J. A. “Drew” Hamilton, Jr., Ph.D.

Chair, NSA Cyber Operations Community of Practice

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

This work funded by NSA Contract #H98230-19-1-0291

CCI
2 Research Blvd.
Starkville, MS 39759

Voice: (662) 325-2294
Fax: (662) 325-7692
drew@drew-hamilton.com

Domain 4: Information Security Incident Management

ISACA

CISM

Review Manual

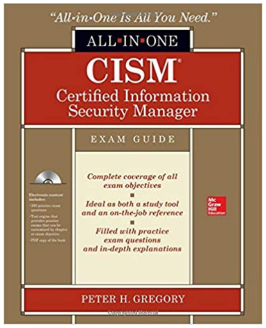
15th Edition

References:

Drew Hamilton Lecture Notes

CISM Review Manual, 15th Edition

CISM All-in-One Exam Guide, 1st Edition


"All-in-One Is All You Need."

ALL•IN•ONE

CISM Certified Information Security Manager

EXAM GUIDE

Complete coverage of all exam objectives

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

PETER H. GREGORY

Domain Outline

- Information Security Incident Management Overview
- Incident Response Procedures
  Incident Management Organization
- Incident Management Resources and Objectives
- Incident Management Metrics and Indicators
- Developing an Incident Management Plan
- Business Continuity and Disaster Recovery Plans
- Executing Response and Recovery Plans
  Post-incident Activities and Investigation

Information Security Incident Management Overview

Domain 4:
Information Security Incident Management

References: ISACA CISM Review Manual 15th Ed.

NIST SP 800-61r2 Incident Response

What is Incident Management?

- Emergency Operations Component of Risk Management
- Incident Management Factors
  - Constituency to be served
  - Mission, goals and objectives
  - Services provided
  - Organizational model and the relationship with the parent organization or customer base.
  - Funding for start-up costs and ongoing operations
  - Resources needed by the computer security incident response team (CSIRT)

What is a computer security incident?

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Incident Response Policy Elements

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy
  - (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure and definition of roles, responsibilities, and levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms.

Incident Response Plan

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

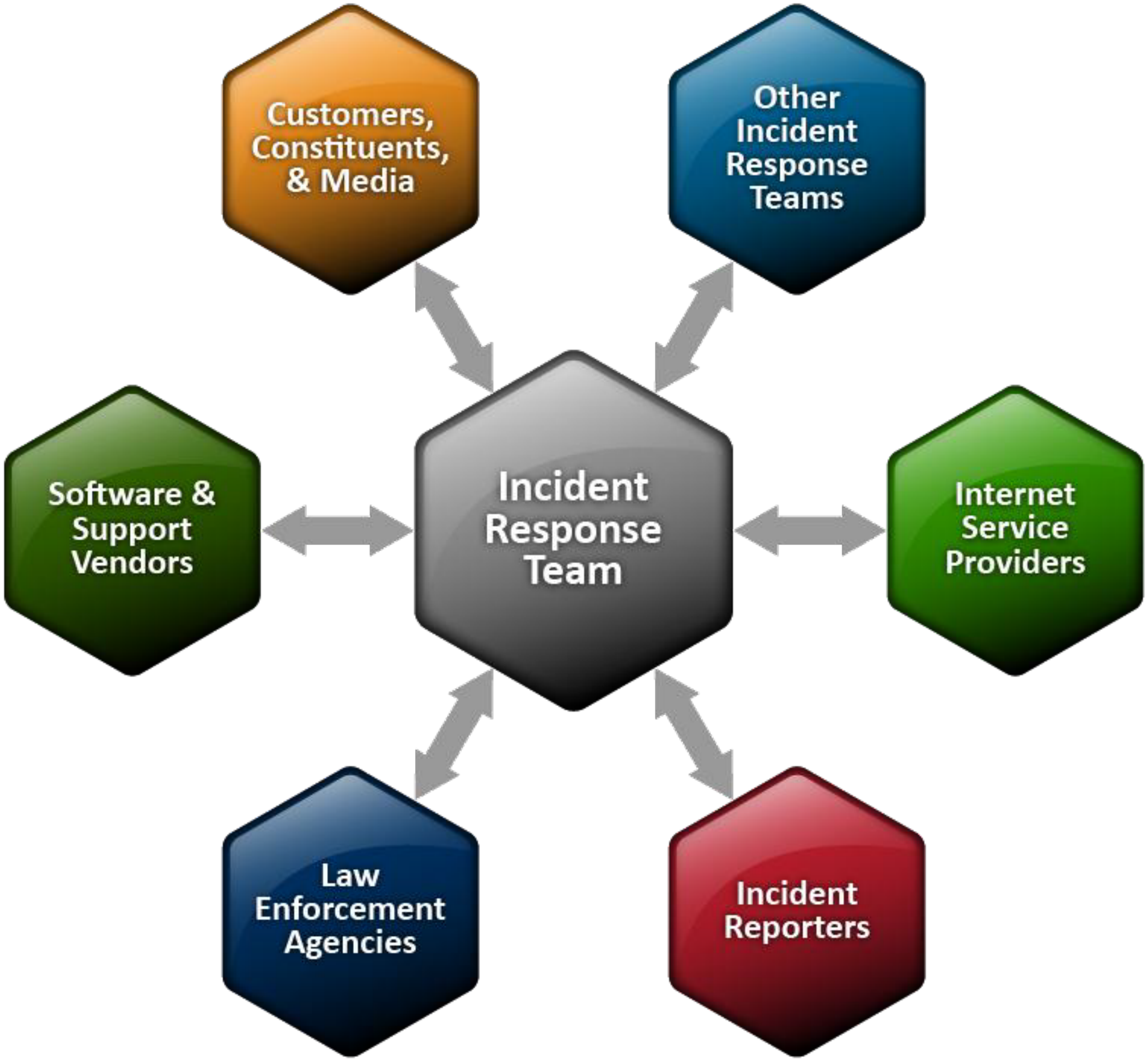
ISACA Incident Response Plan Elements

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Incident Response Procedure Elements

- **Procedures should be based on the incident response policy and plan.**
  - **Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team.**
  - **SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organization are reflected in response operations.**
  - **In addition, following standardized responses should minimize errors, particularly those that might be caused by stressful incident handling situations.**
  - **SOPs should be tested to validate their accuracy and usefulness, then distributed to all team members.**
  - **Training should be provided for SOP users; the SOP documents can be used as an instructional tool. Suggested SOP elements are presented throughout Section 3.**

Communications with Outside Parties


Customers, Constituents, & Media
Other Incident Response Teams
Software & Support Vendors
Incident Response Team
Internet Service Providers
Law Enforcement Agencies
Incident Reporters

The Media

- Conduct training sessions on interacting with the media regarding incidents, which should include the importance of not revealing sensitive information,
  - such as technical details of countermeasures that could assist other attackers, and the positive aspects of communicating important information to the public fully and effectively.
- Establish procedures to brief media contacts on the issues and sensitivities regarding a particular incident before discussing it with the media.
- Maintain a statement of the current status of the incident so that communications with the media are consistent and up-to-date.
- Remind all staff of the general procedures for handling media inquiries.

Mock Inerviews

- The following are examples of questions to ask the media contact:
- Who attacked you? Why?
- When did it happen? How did it happen? Did this happen because you have poor security practices?
- How widespread is this incident? What steps are you taking to determine what happened and to prevent future occurrences?
- What is the impact of this incident? Was any personally identifiable information (PII) exposed? What is the estimated cost of this incident?

Other Outside Parties (1)

- Organization’s ISP.
  - An organization may need assistance from its ISP in blocking a major network-based attack or tracing its origin.
- Owners of Attacking Addresses.
  - If attacks are originating from an external organization’s IP address space, incident handlers may want to talk to the designated security contacts for the organization to alert them to the activity or to ask them to collect evidence.
  - It is highly recommended to coordinate such communications with US-CERT or an ISAC.

Other Outside Parties (2)

- Software Vendors.
  - Incident handlers may want to speak to a software vendor about suspicious activity.
  - This contact could include questions regarding the significance of certain log entries or known false positives for certain intrusion detection signatures, where minimal information regarding the incident may need to be revealed.
  - More information may need to be provided in some cases—for example, if a server appears to have been compromised through an unknown software vulnerability.
  - Software vendors may also provide information on known threats (e.g., new attacks) to help organizations understand the current threat environment.

Other Outside Parties (3)

- **Other Incident Response Teams.**
  - An organization may experience an incident that is similar to ones handled by other teams; proactively sharing information can facilitate more effective and efficient incident handling
- **Affected External Parties.**
  - An incident may affect external parties directly—for example, an outside organization may contact the organization and claim that one of the organization's users is attacking it. Another way in which external parties may be affected is if an attacker gains access to sensitive information regarding them, such as credit card information. In some jurisdictions, organizations are required to notify all parties that are affected by such an incident.

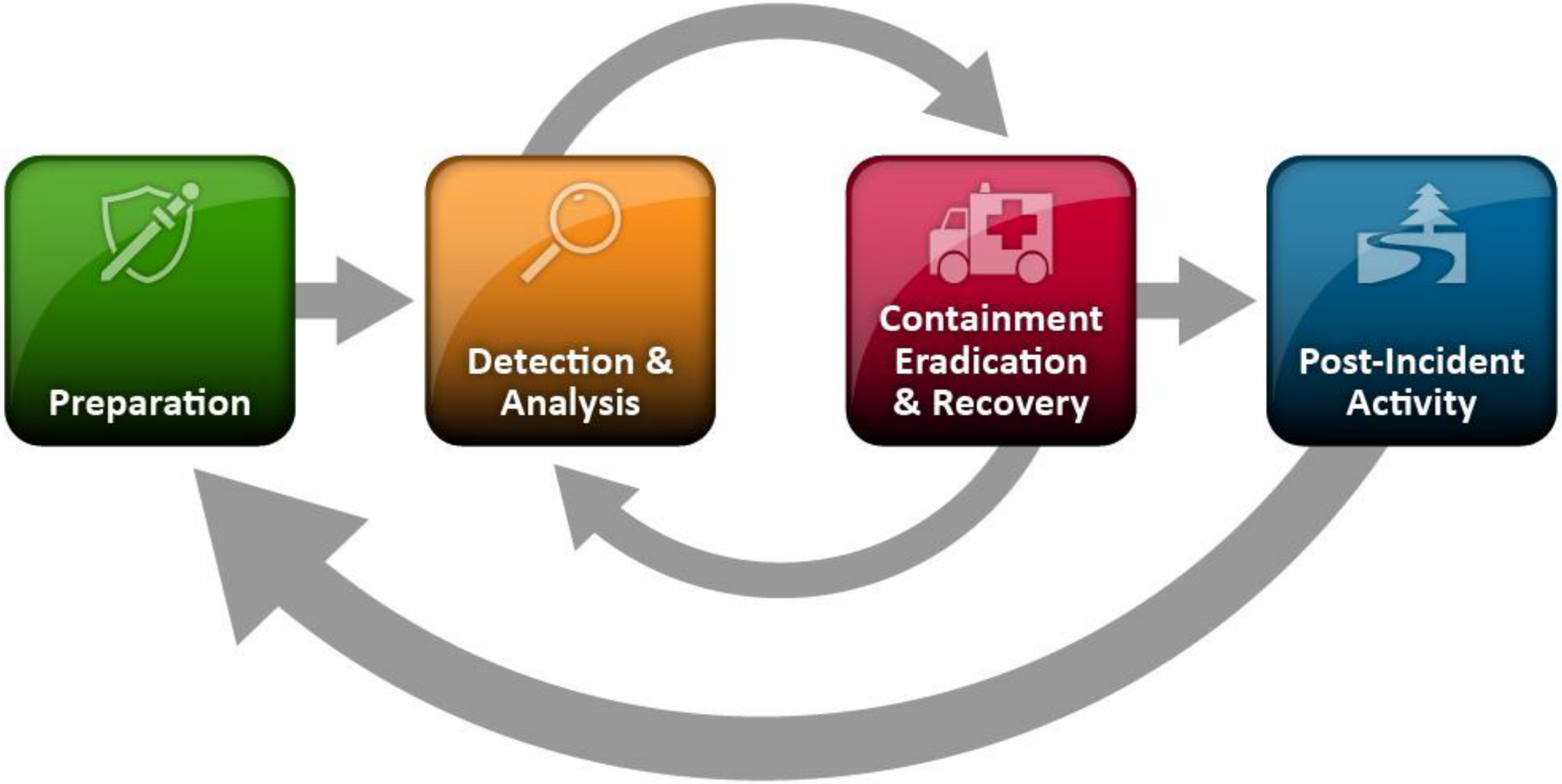
ISACA Gap Analysis

- Gap Analysis – between current incident response capabilities and desired capabilities.
- Processes that need to be improved to be more efficient and effective
- Resources needed to achieve the objectives for the incident response capability

Incident Response Procedures
Incident Management Organization

Domain 4:
Information Security Incident Management

NIST Incident Response Life Cycle



Incident Response Preparation
Incident Handler Communications

- Contact information for team members and others within and outside the organization
  - On-call information for other teams within the organization, including escalation information
- Incident reporting mechanisms
  - phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
- Issue tracking system
  - for tracking incident information, status, etc.
- Smartphones to be carried by team members for off-hour support and onsite communications
- Encryption software to be used for communications among team members, within the organization and with external parties
- War room for central communication and coordination
- Secure storage for securing evidence & other sensitive materials

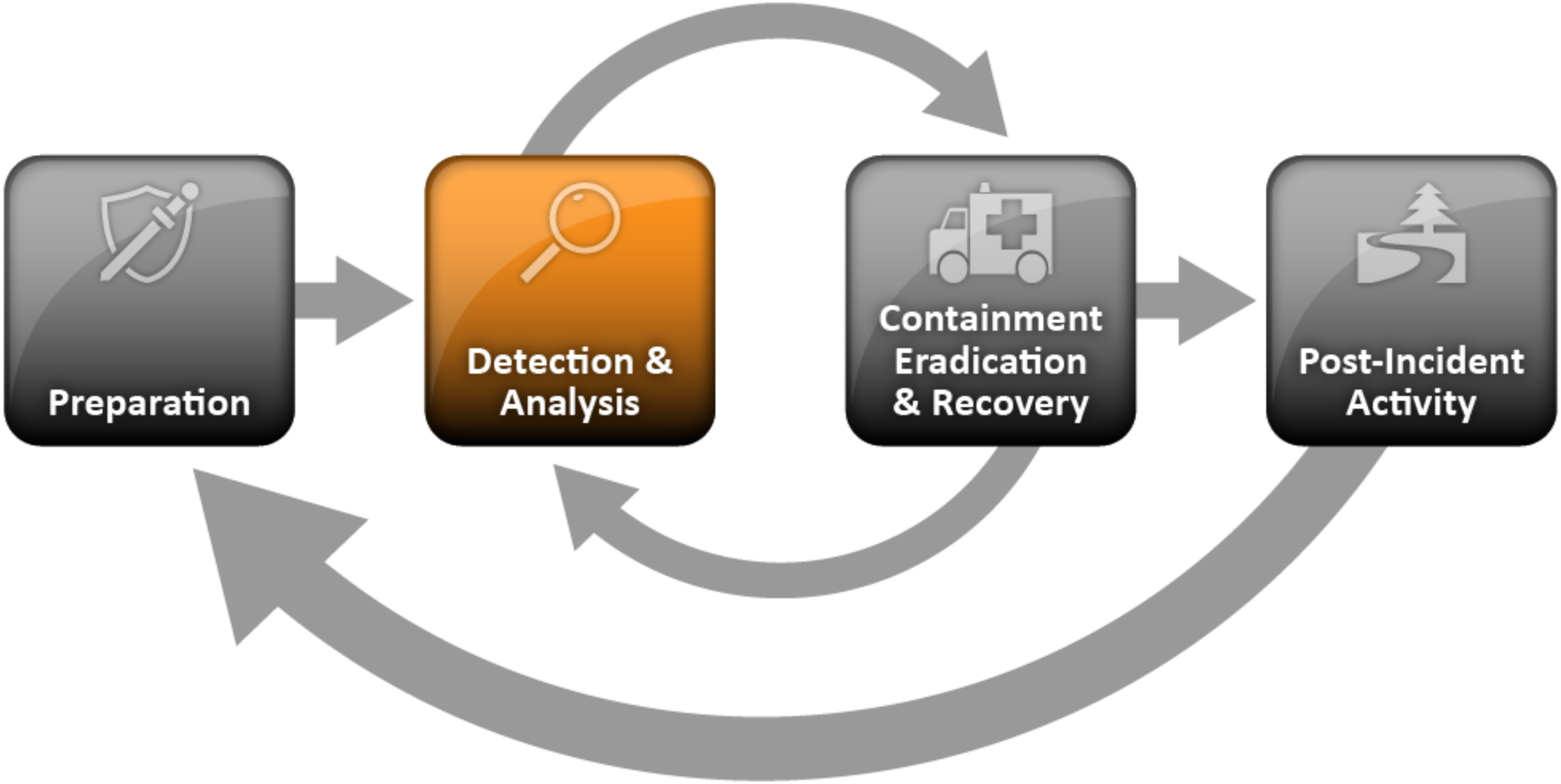
Incident Response Preparation
Incident Analysis Hardware & Software

- Digital forensic workstations and/or backup devices to create disk images, preserve log files, and save other relevant incident data
- Laptops for analyzing data, sniffing packets, and writing reports
- Spares
  - workstations, servers, and networking equipment, or the virtualized equivalents as restoring backups and trying out malware
- Blank removable media
- Portable printer to print copies of log files and other evidence
- Packet sniffers & protocol analyzers
  - capture and analyze network traffic
- Digital forensic software to analyze disk images
- Removable media with trusted versions of programs to be used to gather evidence from systems
- Evidence gathering accessories
  - including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

Incident Response Preparation
Incident Analysis Resources

- Port lists, including commonly used ports and Trojan horse ports
- Documentation for OSs, applications, protocols, and intrusion detection and antivirus products
- Network diagrams and lists of critical assets, such as database servers
- Current baselines of expected network, system, and application activity
- Cryptographic hashes of critical files22 to speed incident analysis, verification, and eradication
- Incident Mitigation Software:
  - Access to images of clean OS and application installations for restoration and recovery purposes

Detection and Analysis



Detection and Analysis
Attack Vectors (1 of 2)

- **External/Removable Media:**
  - An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:**
  - An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
- **Web:**
  - An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- **Email:**
  - An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

Detection and Analysis Attack Vectors (2 of 2)

- **Impersonation:**
  - An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage:**
  - Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- **Loss or Theft of Equipment:**
  - The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
- **Other:**
  - An attack that does not fit into any of the other categories.

Detection and Analysis
Signs of an Incident

- **Incidents may be detected through many different means, with varying levels of detail and fidelity.**
  - **Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.**
- **The volume of potential signs of incidents is typically high**
  - **not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day.**
- **Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.**

Detection and Analysis
Signs of an Incident - Precursors

- Web server log entries that show the usage of a vulnerability scanner
- An announcement of a new exploit that targets a vulnerability of the organization's mail server
- A threat from a group stating that the group will attack the organization.

Source	Description
Alerts	
IDPSs	IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when in fact there has been none. Analysts should manually validate IDPS alerts either by closely reviewing the recorded supporting data or by getting related data from other sources.[31]
SIEMs	Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data (see below).
Antivirus and antispam software	Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users' mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts.
File integrity checking software	File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected.
Third-party monitoring services	Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other incident response teams.
Logs	
Operating system, service and application logs	Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident. Section 3.2.4 discusses the value of centralized logging.
Network device logs	Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices.

Alerts & Logs

Precursors and Indicators (2)

Source	Description
Network flows	A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
Publicly Available Information	
Information on new vulnerabilities and exploits	Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.[32] Organizations such as US-CERT[33] and CERT®/CC periodically provide threat update information through briefings, web postings, and mailing lists.
People	
People from within the organization	Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information how confident they are of the accuracy of the information. Recording this estimate along with the information provided can help considerably during incident analysis, particularly when conflicting data is discovered.
People from other organizations	Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as setting up a phone number and email address, configured to forward messages to the help desk.

Detection and Analysis
Incident Prevention (1 of 2)

- **Risk Assessments.**
  - Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities.
    - This should include understanding the applicable threats, including organization-specific threats.
    - Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached.
- **Host Security.**
  - All hosts should be hardened appropriately using standard configurations.
    - In addition to keeping each host properly patched, hosts should be configured to follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks.
  - Hosts should have auditing enabled and should log significant security-related events.

Detection and Analysis
Incident Prevention (2 of 2)

- **Network Security.**
  - The network perimeter should be configured to deny all activity that is not expressly permitted.
    - This includes securing all connection points, such as virtual private networks (VPNs) and dedicated connections to other organizations.
- **Malware Prevention.**
  - Software to detect and stop malware should be deployed throughout the organization.
    - Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).
- **User Awareness and Training.**
  - Users should be made aware of policies and procedures regarding appropriate use of networks, systems, and applications.

Detection and Analysis
Effective Incident Analysis

- Profile Networks and Systems.
- Understand Normal Behaviors.
- Create a Log Retention Policy.
- Perform Event Correlation.
- Keep All Host Clocks Synchronized.
- Maintain and Use a Knowledge Base of Information.
- Use Internet Search Engines for Research.
- Run Packet Sniffers to Collect Additional Data.
- Filter the Data.
- Seek Assistance from Others.

Detection and Analysis
Incident Documentation

- The current status of the incident
  - (new, in progress, forwarded for investigation, resolved, etc.)
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Chain of custody, if applicable
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken (rebuild the host, upgrade an application)

Detection and Analysis
Incident Prioritization (1 of 2)

- **Functional Impact of the Incident.**
  - Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained.
- **Information Impact of the Incident.**
  - Incidents may affect the confidentiality, integrity, and availability of the organization's information.
  - Incident handlers should consider how this information exfiltration will impact the organization's overall mission.
    - An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization.

Detection and Analysis
Incident Prioritization (2 of 2)

- **Recoverability from the Incident.**
  - The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.
  - In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future.
  - In other cases, an incident may require far more resources to handle than what an organization has available.
  - Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling.

