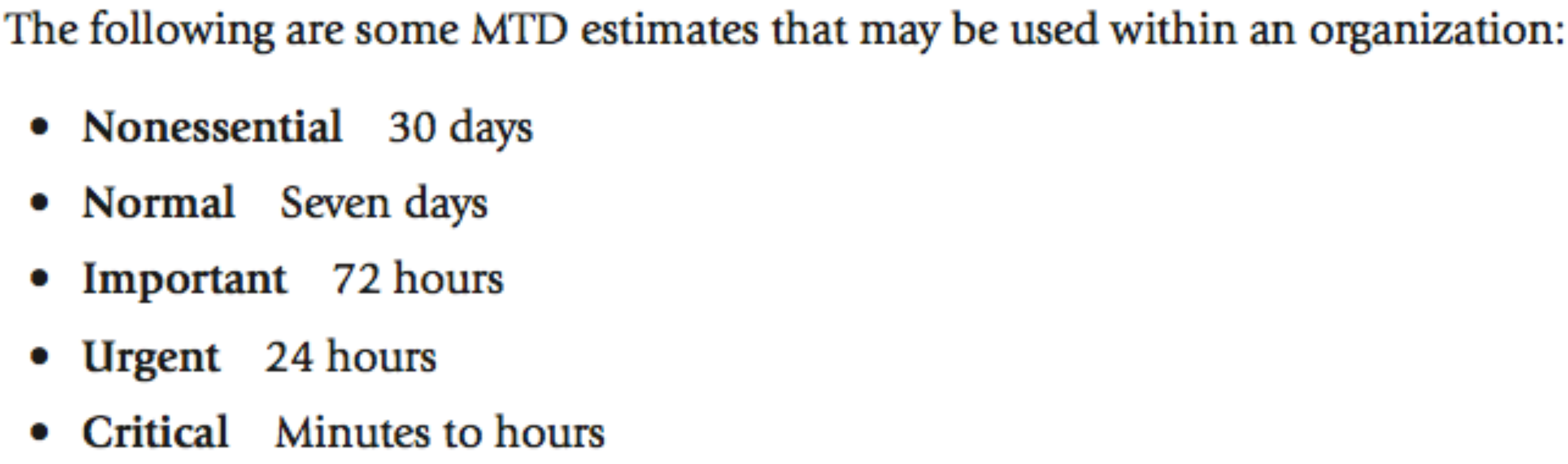
- Equipment malfunction or unavailable equipment
- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

- Loss in reputation and public confidence
- Loss of competitive advantages
- Increase in operational expenses
- Violations of contract agreements
- Violations of legal and regulatory requirements
- Delayed income costs
- Loss in revenue
- Loss in productivity

Maximum Tolerable Downtime

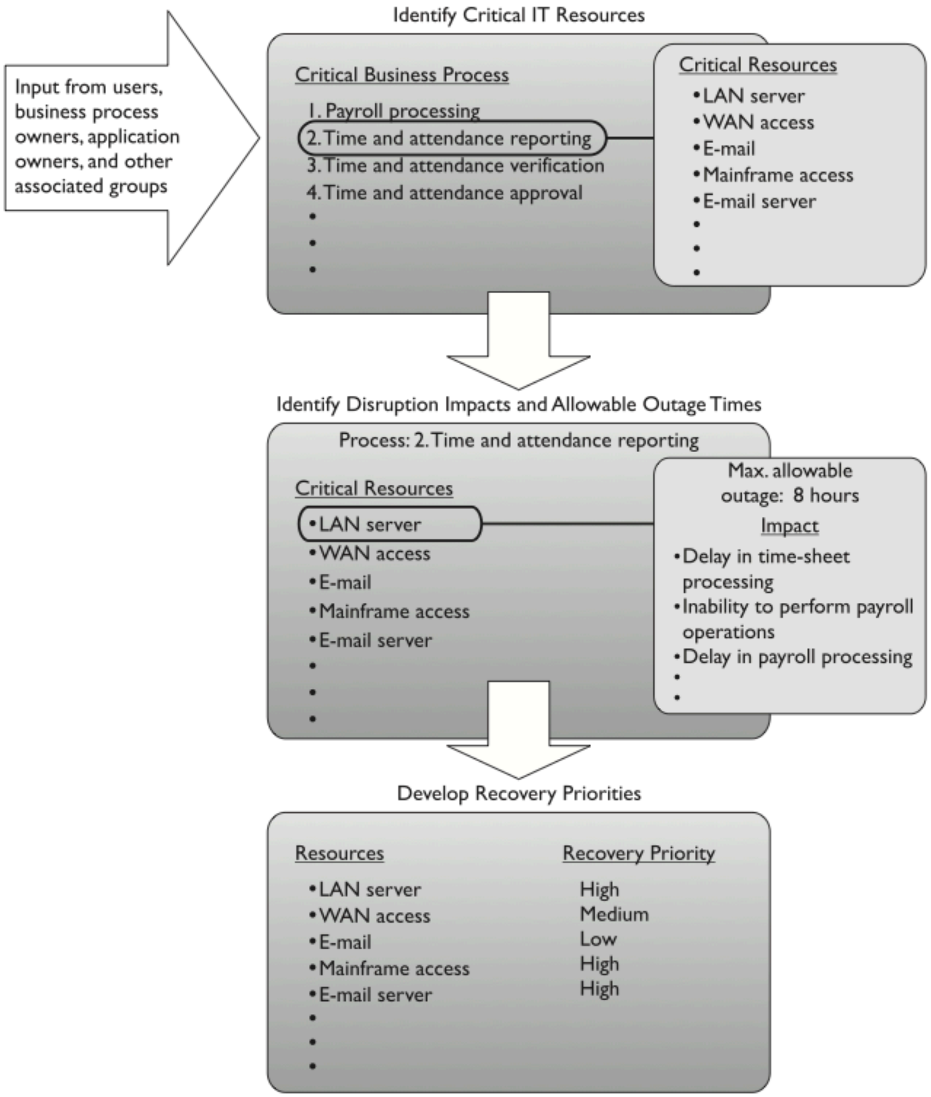
- ***Maximum tolerable downtime(MTD)*** **– the outage time that can be endured by the company.**



The following are some MTD estimates that may be used within an organization:

• **Nonessential**	30 days
• **Normal**	Seven days
• **Important**	72 hours
• **Urgent**	24 hours
• **Critical**	Minutes to hours

Dependency…



Identify Critical IT Resources

Input from users, business process owners, application owners, and other associated groups

Critical Business Process

1. Payroll processing
2. Time and attendance reporting
3. Time and attendance verification
4. Time and attendance approval

-
-
-

Critical Resources

- LAN server
- WAN access
- E-mail
- Mainframe access
- E-mail server
-
-
-

Identify Disruption Impacts and Allowable Outage Times

Process: 2. Time and attendance reporting

Critical Resources

- LAN server
- WAN access
- E-mail
- Mainframe access
- E-mail server
-
-
-

Max. allowable outage: 8 hours

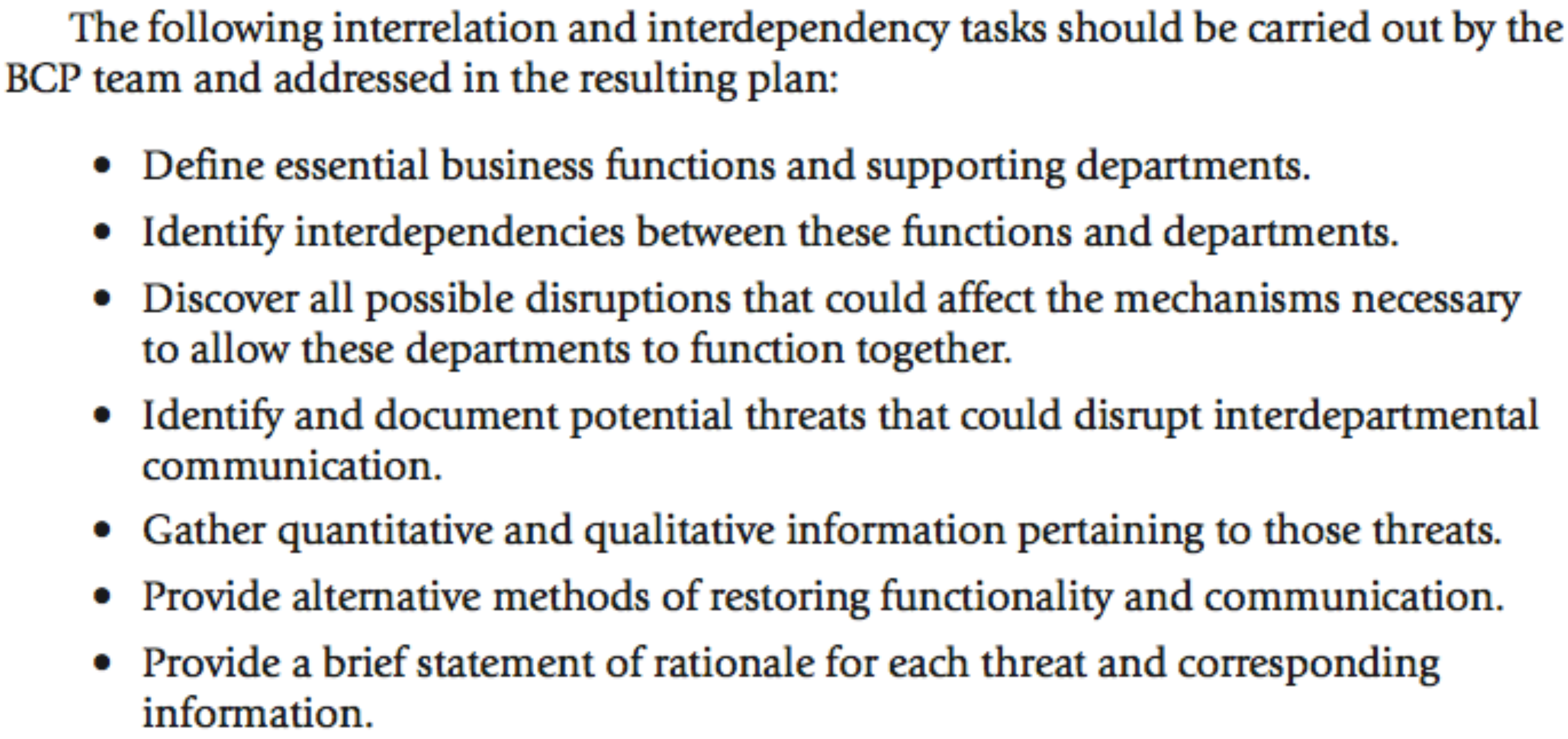
Impact

- Delay in time-sheet processing
- Inability to perform payroll operations
- Delay in payroll processing
-
-

Develop Recovery Priorities

Resources	Recovery Priority
• LAN server	High
• WAN access	Medium
• E-mail	Low
• Mainframe access	High
• E-mail server	High
•	
•	
•	

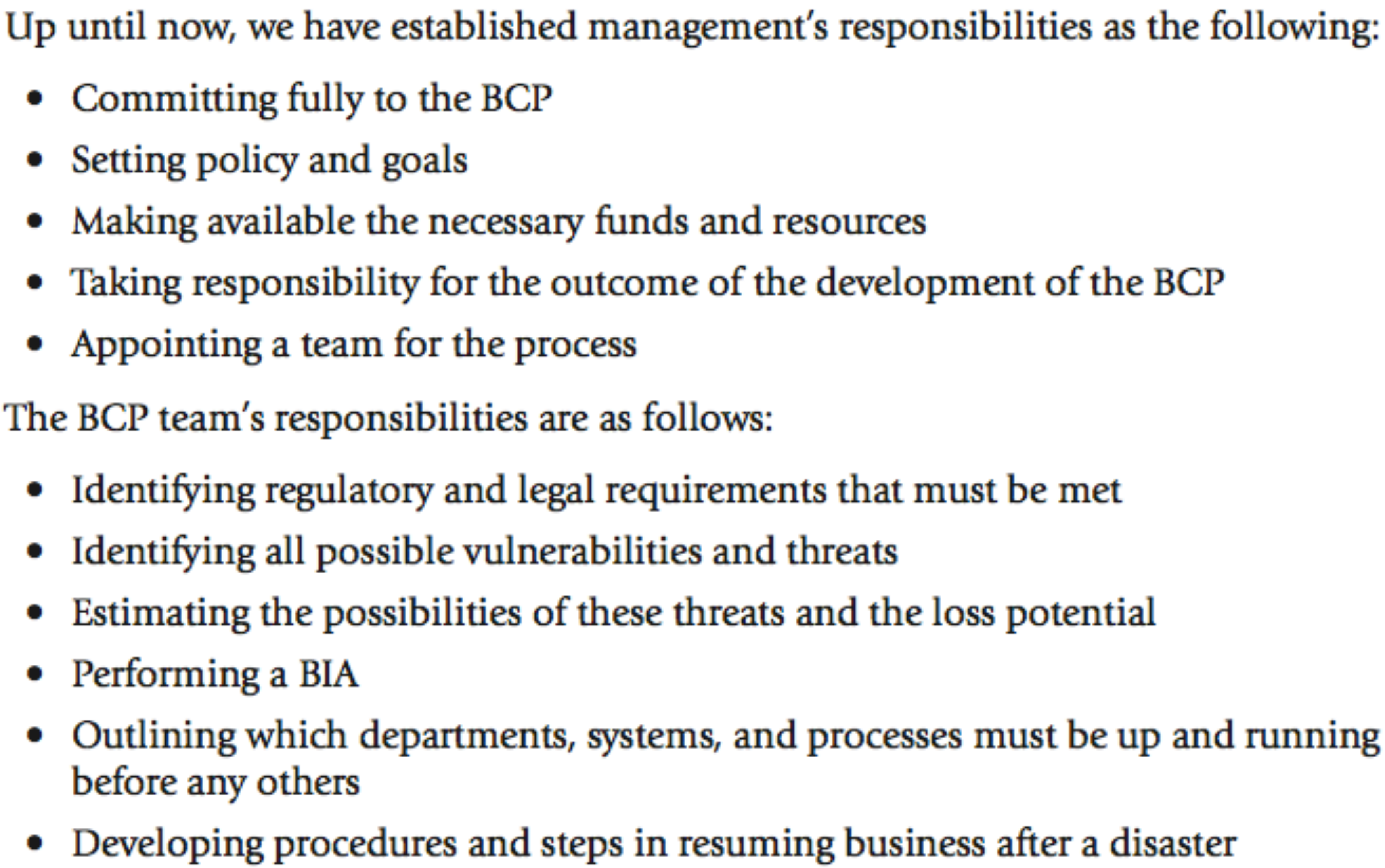
Dependency (continued)



The following interrelation and interdependency tasks should be carried out by the BCP team and addressed in the resulting plan:

- Define essential business functions and supporting departments.
- Identify interdependencies between these functions and departments.
- Discover all possible disruptions that could affect the mechanisms necessary to allow these departments to function together.
- Identify and document potential threats that could disrupt interdepartmental communication.
- Gather quantitative and qualitative information pertaining to those threats.
- Provide alternative methods of restoring functionality and communication.
- Provide a brief statement of rationale for each threat and corresponding information.

Responsibilities (more)



Up until now, we have established management's responsibilities as the following:

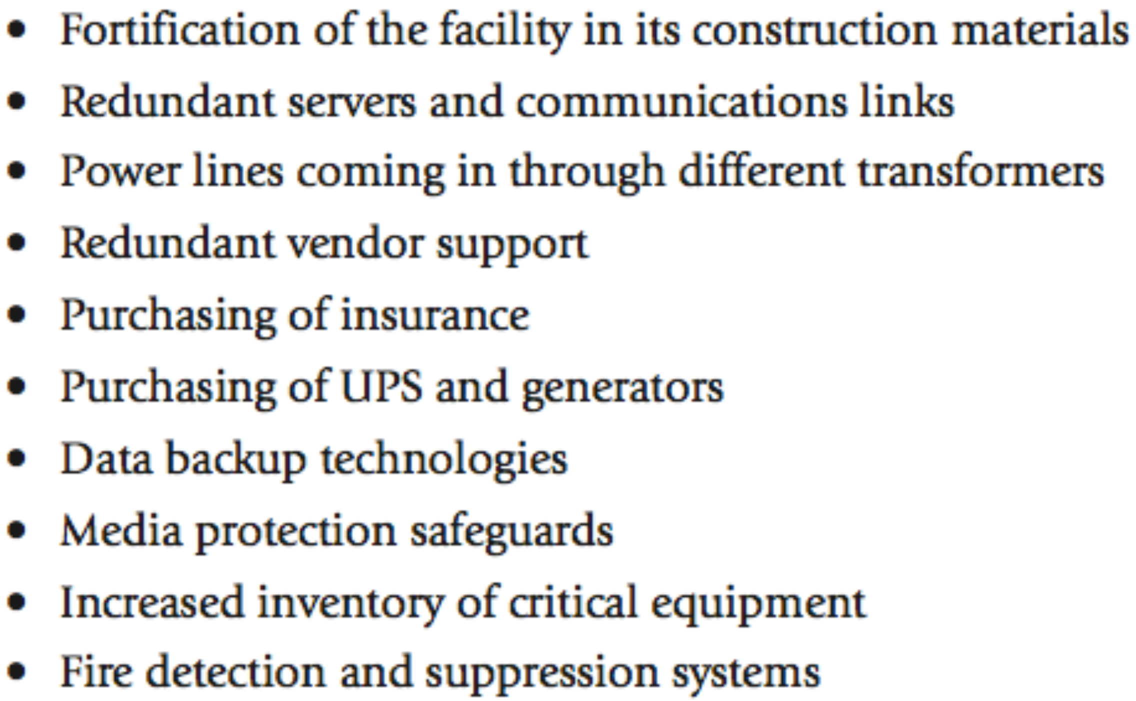
- Committing fully to the BCP
- Setting policy and goals
- Making available the necessary funds and resources
- Taking responsibility for the outcome of the development of the BCP
- Appointing a team for the process

The BCP team's responsibilities are as follows:

- Identifying regulatory and legal requirements that must be met
- Identifying all possible vulnerabilities and threats
- Estimating the possibilities of these threats and the loss potential
- Performing a BIA
- Outlining which departments, systems, and processes must be up and running before any others
- Developing procedures and steps in resuming business after a disaster

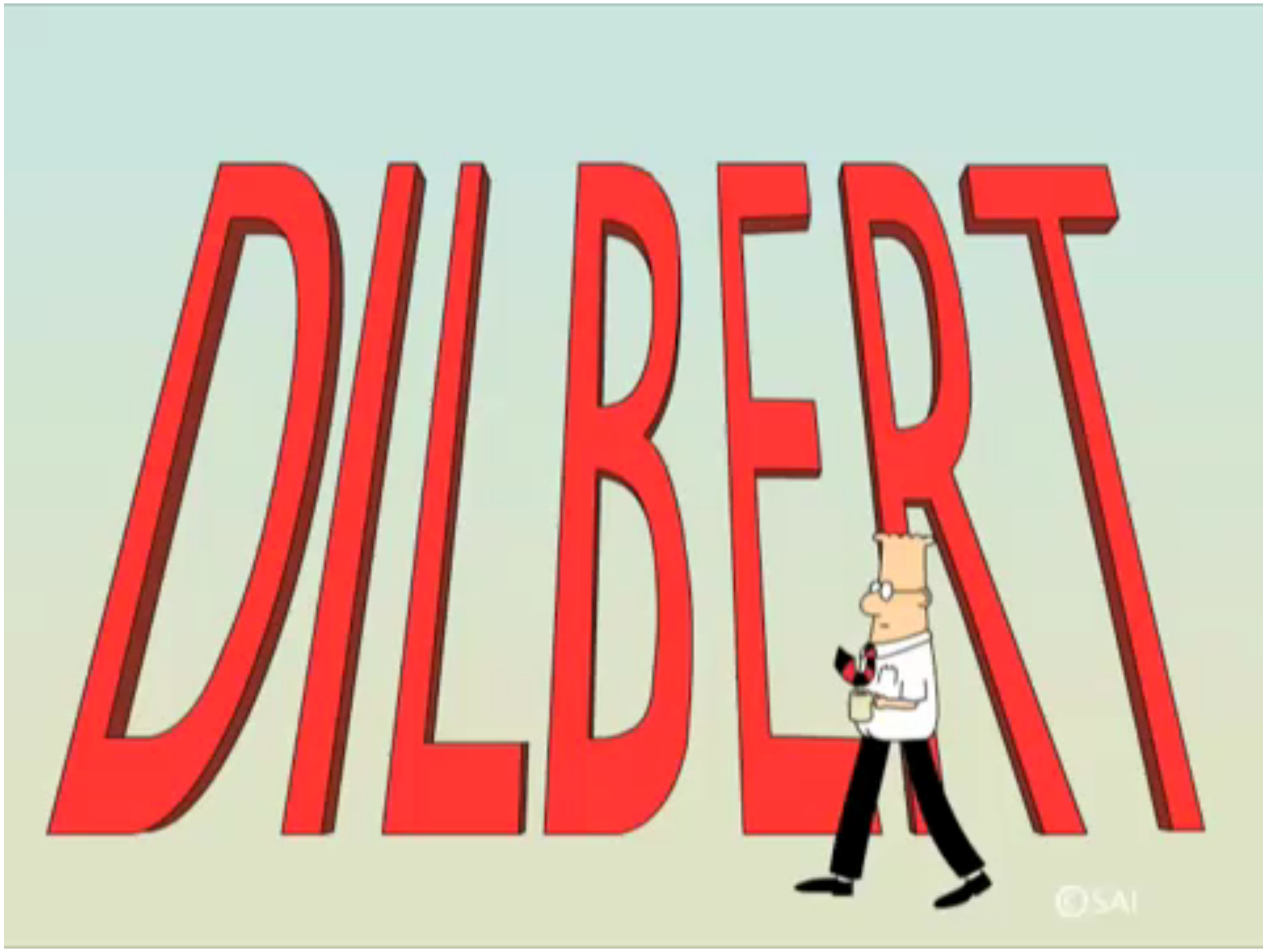
The BIA gives us…

- a guide as to how we should protect ourselves from the things that will cost us the most should they happen.
- EX:



- Fortification of the facility in its construction materials
- Redundant servers and communications links
- Power lines coming in through different transformers
- Redundant vendor support
- Purchasing of insurance
- Purchasing of UPS and generators
- Data backup technologies
- Media protection safeguards
- Increased inventory of critical equipment
- Fire detection and suppression systems

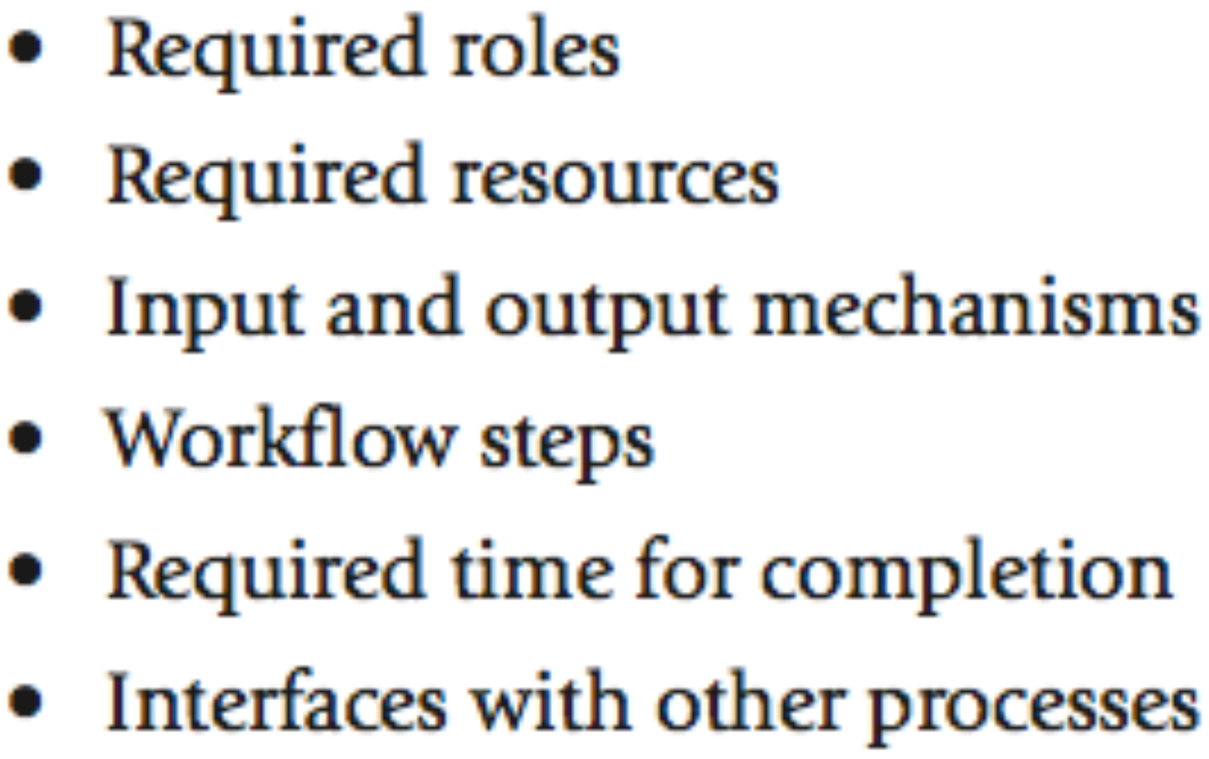
3. Recovery Strategy



Business Process Recovery

- The books example was an e-commerce site selling cars…lame…
- So here is mine – the Emperor wants to blow up a planet…
  - Validate that the DS is available
  - How long to get to range of the planet?
  - Provide with an estimate
  - Validate the order
  - Send receipt, and tracking info
  - Send coordinates to flyer dudes
  - Send command to destroy that planet

BCP Team needs to know these steps…

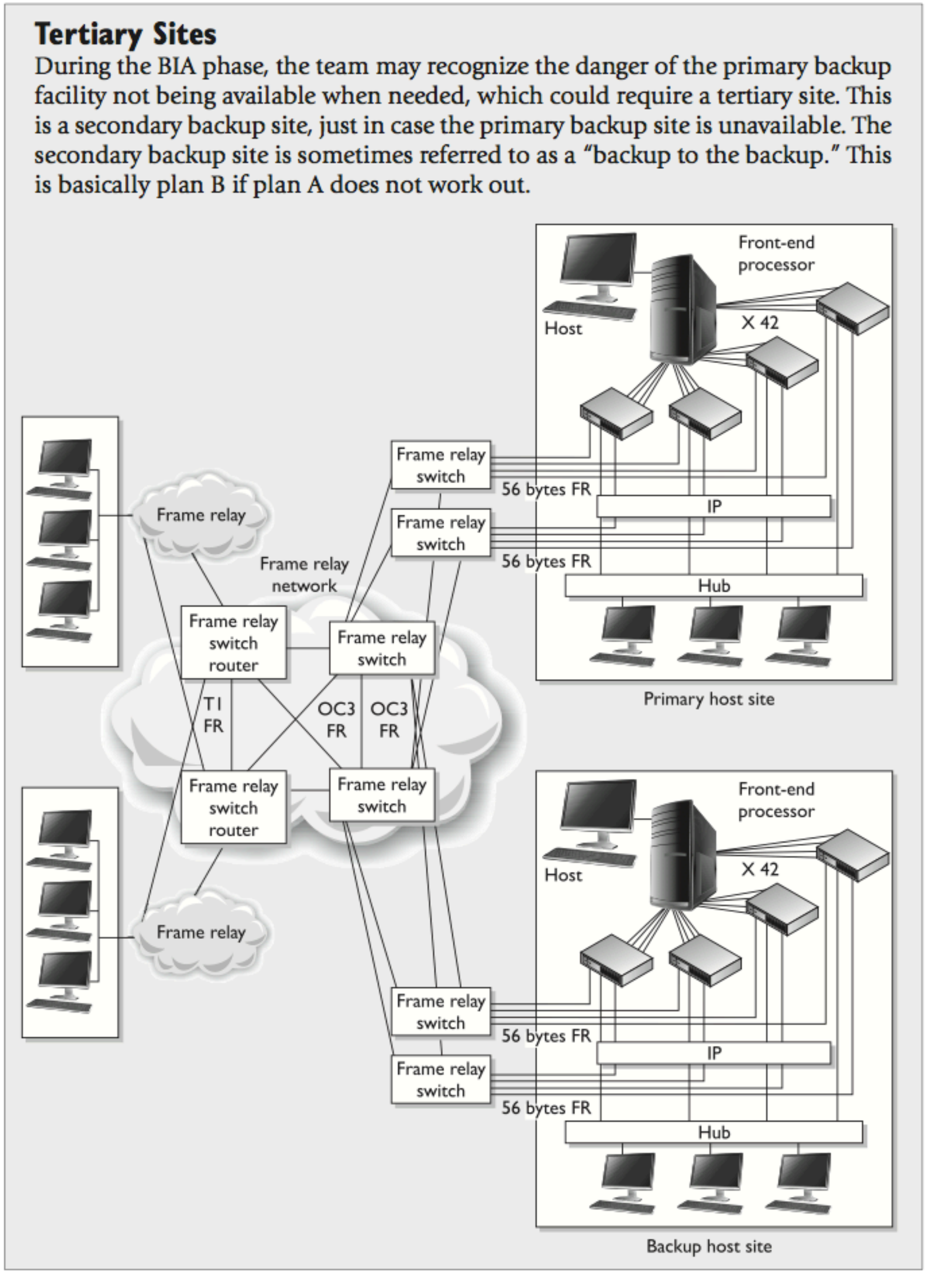


- Required roles
- Required resources
- Input and output mechanisms
- Workflow steps
- Required time for completion
- Interfaces with other processes

4. Plan Design and Development

- Non-disaster: A disruption in service due to a device malfunction or failure.
- Disaster: An event that causes the entire facility to be unusable.
- Catastrophe: A major disruption which destroys the facility.

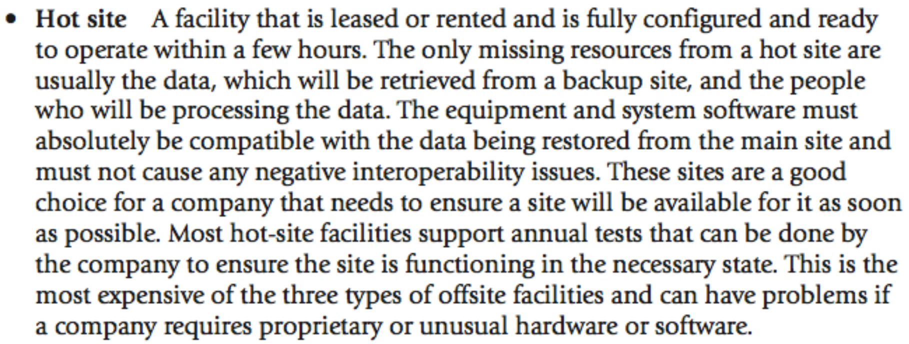
Tertiary Sites Backups



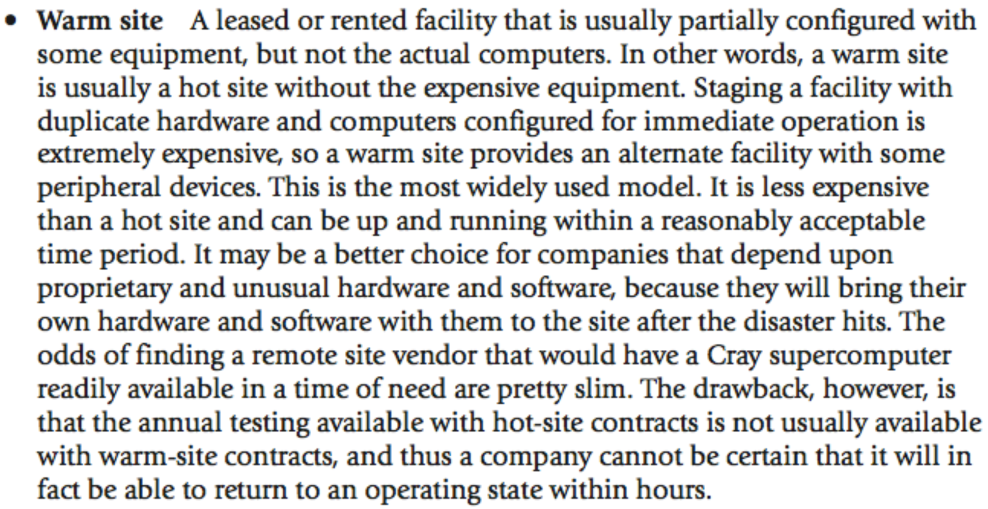
Tertiary Sites

During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site. This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a "backup to the backup." This is basically plan B if plan A does not work out.

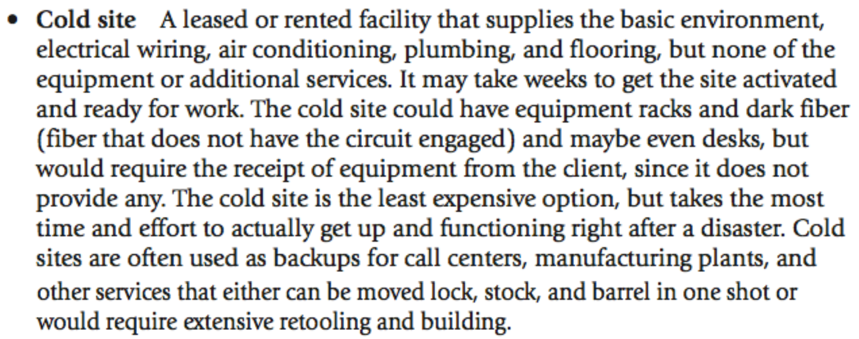
More vocabulary



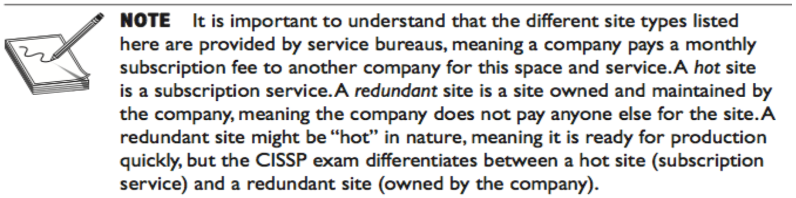
- **Hot site** A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible. Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state. This is the most expensive of the three types of offsite facilities and can have problems if a company requires proprietary or unusual hardware or software.



- **Warm site** A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It is less expensive than a hot site and can be up and running within a reasonably acceptable time period. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits. The odds of finding a remote site vendor that would have a Cray supercomputer readily available in a time of need are pretty slim. The drawback, however, is that the annual testing available with hot-site contracts is not usually available with warm-site contracts, and thus a company cannot be certain that it will in fact be able to return to an operating state within hours.

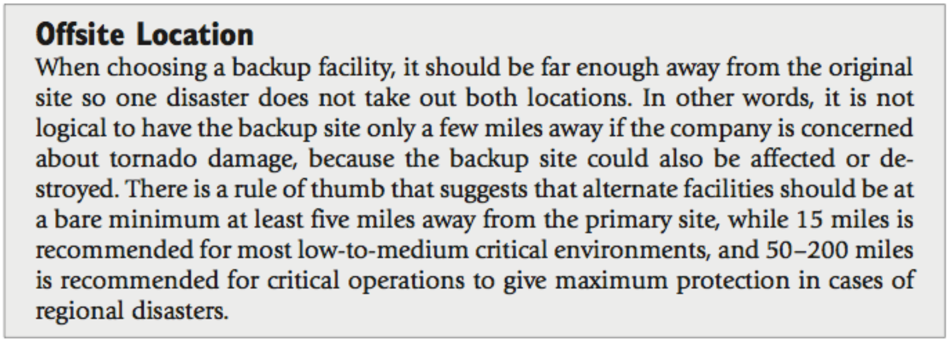


- **Cold site** A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber (fiber that does not have the circuit engaged) and maybe even desks, but would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option, but takes the most time and effort to actually get up and functioning right after a disaster. Cold sites are often used as backups for call centers, manufacturing plants, and other services that either can be moved lock, stock, and barrel in one shot or would require extensive retooling and building.



NOTE It is important to understand that the different site types listed here are provided by service bureaus, meaning a company pays a monthly subscription fee to another company for this space and service. A *hot* site is a subscription service. A *redundant* site is a site owned and maintained by the company, meaning the company does not pay anyone else for the site. A redundant site might be "hot" in nature, meaning it is ready for production quickly, but the CISSP exam differentiates between a hot site (subscription service) and a redundant site (owned by the company).

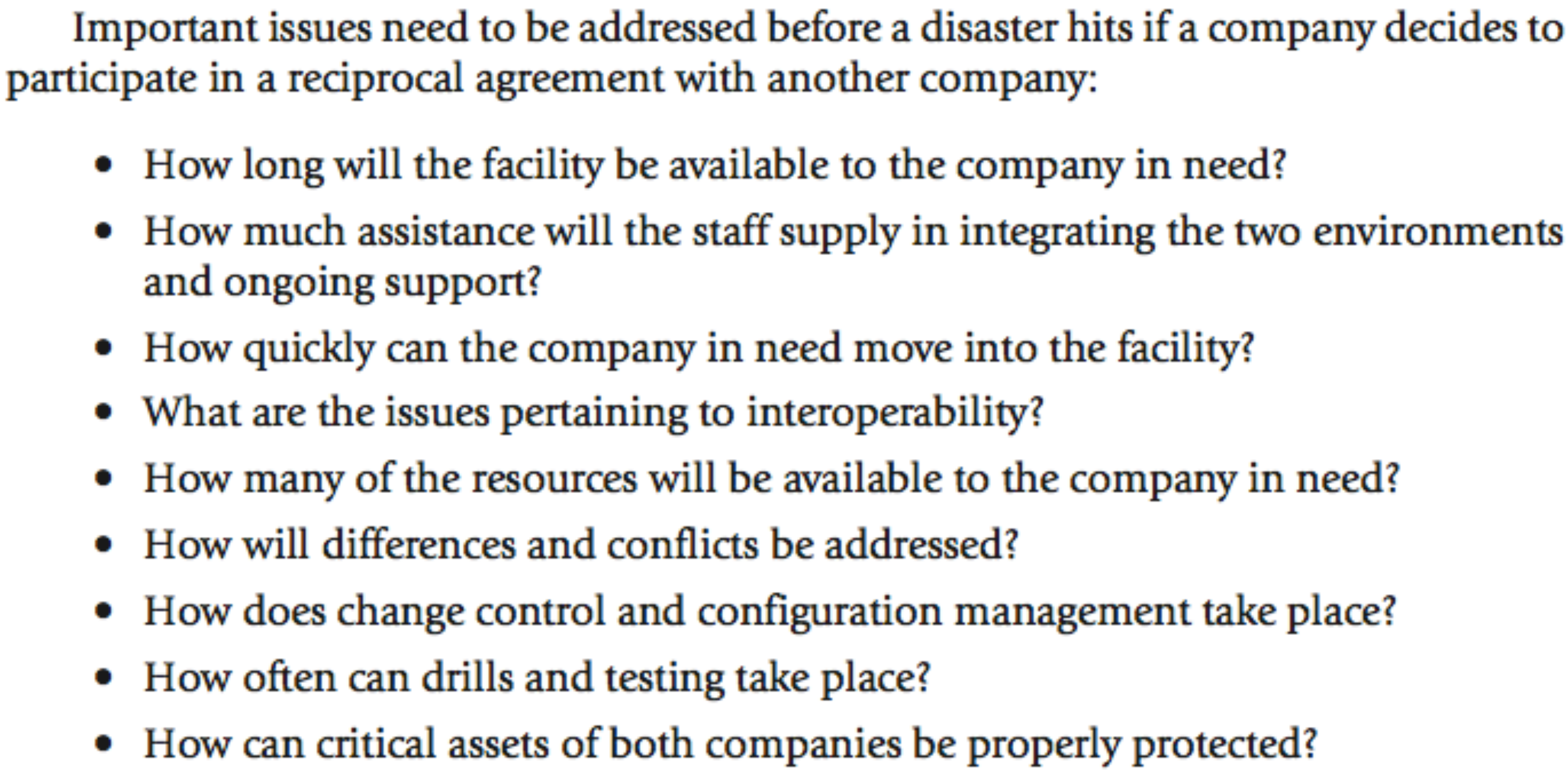
Don’t do this…



Offsite Location

When choosing a backup facility, it should be far enough away from the original site so one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed. There is a rule of thumb that suggests that alternate facilities should be at a bare minimum at least five miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50–200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Reciprocal Agreement

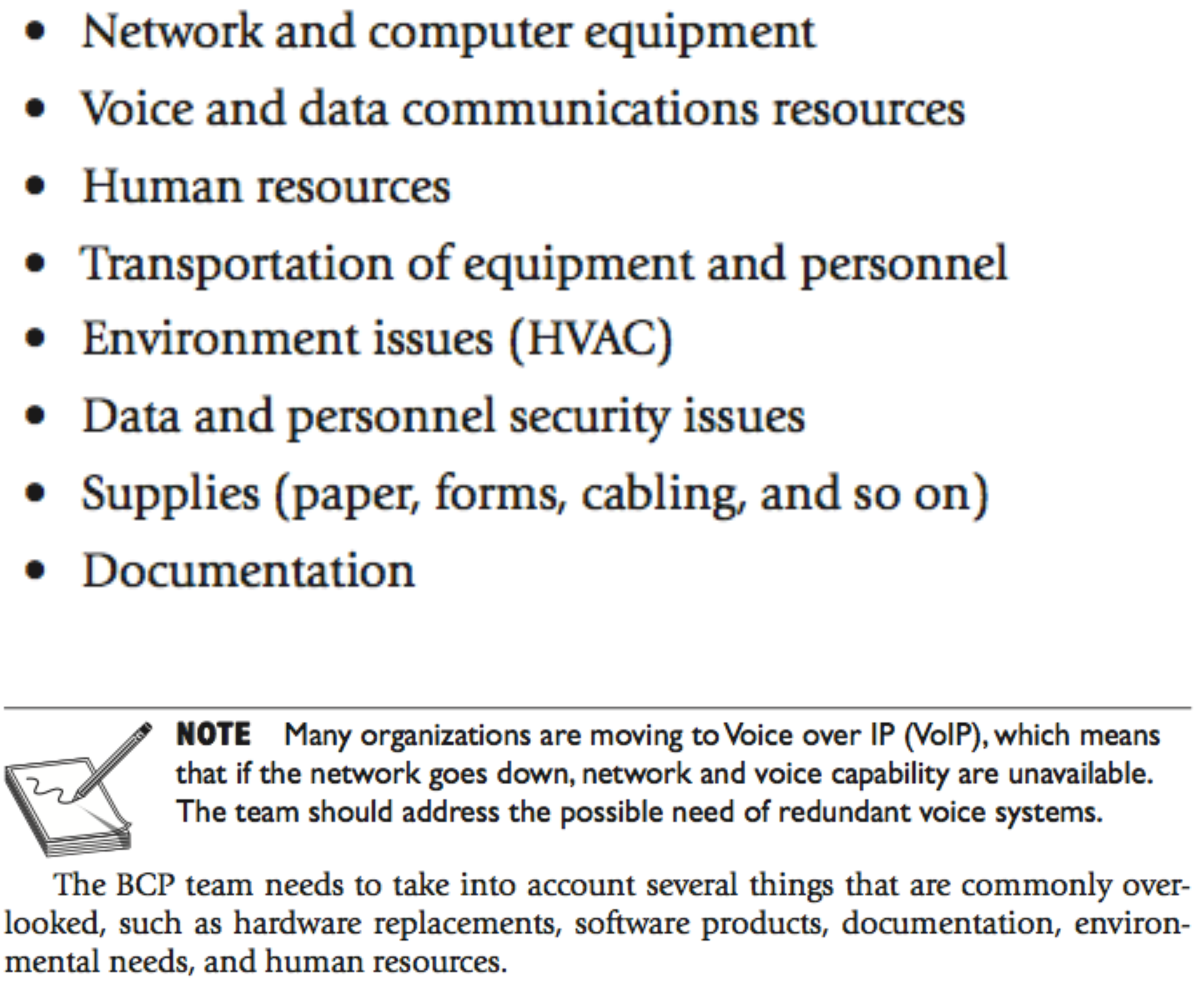


Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

- How long will the facility be available to the company in need?
- How much assistance will the staff supply in integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the resources will be available to the company in need?
- How will differences and conflicts be addressed?
- How does change control and configuration management take place?
- How often can drills and testing take place?
- How can critical assets of both companies be properly protected?