NIST Functional Impact Categories

Category	Definition
None	No effect to the organization’s ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

NIST Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

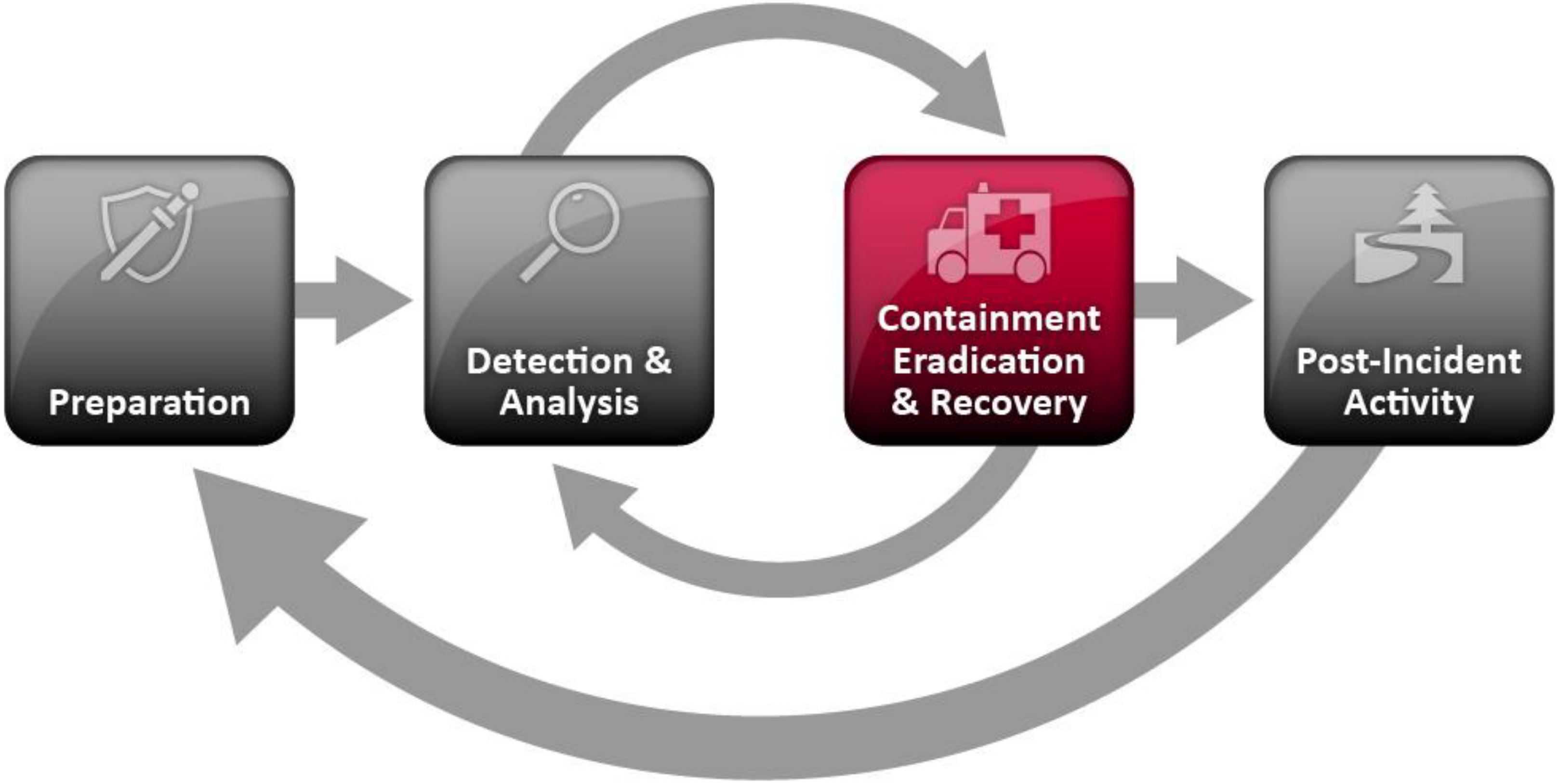
NIST Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Detection and Analysis
Incident Notification

- CIO
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources
  - (for cases involving employees, such as email harassment)
- Public affairs (if appropriate)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies)
- Law enforcement (if appropriate)

Containment, Eradication & Recovery



Containment, Eradication & Recovery
Choosing a Containment Strategy

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability
  - (network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
  - (partial containment, full containment)
- Duration of the solution
  - (emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

Containment, Eradication & Recovery Evidence Gathering and Handling

- **Detailed logs including:**
  - Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
  - Name, title, and phone number of each individual who collected or handled the evidence during the investigation
  - Time and date (including time zone) of each occurrence of evidence handling
  - Locations where the evidence was stored.

Containment, Eradication & Recovery Identifying the Attacking Hosts (1 of 3)

- **Validating the Attacking Host’s IP Address.**
  - New incident handlers often focus on the attacking host’s IP address.
  - The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests.
  - A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes.
  - Also, the attacker may have received a dynamic address that has already been reassigned to someone else.

Containment, Eradication & Recovery Identifying the Attacking Hosts (2 of 3)

- **Researching the Attacking Host through Search Engines.**
  - **Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack—for example, a mailing list message regarding a similar attack.**
- **Using Incident Databases.**
  - **Several groups collect and consolidate incident data from various organizations into incident databases.**
  - **This information sharing may take place in many forms, such as trackers and real-time blacklists.**
  - **The organization can also check its own knowledge base or issue tracking system for related activity.**

Containment, Eradication & Recovery Identifying the Attacking Hosts (3 of 3)

- **Monitoring Possible Attacker Communication Channels.**
  - Incident handlers can monitor communication channels that may be used by an attacking host.
  - For example, many bots use IRC as their primary means of communication.
  - Also, attackers may congregate on certain IRC channels to brag about their compromises and share information.
  - However, incident handlers should treat any such information that they acquire only as a potential lead, not as fact.

Containment, Eradication & Recovery Eradication

- After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.
- During eradication, it is important to identify all affected hosts within the organization so that they can be remediated.
- For some incidents, eradication is either not necessary or is performed during recovery.

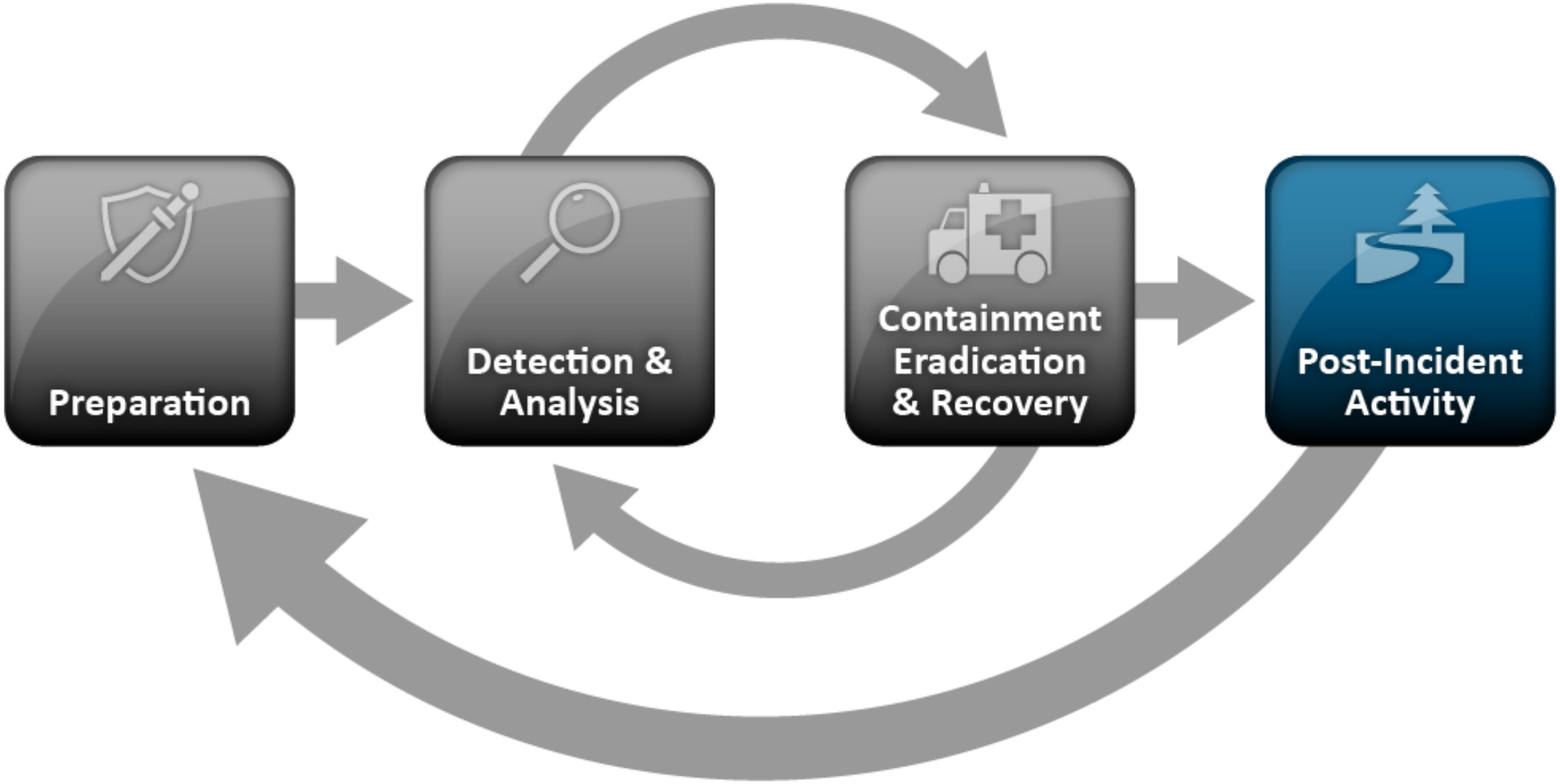
Containment, Eradication & Recovery Recovery (1 of 2)

- In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents.
  - Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists).
  - Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Containment, Eradication & Recovery Recovery (2 of 2)

- Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.
- For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents.
- The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

Post-Incident Activity



Post Incident Activity
Lessons Learned

- Exactly what happened, and at what times?
- How well did staff & management perform in dealing with the incident?
  - Were the documented procedures followed?
  - Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post Incident Activity Metrics

- Number of Incidents Handled
- Time Per Incident.
- Objective Assessment of Each Incident.
- Subjective Assessment of Each Incident.
- Evaluate Against:
  - Incident response policies, plans, and procedures
  - Tools and resources
  - Team model and structure
  - Incident handler training and education
  - Incident documentation and reports

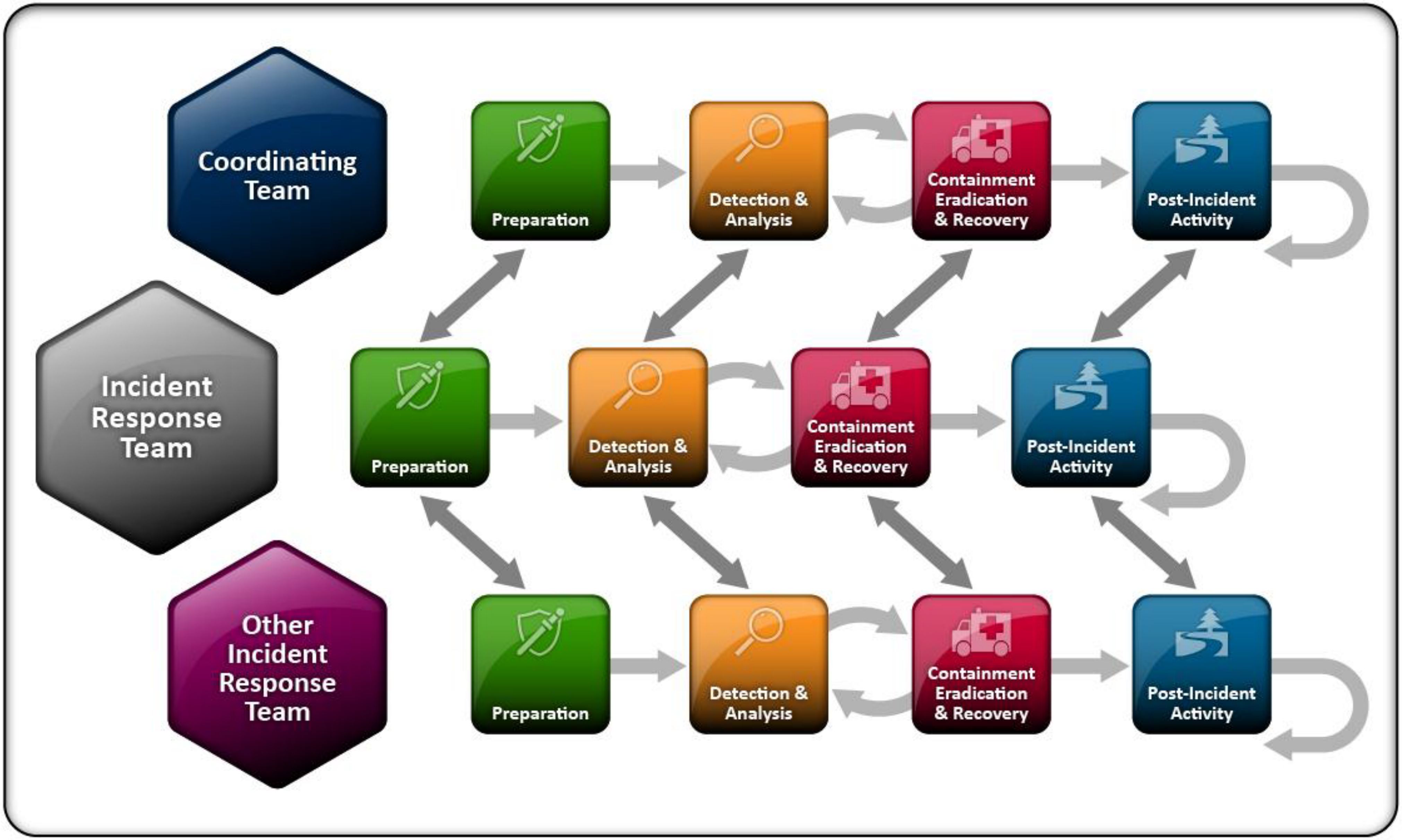
Post Incident Activity Retention Strategies

- **Prosecution.**
  - If it is possible that the attacker will be prosecuted, evidence may need to be retained until all legal actions have been completed.
    - In some cases, this may take several years.
- **Data Retention.**
  - Most organizations have data retention policies that state how long certain types of data may be kept.
    - For example, an organization may state that email messages should be retained for only 180 days.
- **Cost.**
  - Original hardware (e.g., hard drives, compromised systems) that is stored as evidence, as well as hard drives and removable media that are used to hold disk

NIST Incident Response Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST Incident Response Coordination



Roles and Responsibilities (CMU ISO)

- Incident Response Coordinator
  - ISO employee who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.
- Incident Response Handlers
  - are employees of the ISO, other CMU staff, or outside contractors who gather, preserve and analyze evidence so that an incident can be brought to a conclusion.
- Insider Threats (defined by CERT)
  - current or former employees, contractors, or business partners who have access to an organization’s restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization’s information or systems.
    - This particular threat is defined because it requires special organizational and technical amendments to the Incident Response Plan.

Roles and Responsibilities (CMU ISO) 2

- **Law Enforcement**
  - includes the CMU Police, federal, state and local law enforcement agencies, and U.S. government agencies that present warrants or subpoenas for the disclosure of information.
    - Interactions with these groups will be coordinated with the Office of General Counsel.
    - CMU Office of General Counsel (OGC) is the liaison between the ISO and outside Law Enforcement, and will provide counsel on the extent and form of all disclosures to law enforcement and the public.
- **Officers**
  - Officers are the staff designates for various regulatory frameworks to which the University is required to comply.
- **Users**
  - members of the CMU community or anyone accessing an Information System, Institutional Data or CMU networks who may be affected by an incident.

Incident Management Resources and Objectives

Domain 4:
Information Security Incident Management

Incident Management Resources

- IT Department
- Internal Audit
- Legal Department
- Physical Security
- Risk Management
- Insurance Department
- PR Department
- Sales and Marketing
- Senior Management
- Compliance Office
- Privacy Officer

Incident Response Plan (IRP)

- Policies, Standards and Procedures that support an Incident Response Plan
  - Alignment of activities with Incident Management Team (IMT)
  - Set accurate expectations
  - Provide guidance for operational needs
  - Maintain consistency and reliability of services
  - Clearly understand roles and responsibilities
  - Set requirements for identified alternate personnel for all important functions.

Incident Response Technology Concepts

- Security principles
  - CIA Triad, Authentication, Integrity, Access Control, Privacy, Non-repudiation
- Security vulnerabilities/weaknesses
  - Physical Security, Phishing, Protocol Design Flaws, Malicious Code, Implementation Flaws, Configuration weaknesses, User Errors
- The Internet
  - Protocols, Configurations
- Operating Systems
  - System Configuration, System Forensics, Log Files, System Privileges
- Malicious Code
- Programming Skills

Incident Response Team Organization

- Central IRT
  - Single IRT, typical in small organizations
- Distributed IRT
  - Geographically dispersed and/or functionally distributed
- Coordinating IRT
  - Central team to manage distributed IRTs
- Outsourced IRT
- Staff Composition Factors
  - Type
  - Mission
  - Nature and range of service offered
  - Constituency size and technology base
  - Anticipated incident load
  - Severity or complexity of incident reports
  - Funding

Computer Security Incident Response Teams (CSIRT) (CISA DHS)

- CSIRT - Computer Security Incident Response Team
- CSIRC - Computer Security Incident Response Capability or Center
- CIRC - Computer Incident Response Capability or Center
- CIRT - Computer Incident Response Team
- IHT - Incident Handling Team
- IRC - Incident Response Center or Incident Response Capability
- IRT - Incident Response Team
- SERT - Security Emergency Response Team
- SIRT - Security Incident Response Team

DHS CSIRT Definition

- A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing part of the incident management capability for a particular organization.
- When a CSIRT exists in an organization, it is generally the focal point for coordinating and supporting incident response.
- By definition, a CSIRT must perform—at a minimum—incident handling activities.
- This entails analyzing and resolving events and incidents that are reported by end users or are observed through proactive network and system monitoring.

CSIRT Incident Handling Activities (1)

- **determining the impact, scope, & nature of the event or incident**
- **understanding the technical cause of the event or incident**
- **identifying what else may have happened or other potential threats resulting from the event or incident**
- **researching and recommending solutions and workarounds**
- **coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency,*Constituency* refers to the group or individuals being supported and serviced by the CSIRT.**

CSIRT Incident Handling Activities (2)

- disseminating information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts, advisories, Web pages, and other technical publications
- coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement
- maintaining a repository of incident and vulnerability data and activity related to the constituency that can be used for correlation, trending, and developing lessons learned to improve the security posture and incident management processes of an organization

Source: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

Additional CSIRT Activities (1 of 2)

- recommend best practices regarding secure configurations, defense-in-depth strategies for protecting systems, networks, and critical data and assets, and incident prevention
- perform or participate in vulnerability assessment and handling, artifact analysis
- provide input into or participate in security audits or assessments such as infrastructure reviews, best practice reviews, vulnerability scanning, or penetration testing

Additional CSIRT Activities (2 of 2)

- conduct public monitoring or technology watch activities such as reviewing security web sites, mailing list, or general news and vendor sites to identify new or emerging technical developments, intruder activities, future threats, legal and legislative rulings, social or political threats, or new defensive strategies
- support legal and law enforcement efforts through the collection and analysis of forensics evidence (provided that staff have the appropriate expertise, training, and tools)

Source: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

CSIRT & Business Intelligence

- CSIRT can provide the information it collects on the types of threats and attacks that currently impact or could potentially threaten the enterprise
- CSIRT can provide its expertise in general intruder attacks and trends and corresponding mitigation strategies
- CSIRT can provide its understanding of infrastructure and policy weakness and strengths based on performed incident postmortems

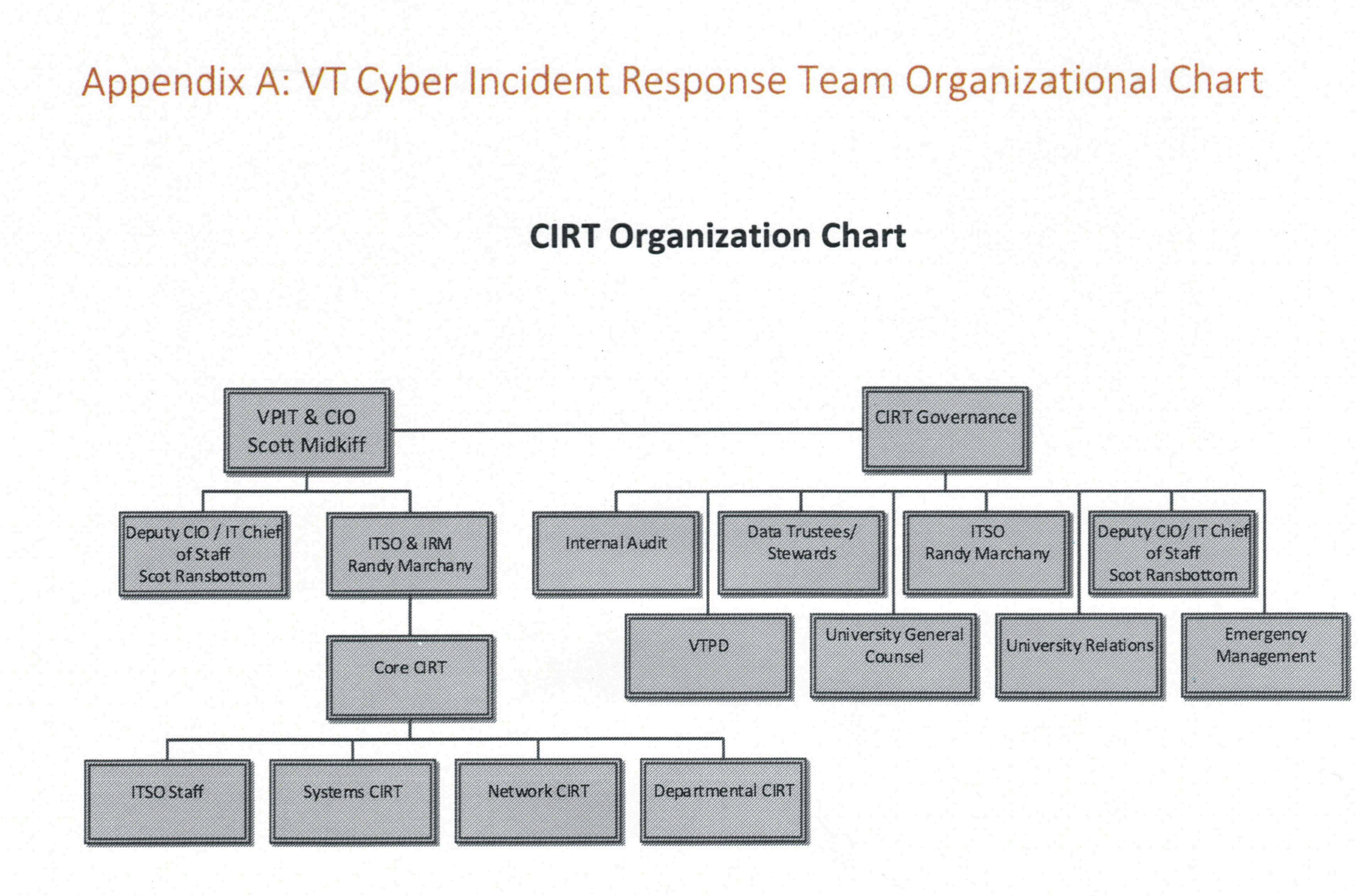
Source: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

CSIRT Required Processes

- notification and communication
- analysis, response, and resolution
- collaboration and coordination
- maintenance and tracking of records
- evaluation and quality assurance
- Plus
  - Incident tracking and correlation
  - Performing incident postmortems
  - CSIRTS in Software Development Organizations

Source: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

Va Tech CIRT Org Chart



Appendix A: VT Cyber Incident Response Team Organizational Chart

CIRT Organization Chart

VPIT & CIO
Scott Midkiff

CIRT Governance

Deputy CIO / IT Chief of Staff
Scot Ransbottom

ITSO & IRM
Randy Marchany

Core CIRT

ITSO Staff

Systems CIRT

Network CIRT

Departmental CIRT

Internal Audit

Data Trustees/ Stewards

ITSO
Randy Marchany

Deputy CIO/ IT Chief of Staff
Scot Ransbottom

VTPD

University General Counsel

University Relations

Emergency Management

ISACA Incident Response Objectives

- Handle incidents when they occur so the exposure can be contained or eradicated to enable recovery within the recovery time objectives (RTOs).
- Restore systems to normal operations
- Prevent previous incidents from recurring by documenting and learning from past incidents.
- Deploy proactive countermeasures to prevent/ minimize the probability of incidents from taking place.

Incident Management Metrics and Indicators

Domain 4:
Information Security Incident Management

Metrics

- **Maximum Tolerable Downtime**
  - (MTD) is the time after which the process being unavailable creates irreversible consequences generally, exceeding the MTD results with severe damage to the viability of the business.
- **Maximum Tolerable Outage**
  - (MTO) is a common measure in both disaster recovery and business continuity. It is the maximum amount of time a system or resource can remain unavailable before its loss starts to have an unacceptable impact on the goals or the survival of an organization.

Key Recovery Targets

- Recovery time objective (RTO)
  - maximum period that elapses from the onset of a disaster until the resumption of service.
- Recovery point objective (RPO)
  - maximum data loss from the onset of a disaster.
- Recovery capacity objective (RCapO)
  - processing or storage capacity of an alternate process or system, as compared to the primary process or system.
- Recovery consistency objective (RCO)
  - consistency and integrity of processing in a recovery system, as compared to the primary processing system.

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.

Incident Management Metrics (ISACA)

- **Total number of reported incidents**
- **Total number of detected incidents**
- **Number of days without incident**
- **Average incident response time relative to RTO**
- **Average time to resolve an incident**
- **Total number of incidents successfully resolved**
- **Incidents not resolved successfully**
- **Proactive and preventative measures taken**
- **Total # of employees receiving security training**
- **Total damages from incidents (reported & detected)**
- **Total savings from potential incident prevention**
- **Total labor responding to incidents**
- **Detection and notification times**

Incident Response Metrics (Gregory)

- Number of incidents of each incident severity and type
- Dwell time (time from start of incident to the time the organization became
- aware of the incident)
- Time required to contain the incident
- Time required to resolve and close incidents
- Number of times incident response SLAs were not met
- Improvements identified and implemented based on table-top exercises and lessons learned from actual incidents
- Number or percentage of employees receiving security awareness training, as well as any correlation between this and the number of incidents
- Number of records compromised
- Number of external people affected and notified
- Total cost required to resolve each incident

Samanage Metrics

1. Incident Response Time
2. First-Time Resolution Rate
3. SLA Compliance Ratio
4. Cost per Ticket
5. Number of Active Tickets
6. Recategorized Incidents
7. Reopen Rate
8. Incidents per Department
9. Incidents by Type
10. Incidents not Initiated via Self-Service
11. Incidents With Associated Problems
12. Escalated Incidents
13. Incidents Resolved Remotely
14. Incidents With No Known Resolution
15. Ticket Volume

Incident Response Metrics

1. Detection success
2. Detection to decision
3. Decision speed
4. False positive rates
5. Time to mitigation/containment

Bonus Metric

- Security versus administrative tasks
  - – Cody Cornell, Swimlane

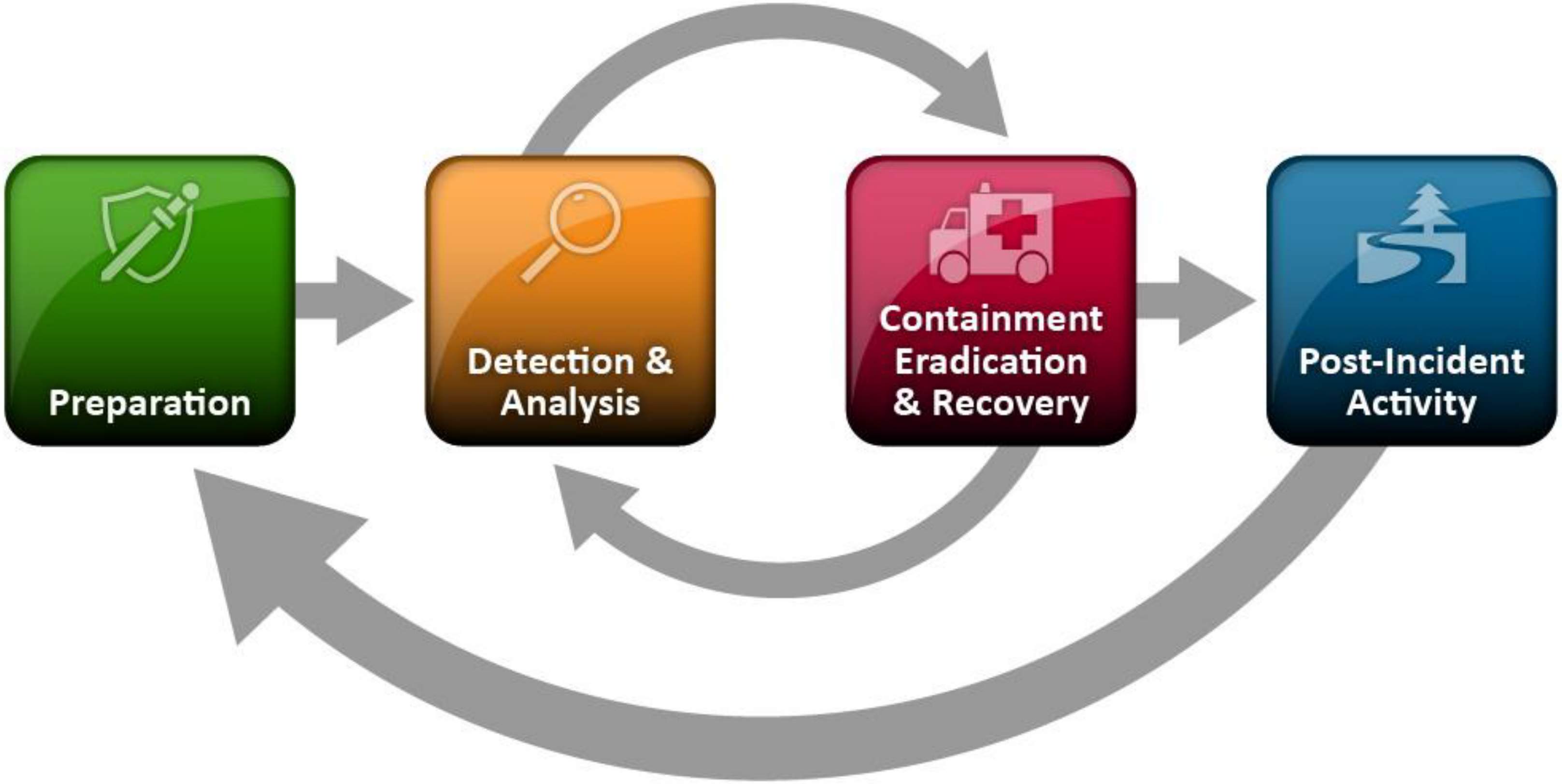
Developing an Incident Response Plan

Domain 4:
Information Security Incident Management

3 Case Studies

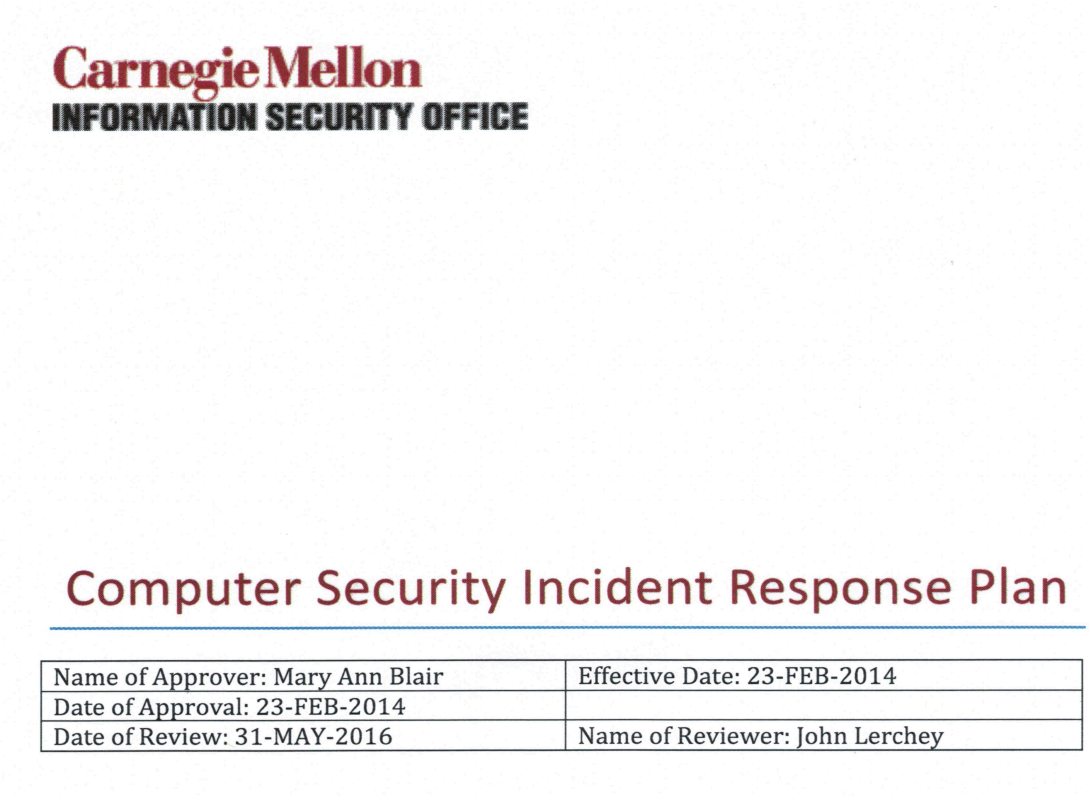
1. **Carnegie Mellon Information Security Office**
   - https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan.pdf
2. **State of Connecticut Incident Response Plan Template**
3. **Virginia Tech Guide for Cyber Security Incident Response**
   - https://security.vt.edu/content/dam/security_vt_edu/downloads/incident_response.pdf

NIST Incident Response Life Cycle



Incident Response Lifecycle

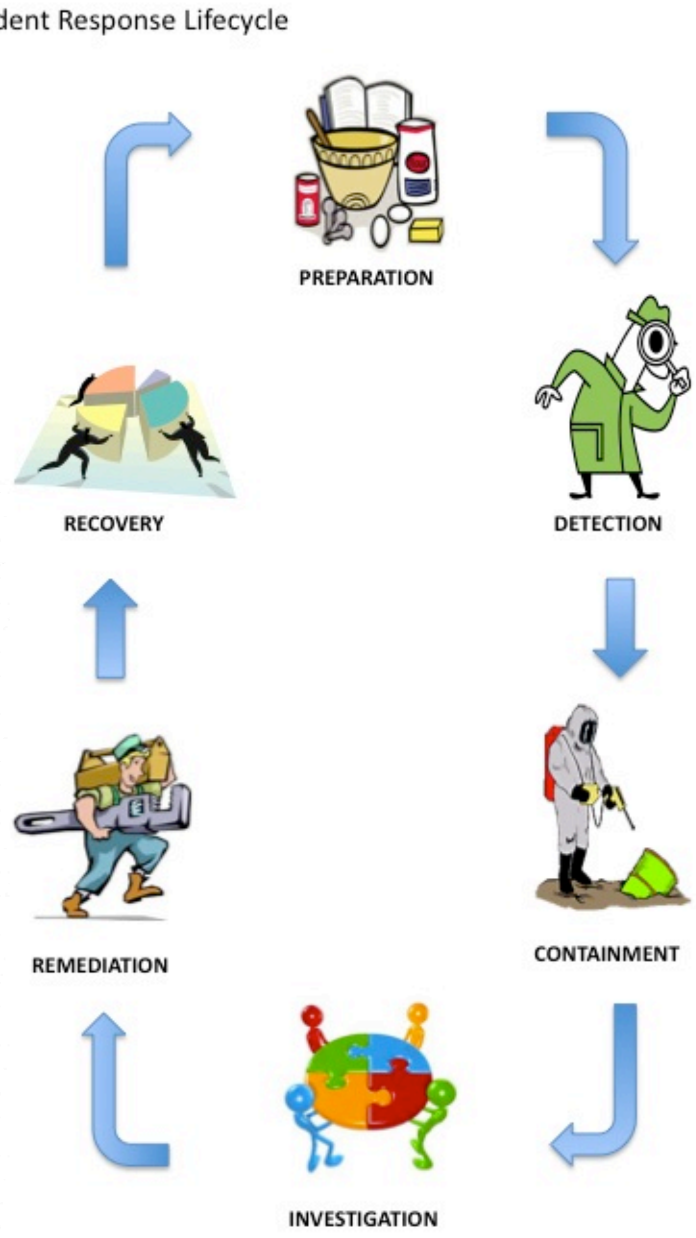
- **CMU Computer Security Incident Response Plan**



Carnegie Mellon
INFORMATION SECURITY OFFICE

Computer Security Incident Response Plan

Name of Approver: Mary Ann Blair	Effective Date: 23-FEB-2014
Date of Approval: 23-FEB-2014	
Date of Review: 31-MAY-2016	Name of Reviewer: John Lerchey



The Incident Response Lifecycle

https://www.cmu.edu/iso/governance/procedures/docs/incidentresponseplan.pdf

CMU Incident Response Plan Intro

- Purpose
- Scope
- Maintenance
- Authority
- Relationship to other Policies
- Relationship to Other Groups at CMU

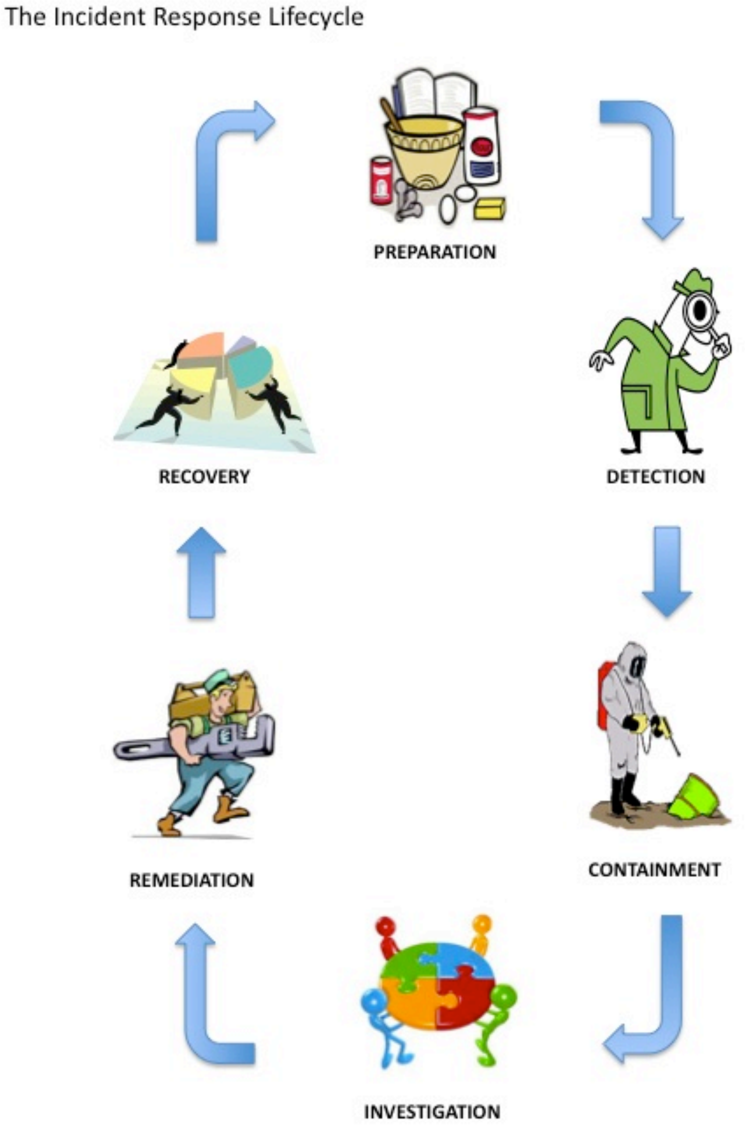
CMU IRP Definitions

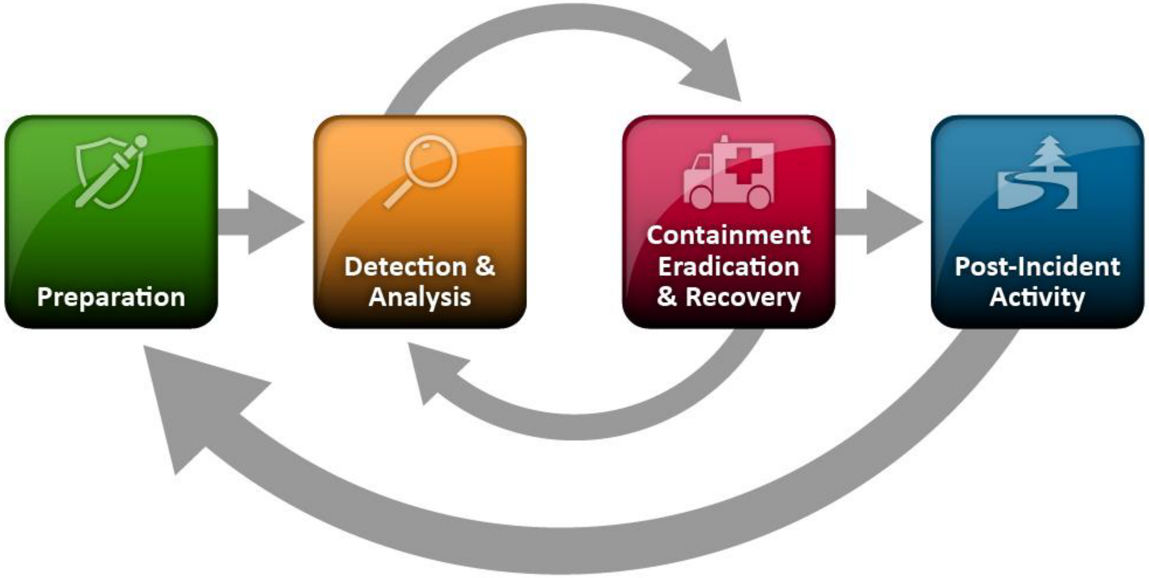
- Event
- Incident
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)

CMU IRP Roles & Responsibilities

- Incident Response Coordinator
- Incident Response Handlers
- Insider Threats
- Law Enforcement
- Office of General Counsel
- Officers
- Users

CMU Incident Response Phases





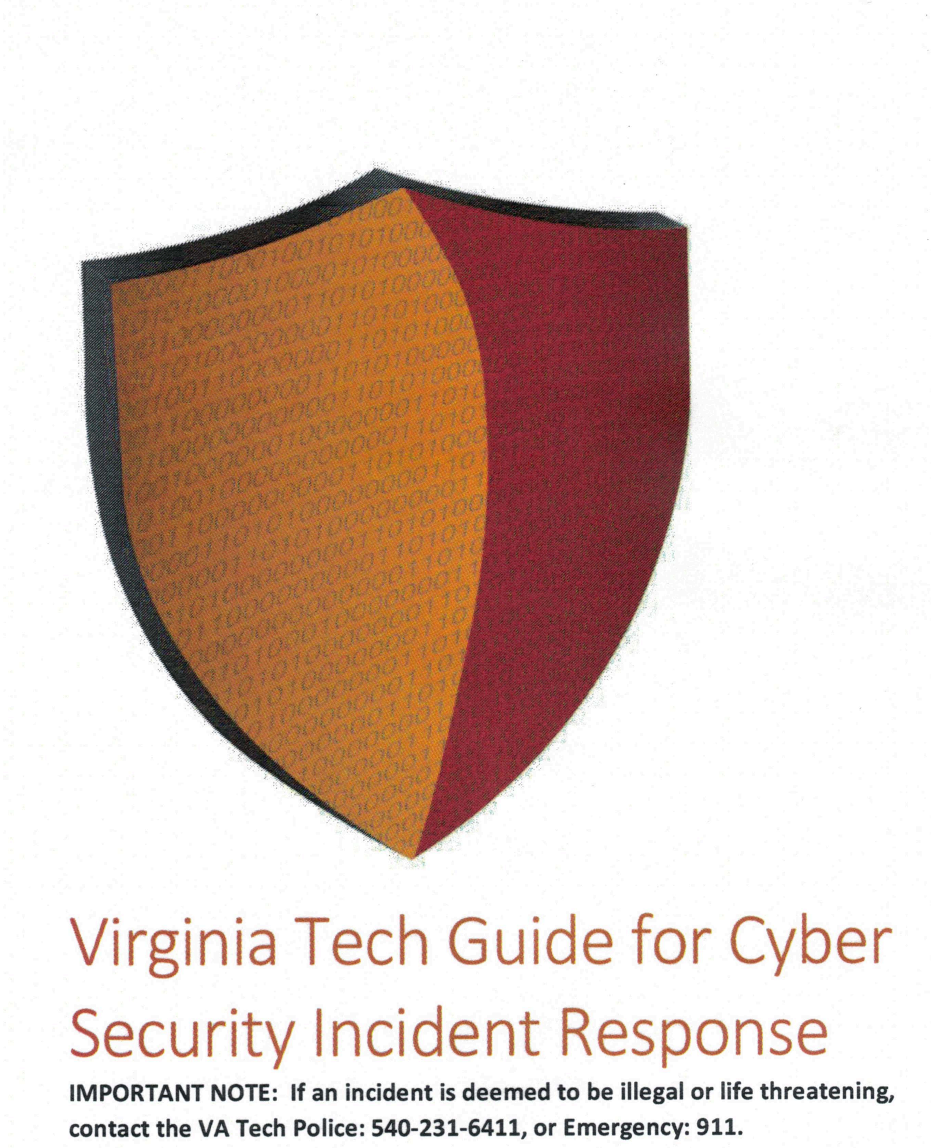
CMU Guidelines for the Incident Response Process

- Insider Threats
- Interactions with Law Enforcement
- Communications Plan
- Privacy

Documentation, Tracking, Reporting

- All incident response activities will be documented to include artifacts obtained using methods consistent with chain of custody and confidentiality requirements.
- Incidents will be prioritized and ranked according to their potential to disclose restricted data.
  - As an investigation progresses, that ranking may change, resulting in a greater or lesser prioritization of ISO resources.
- Incidents will be reviewed post-mortem to assess whether the investigational process was successful and effective.
  - Subsequent adjustments may be made to methods and procedures used by the ISO and by other participants to improve the incident response process.
- Artifacts obtained during the course of an investigation may be deleted after the conclusion of the investigation and post-mortem analysis unless otherwise directed by OGC.