Supply and technology recovery

- **Granular level backup items:**



- Network and computer equipment
- Voice and data communications resources
- Human resources
- Transportation of equipment and personnel
- Environment issues (HVAC)
- Data and personnel security issues
- Supplies (paper, forms, cabling, and so on)
- Documentation

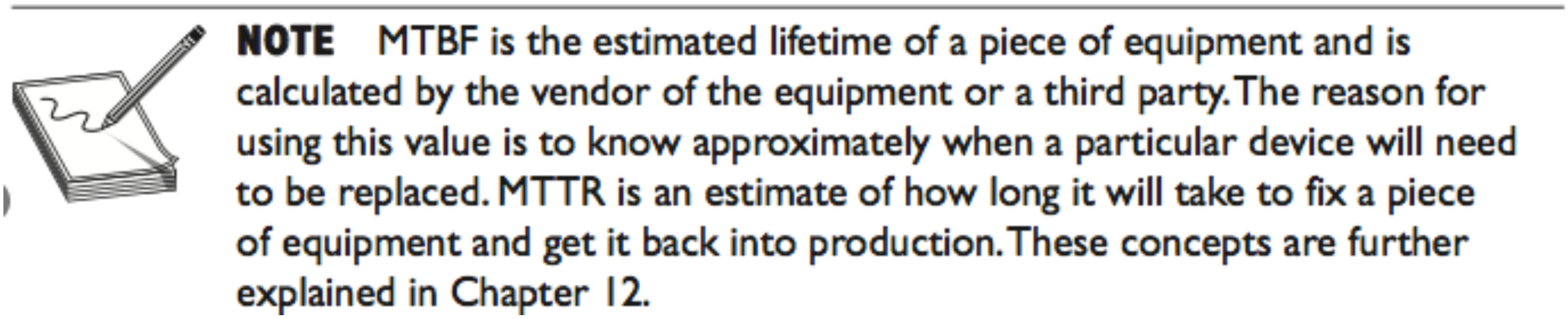
NOTE Many organizations are moving to Voice over IP (VoIP), which means that if the network goes down, network and voice capability are unavailable. The team should address the possible need of redundant voice systems.

The BCP team needs to take into account several things that are commonly overlooked, such as hardware replacements, software products, documentation, environmental needs, and human resources.

Hardware backups

- Usually a plan of keeping machine images and buying equipment as it is needed.

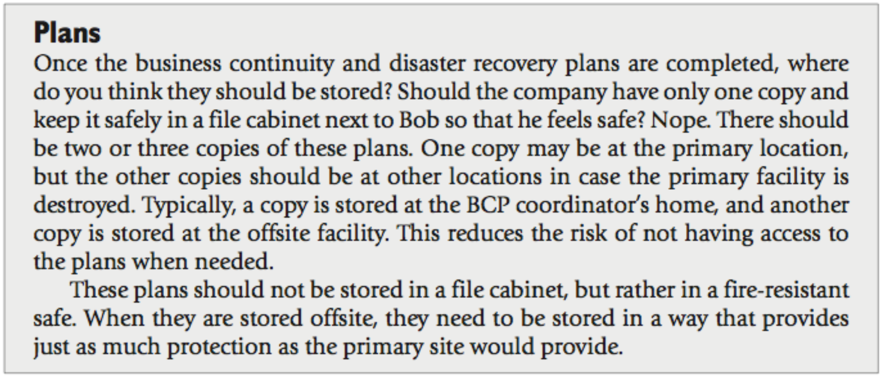
- Service level agreement needs to specify a delivery time for the equipment.



NOTE MTBF is the estimated lifetime of a piece of equipment and is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. MTTR is an estimate of how long it will take to fix a piece of equipment and get it back into production. These concepts are further explained in Chapter 12.

Documentation

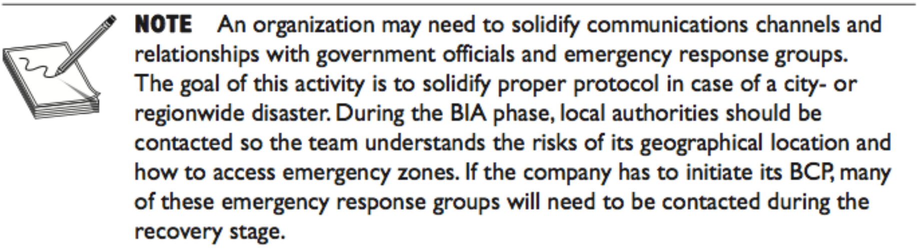
- Write down the plan…(seriously, this was a whole page in the book…der)



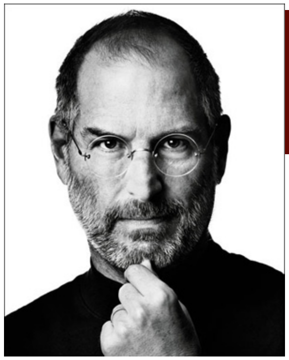
Plans

Once the business continuity and disaster recovery plans are completed, where do you think they should be stored? Should the company have only one copy and keep it safely in a file cabinet next to Bob so that he feels safe? Nope. There should be two or three copies of these plans. One copy may be at the primary location, but the other copies should be at other locations in case the primary facility is destroyed. Typically, a copy is stored at the BCP coordinator's home, and another copy is stored at the offsite facility. This reduces the risk of not having access to the plans when needed.

These plans should not be stored in a file cabinet, but rather in a fire-resistant safe. When they are stored offsite, they need to be stored in a way that provides just as much protection as the primary site would provide.



NOTE An organization may need to solidify communications channels and relationships with government officials and emergency response groups. The goal of this activity is to solidify proper protocol in case of a city- or regionwide disaster. During the BIA phase, local authorities should be contacted so the team understands the risks of its geographical location and how to access emergency zones. If the company has to initiate its BCP, many of these emergency response groups will need to be contacted during the recovery stage.



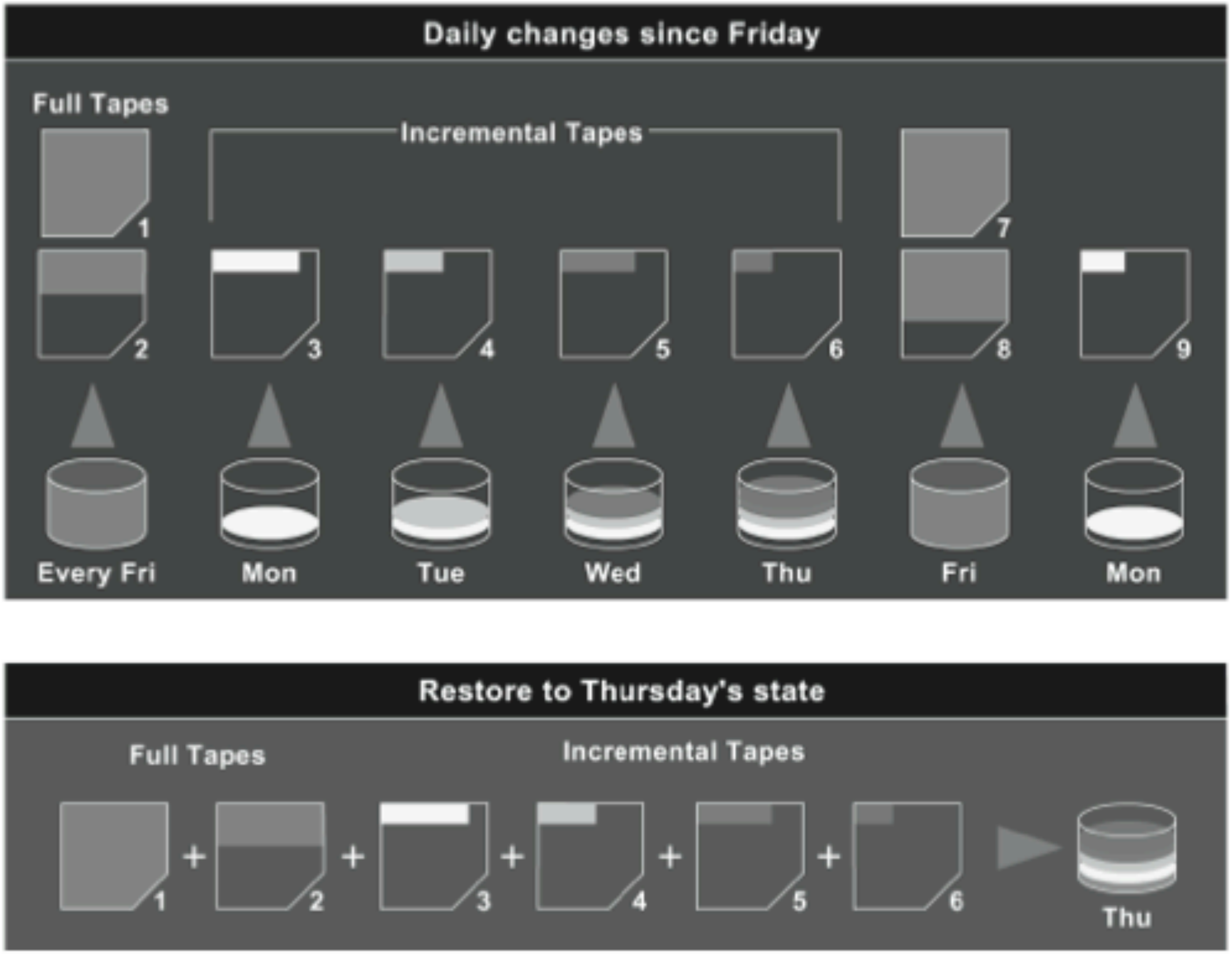
Human resources

- *Executive succession planning* – deputies, replacements, etc. Still has an effects…
- How are you going to get people to work a backup site 250 miles away?
- Usually a skeleton team, so need to identify the critical functions.

5. Implementation

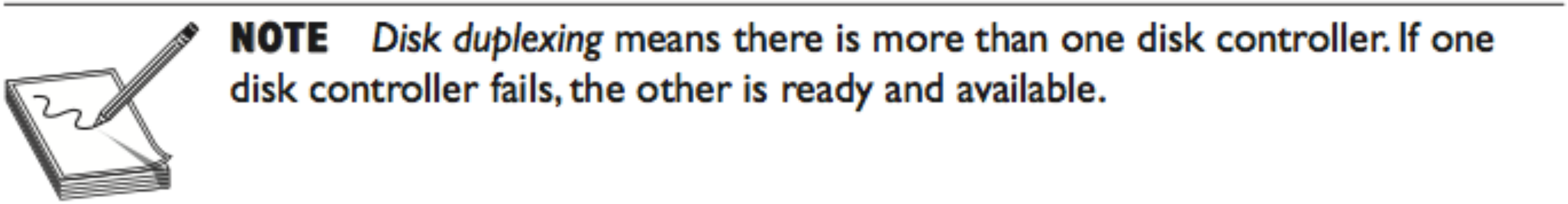
- Data Backups
- Different types of media stored in different locations
- Definitions and steps –
  - 1) *full backup* – all data saved
  - 2) *differential process* – saves the modified files since↓, restore full, then differential
  - 3) *last full backup* – last full backup
  - 4) *incremental process* – back up all the files that have changed since the last full backup

Figure 9-2
Backup software may alter the archive bit.



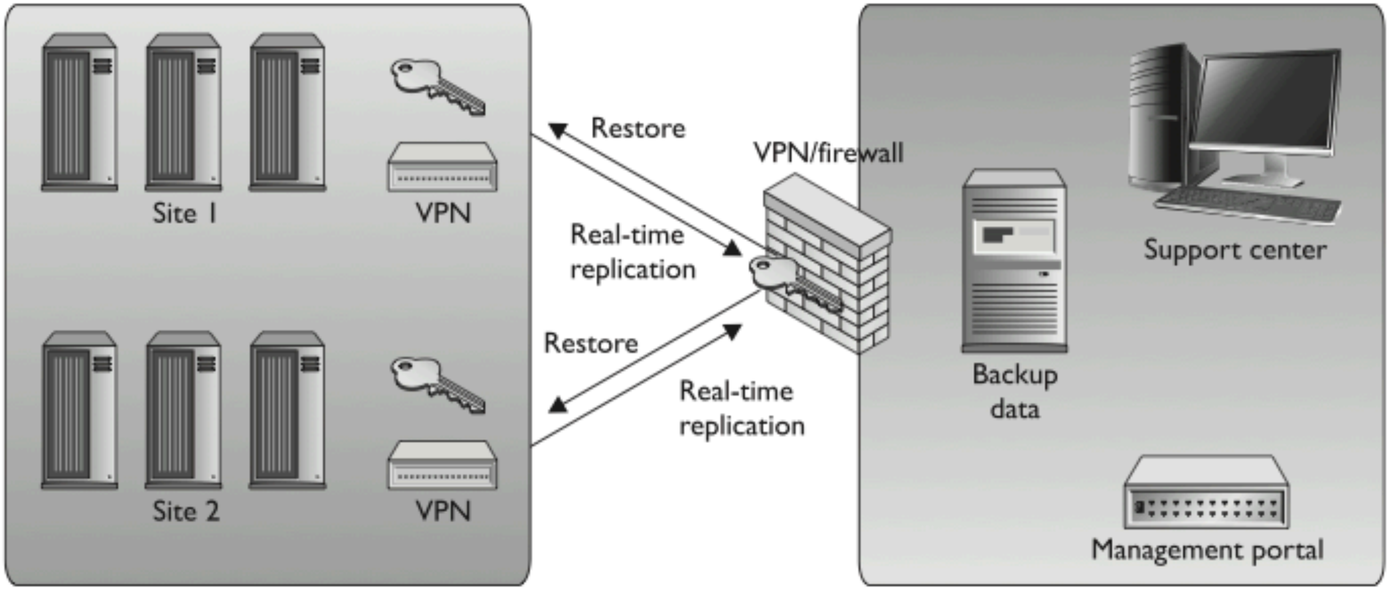
More vocabulary

- *Electronic vaulting* – makes copies of files as they are modified and periodically transmits them to an offsite backup site
- *Disk shadowing* – similar to data mirroring, provides fault tolerance by duplicating hardware and maintaining more than one copy
- *Remote journaling* – another method of transmitting data offsite, but this usually only includes moving the journal or transaction logs to the offsite facil- ity, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data.



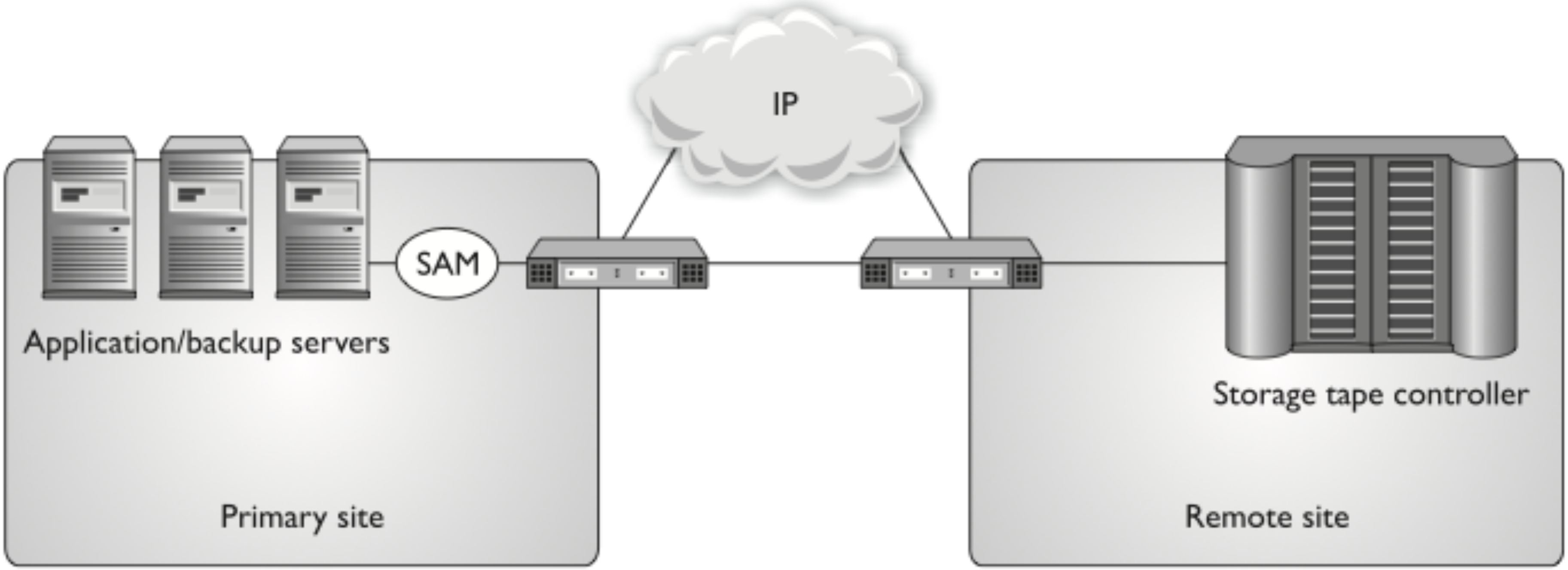
NOTE *Disk duplexing* means there is more than one disk controller. If one disk controller fails, the other is ready and available.

Make sure you can restore…



NOTE Remote journaling takes place in real time and transmits only the file deltas. Electronic vaulting takes place in batches and moves the entire file that has been updated.

Tape Vaulting - the data are sent over a serial line to a backup tape system at the offsite facility



So, basically using magic to the management…awesome diagram

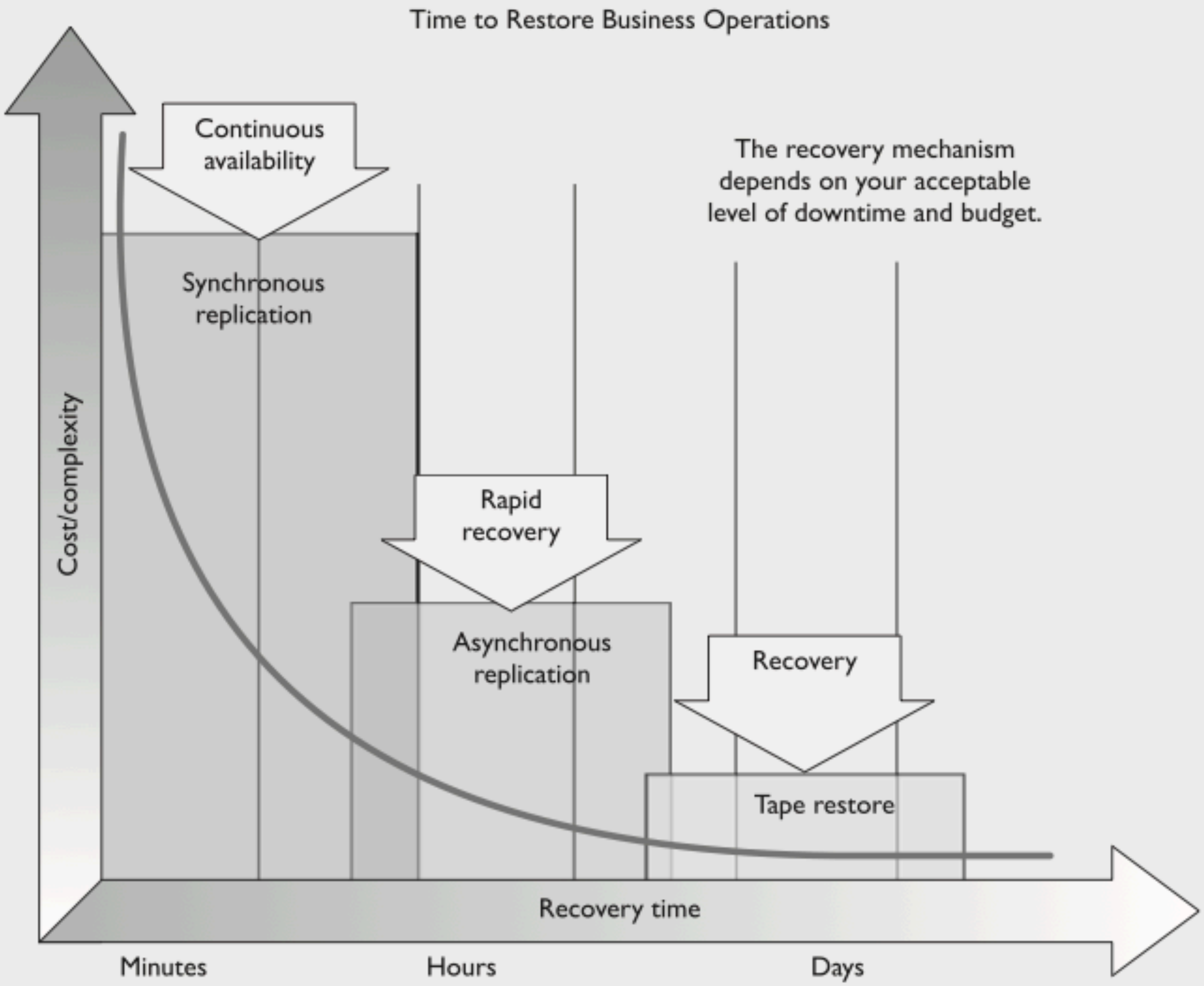
Choose a backup facility

- Can the media be accessed in the necessary timeframe?
- Is the facility closed on weekends and holidays, and does it only operate during specific hours of the day?
- Are the access control mechanisms tied to an alarm and/or the police station?
- Does the facility have the capability to protect the media from a variety of threats?
- What is the availability of a bonded transport service?
- Are there any geographical environmental hazards such as floods, earthquakes, tornadoes, and so on?
- Is there a fire detection and suppression system?
- Does the facility provide temperature and humidity monitoring and control?
- What type of physical, administrative, and logical access controls are used?

Which Data Recovery Solution?

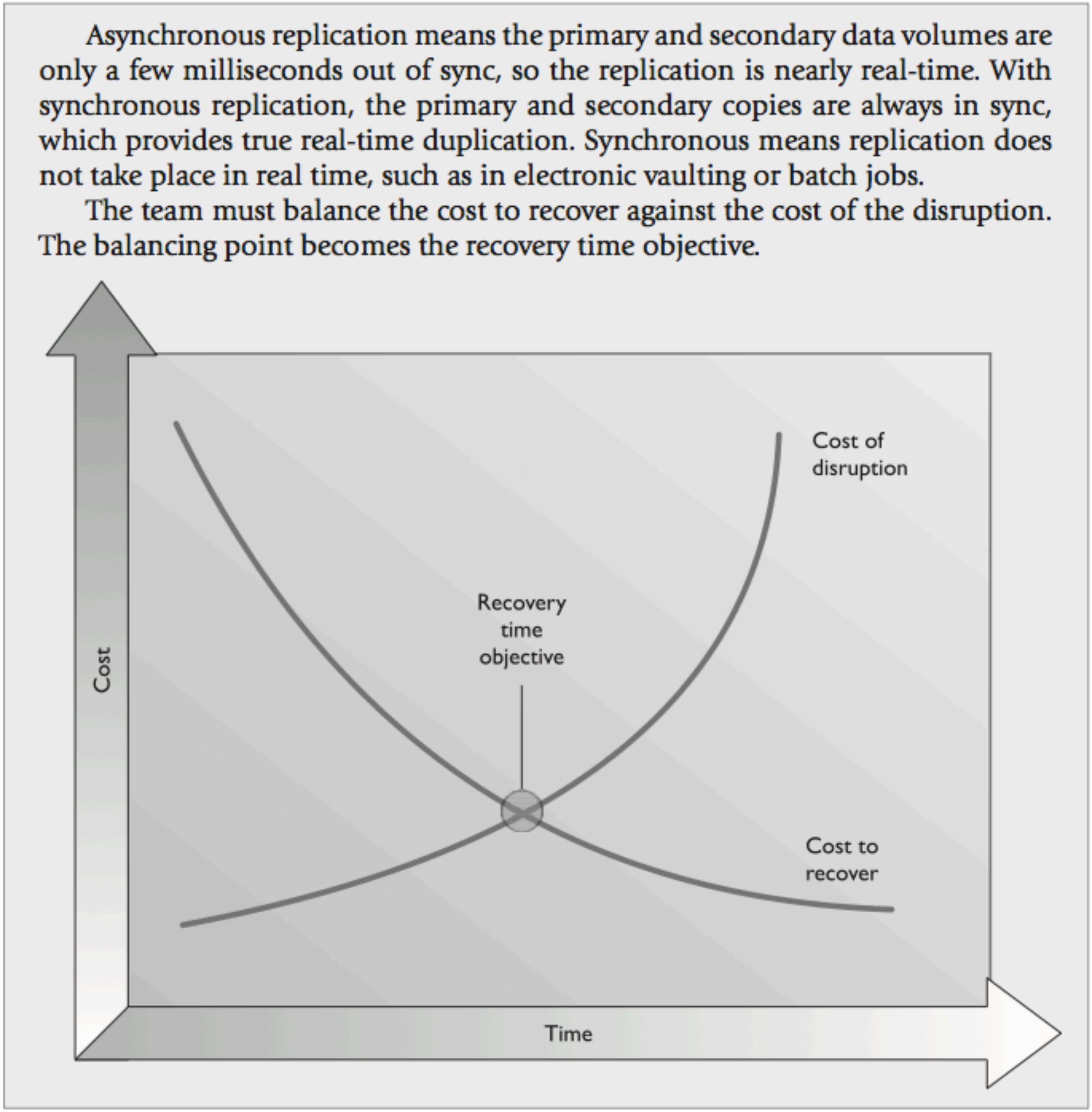
Data classification based on business criticality should have been performed by now.

- The BCP project team needs to divide the data by importance of fast recovery.
- Critical data that need to be continuously available can be restored via electronic vaulting (or remote journaling).
- Other data types can be restored via tapes or mirror systems.



Time to Restore Business Operations

The recovery mechanism depends on your acceptable level of downtime and budget.

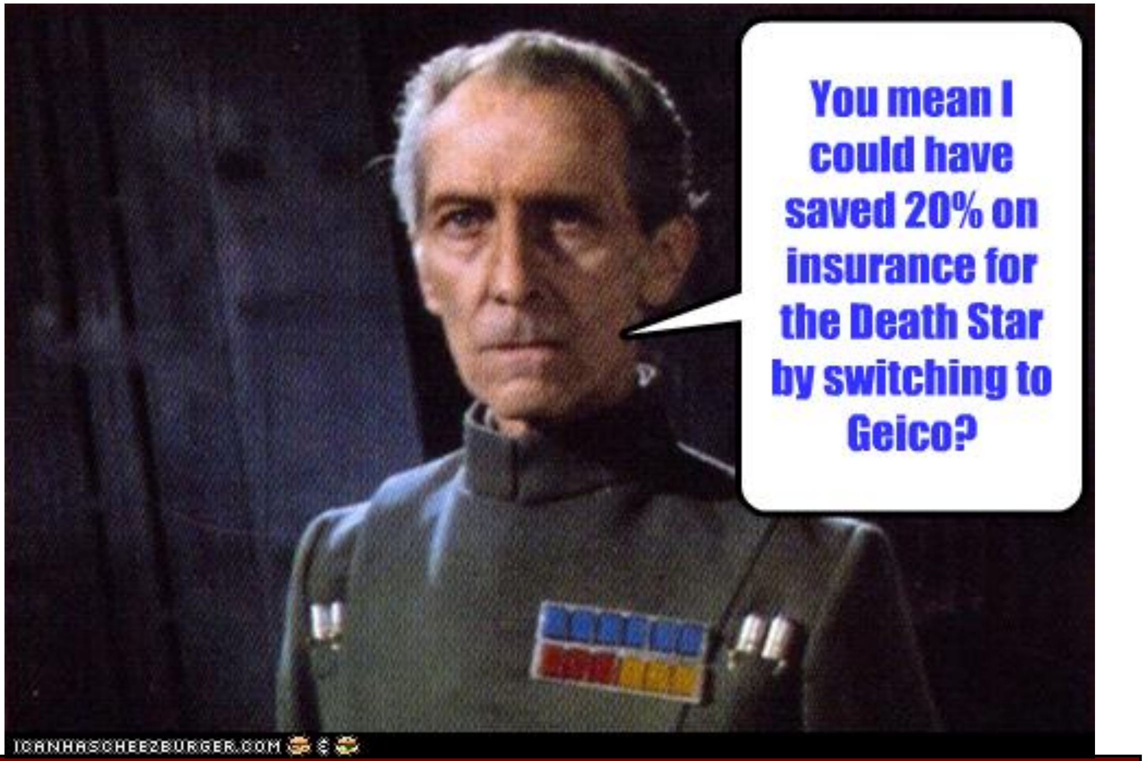


Asynchronous replication means the primary and secondary data volumes are only a few milliseconds out of sync, so the replication is nearly real-time. With synchronous replication, the primary and secondary copies are always in sync, which provides true real-time duplication. Synchronous means replication does not take place in real time, such as in electronic vaulting or batch jobs.

The team must balance the cost to recover against the cost of the disruption. The balancing point becomes the recovery time objective.

Cyberinsurance?

- Not even kidding…Cyberinsurance is a new type of coverage that insures losses caused by denial-of-service attacks, malware damages, hackers, electronic theft, privacy-related lawsuits, and more.
- A company could also choose to purchase a business interruption insurance policy.


You mean I could have saved 20% on insurance for the Death Star by switching to Geico?
ICANHASCHEEZBURGER.COM

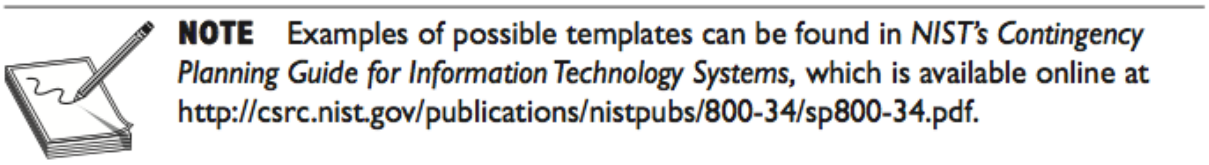
Restoration Teams

- The *restoration team* should be responsible for getting the alternate site into a working and functioning environment, and the *salvage team* should be responsible for starting the recovery of the original site.
- A role, or a team, needs to be created to carry out a damage assessment once a disaster has taken place. The assessment procedures should be properly documented and include the following steps:
  - Determine the cause of the disaster.
  - Determine the potential for further damage.
  - Identify the affected business functions and areas. Identify the level of functionality for the critical resources.
  - Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated MTD values to restore operations, then a disaster should be declared, and the BCP should be put into action.

What team to call? Reconstruction phase…

Different organizations have different criteria, because the business drivers and critical functions will vary from organization to organization. The criteria may comprise some or all of the following elements:

- **Danger to human life**
- **Danger to state or national security**
- **Damage to facility**
- **Damage to critical systems**
- **Estimated value of downtime that will be experienced**



NOTE Examples of possible templates can be found in *NIST's Contingency Planning Guide for Information Technology Systems*, which is available online at http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

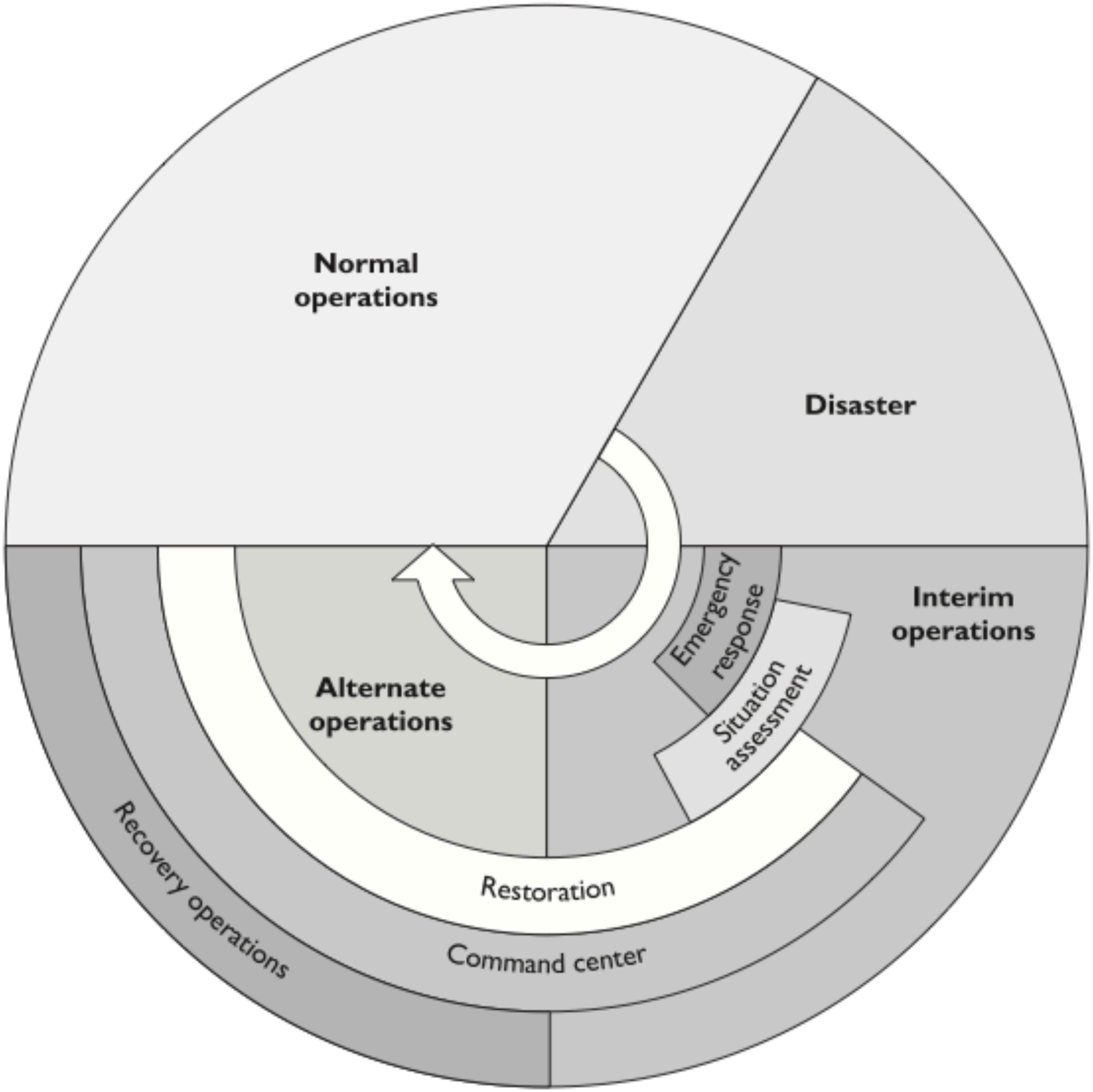
Reconstruction Issues

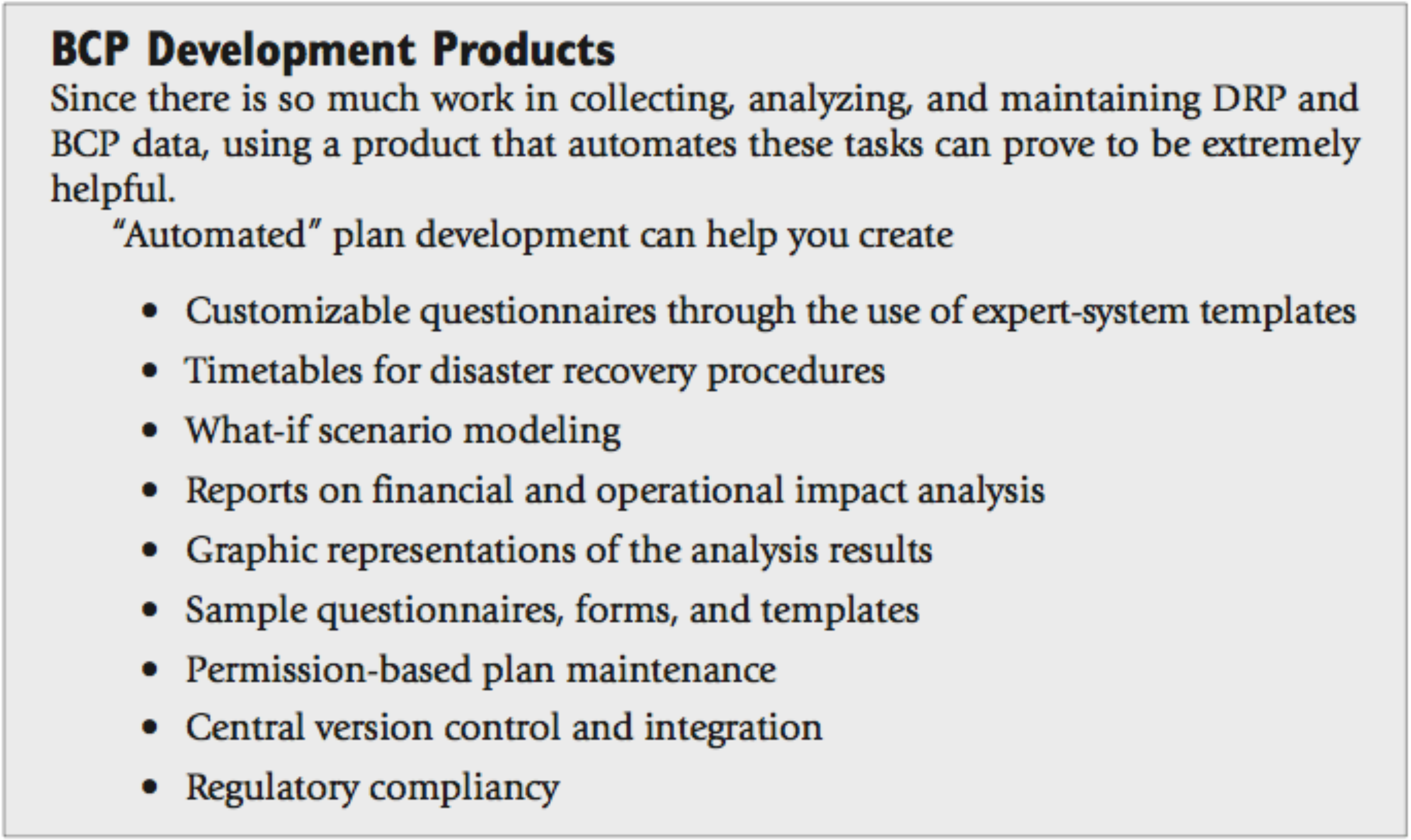
The following lists a few of these issues:

- Ensuring the safety of employees
- Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
- Ensuring that the necessary equipment and supplies are present and in working order
- Ensuring proper communications and connectivity methods are working
- Properly testing the new environment

Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:

- Back up data from the alternate site and restore it within the new facility.
- Carefully terminate contingency operations.
- Securely transport equipment and personnel to the new facility.


Normal operations
Disaster
Interim operations
Emergency response
Situation assessment
Alternate operations
Restoration
Command center
Recovery operations



BCP Development Products

Since there is so much work in collecting, analyzing, and maintaining DRP and BCP data, using a product that automates these tasks can prove to be extremely helpful.