Viriginia Tech (VPI)



Virginia Tech Guide for Cyber Security Incident Response

IMPORTANT NOTE: If an incident is deemed to be illegal or life threatening, contact the VA Tech Police: 540-231-6411, or Emergency: 911.

VPI Introduction

- Authority
- Purpose and Scope
- Audience
- Document Structure (next slide)
- Section 2 discusses the need for cyber incident response capabilities, and outlines possible cyber incident response team structures as well as other groups within the organization that may participate in cyber incident response handling.
- Section 3 provides guidelines for effective, efficient, and consistent incident response capabilities and reviews the cyber security incident response elements.

VPI Document Structure

- Appendix A – VT Cyber Incident Response Teams Organizational Chart
- Appendix B – Communication Workflow for Sensitive Data Exposure
- Appendix C – CIRT Team, IT Council, Compliance Officers Directories
- Appendix D – Incident Handling Checklist
- Unix, Linux and Windows Forensics checklists
- Appendix E – Detection and Analysis Information Gathering Outline
- Appendix F – Communication Plan Worksheet
- Appendix G – Internal Audit Guidelines for unacceptable computer use
- Appendix H – University Policies and Standards
- Appendix I – Workflow Diagram for Incident Escalation
- Appendix J – Contact information for local police and FBI
- Appendix K – Generalized Cyber Incident Escalation and Workflow Diagram
- Appendix L – Acronyms
- Appendix M – Step by Step Cyber Incident Response

VPI Section 2 - Incident Examples

- An incident in which an attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- An incident in which users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An incident where an attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- An incident where a user provides or exposes sensitive information to others through peer-to-peer file sharing services.

VPI Section 2 CSIRT Mission

1. Limit the impact of cyber incidents in a way that safeguards the well-being of the University community.
2. Protect the information technology infrastructure of the University.
3. Protect sensitive University data from disclosure, modification, and exfiltration.
4. Collect the information necessary to pursue investigation(s) at the request of the proper University authority.

VPI Section 2 CIRT Response Goals

- To protect the well-being of the University community.
- To protect the confidentiality, integrity, and availability of University systems, networks and data.
- To help University personnel recover their business processes after computer or network security incidents.
- To provide a consistent response strategy to system and network threats that put Virginia Tech data and systems at risk.
- To develop and activate a communications plan including initial reporting of the incident as well as ongoing communications as necessary.
- To address cyber related legal issues.
- To coordinate efforts with external Computer Incident Response Teams.
- To minimize the University’s reputational risk by notifying appropriate University officials of cyber incidents that may become high profile events and implementing timely and appropriate corrective actions.

VPI Cyber Incident Response Plan

- **Preparation:**
  - Maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
- **Identification:**
  - Confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
- **Containment:**
  - Minimizing loss, theft of information, or service disruption.
- **Eradication:**
  - Eliminating the threat.
- **Recovery:**
  - Restoring computing services quickly and securely.
- **Post-incident activities:**
  - Assessing response to better handle future incidents through utilization of reports, “Lessons Learned,” and after-action activities, or mitigation of exploited weaknesses to prevent similar incidents from occurring in the future.

VPI Authority for Cyber Incident Response

- Vice President for Information Technology and Chief Information Officer (CIO)
  - empowered to respond to IT security incidents by BOV Resolution “Information Technology Security and Authority”.
  - http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf
- Information Technology Security Officer (ITSO)
  - delegated authority by CIO to decide whether to activate CIRT, notifies Incident Governance Team of decision
- VPI CIRT Governance Team
  - a broad range of University stakeholders (see Appendix A).
- University Legal Counsel
  - any law enforcement/legal actions, questions about information disclosure, legal aspects of the investigation.

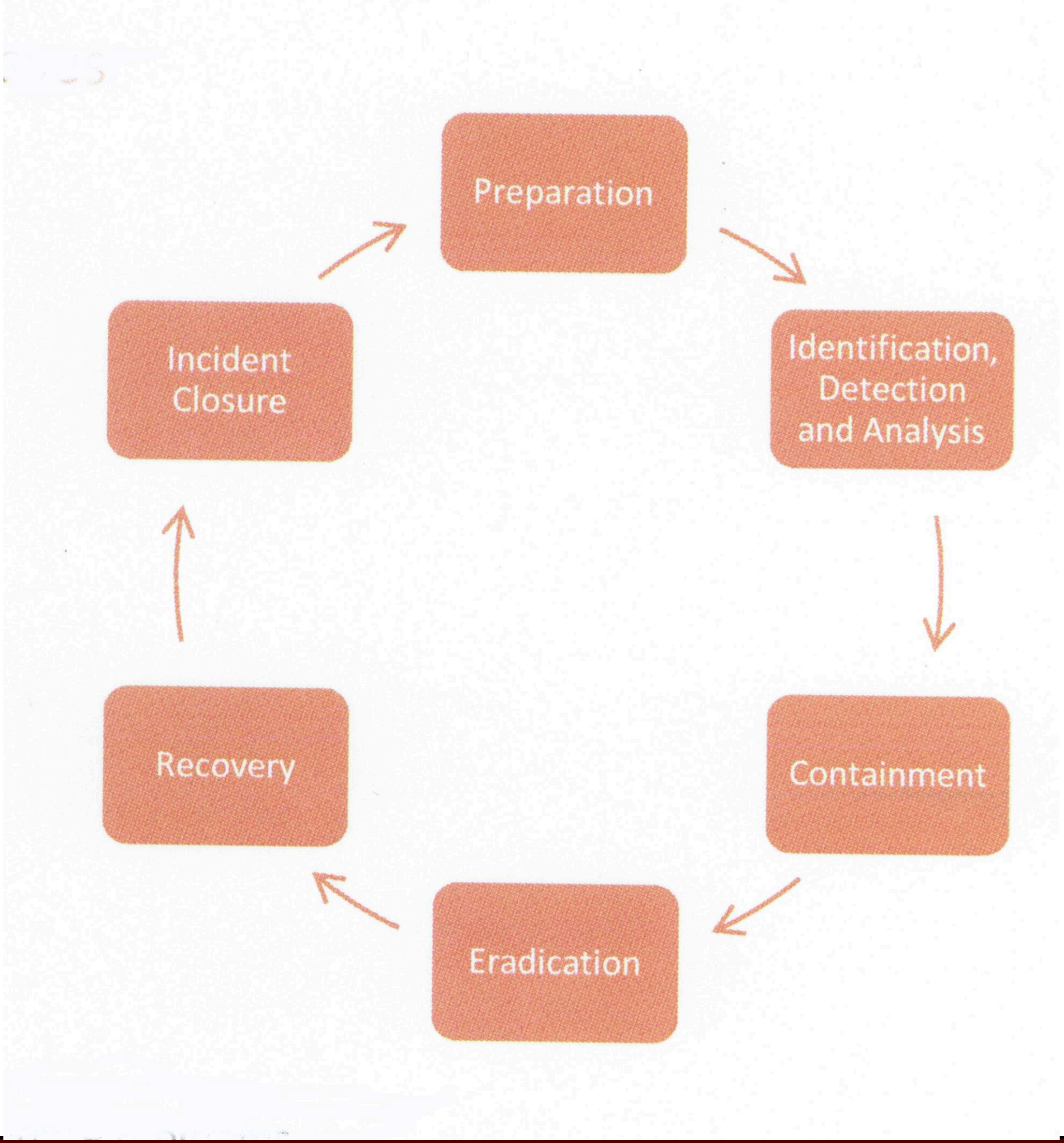
VPI Authority for Cyber Incident Response

- University President
  - personnel actions for staff
- Executive Vice President and Provost
  - personnel actions for faculty
- University Internal Audit
  - data integrity of critical University data, compliance with University procedures and fraud investigations
- Division of Student Affairs/Student Conduct
  - offenses by Virginia Tech students
- Virginia Tech Police Department
  - criminal matters
- Data Trustees/Stewards
  - sensitive or non-public data access and governance (data trustees and stewards are listed in the “Standard for Administrative Data Management”

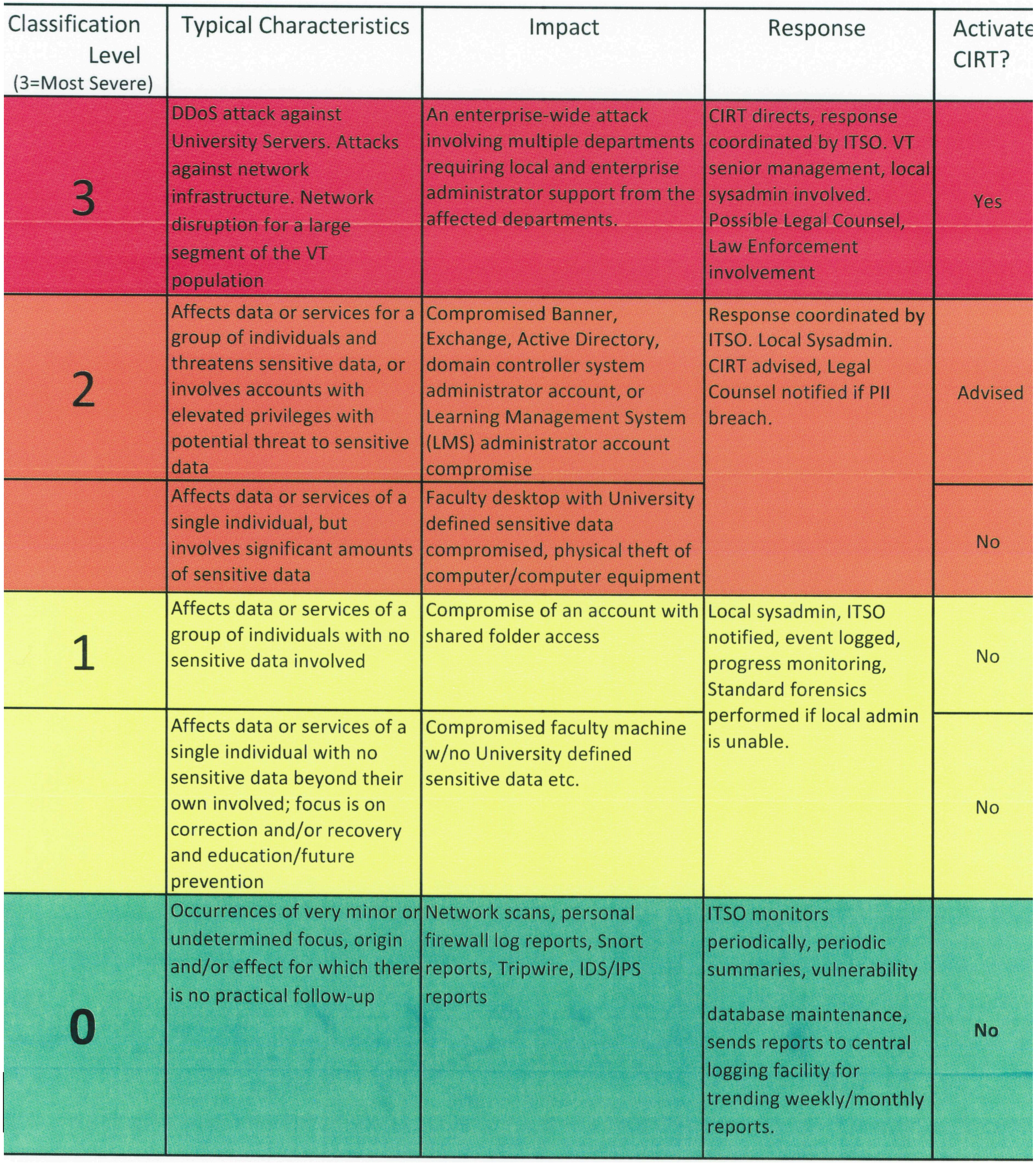
VPI Cyber Incident Response Governance Team

- Vice President for Information Technology & CIO
- Information Technology Security Officer
- University Legal Counsel
- University Internal Audit
- VT Police Department
- Data Trustees/Stewards
- University Relations

VPI Sec. 3 Incident Response Processes



VPI CIRT Incident Response Classification Matrix



Classification Level (3=Most Severe)	Typical Characteristics	Impact	Response	Activate CIRT?
3	DDoS attack against University Servers. Attacks against network infrastructure. Network disruption for a large segment of the VT population	An enterprise-wide attack involving multiple departments requiring local and enterprise administrator support from the affected departments.	CIRT directs, response coordinated by ITSO. VT senior management, local sysadmin involved. Possible Legal Counsel, Law Enforcement involvement	Yes
2	Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data	Compromised Banner, Exchange, Active Directory, domain controller system administrator account, or Learning Management System (LMS) administrator account compromise	Response coordinated by ITSO. Local Sysadmin. CIRT advised, Legal Counsel notified if PII breach.	Advised
	Affects data or services of a single individual, but involves significant amounts of sensitive data	Faculty desktop with University defined sensitive data compromised, physical theft of computer/computer equipment		No
1	Affects data or services of a group of individuals with no sensitive data involved	Compromise of an account with shared folder access	Local sysadmin, ITSO notified, event logged, progress monitoring, Standard forensics performed if local admin is unable.	No
	Affects data or services of a single individual with no sensitive data beyond their own involved; focus is on correction and/or recovery and education/future prevention	Compromised faculty machine w/no University defined sensitive data etc.		No
0	Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up	Network scans, personal firewall log reports, Snort reports, Tripwire, IDS/IPS reports	ITSO monitors periodically, periodic summaries, vulnerability database maintenance, sends reports to central logging facility for trending weekly/monthly reports.	No

State of Connecticut Template

- Left as an exercise
- Document found on resource page of course web site

Incident Response Plan

State of Connecticut

Release 1.6

Business Continuity and Disaster Recovery Plans

Domain 4:
Information Security Incident Management

Additional References:

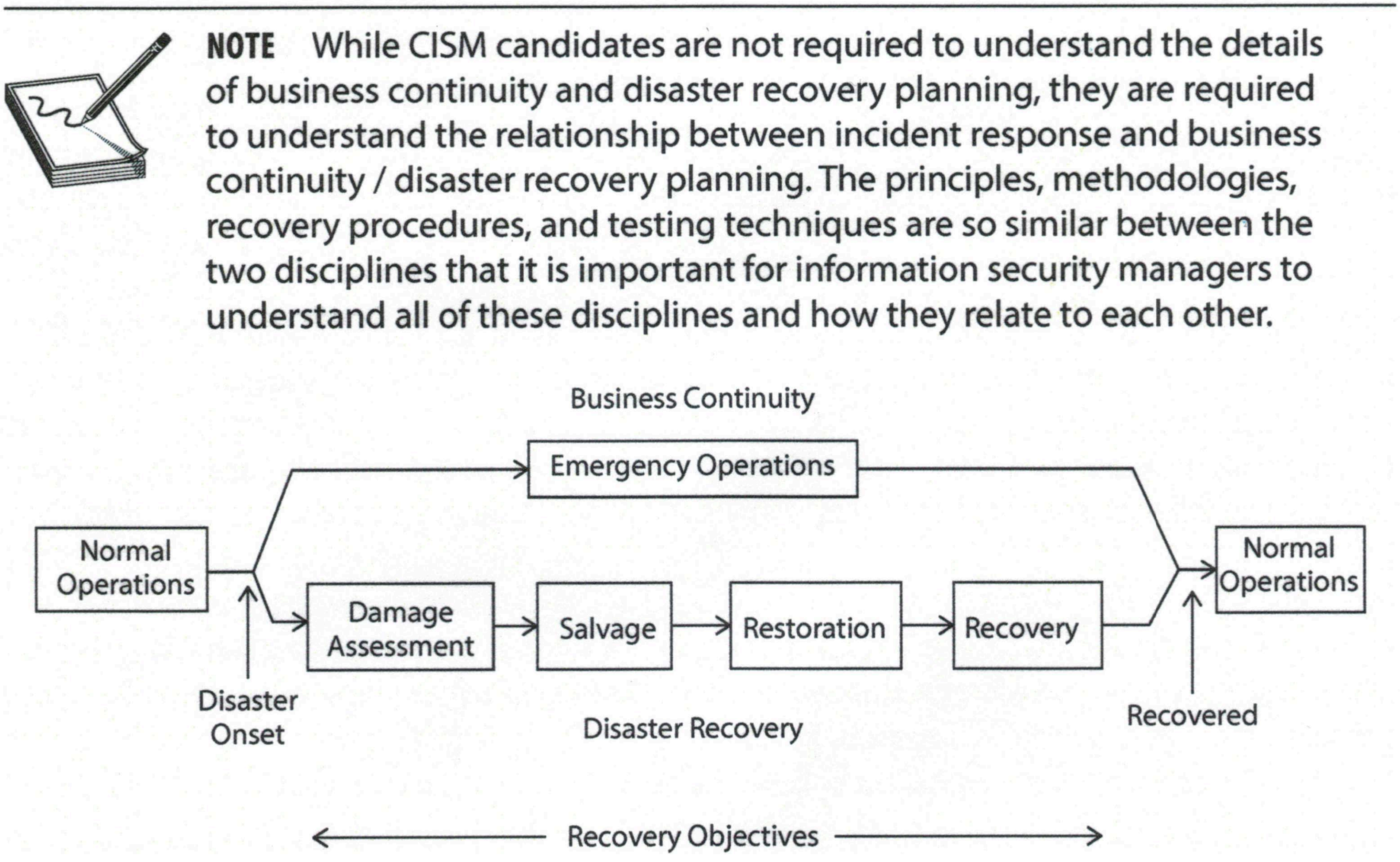
Dr. C.W. Perr

ISC2 CISSP CBK

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

Relationship Betweem BCP and DRP



NOTE While CISM candidates are not required to understand the details of business continuity and disaster recovery planning, they are required to understand the relationship between incident response and business continuity / disaster recovery planning. The principles, methodologies, recovery procedures, and testing techniques are so similar between the two disciplines that it is important for information security managers to understand all of these disciplines and how they relate to each other.