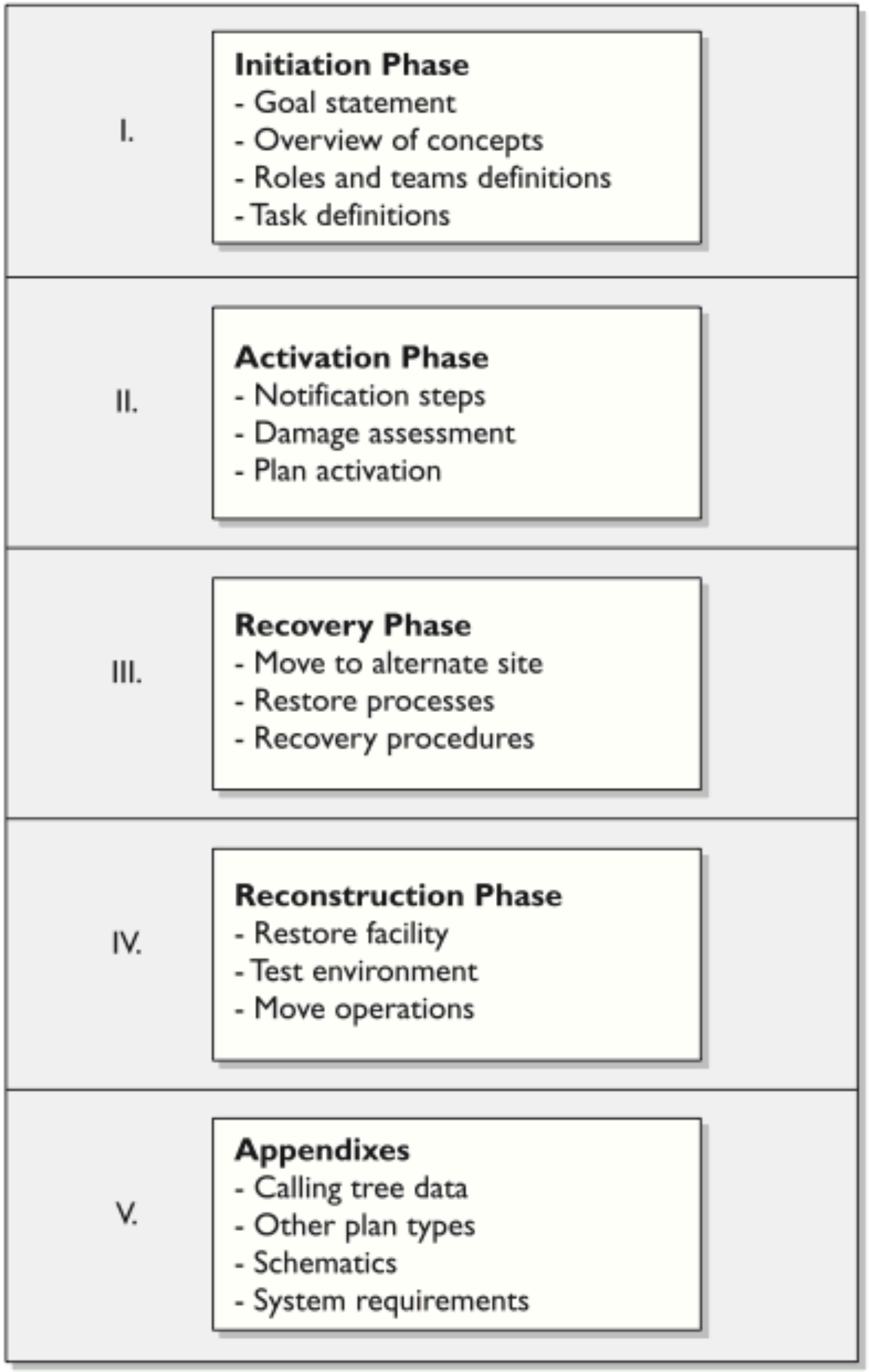
"Automated" plan development can help you create

- Customizable questionnaires through the use of expert-system templates
- Timetables for disaster recovery procedures
- What-if scenario modeling
- Reports on financial and operational impact analysis
- Graphic representations of the analysis results
- Sample questionnaires, forms, and templates
- Permission-based plan maintenance
- Central version control and integration
- Regulatory compliancy

Goals

- To be useful, a goal must contain certain key information, such as the following:
- Responsibility
  - Each individual involved with recovery and continuity should have their responsibilities spelled out in writing to ensure a clear understanding in a chaotic situation. Each task should be assigned to the individual most logically situated to handle it. These individuals must know what is expected of them, which is done through training, drills, communication, and documentation. So, for example, instead of just running out of the building screaming, an individual must know that he is responsible for shutting down the servers before he can run out of the building screaming.
- Authority
  - In times of crisis, it is important to know who is in charge. Teamwork is important in these situations, and almost every team does much better with an established and trusted leader. Such leaders must know that they are expected to step up to the plate in a time of crisis and understand what type of direction they should provide to the rest of the employees. Clear- cut authority will aid in reducing confusion and increasing cooperation.
- Priorities
  - It is extremely important to know what is critical versus what is merely nice to have. Different departments provide different functionality for an organization. The critical departments must be singled out from the departments that provide functionality that the company can live without for a week or two. It is necessary to know which department must come online first, which second, and so on. That way, the efforts are made in the most useful, effective, and focused manner. Along with the priorities of departments, the priorities of systems, information, and programs must be established. It may be necessary to ensure that the database is up and running before working to bring the file server online. The general priorities must be set by the management with the help of the different departments and IT staff.
- Implementation and testing
  - It is great to write down very profound ideas and develop plans, but unless they are actually carried out and tested, they may not add up to a hill of beans. Once a continuity plan is developed, it actually has to be put into action. It needs to be documented and put in places that are easily accessible in times of crisis. The people who are assigned specific tasks need to be taught and informed how to fulfill those tasks, and dry runs must be done to walk people through different situations. The drills should take place at least once a year, and the entire program should be continually updated and improved.

Figure 9-3
The general structure of a business continuity plan



I.

Initiation Phase
- Goal statement
- Overview of concepts
- Roles and teams definitions
- Task definitions

II.

Activation Phase
- Notification steps
- Damage assessment
- Plan activation

III.

Recovery Phase
- Move to alternate site
- Restore processes
- Recovery procedures

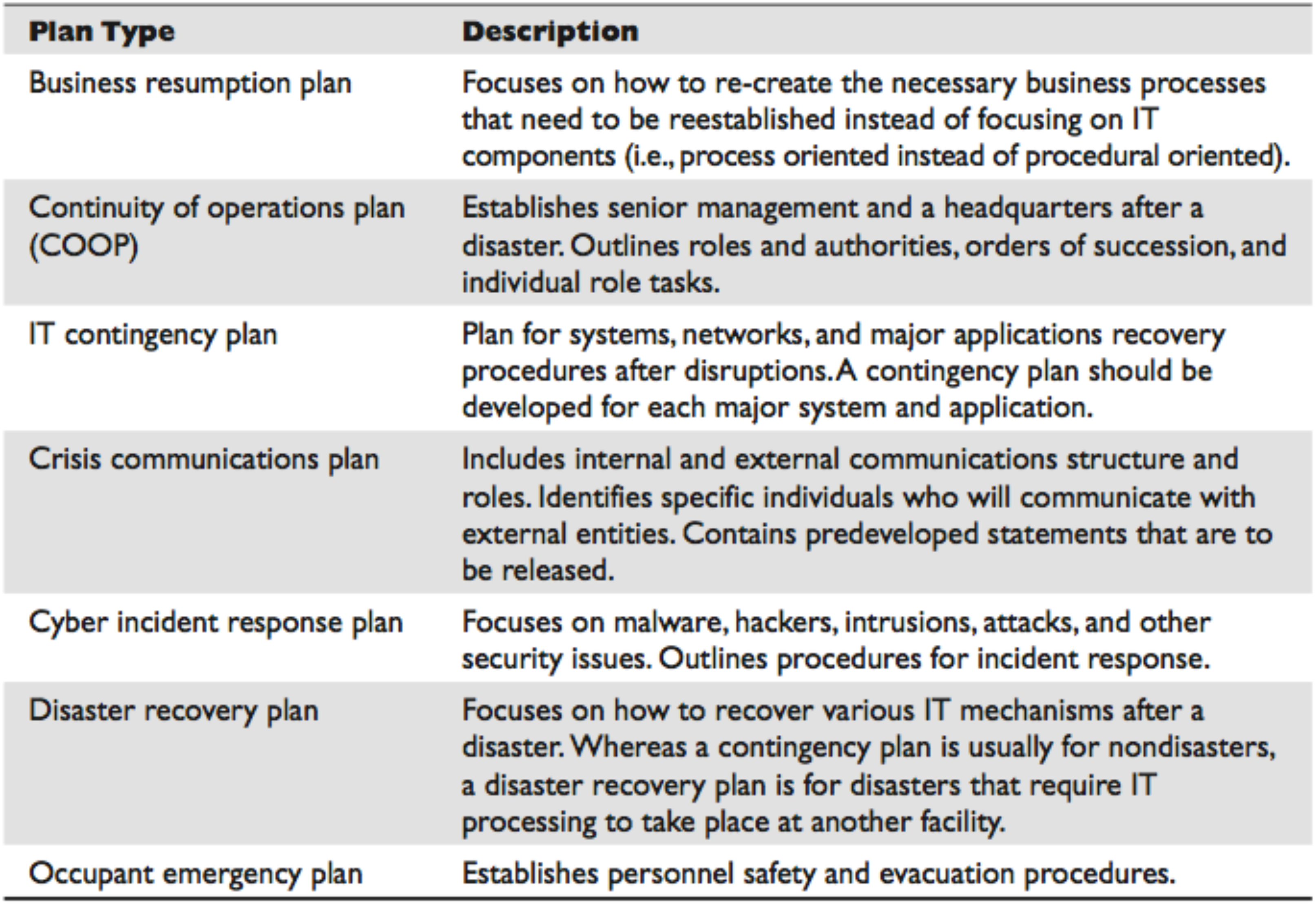
IV.

Reconstruction Phase
- Restore facility
- Test environment
- Move operations

V.

Appendixes
- Calling tree data
- Other plan types
- Schematics
- System requirements

6. Testing



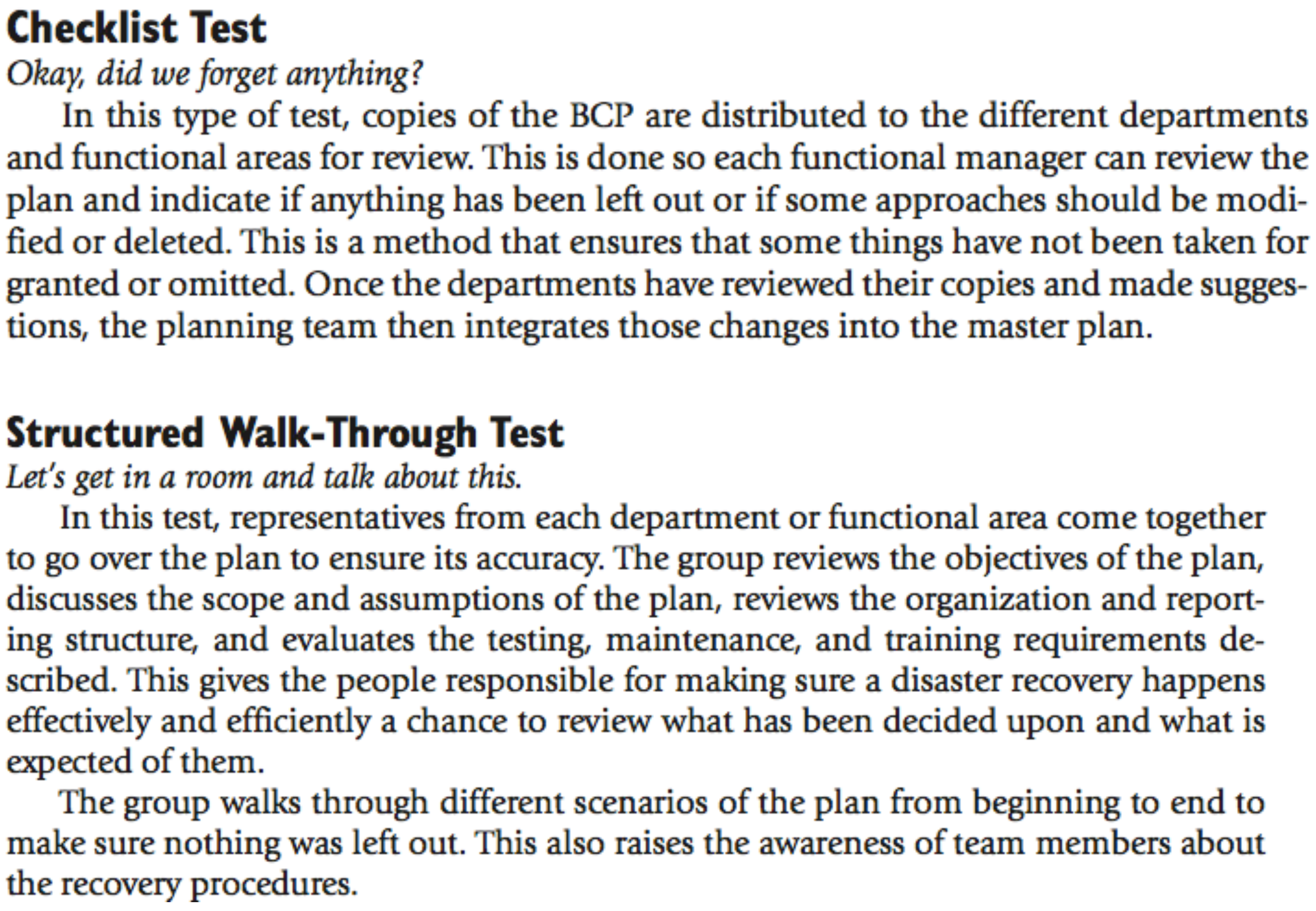
Plan Type	Description
Business resumption plan	Focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on IT components (i.e., process oriented instead of procedural oriented).
Continuity of operations plan (COOP)	Establishes senior management and a headquarters after a disaster. Outlines roles and authorities, orders of succession, and individual role tasks.
IT contingency plan	Plan for systems, networks, and major applications recovery procedures after disruptions. A contingency plan should be developed for each major system and application.
Crisis communications plan	Includes internal and external communications structure and roles. Identifies specific individuals who will communicate with external entities. Contains predeveloped statements that are to be released.
Cyber incident response plan	Focuses on malware, hackers, intrusions, attacks, and other security issues. Outlines procedures for incident response.
Disaster recovery plan	Focuses on how to recover various IT mechanisms after a disaster. Whereas a contingency plan is usually for nondisasters, a disaster recovery plan is for disasters that require IT processing to take place at another facility.
Occupant emergency plan	Establishes personnel safety and evacuation procedures.

Table 9-2 Different Types of Recovery Plans

Testing Factoids -

- Should be performed annually
- Exercises vs. test. Test pass/fail. Exercises to learn.
- Prepare personnel for what they might face.
- The team of testers must agree upon what exactly is getting tested and how to properly determine success or failure. The team must agree upon the timing and duration of the exercise, who will participate in the exercise, who will receive which assignments, and what steps should be taken. Also, the team needs to determine whether hardware, software, personnel, procedures, and communications lines are going to be tested, and whether it is some, all, or a subset combination.
  - Choose a subset to train a small sub-group at first, and then when everyone is ready take the time of the whole group.

Types of tests



Checklist Test

Okay, did we forget anything?

In this type of test, copies of the BCP are distributed to the different departments and functional areas for review. This is done so each functional manager can review the plan and indicate if anything has been left out or if some approaches should be modified or deleted. This is a method that ensures that some things have not been taken for granted or omitted. Once the departments have reviewed their copies and made suggestions, the planning team then integrates those changes into the master plan.

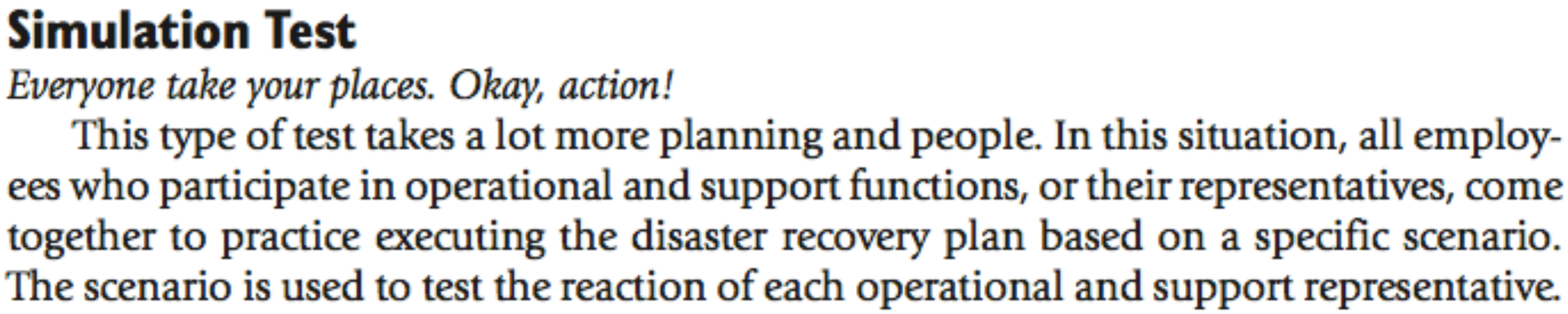
Structured Walk-Through Test

Let's get in a room and talk about this.

In this test, representatives from each department or functional area come together to go over the plan to ensure its accuracy. The group reviews the objectives of the plan, discusses the scope and assumptions of the plan, reviews the organization and reporting structure, and evaluates the testing, maintenance, and training requirements described. This gives the people responsible for making sure a disaster recovery happens effectively and efficiently a chance to review what has been decided upon and what is expected of them.

The group walks through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of team members about the recovery procedures.

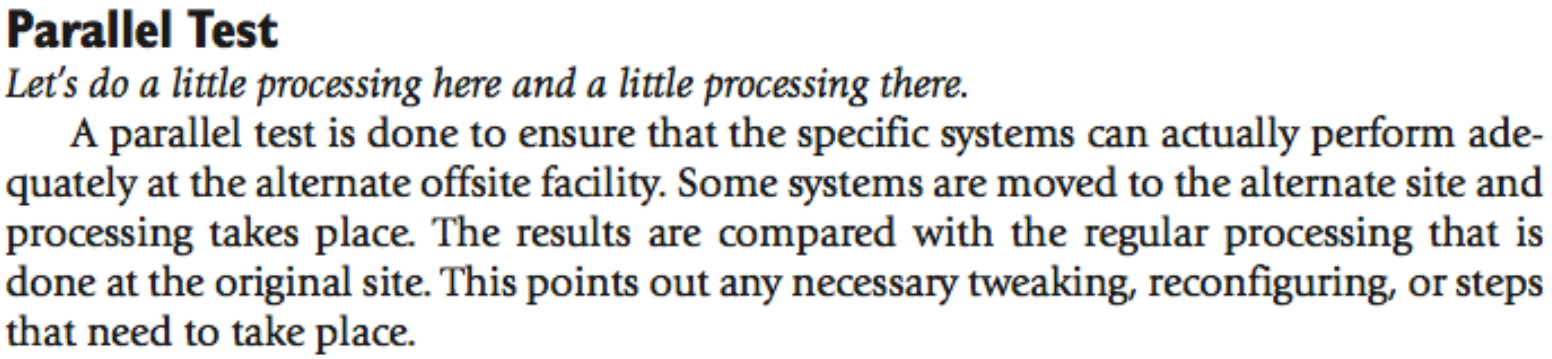
Types of tests (continued)



Simulation Test

Everyone take your places. Okay, action!

This type of test takes a lot more planning and people. In this situation, all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario. The scenario is used to test the reaction of each operational and support representative.

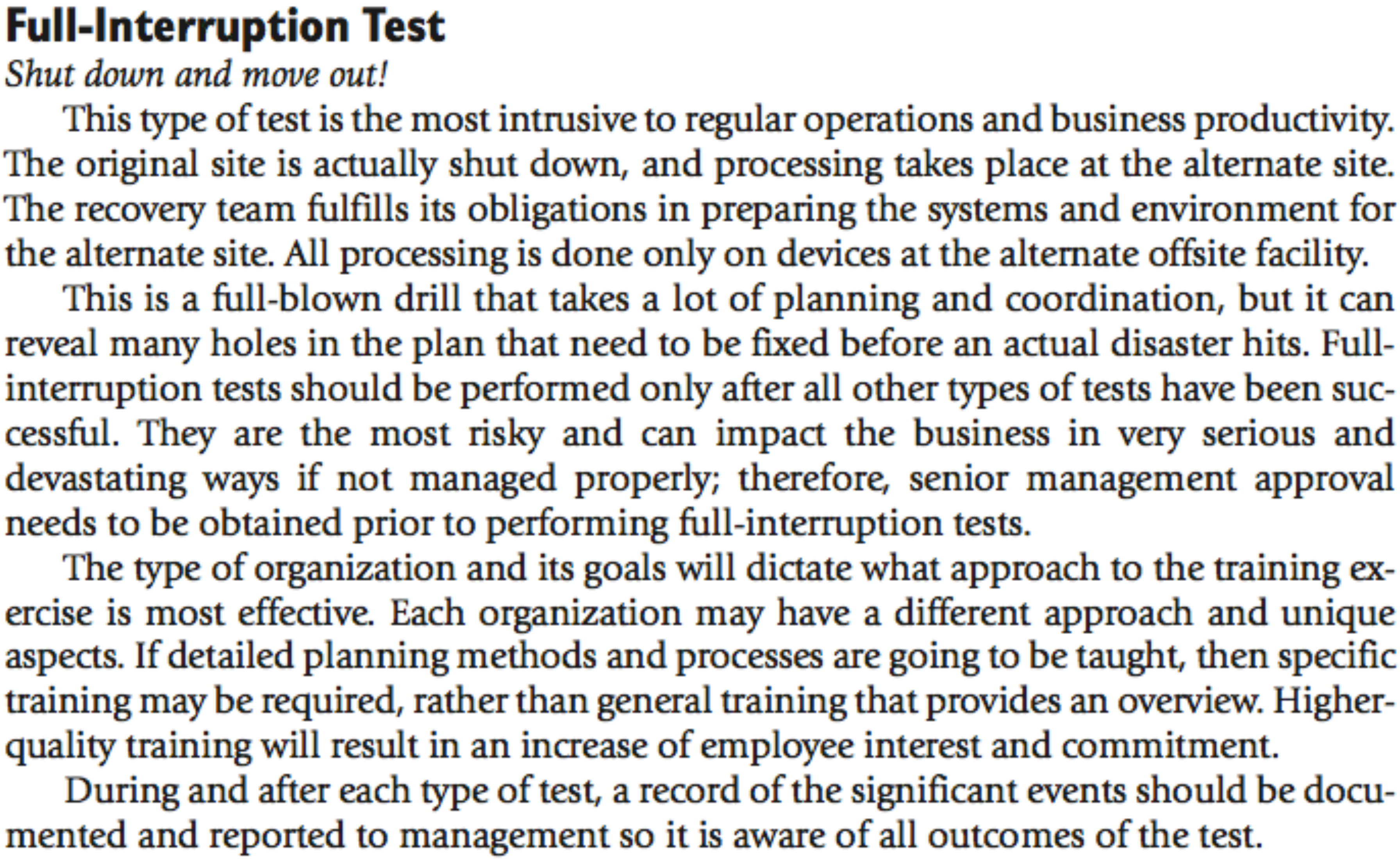


Parallel Test

Let's do a little processing here and a little processing there.