Business Continuity

Emergency Operations

Normal Operations

Damage Assessment

Salvage

Restoration

Recovery

Normal Operations

Disaster Onset

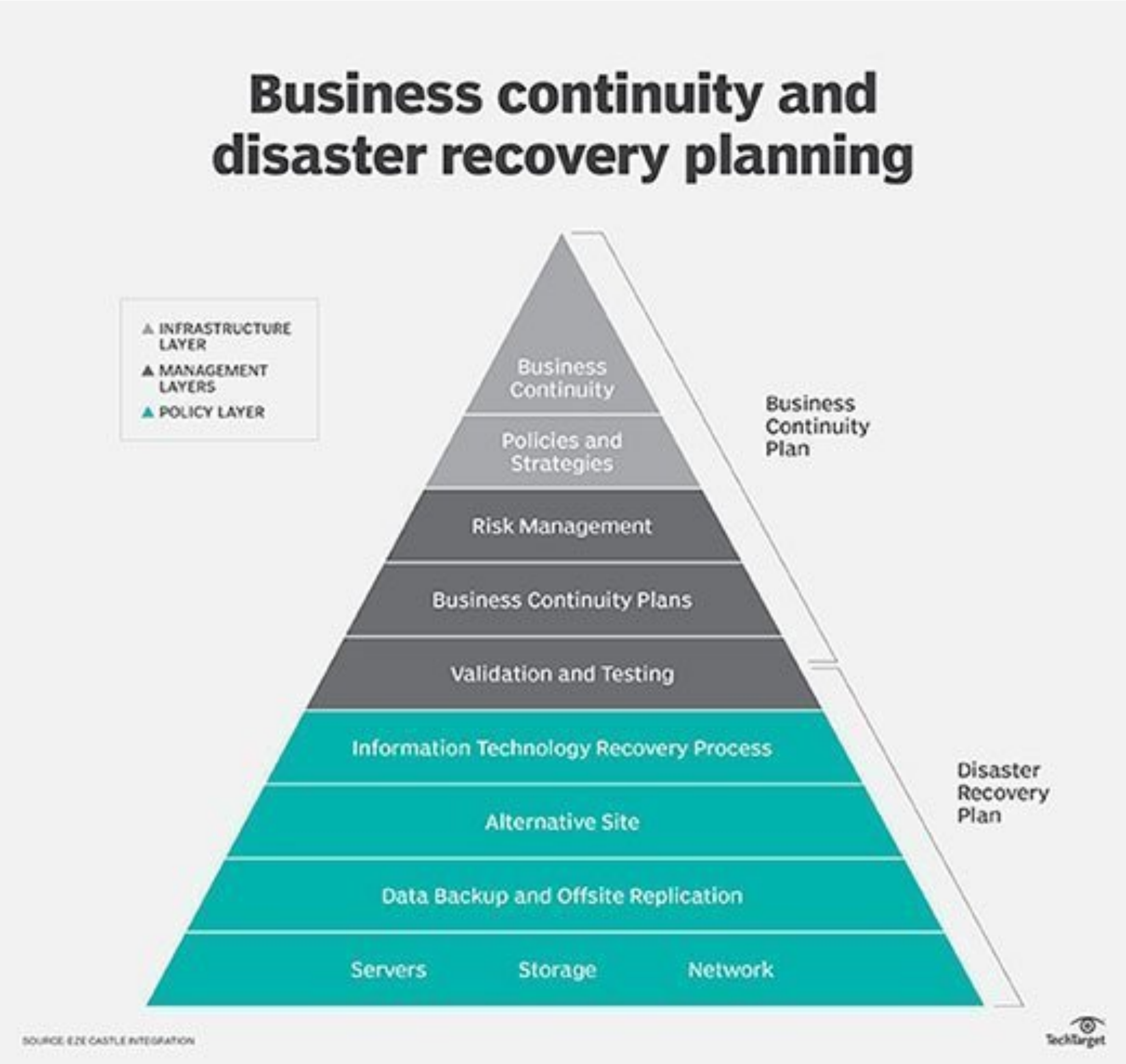
Disaster Recovery

Recovered

Recovery Objectives

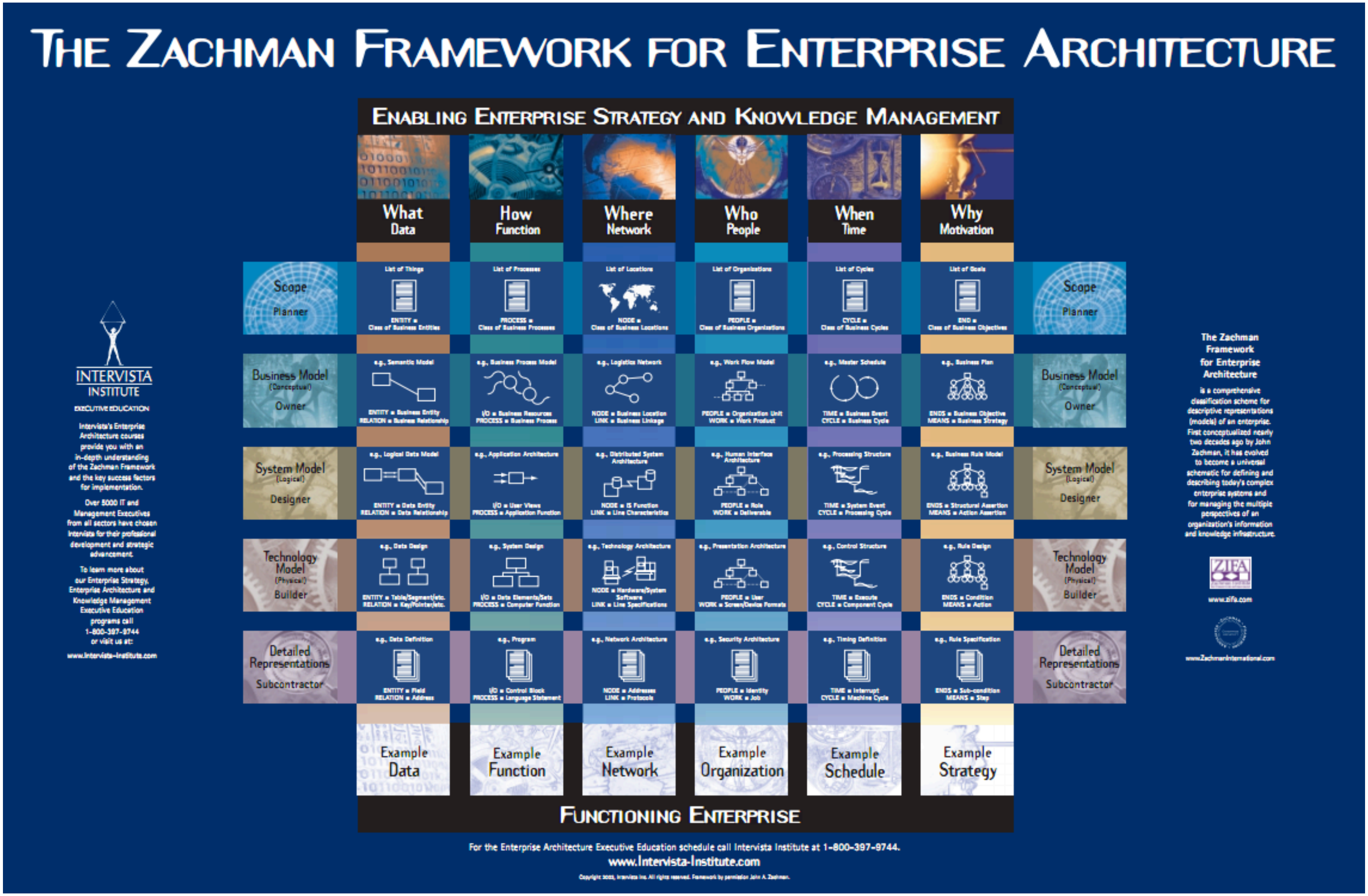
Ref: All-in-One CISM by Peter H. Gregory

BCP and DRP Components



SOURCE: EZE CASTLE INTEGRATION

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

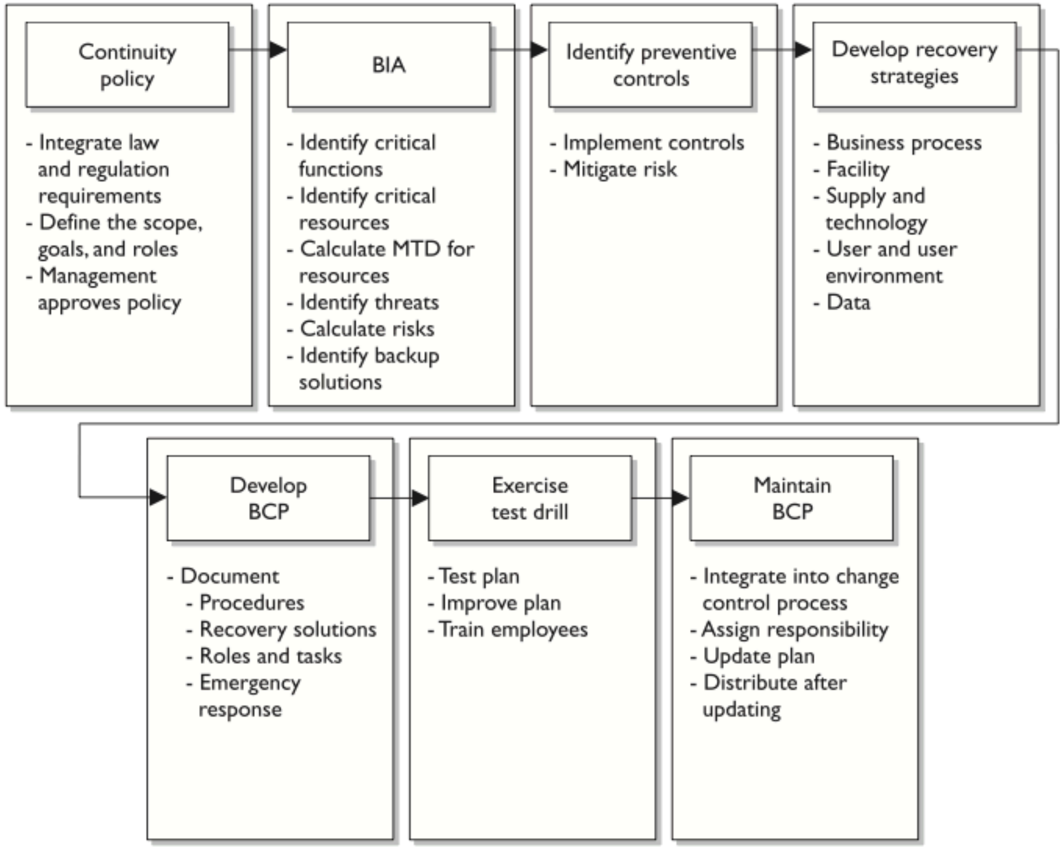
For the Enterprise Architecture Executive Education schedule call Intervista Institute at 1-800-397-9744.

www.Intervista-Institute.com

A BCP requires a BIA

- Before doing a Business Continuity Plan (BCP), you must first develop a Business Impact Analysis (BIA).

- Source: ISC2



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 a BCP? (C.W. Perr, Ph.D.)

- 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.

BCP, BIA and DRP

- Many people combine a business continuity plan (BCP) and a disaster recovery plan (DRP) as though they are a single document. However, they are different.
- Here are some key points:
  - The BCP has a wide scope and helps an organization continue to operate even if disaster occurs.
  - The BIA is part of the BCP and identifies critical systems and services.
  - You then create DRPs to ensure you have methods/procedures/processes to restore these critical systems in the event of the disaster.
- Source: GetAheadGetCertified

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

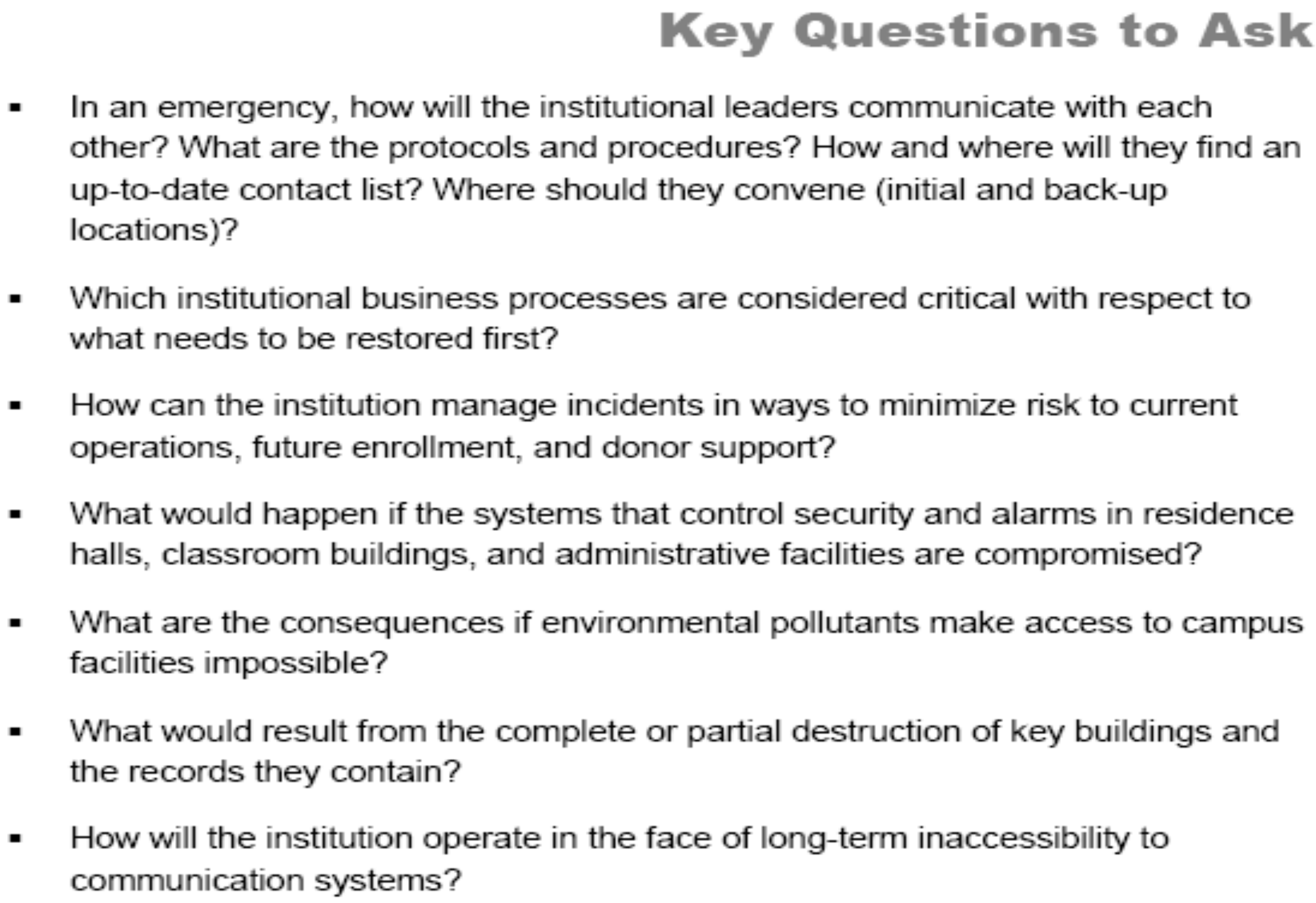
is:

- 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

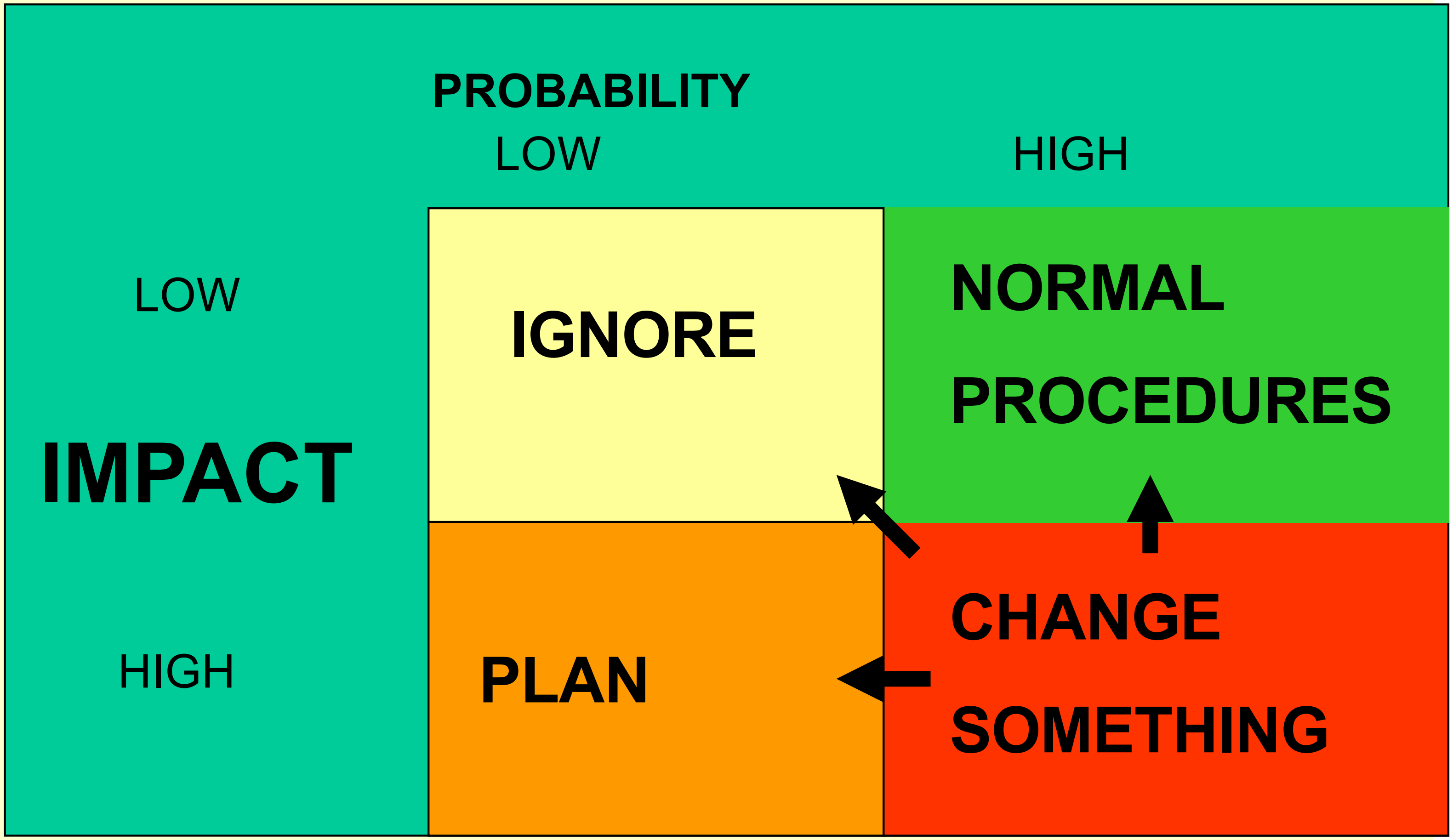


Key Questions to Ask

- 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

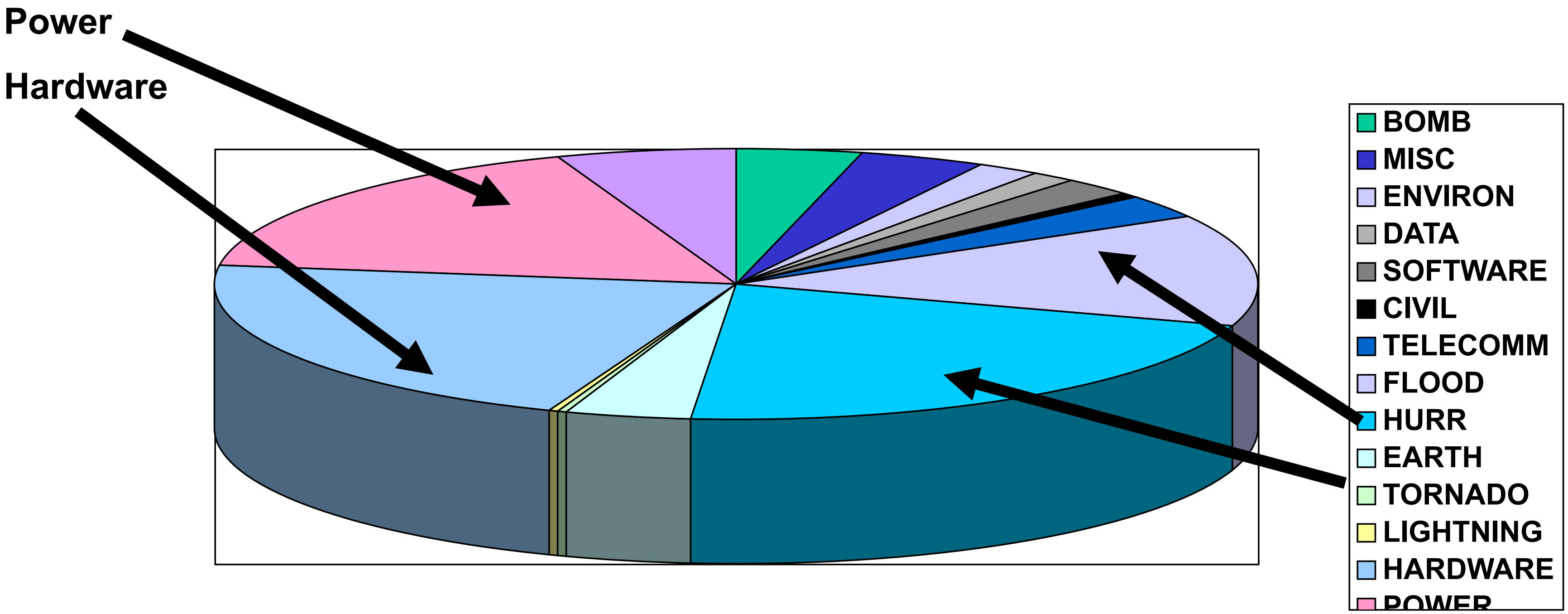
The Risk Matrix



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

Business Continuity Planning

Network Operations Disruptions



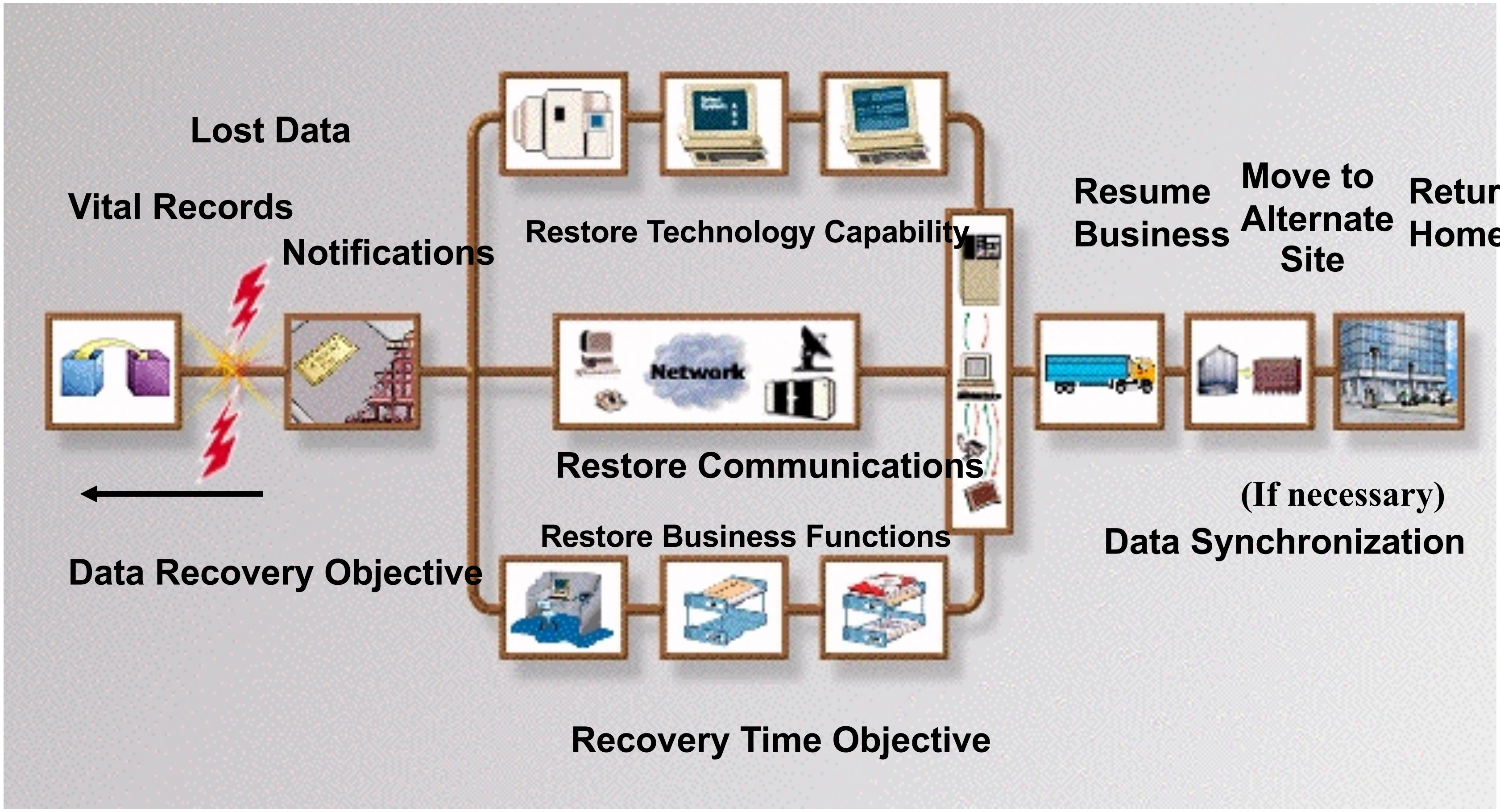
Source: Gartner Group and Comdisco

Business Continuity Planning

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

Business Continuity Planning

High Level Look at a Recovery Effort



© Lucent technologies

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…

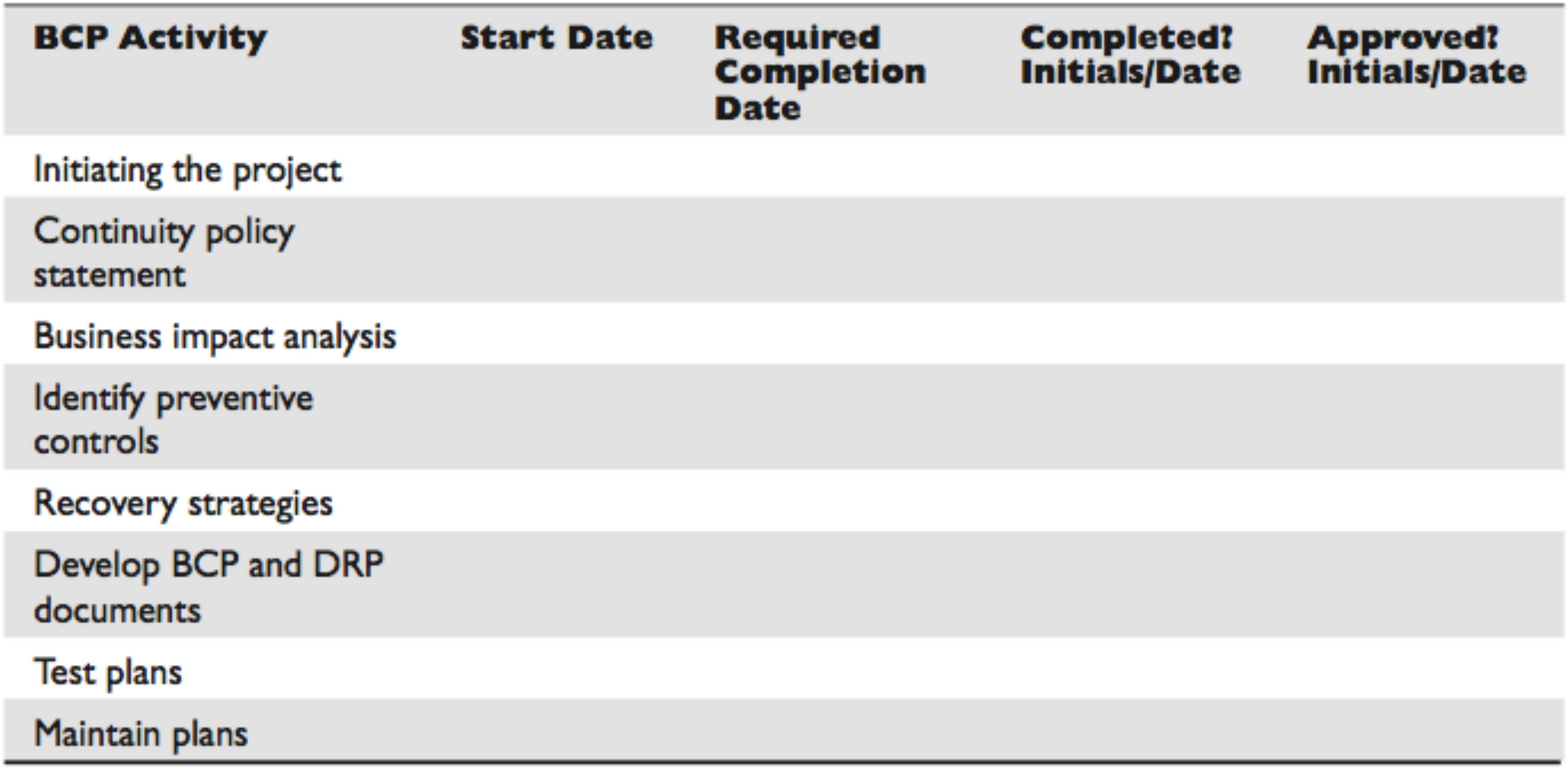
Project Initiation (continued)