A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility. Some systems are moved to the alternate site and processing takes place. The results are compared with the regular processing that is done at the original site. This points out any necessary tweaking, reconfiguring, or steps that need to take place.

The mother of all tests…



Full-Interruption Test

Shut down and move out!

This type of test is the most intrusive to regular operations and business productivity. The original site is actually shut down, and processing takes place at the alternate site. The recovery team fulfills its obligations in preparing the systems and environment for the alternate site. All processing is done only on devices at the alternate offsite facility.

This is a full-blown drill that takes a lot of planning and coordination, but it can reveal many holes in the plan that need to be fixed before an actual disaster hits. Full-interruption tests should be performed only after all other types of tests have been successful. They are the most risky and can impact the business in very serious and devastating ways if not managed properly; therefore, senior management approval needs to be obtained prior to performing full-interruption tests.

The type of organization and its goals will dictate what approach to the training exercise is most effective. Each organization may have a different approach and unique aspects. If detailed planning methods and processes are going to be taught, then specific training may be required, rather than general training that provides an overview. Higher-quality training will result in an increase of employee interest and commitment.

During and after each type of test, a record of the significant events should be documented and reported to management so it is aware of all outcomes of the test.

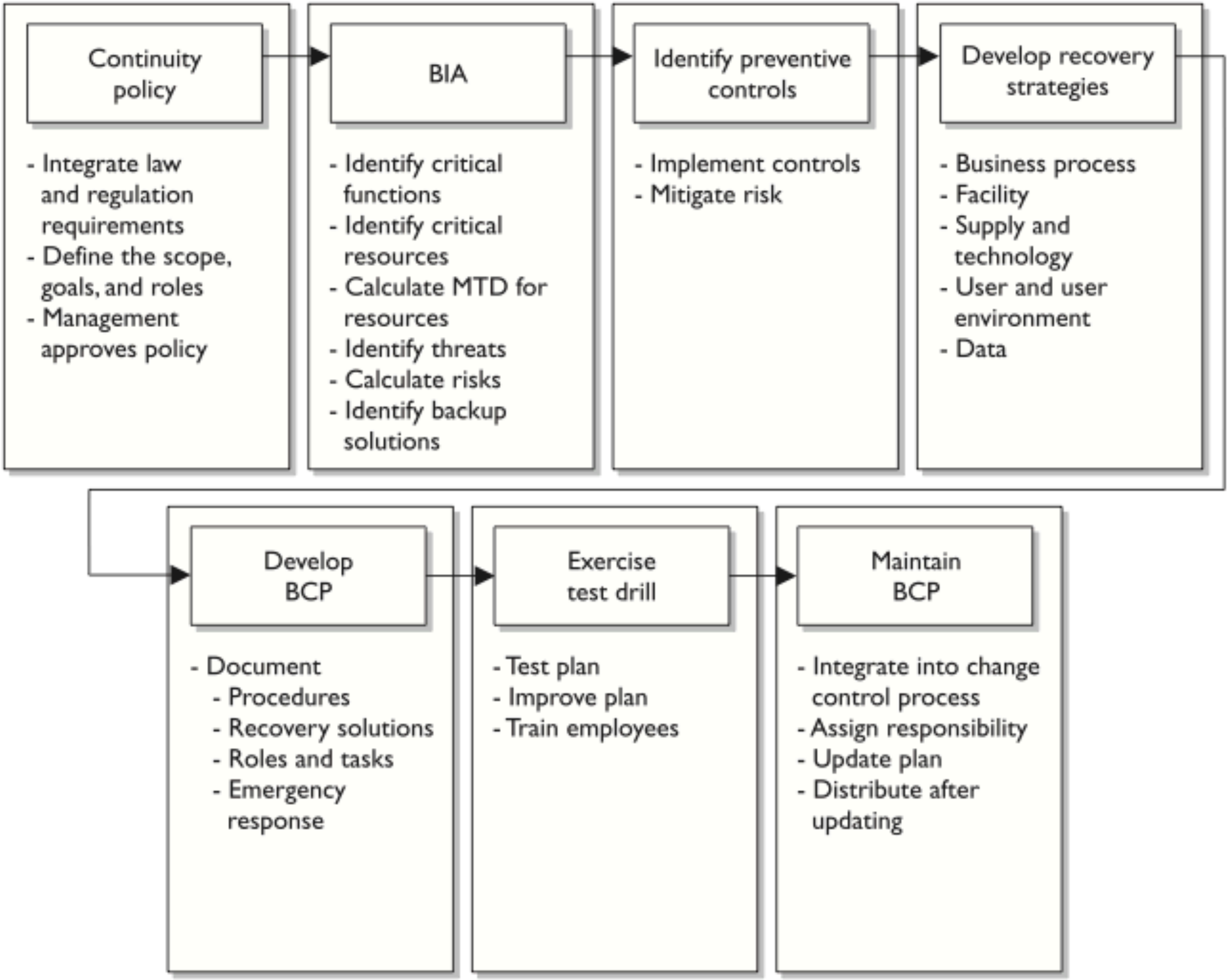
Procedure: Personnel Evacuation Description	Location	Names of Staff Trained to Carry Out Procedure	Date Last Carried Out
Each floor within the building must have two individuals who will ensure that all personnel have been evacuated from the building after a disaster. These individuals are responsible for performing employee head count, communicating with the BCP coordinator, and assessing emergency response needs for their employees.	West wing parking lot	David Miller Mike Lester	Drills were carried out on May 4, 2005.
Comments: These individuals are responsible for maintaining an up-to-date listing of employees on their specific floor. These individuals must have a company-issued walkie-talkie and proper training for this function.			

Table 9-3 Sample Emergency Response Procedure

7. Maintain the Plan!

- **The main reasons plans become outdated include the following:**
  - **The business continuity process is not integrated into the change management process.**
  - **Infrastructure and environment changes occur.**
  - **Reorganization of the company, layoffs, or mergers occur.**
  - **Changes in hardware, software, and applications occur.**
  - **After the plan is constructed, people feel their job is done.**
  - **Personnel turns over.**
  - **Large plans take a lot of work to maintain.**
  - **Plans do not have a direct line to profitability.**

- **Organizations can keep the plan updated by taking the following actions:**
  - **Make business continuity a part of every business decision.**
  - **Insert the maintenance responsibilities into job descriptions.**
  - **Include maintenance in personnel evaluations.**
  - **Perform internal audits that include disaster recovery and continuity documentation and procedures.**
  - **Perform regular drills that use the plan.**
  - **Integrate the BCP into the current change management process.**



Continuity policy

- Integrate law and regulation requirements
- Define the scope, goals, and roles
- Management approves policy

BIA

- Identify critical functions
- Identify critical resources
- Calculate MTD for resources
- Identify threats
- Calculate risks
- Identify backup solutions

Identify preventive controls

- Implement controls
- Mitigate risk

Develop recovery strategies

- Business process
- Facility
- Supply and technology
- User and user environment
- Data

Develop BCP

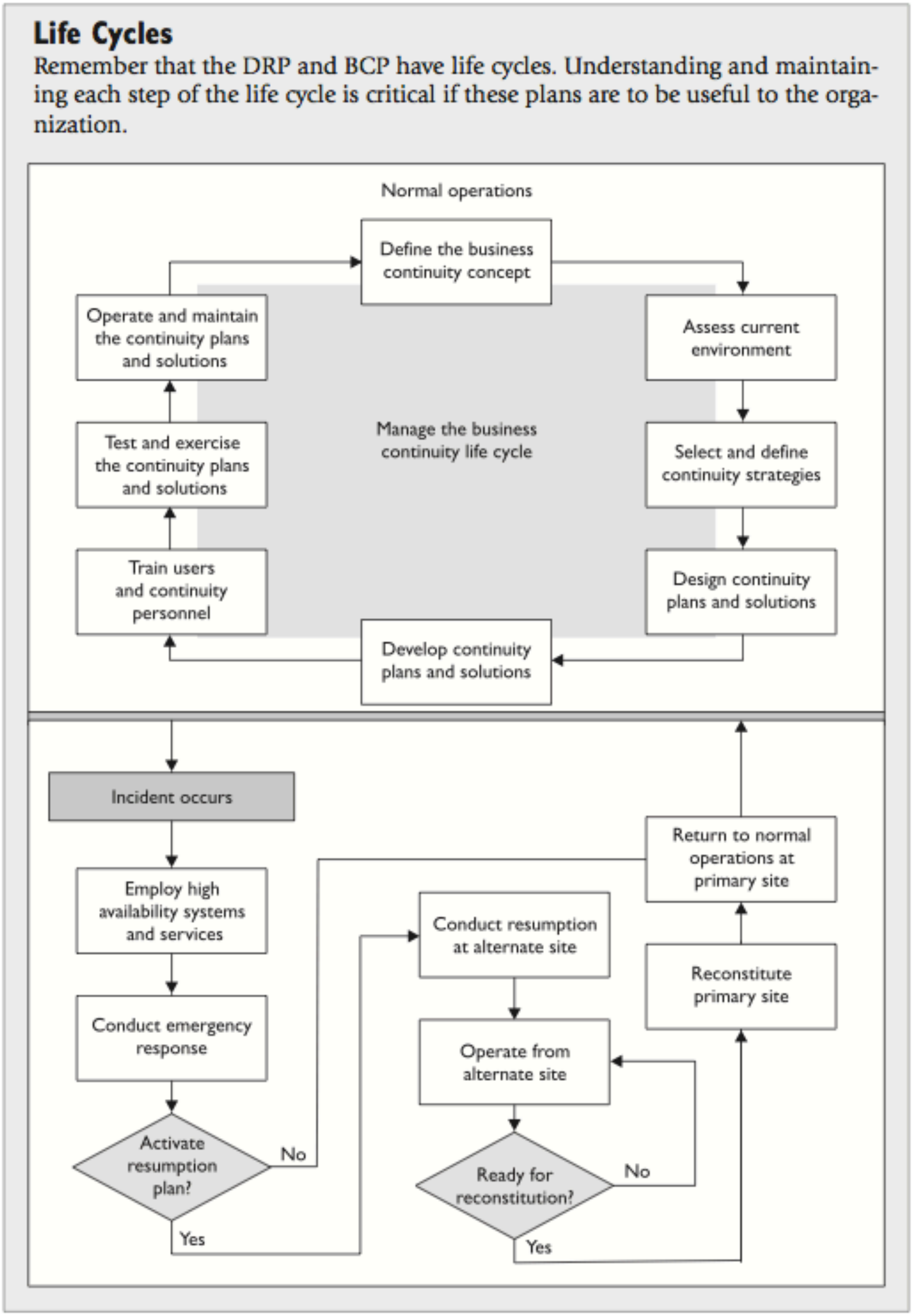
- Document
  - Procedures
  - Recovery solutions
  - Roles and tasks
  - Emergency response

Exercise test drill

- Test plan
- Improve plan
- Train employees

Maintain BCP

- Integrate into change control process
- Assign responsibility
- Update plan
- Distribute after updating



Life Cycles

Remember that the DRP and BCP have life cycles. Understanding and maintaining each step of the life cycle is critical if these plans are to be useful to the organization.

Normal operations
Define the business continuity concept
Assess current environment
Select and define continuity strategies
Design continuity plans and solutions
Develop continuity plans and solutions
Train users and continuity personnel
Test and exercise the continuity plans and solutions
Operate and maintain the continuity plans and solutions
Manage the business continuity life cycle
Incident occurs
Employ high availability systems and services
Conduct emergency response
Activate resumption plan?
No
Yes
Conduct resumption at alternate site
Operate from alternate site
Ready for reconstitution?
No
Yes
Reconstitute primary site
Return to normal operations at primary site

Quick Tips

- A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained and that help minimize losses of life, operations, and systems.
- A BCP provides procedures for emergency responses, extended backup operations, and post-disaster recovery.
- A BCP should reach enterprisewide, with individual organizational units each having their own detailed continuity and contingency plans.
- A BCP needs to prioritize critical applications and provide a sequence for efficient recovery.
- A BCP requires senior executive management support for initiating the plan and final approval.
- BCPs can quickly become outdated due to personnel turnover, reorganizations, and undocumented changes.
- Executives may be held liable if proper BCPs are not developed and used.
- Threats can be natural, manmade, or technical.
- The steps of recovery planning include initiating the project; performing business impact analyses; developing a recovery strategy; developing a recovery plan; and implementing, testing, and maintaining the plan.
- The project initiation phase involves getting management support, developing the scope of the plan, and securing funding and resources.
- The business impact analysis is one of the most important first steps in the planning development. Qualitative and quantitative data needs to be gathered, analyzed, interpreted, and presented to management.
- Executive commitment and support are the most critical elements in developing the BCP.
- A business case must be presented to gain executive support. This is done by explaining regulatory and legal requirements, exposing vulnerabilities, and providing solutions
- Plans should be prepared by the people who will actually carry them out.
- The planning group should comprise representatives from all departments or organizational units.
- The BCP team should identify the individuals who will interact with external entities such as the press, shareholders, customers, and civic officials. Response to the disaster should be done quickly and honestly, and should be consistent with any other employee response.
- Disaster recovery and continuity planning should be brought into normal business decision-making procedures.
- The loss criteria for disasters include much more than direct dollar loss. They may include added operational costs, loss in reputation and public confidence, loss of competitive advantage, violation of regulatory or legal requirements, loss in productivity, delayed income, interest costs, and loss in revenue.
- A survey should be developed and given to the most knowledgeable people within the company to obtain the most realistic information pertaining to a company's risk and recovery procedures.
- The plan's scope can be determined by geographical, organizational, or functional means.
- Many things need to be understood pertaining to the working environment so it can be replicated at an alternate site after a disaster.
- Subscription services can supply hot, warm, or cold sites.
- A reciprocal agreement is one in which a company promises another company it can move in and share space if it experiences a disaster and vice versa. Reciprocal agreements are very tricky to implement and are unenforceable. However, they are cheap and sometimes the only choice.
- A hot site is fully configured with hardware, software, and environmental needs. It can usually be up and running in a matter of hours. It is the most expensive option, but some companies cannot be out of business longer than a day without detrimental results.
- A warm site does not have computers, but it does have some peripheral devices such as disk drives, controllers, and tape drives. This option is less expensive than a hot site, but takes more effort and time to get operational.
- A cold site is just a building with power, raised floors, and utilities. No devices are available. This is the cheapest of the three options, but can take weeks to get up and operational.
- When returning to the original site, the least critical organizational units should go back first.
- An important part of the disaster recovery and continuity plan is to communicate its requirements and procedures to all employees.
- Testing, drills, and exercises demonstrate the actual ability to recover and can verify the compatibility of backup facilities.
- Before tests are performed, there should be a clear indication of what is being tested, how success will be determined, and how mistakes should be expected and dealt with.
- A checklist test is one in which copies of the plan are handed out to each functional area to ensure the plan properly deals with the area's needs and vulnerabilities.
- A structured walk-through test is one in which representatives from each functional area or department get together and walk through the plan from beginning to end.
- A simulation test is one in which a practice execution of the plan takes place. A specific scenario is established, and the simulation continues up to the point of actual relocation to the alternate site.
- A parallel test is one in which some systems are actually run at the alternate site.
- A full-interruption test is one in which regular operations are stopped and where processing is moved to the alternate site.
- Remote journaling involves transmitting the journal or transaction log offsite to a backup facility.

Digital Forensics
Risk Analysis

Reference:

Drew Hamilton Lecture Notes

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

The Spirit of Forensic Discovery

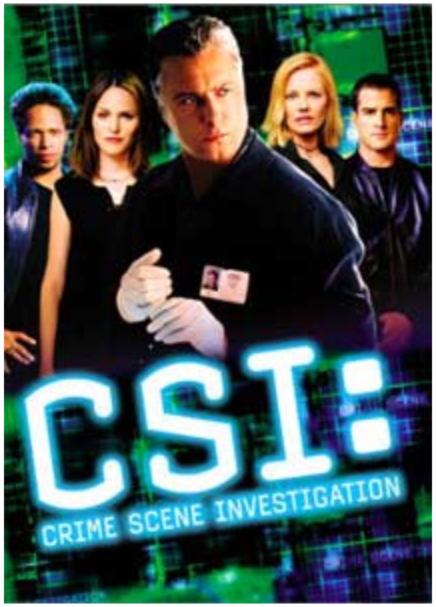
- Now, a few words on looking for things:
  - When you go looking for something specific, your chances of finding it are very bad.
  - Because, of all the things in the world, you're only looking for one of them.
  - When you go looking for anything at all, your chances of finding it are very good.
  - Because, of all the things in the world, you're sure to find some of them.

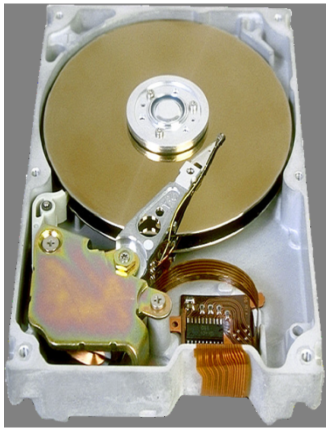
-- Darryl Zero, The Zero Effect

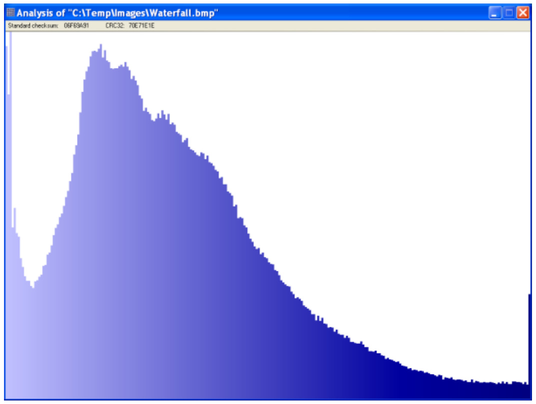
Digital forensics is:

- The lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and meta-data derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations.

  - Larry Leibrock, PhD, 1998







Analysis of "C:\Temp\Images\Waterfall.bmp"

Standard checksum: 06F69A91 CRC32: 70E71E1E

Digital forensics is not:

- Pro-active security
  - It is reactive to an event or request
- About finding the bad guy
  - It is about finding evidence of value
- Something you do for fun
  - Proper forensic investigations require expertise
- Quick
  - 6 TB drives are becoming easily available

Who uses digital evidence?

- Criminal justice agencies, CID, NIS, AFOSI
- Prosecutor’s Office/DA
- Federal, State, District & City Attorneys and Judges
- Corporate Counsels
- Civil and Criminal Counsels
- Human Resources
- Auditors
- Crackers/Hackers - Caution

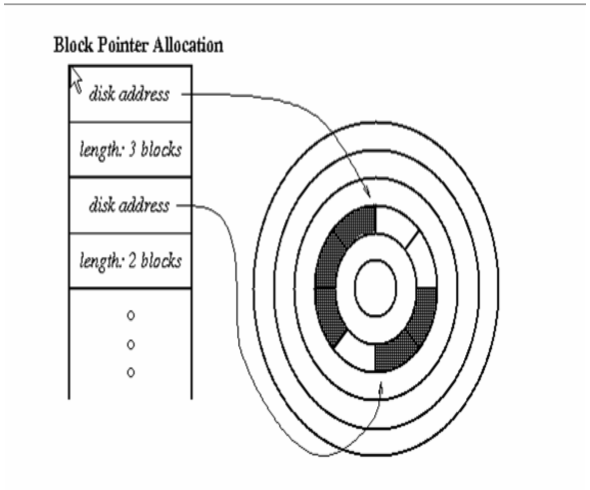
Types of digital forensics:

- Device-level investigation
- Network investigation
- Software investigation
- Steganographic investigation
  - Digital Imagery
  - Digital Sound
  - Digital Video
  - Encrypted or Embedded Content
  - Watermarking

Desired Outcome of Forensics:

Establish links:

- User ⇔ Platform
- Platform ⇔ O/S
- O/S ⇔ Logon
- Logon ⇔ Application
- Application ⇔ Data



Digital forensic process:

- Observe and evaluate environment
  - “If it is on, leave it on – if it is off, leave it off.”
- Gather and safeguard evidence
- Maintain a clear chain of custody
- Perform an evidentiary evaluation
- Document findings
- Provide expert testimony as required

The Process of Digital Forensic Science

- The primary activities of DFS are investigative in nature.
- The investigative process encompasses
  - Identification
  - Preservation
  - Collection
  - Examination
  - Analysis
  - Presentation
  - Decision

Computer Forensic Activities

Computer forensics activities commonly include:

- **the secure collection of computer data**
- **the identification of suspect data**
- **the examination of suspect data to determine details such as origin and content**
- **the presentation of computer-based information**
- **the application of a country's laws to computer practice.**

The 3 As

- The basic methodology consists of the 3 As:
  - Acquire the evidence without altering or damaging the original
  - Authenticate the image
  - Analyze the data without modifying it

“The Computer”

- Computer as *Target* of the incident
  - Get to instructor’s test preparation
  - Access someone else’s homework
  - Access/Change a grade
  - Access financial information
  - “Denial of Service”
- Computer as *Tool* of the incident
  - Word processing used to create plagiarized work
  - E-mail sent as threat or harassment
  - Printing used to create counterfeit material
- Computer as *Incidental* to the incident
  - E-mail/file access used to establish date/timelines
  - Stored names and addresses of contacts or others potentially involved in the incident

Locard Principle of Exchange

- "..when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived."
- (Edmund Locard, 1910)

Forensic Principles

1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
2. Upon seizing digital evidence, actions taken should not change that evidence.
3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
5. An Individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Chain of Custody

- Protects integrity of the evidence
- Effective process of documenting the complete journey of the evidence during the life of the case
- Allows you to answer the following questions:
  - Who collected it?
  - How & where?
  - Who took possession of it?
  - How was it stored & protected in storage?
  - Who took it out of storage & why?