- 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

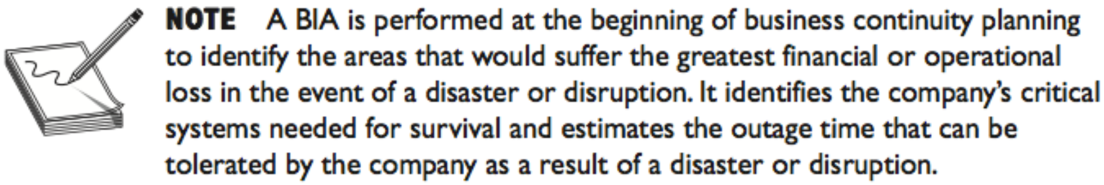
- Objective-to-task mapping
- Resource-to-task mapping
- Milestones
- Budget estimates
- Success factors
- Deadlines

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

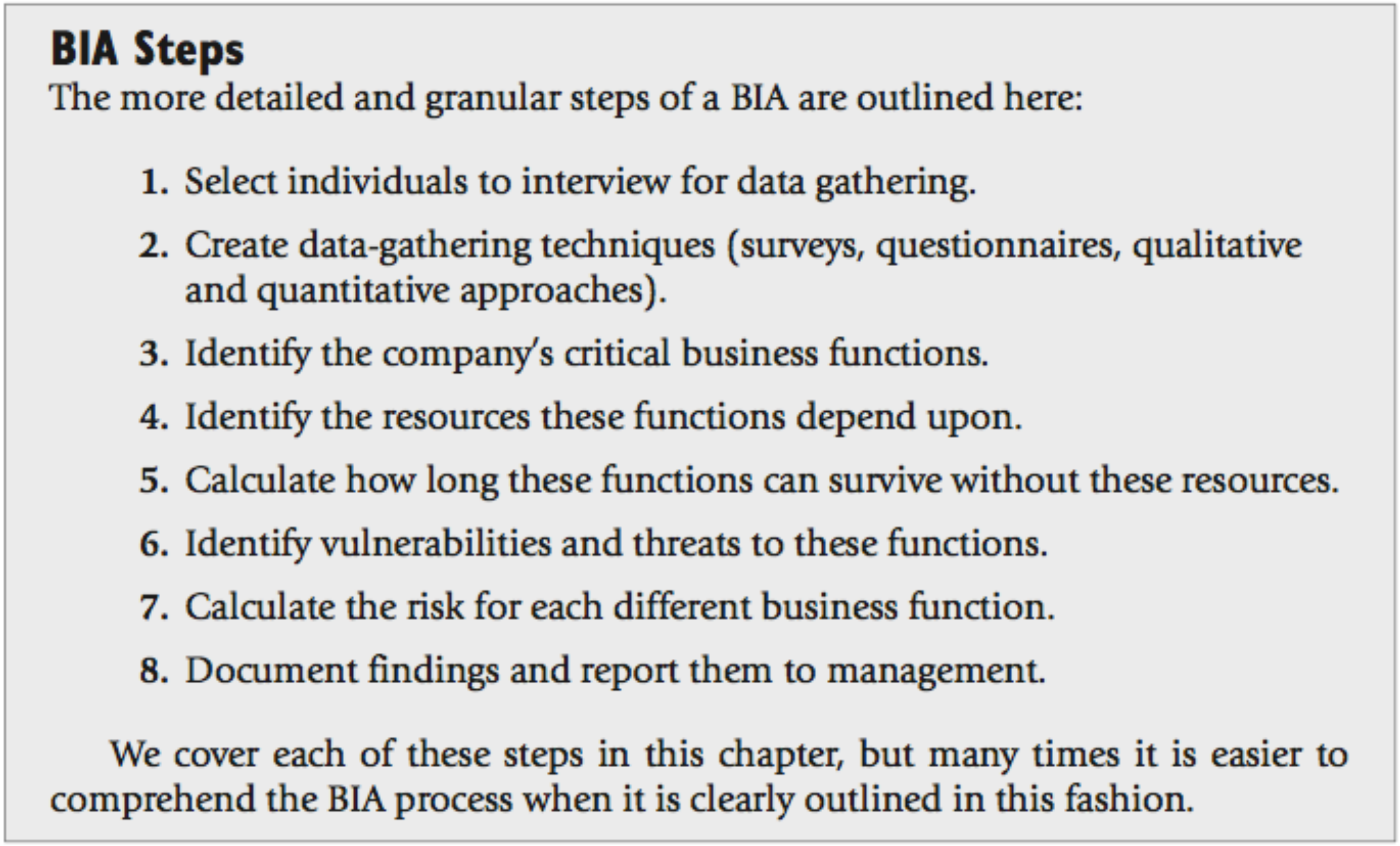
- ***How bad will this hurt and how long can we deal with this level of pain?***
- **Business impact analysis answers this.**
  - **Functional analysis: based on business, functions, activities, and transactions.**
  - **Threats are mapped based on:**
    - **Maximum tolerable downtime**
    - **Operational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



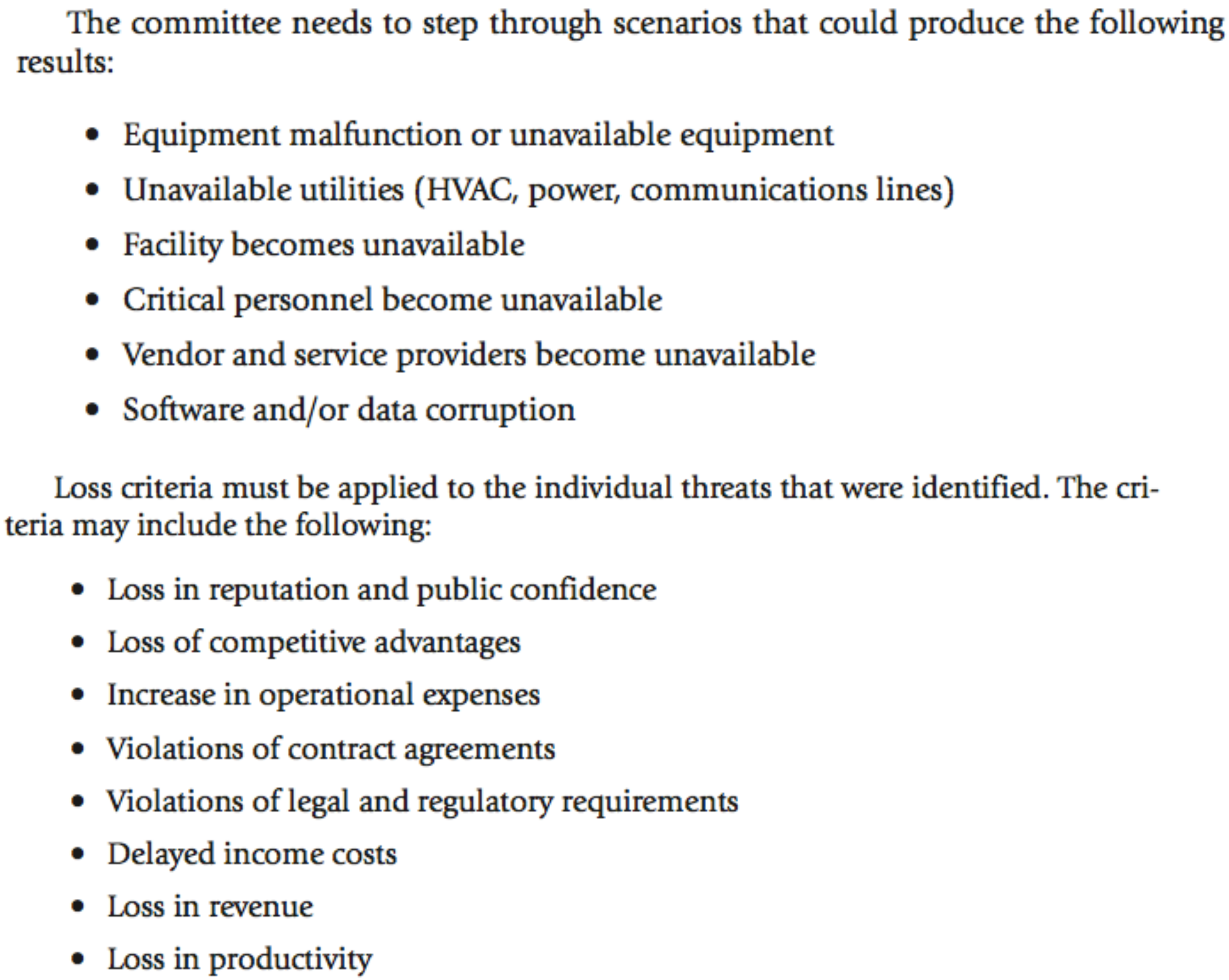
BIA Steps

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:

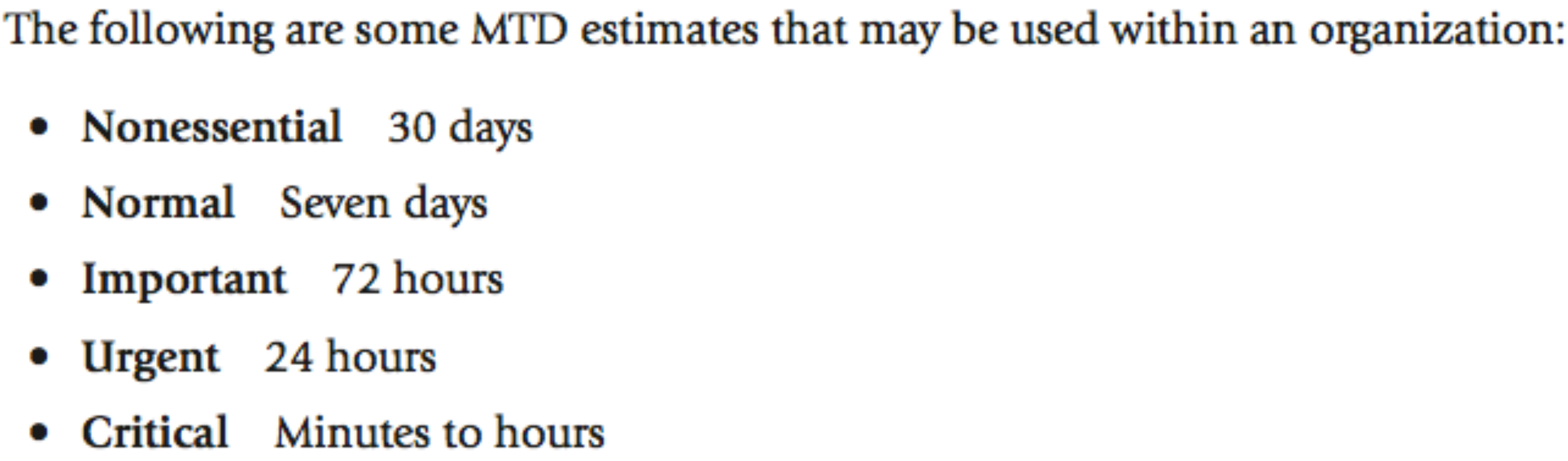
- Equipment malfunction or unavailable equipment
- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

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

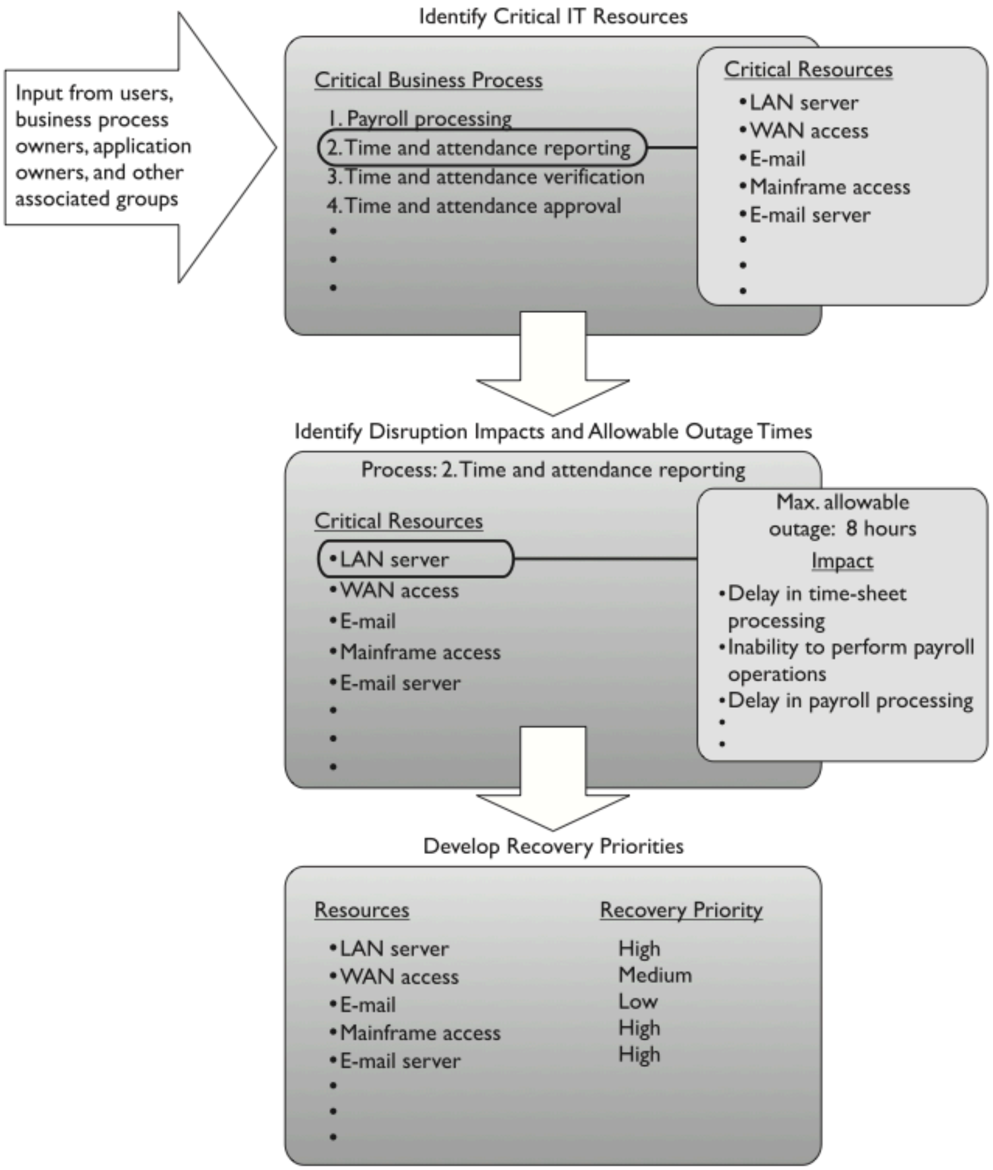
- ***Maximum tolerable downtime (MTD)*** **– the outage time that can be endured by the company.**



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…



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

Identify Critical IT Resources

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

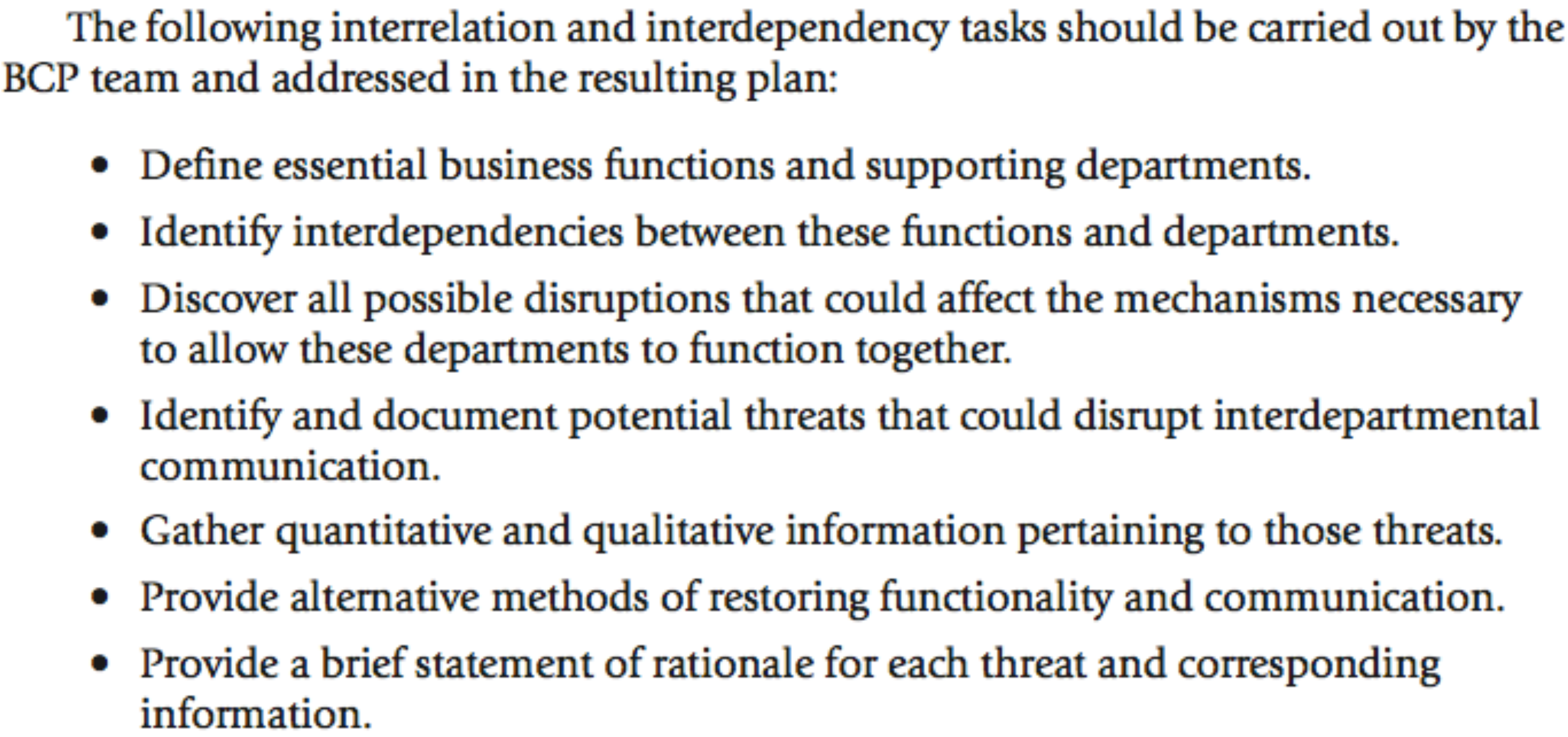
Impact

- 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
•	
•	
•	

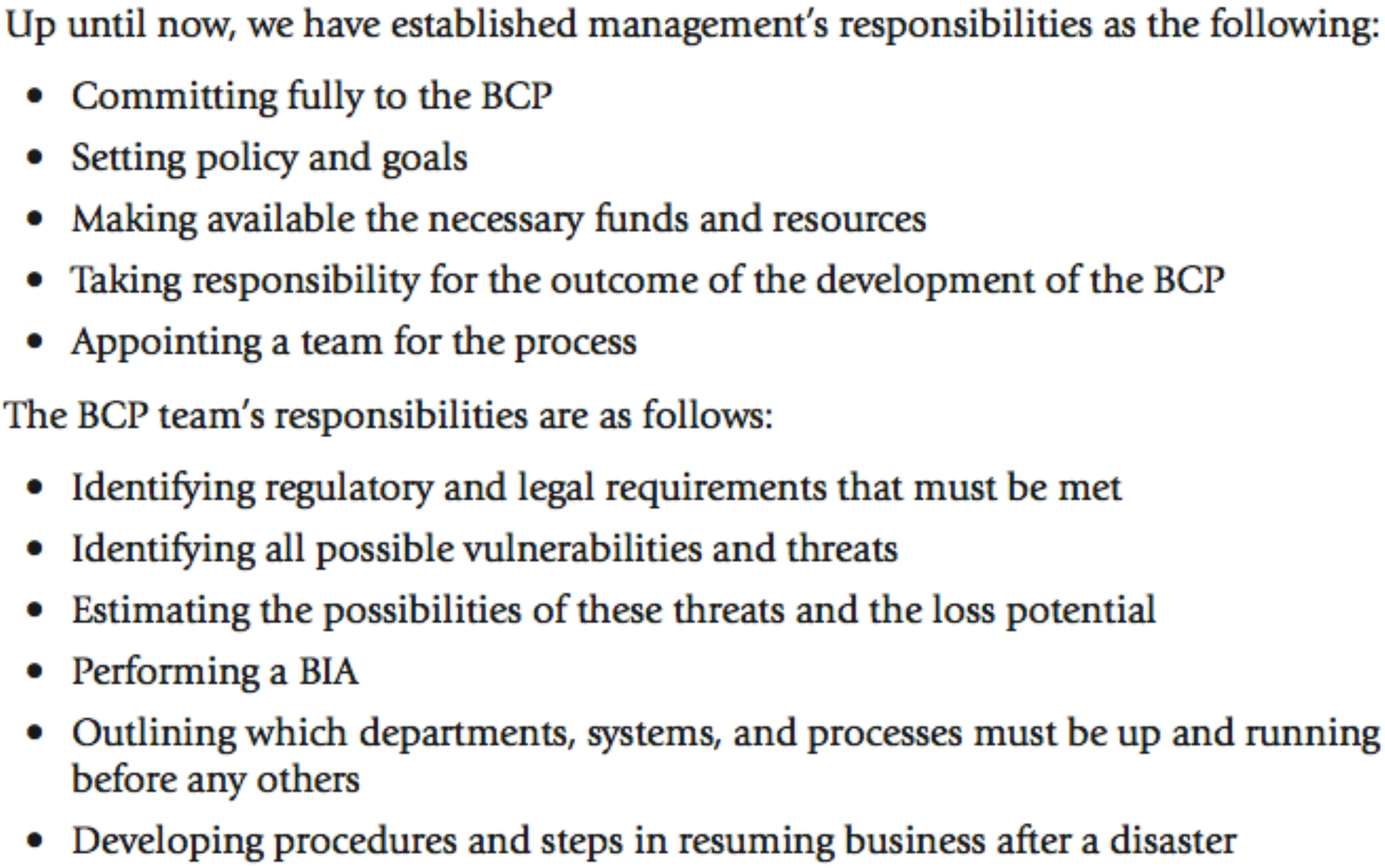
Dependency (continued)