Why use images

- In keeping with the second IOCE principle, care must be taken not to change the evidence.
- Most media are “magnetic based” and the data is volatile:
  - Registers & Cache
  - Process tables, ARP Cache, Kernel stats
  - Contents of system memory
  - Temporary File systems
  - Data on the disk
- Examining a live file system changes the state of the evidence (MAC times)
- The computer/media is the “crime scene”
- Protecting the crime scene is paramount as once evidence is contaminated it cannot be decontaminated.
- Really only one chance to do it right!

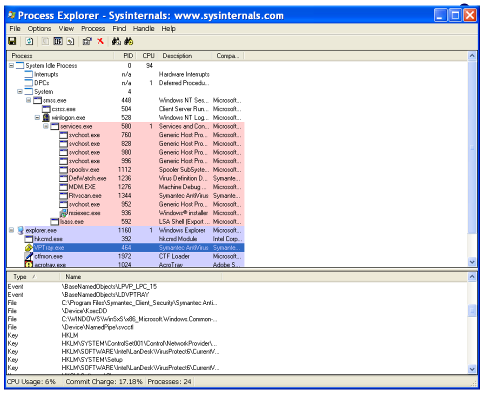
General Evidence Dos & Don’ts

1. Minimize Handling/Corruption of Original Data
2. Account for Any Changes and Keep Detailed Logs of Your Actions
3. Comply with the Five Rules of Evidence
4. Do Not Exceed Your Knowledge
5. Follow Your Local Security Policy and Obtain Written Permission
6. Capture as Accurate an Image of the System as Possible
7. Be Prepared to Testify
8. Ensure Your Actions are Repeatable
9. Work Fast
10. Proceed From Volatile to Persistent Evidence
11. Don't Run Any Programs on the Affected System
12. Document Document Document!!!!

- Source: AusCERT 2003 (www.auscert.org)

Digital forensic utilities:

- Focused Products
  - HELIX
  - WinHex
  - Vision
  - S-Tools

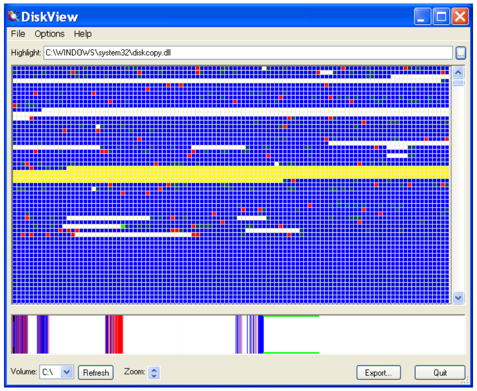


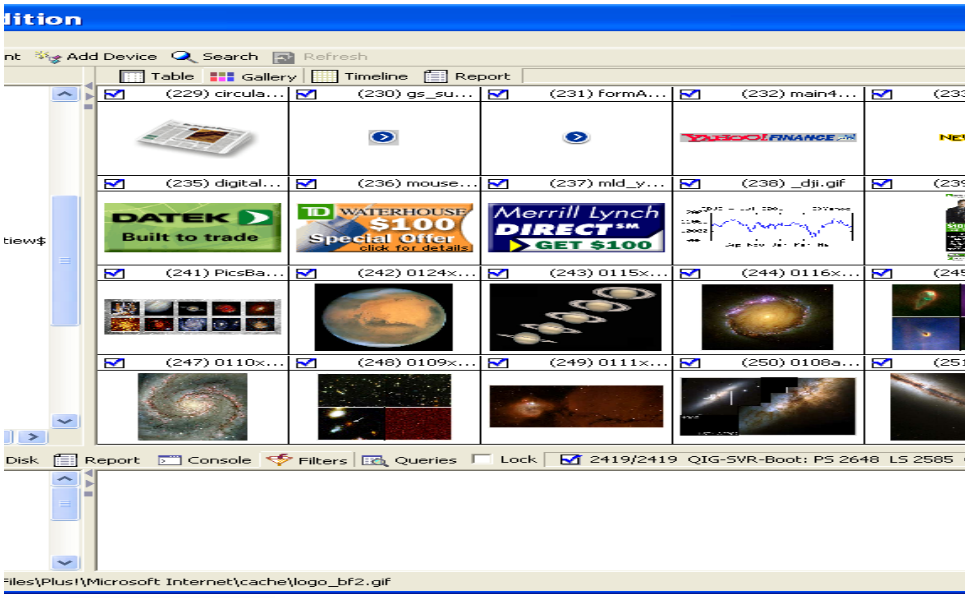
Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Handle Help

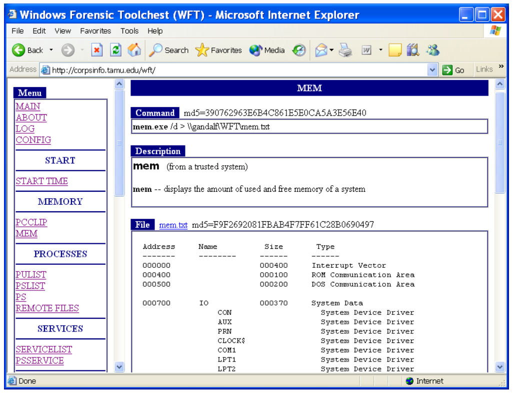
```
Process                    PID    CPU  Description           Compa...
System Idle Process          0     94
  Interrupts               n/a         Hardware Interrupts
  DPCs                     n/a      1  Deferred Procedu...
  System                     4
    smss.exe               448         Windows NT Ses...     Microsoft...
      csrss.exe            504         Client Server Run...  Microsoft...
      winlogon.exe         528         Windows NT Log...     Microsoft...
        services.exe       580      1  Services and Con...   Microsoft...
          svchost.exe      760         Generic Host Pro...   Microsoft...
          svchost.exe      828         Generic Host Pro...   Microsoft...
          svchost.exe      980         Generic Host Pro...   Microsoft...
          svchost.exe      996         Generic Host Pro...   Microsoft...
          spoolsv.exe     1112         Spooler SubSyste...   Microsoft...
          DefWatch.exe    1236         Virus Definition D... Symante...
          MDM.EXE         1276         Machine Debug ...     Microsoft...
          Rtvscan.exe     1344         Symantec AntiVirus    Symante...
          svchost.exe      952         Generic Host Pro...   Microsoft...
          msiexec.exe      936         Windows® installer    Microsoft...
        lsass.exe          592         LSA Shell (Export ... Microsoft...
explorer.exe              1160      1  Windows Explorer      Microsoft...
  hkcmd.exe                392         hkcmd Module          Intel Corp...
  VPTray.exe               464         Symantec AntiVirus    Symante...
  ctfmon.exe              1972         CTF Loader            Microsoft...
  acrotray.exe            1024         AcroTray              Adobe S...

Type     Name
Event    \BaseNamedObjects\LPVP_LPC_15
Event    \BaseNamedObjects\LDVPTRAY
File     C:\Program Files\Symantec_Client_Security\Symantec Anti...
File     \Device\KsecDD
File     C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-...
File     \Device\NamedPipe\svcctl
Key      HKLM
Key      HKLM\SYSTEM\ControlSet001\Control\NetworkProvider\...
Key      HKLM\SOFTWARE\Intel\LanDesk\VirusProtect6\CurrentV...
Key      HKLM\SYSTEM\Setup
Key      HKLM\SOFTWARE\Intel\LanDesk\VirusProtect6\CurrentV...

CPU Usage: 6%   Commit Charge: 17.18%   Processes: 24
```

Commercial Suites

- EnCase
- Forensic Toolkit
- DMZ F.I.R.E.
- Maresware







Windows Forensic Toolchest (WFT) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://corpsinfo.tamu.edu/wft/
Go Links
Menu
MAIN
ABOUT
LOG
CONFIG
START
START TIME
MEMORY
PCCLIP
MEM
PROCESSES
PULIST
PSLIST
PS
REMOTE FILES
SERVICES
SERVICELIST
PSSERVICE
MEM
Done
Internet

Command md5=390762963E6B4C861E5E0CA5A3E56E40

```
mem.exe /d > \\gandalf\WFT\mem.txt
```

Description

mem (from a trusted system)

mem -- displays the amount of used and free memory of a system

File mem.txt md5=F9F2692081FBAB4F7FF61C28B0690497

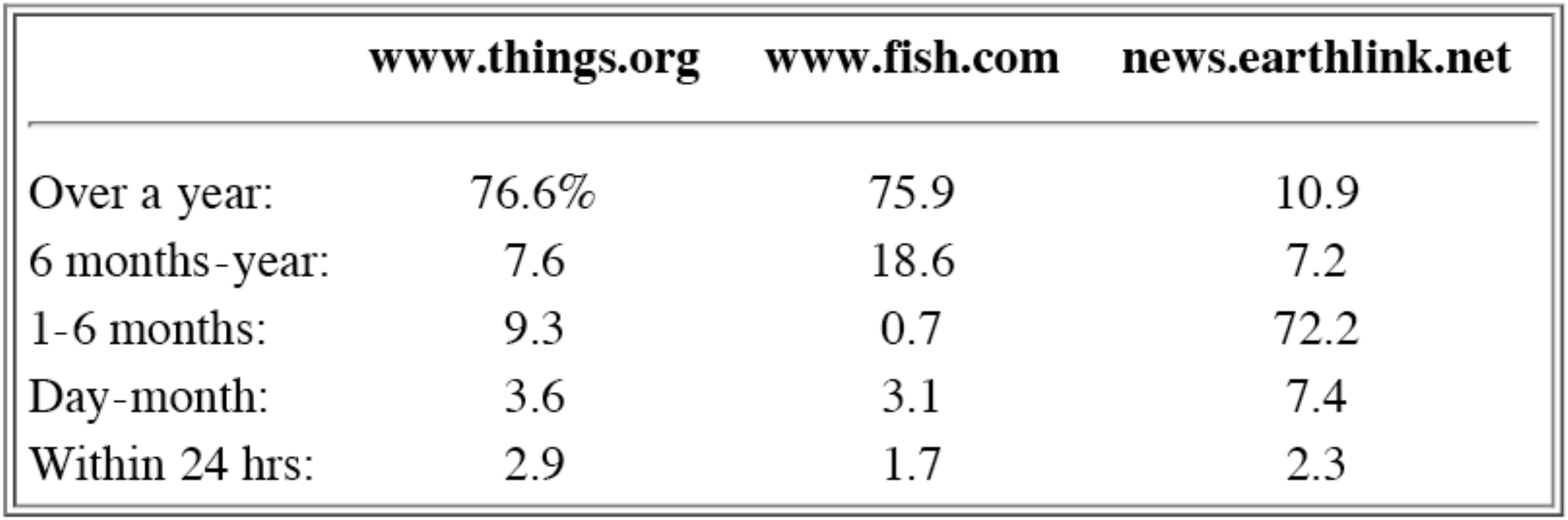
```
Address    Name        Size     Type
-------    ---------   ------   ------
000000                 000400   Interrupt Vector
000400                 000100   ROM Communication Area
000500                 000200   DOS Communication Area

000700     IO          000370   System Data
             CON                  System Device Driver
             AUX                  System Device Driver
             PRN                  System Device Driver
             CLOCK$               System Device Driver
             COM1                 System Device Driver
             LPT1                 System Device Driver
             LPT2                 System Device Driver
```

Digital forensic tools:

- Blockers
- Drive Cloning
- Hot-operation Appliances

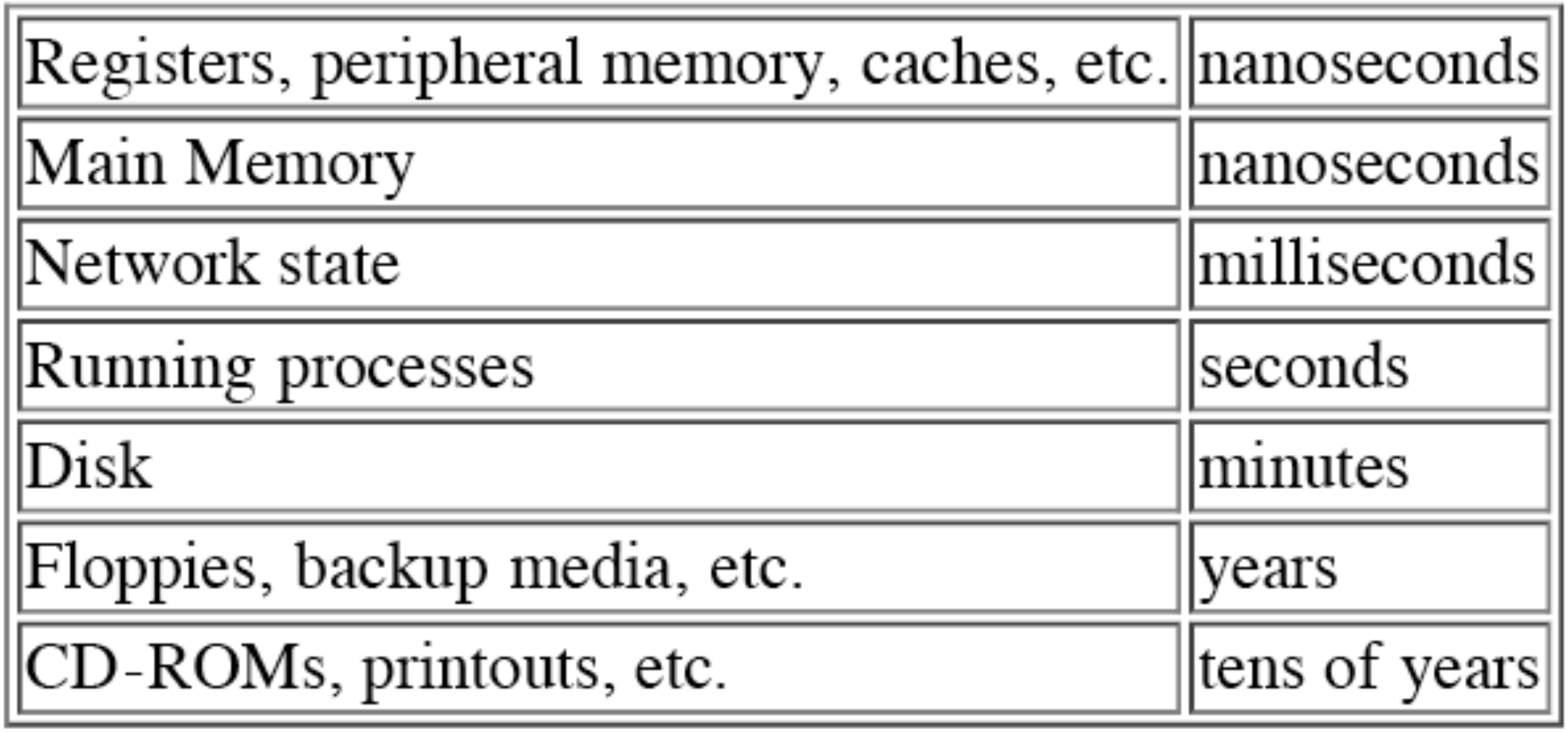
% of files read or executed recently for a number of internet servers

- The vast majority of files on two fairly typical web servers have not been used at all in the last year.
  - Even on an extraordinarily heavily used) Usenet news system less than 10% of the files were used within the last 30 days.
- There are lots of files gathering electronic dust.
  - Similar patterns emerge from Windows PCs and other desktop systems.
  - Often more than 90% of files haven't been touched in the past year.



	www.things.org	www.fish.com	news.earthlink.net
Over a year:	76.6%	75.9	10.9
6 months-year:	7.6	18.6	7.2
1-6 months:	9.3	0.7	72.2
Day-month:	3.6	3.1	7.4
Within 24 hrs:	2.9	1.7	2.3

Order of Volatility



Registers, peripheral memory, caches, etc.	nanoseconds
Main Memory	nanoseconds
Network state	milliseconds
Running processes	seconds
Disk	minutes
Floppies, backup media, etc.	years
CD-ROMs, printouts, etc.	tens of years

- **Forensic analysis of a system revolves around a cycle of data gathering and processing of the information gathered.**
- **The original data is safeguarded in a pristine state and any analysis should be performed on a copy of the computer's data.**

Monitoring Risks

- Power cycling a machine clears registers, main memory, etc.
- Direct access to a running device promotes greater understanding over higher levels of certainty, which could potentially make such methodology more suspect in a court of law.
- Paradoxically, however, the uncertainty - primarily in the data collection methods - can actually give a greater breadth of knowledge and more confidence in any conclusions that are drawn.
- This process requires consistent mechanisms for gathering data and a good understanding of any side effects of the same.
- To obtain dependable results automation is a is a near-necessity for gathering forensic data.

The Heisenberg principle of data gathering and system analysis.

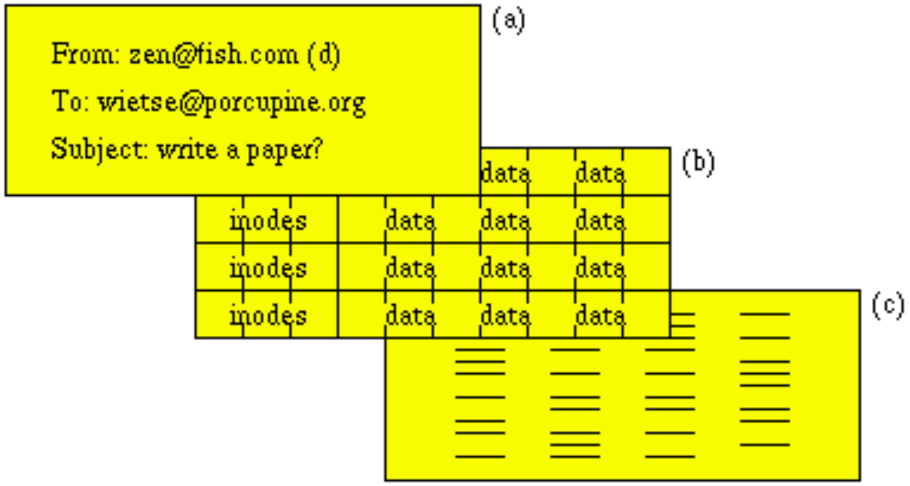
- It's not simply difficult to gather all the information on a computer, it is essentially impossible.
  - Farmer and Venema dub this the Heisenberg principle of data gathering and system analysis.
    - Virtual machines may be used to capture activity down to the actual machine code instructions [Dunlap, 2002], but on a practical level this is not possible on general-purpose computers and all their peripherals.
- Computers aren't defined by their state at any given time, but over a continuum.
- Memory, processes and files can change so rapidly that recording even the bulk of those fluctuations in an accurate and timely fashion is not possible without dramatically disturbing the operation of a typical computer system.

Scalability of Analysis

- Take the UNIX `date` program, which prints the current date and time, as an example.
- If we monitor it with `strace`, a program that traces a program as it runs, `date` executes over 100 system calls in a fraction of a second (including those to get the time, check the timezone you're in, print out the result, etc.)
- If we went further and monitored the machine code that the CPU executes in performing this work we would have many thousands pieces of information to consider.
- But even instrumenting all the programs on a computer doesn't tell the whole story, for the computer's video card, disk controller, and other peripherals each have their own tale to tell, with memory, processors, and storage of their own.
- We can never truly recover the past. But we will show that you don't need all the data to draw reasonable conclusions about what happened.

Layers & Illusions

- The perception of files and directories with attributes is one of the illusions that computer systems create for us, just like the underlying illusion of data blocks & metadata (inode) blocks.



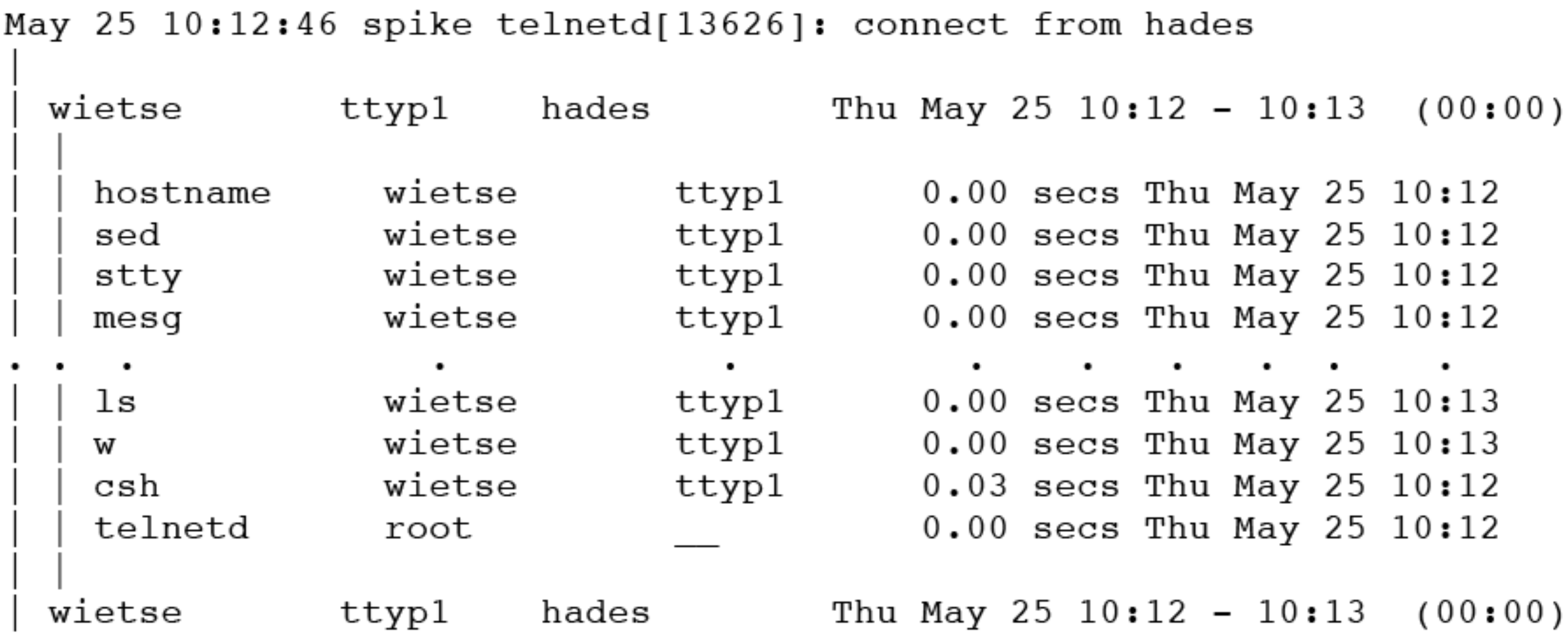
- In reality, computer file systems allocate space from a linear array of equal-size disk blocks, and reserve some of that storage capacity for their own purposes.
- However, the illusion of files and of directories with attributes is much more useful for application programs and their users.

Levels of Abstraction

- Even the notion of linear array of equal-sized disk blocks is an illusion.
  - Real disks have heads and platters.
  - They store information as magnetic domains and also reserve some of the storage capacity for their own purposes.
  - The illusion of a linear sequence of equal-sized disk blocks has only one purpose: to make the implementation of file systems easier.
- As we peel away layer after layer of illusions, information becomes more and more accurate because it has undergone less and less processing.
- As we descend closer and closer towards the level of raw bits, the information becomes less meaningful because we know less and less about its purpose.
- This issue of ambiguity versus accuracy is just one consequence of layering

TCP wrapper logging

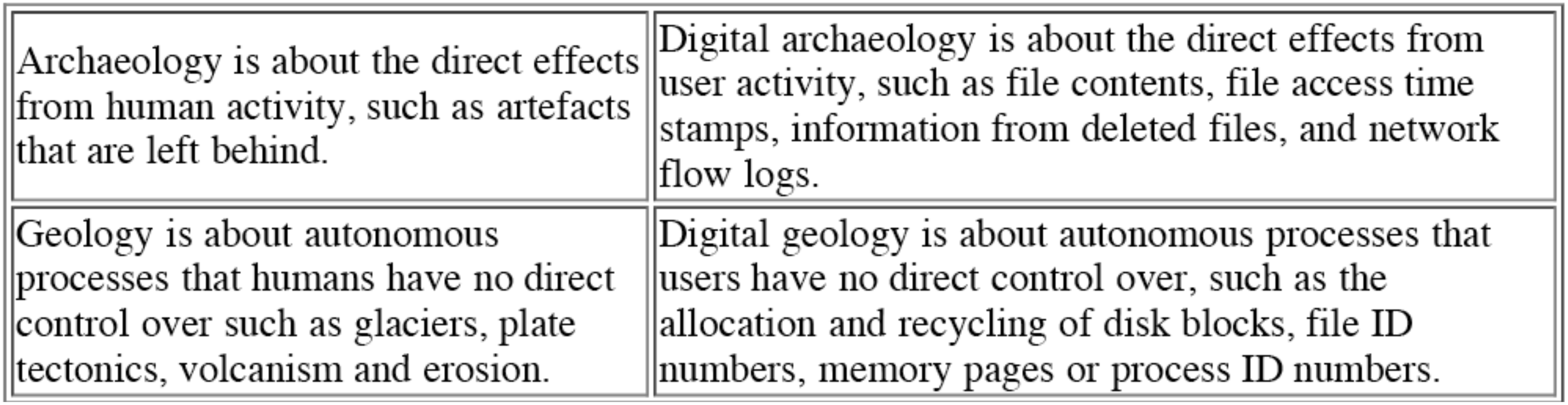
- **On May 25 10:12:46 local time, machine spike received a telnet connection from machine hades.**
  - **The TCP Wrapper logs connection events only, so there is no corresponding record for the end of the telnet connection.**
  - **The `last` command output shows that user wietse was logged in on terminal port ttyp1 from host hades and that the login session lasted from 10:12 until 10:13, for a total amount of time of less than two minutes.**



```
May 25 10:12:46 spike telnetd[13626]: connect from hades
 |
 | wietse       ttyp1    hades        Thu May 25 10:12 - 10:13  (00:00)
 | |
 | | hostname     wietse       ttyp1       0.00 secs Thu May 25 10:12
 | | sed          wietse       ttyp1       0.00 secs Thu May 25 10:12
 | | stty         wietse       ttyp1       0.00 secs Thu May 25 10:12
 | | mesg         wietse       ttyp1       0.00 secs Thu May 25 10:12
 . .  .            .            .          .    .    .   .   .    .
 | | ls           wietse       ttyp1       0.00 secs Thu May 25 10:13
 | | w            wietse       ttyp1       0.00 secs Thu May 25 10:13
 | | csh          wietse       ttyp1       0.03 secs Thu May 25 10:12
 | | telnetd      root         __          0.00 secs Thu May 25 10:12
 | |
 | wietse       ttyp1    hades        Thu May 25 10:12 - 10:13  (00:00)
```

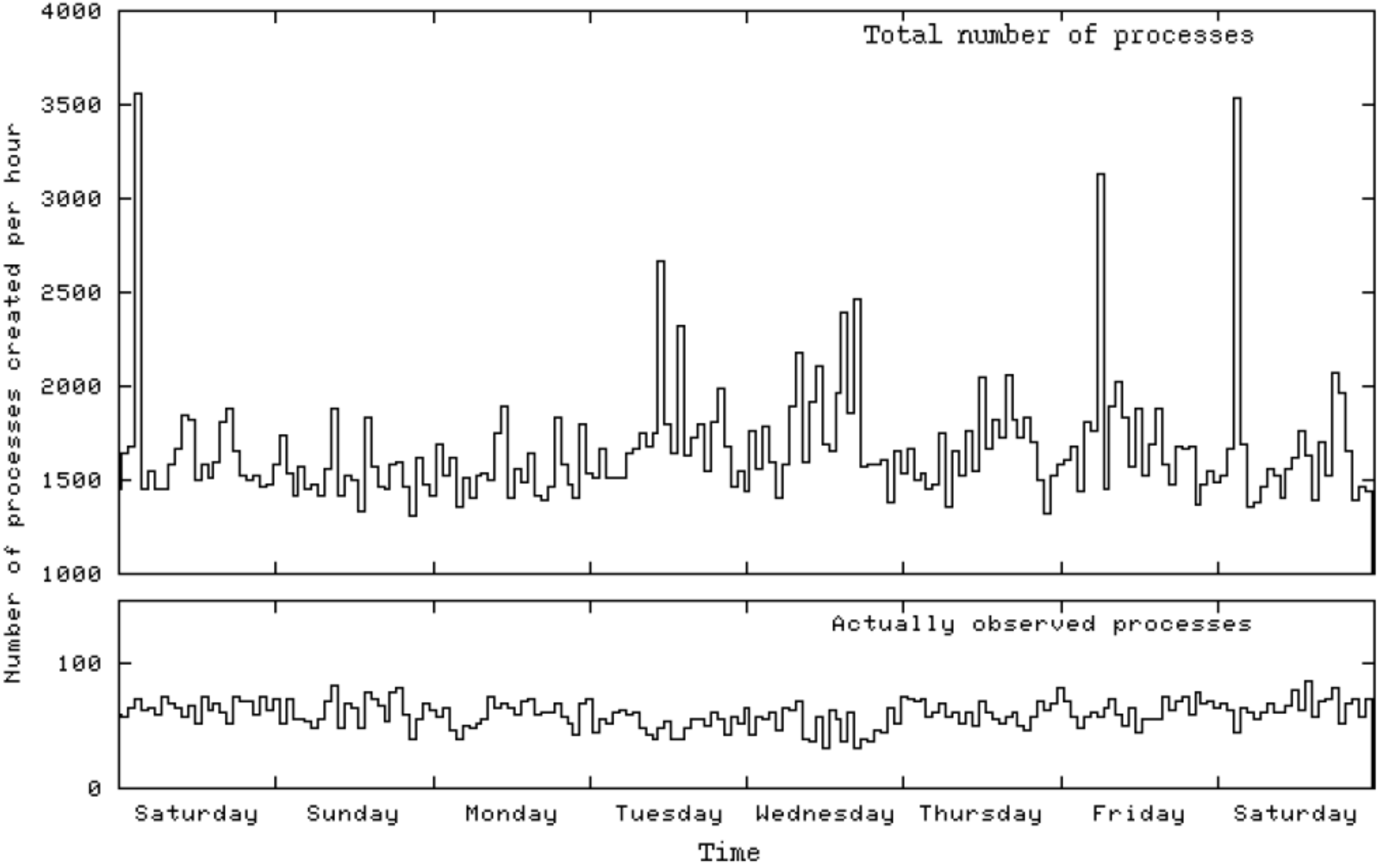
Archaeology versus Geology

- Over time, computer systems have become more & more complex.
- Users see systems become increasingly mature & stable.
- Under the surface, however, computer systems have become less and less predictable in when and where they store information, and in how they recycle storage space.
- The information that we find on a disk, in main memory, or in network packets is affected by a multitude of processes that have trashed each other's footsteps and fingerprints.
- Traditionally, these less predictable processes have been ignored by computer forensics.



Archaeology is about the direct effects from human activity, such as artefacts that are left behind.	Digital archaeology is about the direct effects from user activity, such as file contents, file access time stamps, information from deleted files, and network flow logs.
Geology is about autonomous processes that humans have no direct control over such as glaciers, plate tectonics, volcanism and erosion.	Digital geology is about autonomous processes that users have no direct control over, such as the allocation and recycling of disk blocks, file ID numbers, memory pages or process ID numbers.

Total process creation rate (above) and actually observed rate (below) for a small FreeBSD mail server. The two peaks at 02:00 on Saturday morning are caused by a weekly housekeeping job.



Data Security and Privacy Practices
Risk Analysis

Reference:

Drew Hamilton Lecture Notes

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Why Is Privacy Important?

- Data is a corporate asset, like any other
- Corporate data is at a higher risk of theft or misuse than ever before
- Companies have obligations to protect data
  - Laws, regulations, guidelines
  - Contracts with third parties
  - Privacy policies for users of websites, other online features

CMU Privacy Statistics

- A matter of corporate governance:
  - Does your board review and approve top-level policies on privacy and IT security risks?
    - 23% - regularly
    - 28% - occasionally
    - 42% - rarely or never
  - Does your board review and approve annual budgets for privacy and IT security programs?
    - 28% - regularly
    - 10% - occasionally
    - 54% - rarely or never

Carnegie Mellon CyLab 2012 Report

Information Privacy, Security

- Data privacy, data security risks are not limited to financial, healthcare, utility sectors. Retail sector is vulnerable as well
  - Zaxby's reported finding malware at 100 of its 560 locations in 10 states that could extract names, credit and debit card numbers
  - Papa John's agreed to pay $16.5 million to settle a class action over claims that it sent unauthorized texts to customers in violation of the Telephone Consumer Protection Act
- Breaches of data privacy, data security can result in
  - Damage to reputation
  - Disruption of operations
  - Legal liability under new and amended laws, regulations, and guidelines, as well as under contracts
  - Financial costs

Sensitive Data (U.S. Government)

- Unclassified
- Sensitive but Unclassified (SBU)
- FOUO
- Confidential
- Secret
- Top Secret
- Top Secret Compartmented
- So secret that the classification itself is classified
  - Other countries have other designations
    - →secret discreet
    - →NOFORN

Commercial business/private sector classification levels

- Confidential / Private
  - Confidential is company data
  - Private is related to individuals
- Sensitive
- Public

Disposition of media and data

1. Use of sanitizing software

2. Physical destruction of the electronic media

3. Documentation of sanitation or destruction of electronic media

What is Media Sanitization?
(NIST SP 800-88)

Dispose: (not really sanitized) Just tossed away.

Clear: Resistant to keyboard attacks.

Purge: Resistant to laboratory attacks.

Destroy: Resistant to recreation of media

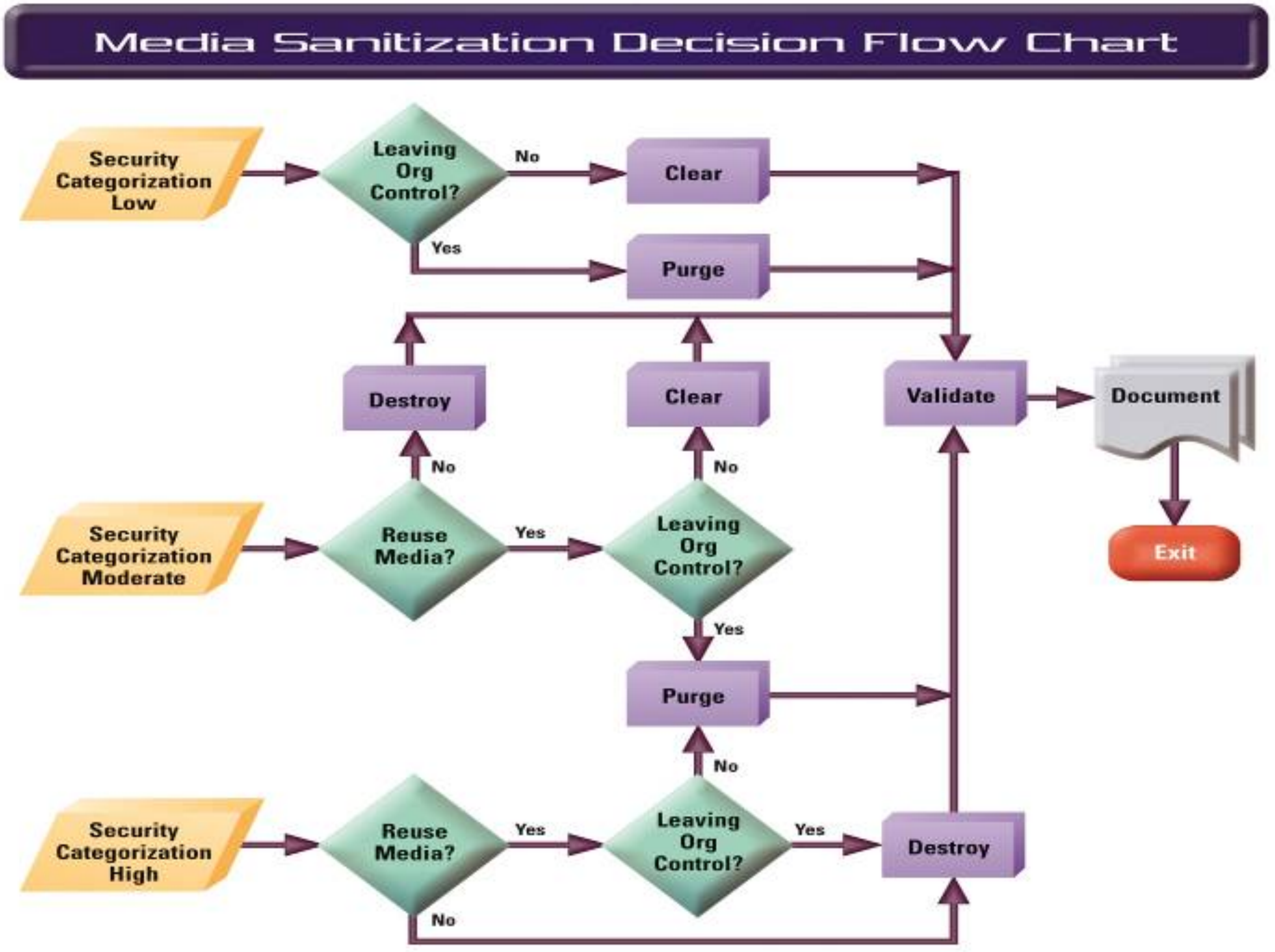
NIST SP800-88 is not intended to replace a sanitization program that is:

- Effective
- Operational
- Compliant with FIPS 200 and satisfies SP 800-53 Rev 1 and 800-53A.

Media Sanitation (NIST SP 800-88)

- **How to sanitize media?**
  - Identify your media and know your information.
  - Decide on a sanitization method.
  - Find supportive tools.
  - Validate your tools/policies/procedures.
- **What is reasonable?**
  - Don’t degauss the paper or spend $5K to sanitize a $50 HD.
  - Scale it up for ease, risk, resources.
  - Make cost effective risk based decisions weighing environmental factors that may be unique to your agency.
- **Know what information is where.**
  - What media are you using across your agency.
    - Is there non agency media on your systems?
  - What information is on that media.
  - What information is not on media.
  - Loose control of your information locations = loose control of your sanitization.

Media Sanitation



Types of Information

- "Personally identifiable information" (PII) can be linked to a specific individual
  - Name, e-mail, full postal address, birth date, Social Security number, driver's license number, account numbers
- "Non-personally identifiable information" (non-PII) cannot, by itself, be used to identify a specific individual
  - Aggregate data, zip code, area code, city, state, gender, age

PII or not PII?

- "Anomyzed" data that is "de-anomyzed"
  - IP address linked to domain name that identifies a person

- Non-PII that, when linked with other data, can effectively identify a person – "persistent identifiers"
  - Geolocation data
  - Site history and viewing patterns

PII Protections

- Data privacy laws govern businesses' collection, use, and sharing of information about individuals
- Federal, state, and foreign laws apply
- Laws govern both physical and electronic security of information

Legal Protections for PII

- **U.S. laws are a patchwork, developed by sector (compared to European Community' s uniform, centralized law)**
  - **Challenges in determining**
    - **Which laws apply to which activities**
    - **How to comply when multiple, sometimes inconsistent, laws apply.**

Website Privacy

- Do you need one?
  - No, if your website:
    - Is merely static
    - Is business-to-business (B2B) only, and collects no PII from consumers
  - Yes, otherwise
- What must it cover?
  - Actual practices for PII and information that reasonably could be associated with a person or device, regarding
    - Collection
    - Storage
    - Use
    - Sharing

Website Privacy Policies

- Special concerns if information involves
  - Financial information
  - Medical information
  - Children's information
- Special concerns for specific jurisdictions
  - European Union
  - California
- Opt outs from information collection available?
- Caution regarding links to third party sites
- Notice whenever privacy practices change
- Do not overpromise: "We will never share your information . . ."

Best Practices: Privacy Audit

- Review, assess policies and practices for data
  - Collection
  - Storage
  - Use
  - Disclosure
  - Protection
  - Destruction
- Identify exposure to data privacy, data security risks
- Consider, implement changes to minimize risks
- Develop, adopt best practices going forward

Best Practices: Privacy Audit

- Key benefit: Shows that data privacy and security are not just IT issues; instead, they touch on all parts of the company
  - Audit gathers information not only from IT/IS personnel, but also from personnel with responsibility for legal, marketing, development, sales, supply chain, human resources, international
- Helps ensure visibility, responsibility, accountability for privacy, security issues

Best Practices: Privacy Audit

- Review contracts with vendors that collect or provide PI to company
  - Do contracts have indemnification provisions? Does vendor have resources to indemnify?
- Review potential insurance coverage
  - Property, liability (E&O, D&O, general liability, umbrella), computer crime, business owner package
    - Errors and Omissions
    - Directors and Officers

Best Practices: Privacy Audit

- Consider class action waivers, arbitration provisions in terms of use, other consumer contracts
- Conduct annual reviews of
  - Data security
  - Data privacy
  - Risk management programs
- Develop contingency plans

Best Practices

- Take stock
  - What information do you have?
  - Where is it stored?
  - Who has access to it?
  - Who should have access to it?
- Scale down
  - Collect only what you need
  - Keep it only as long as you need it
  - Don’t use Social Security numbers unnecessarily
  - Restrict access
- Keep it safe
  - Train employees about safe practices
  - Implement
    - Firewalls
    - Strong passwords
    - Antivirus software
  - Use extra caution with laptops, PDAs, cell phones
  - Lock desks, drawers
  - Limit access to sensitive files
  - Secure data shipped or stored offsite

Best Practices (2)

- Destroy what you can
  - Shred, burn, pulverize paper records
  - Use wipe utility programs on computers, portable storage devices
  - Make shredders easily accessible
- Plan ahead
  - Develop contingency plans for a security breach
  - Designate senior staff to coordinate response
  - Investigate right away
  - Take steps to eliminate vulnerabilities
  - Be aware of data breach statutes

Handling a Breach

- Do not panic or overreact
- Get facts: nature, scope of breach
- Determine whether, when to notify affected individuals
- Prevent further unauthorized access
- Preserve evidence, deal with law enforcement (your “frien-emy”?)
- Notify vendors (such as payment processors)
- Notify insurers
- Offer contact person
- Do not forget to alert those “on the front lines”

Part 5 Summary

- Policies, Plans, and Procedures
- Risk Management and Business Impact Analysis
- Incident Response, Disaster Recovery, Continuity of Operations
- Digital Forensics
- Data Security and Privacy Practices