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:

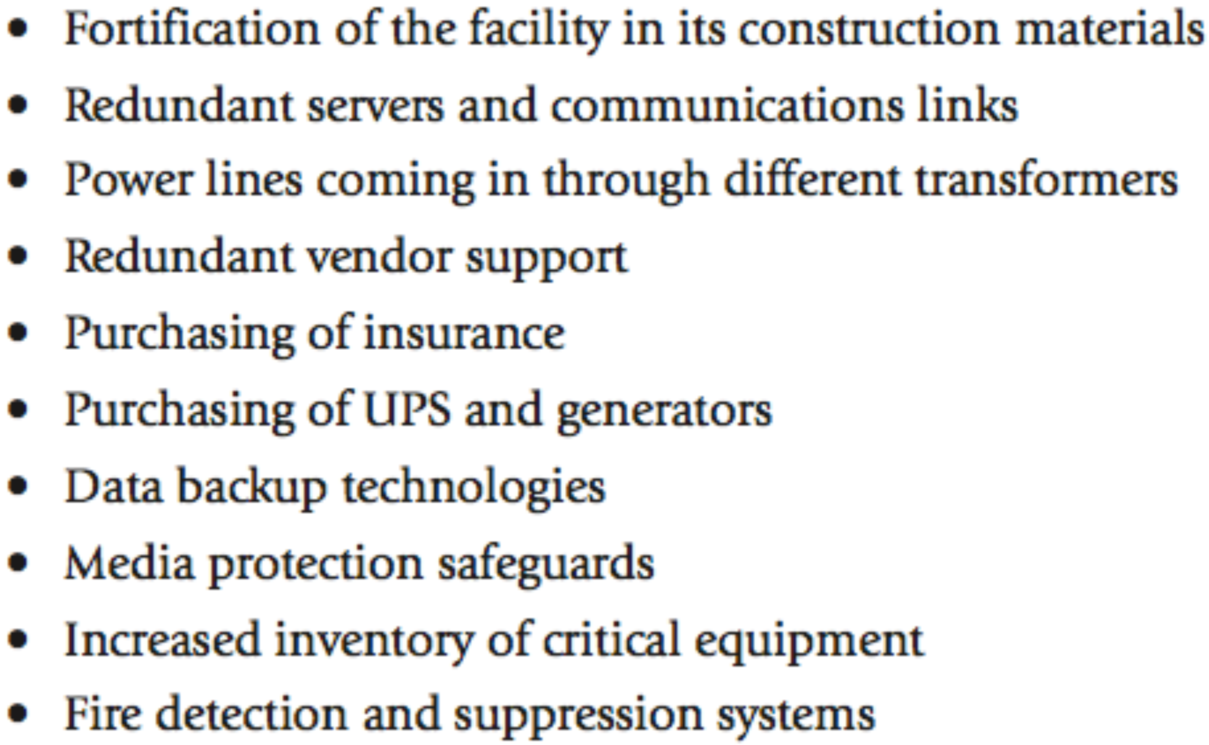
- Committing fully to the BCP
- Setting policy and goals
- Making available the necessary funds and resources
- Taking responsibility for the outcome of the development of the BCP
- Appointing a team for the process

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.**
- **Example:**

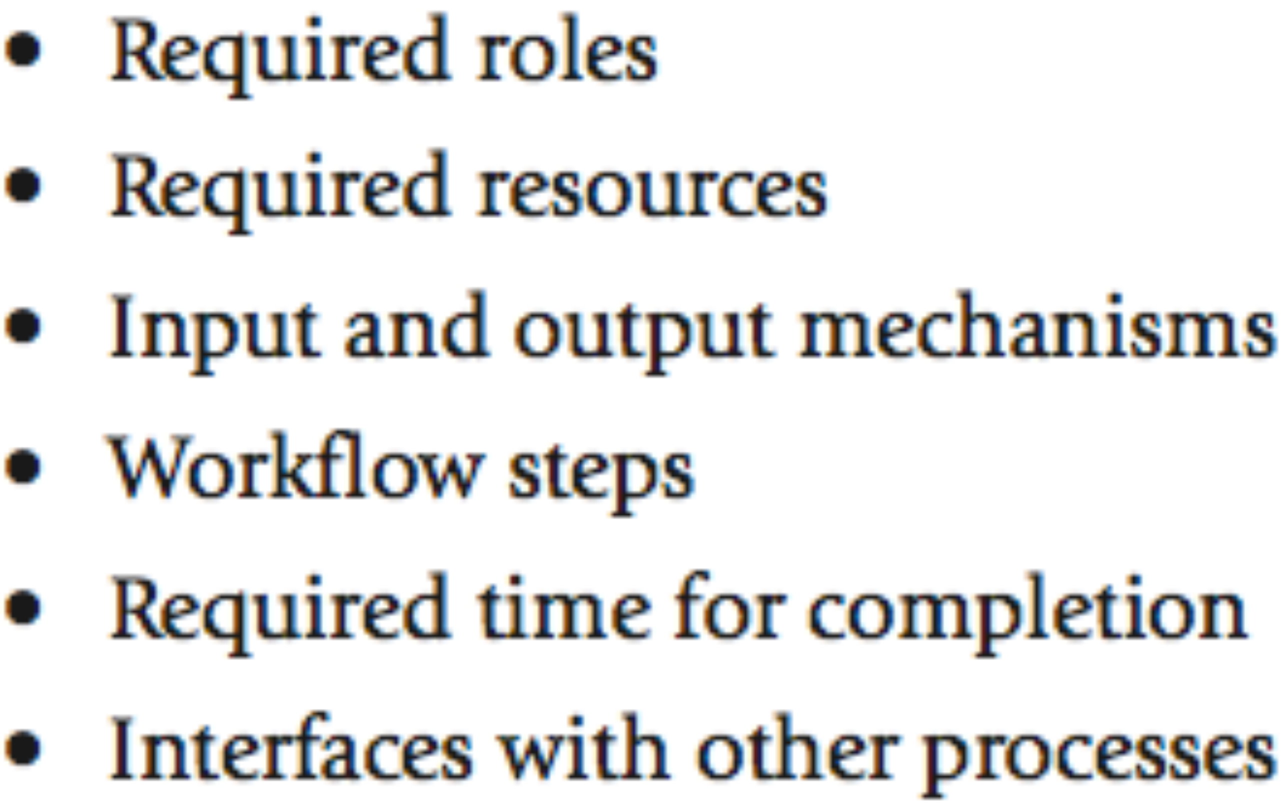


  - Fortification of the facility in its construction materials
  - Redundant servers and communications links
  - Power lines coming in through different transformers
  - Redundant vendor support
  - Purchasing of insurance
  - Purchasing of UPS and generators
  - Data backup technologies
  - Media protection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

Business Process Recovery

- Example – 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

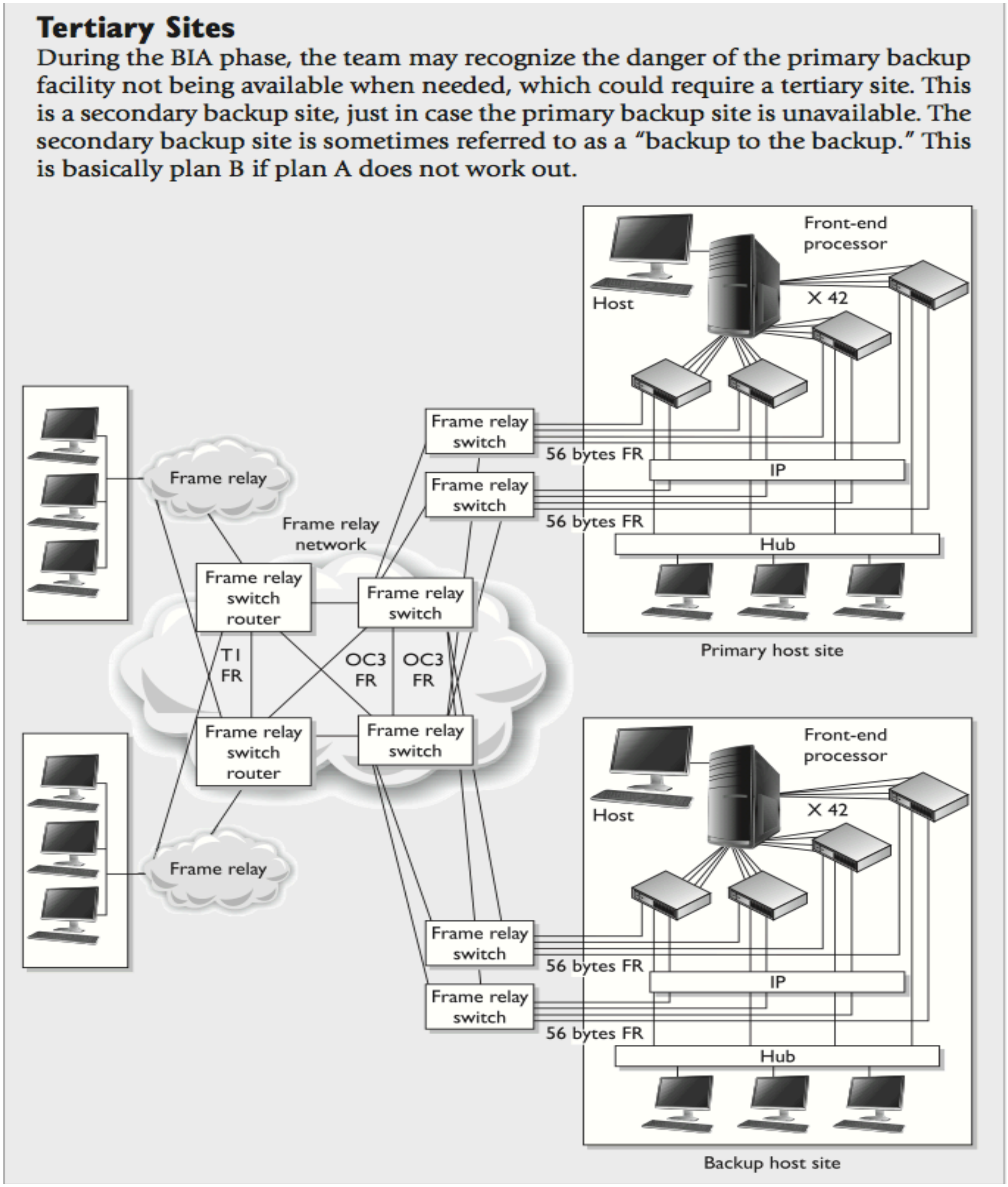
4. Plan Design and Development

- **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.**

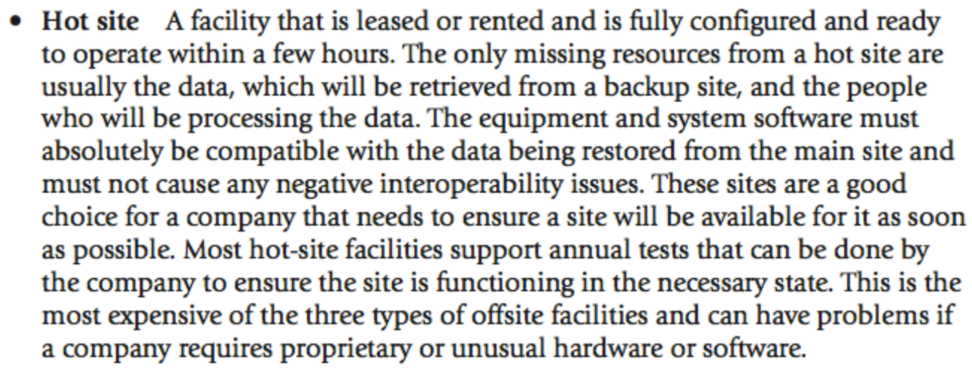
Tertiary Sites Backups



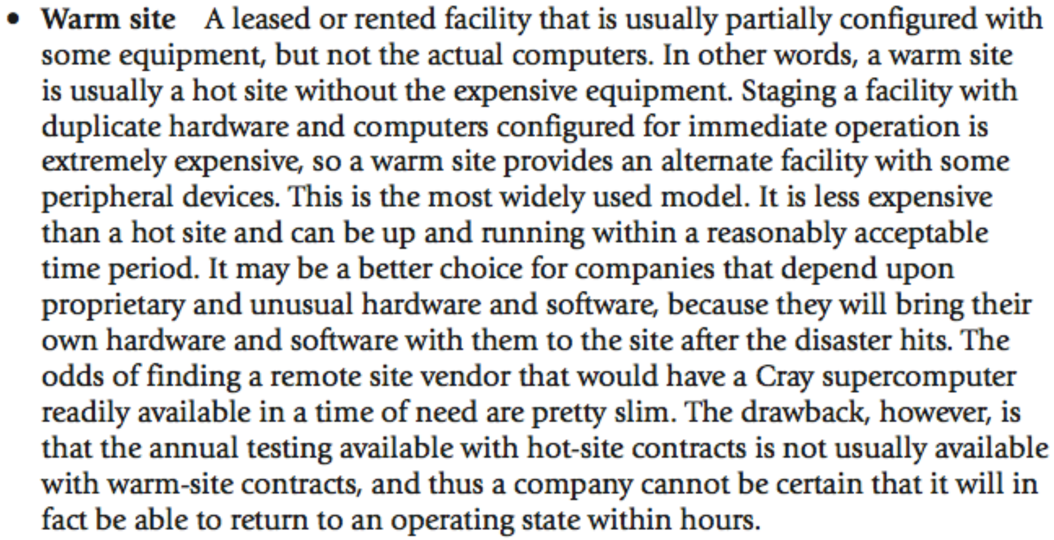
Tertiary Sites

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.

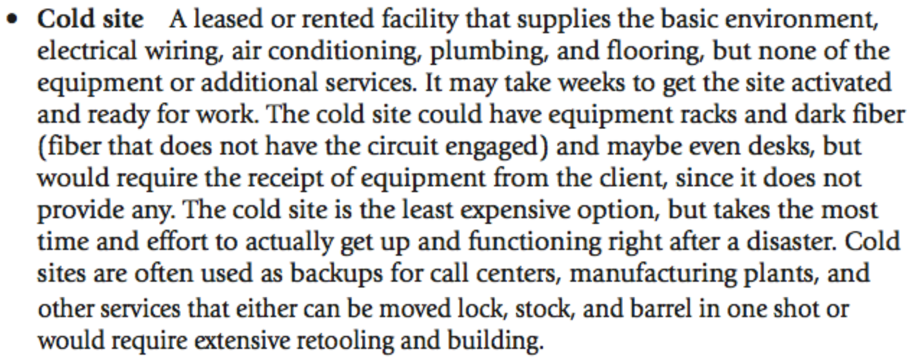
More vocabulary



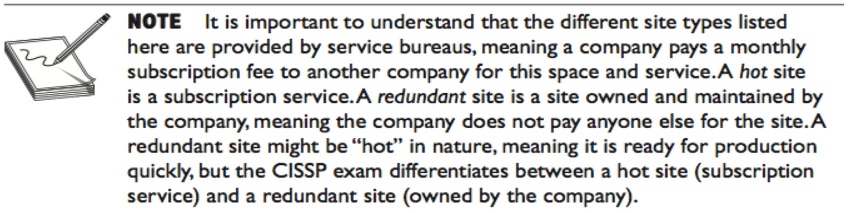
- **Hot site** A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software 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.

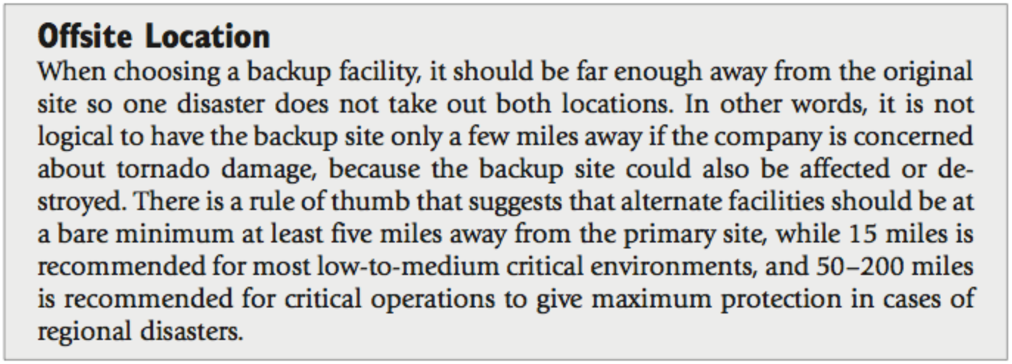


- **Cold site** A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and 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).

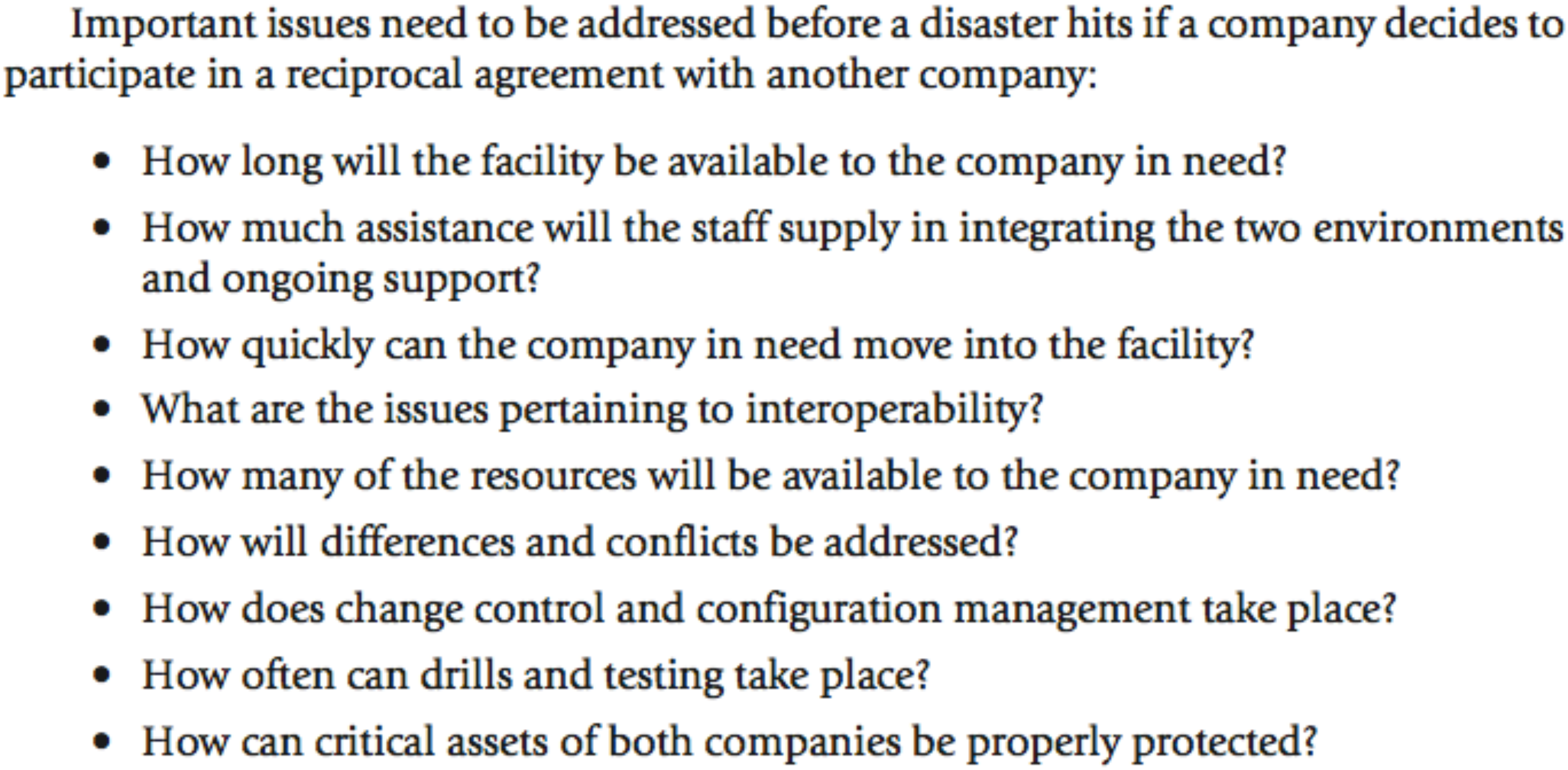
Don’t do this…



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

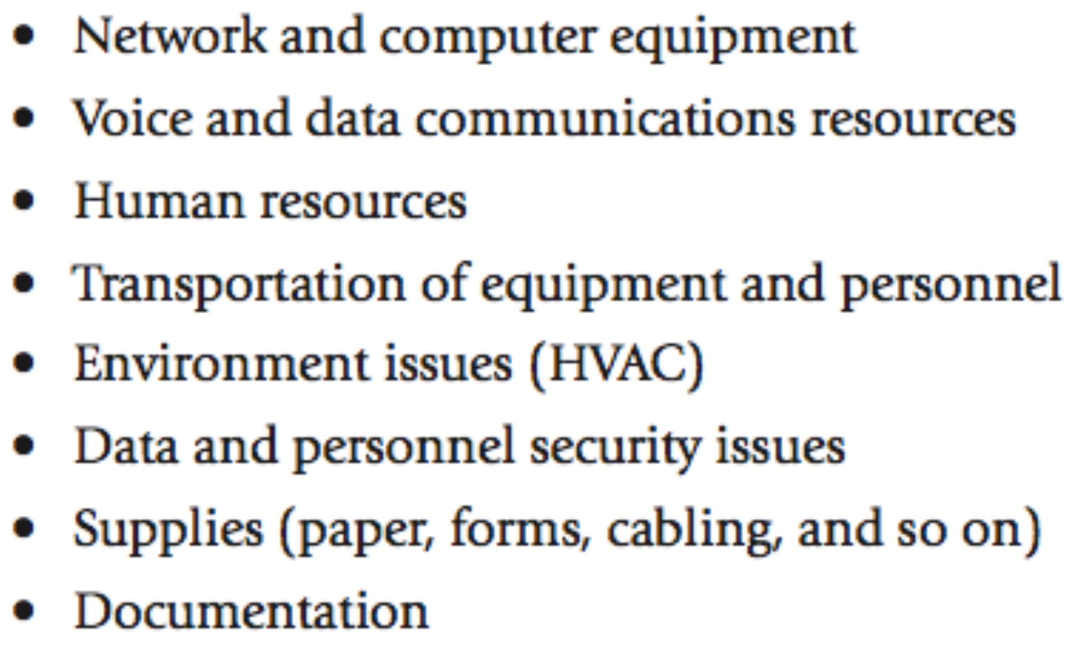


Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

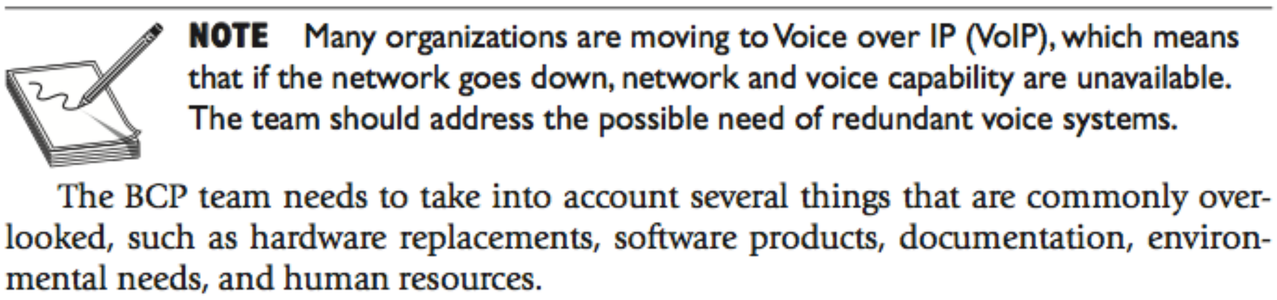
- How long will the facility be available to the company in need?
- How much assistance will the staff supply in integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the 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

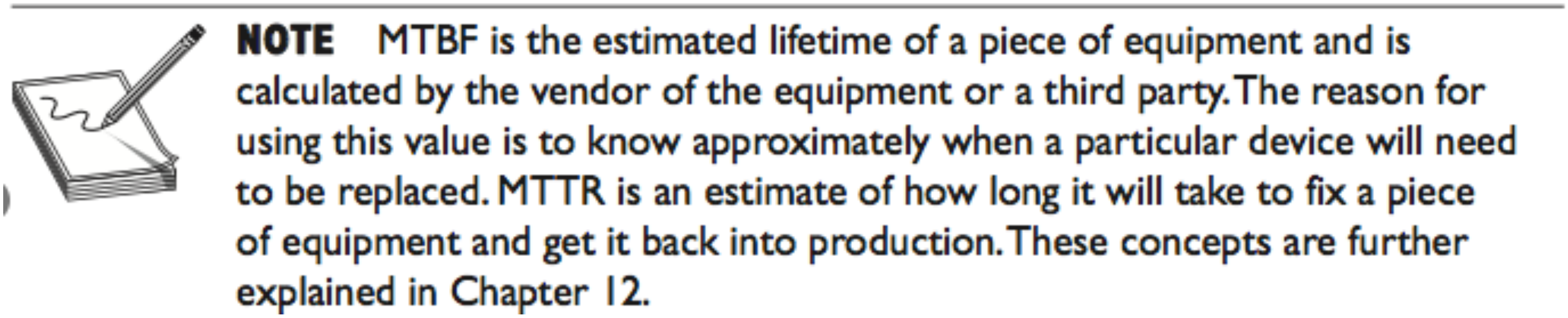


NOTE Many organizations are moving to Voice over IP (VoIP), which means that if the network goes down, network and voice capability are unavailable. The team should address the possible need of redundant voice systems.

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

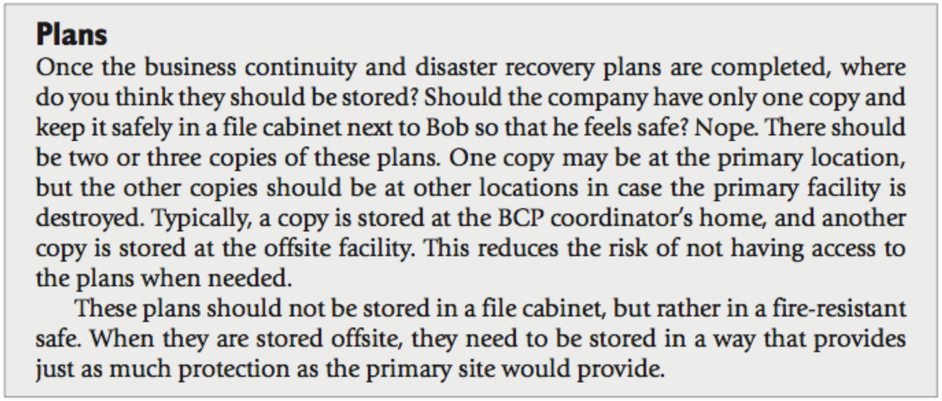
- Usually a plan of keeping machine images and buying equipment as it is needed.
- Service level agreement needs to specify a delivery time for the equipment.



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

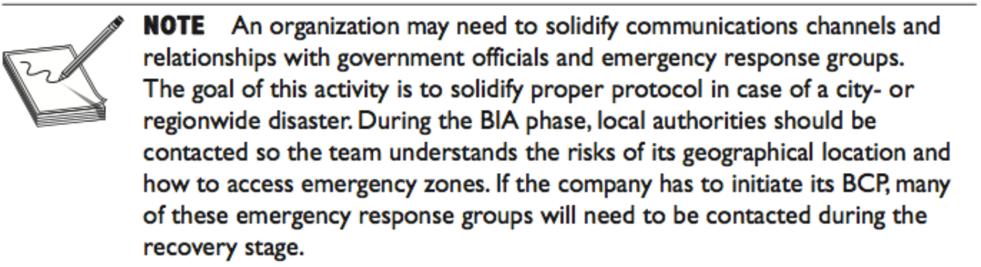
- **Write down the plan…(seriously, this was a whole page in the book…der)**



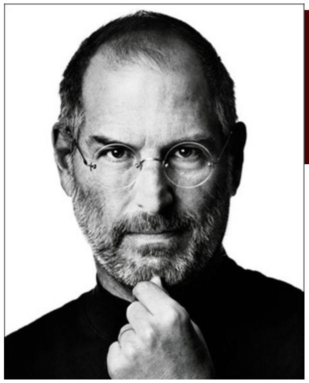
Plans

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…

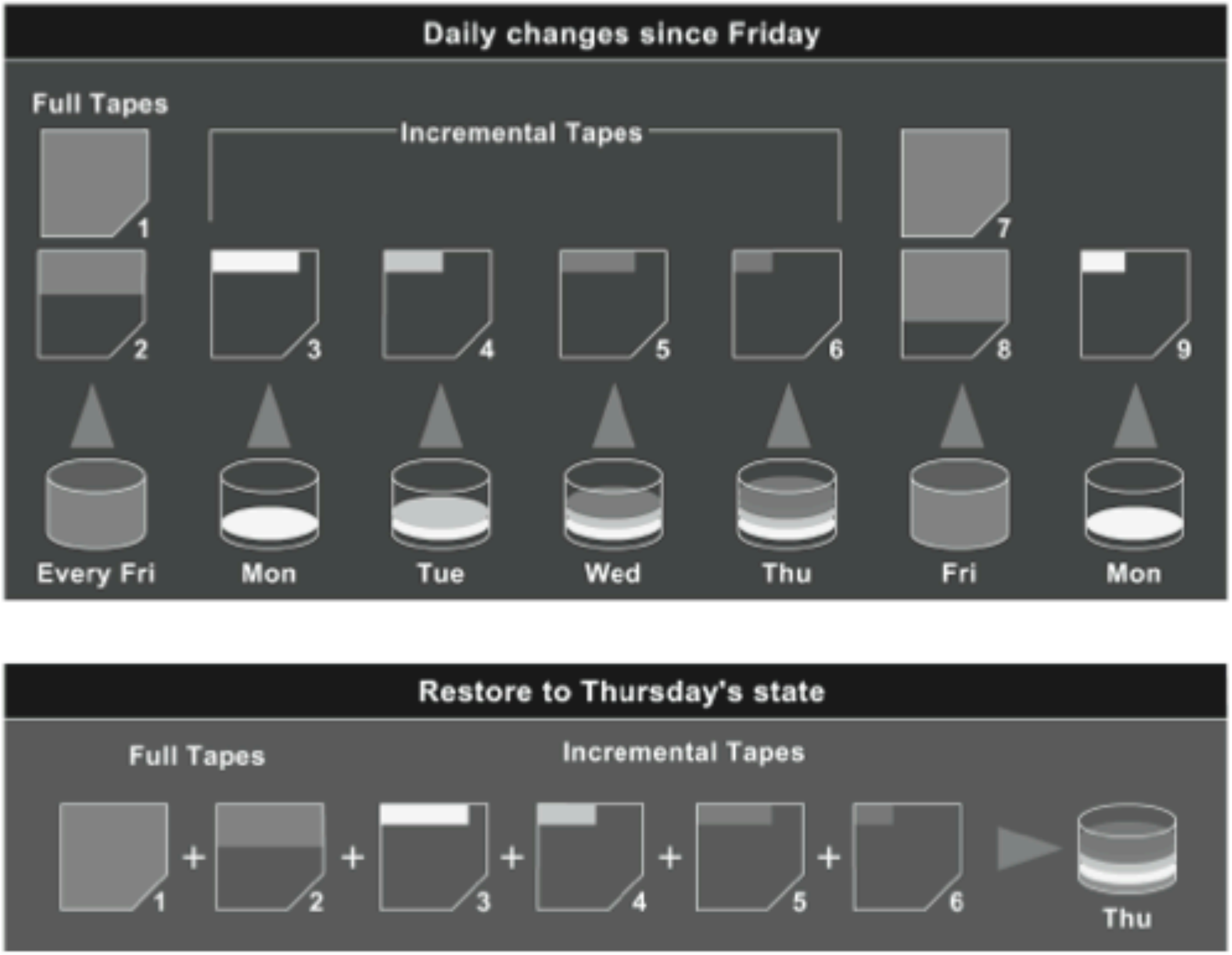
- How are you going to get people to work a backup site 250 miles away?

- 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.

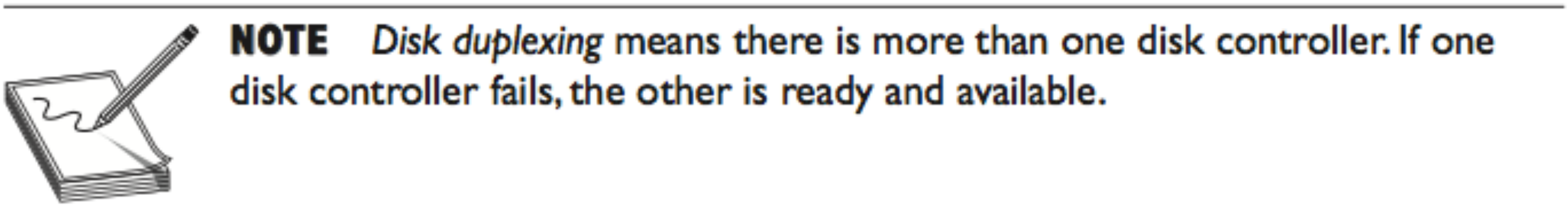


More vocabulary

- ***Electronic vaulting* – makes copies of files as they are modified and periodically transmits them to an offsite backup site**

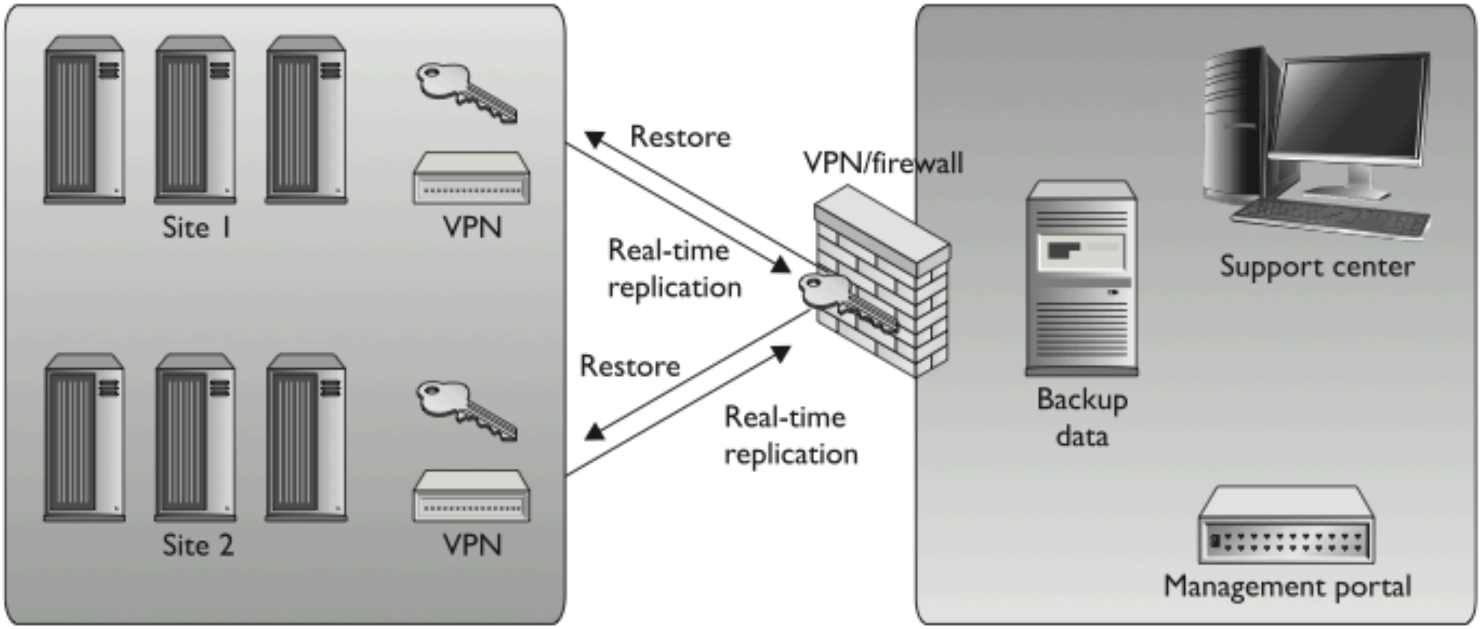
- ***Disk shadowing* – similar to data mirroring, provides fault tolerance by duplicating hardware and maintaining more than one copy**

- ***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.**



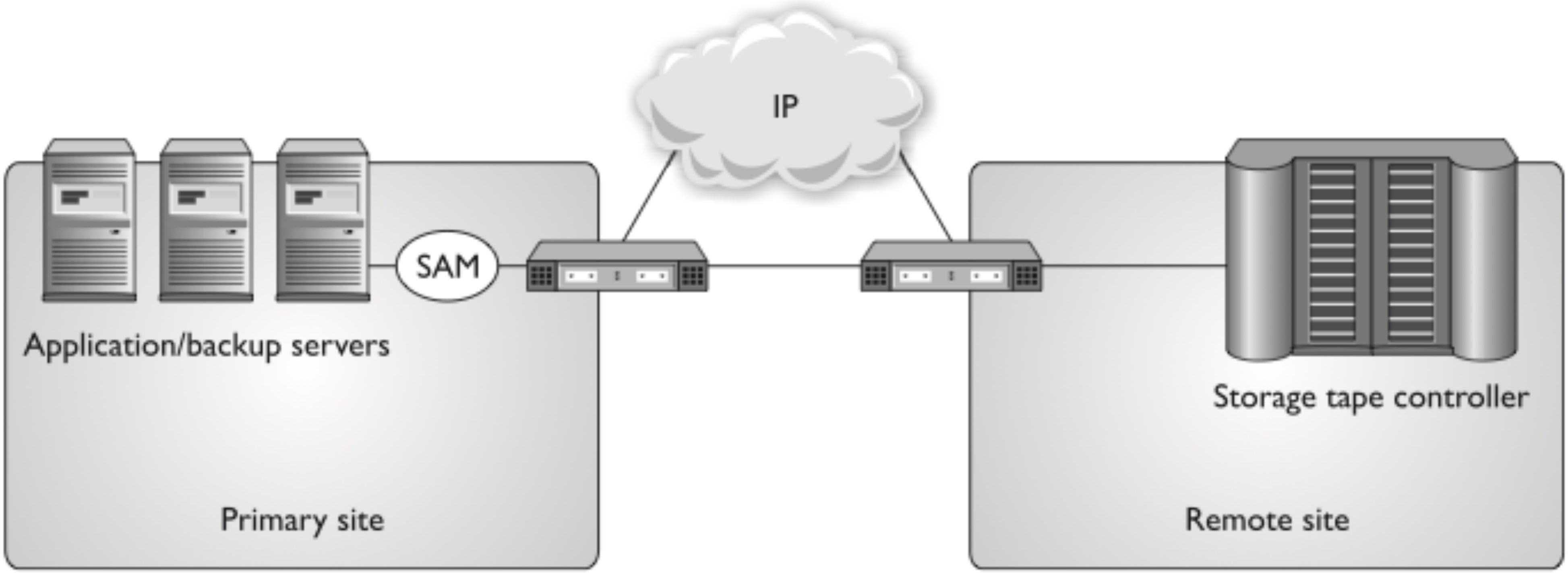
NOTE *Disk duplexing* means there is more than one disk controller. If one disk controller fails, the other is ready and available.

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

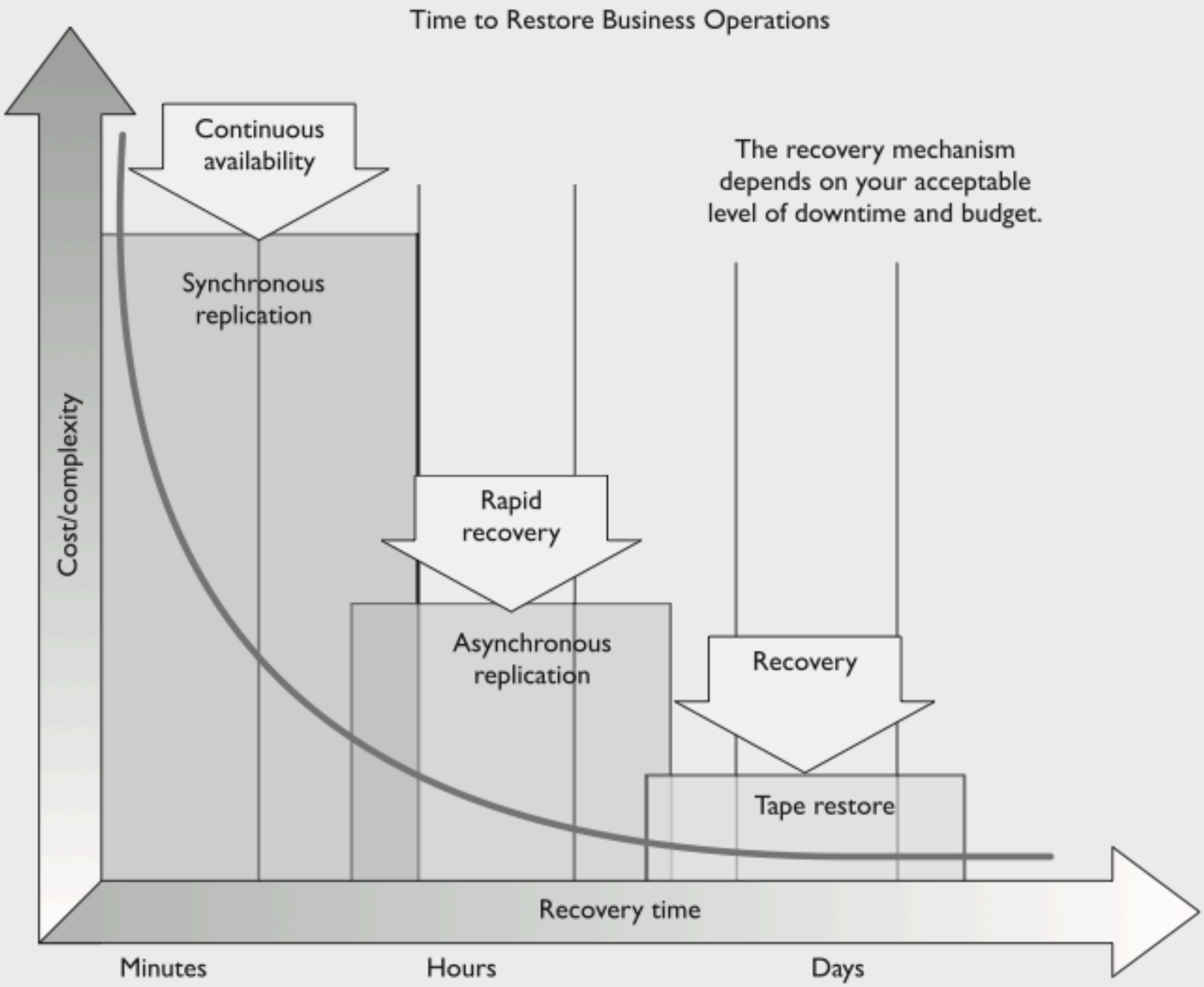
Choose a backup facility

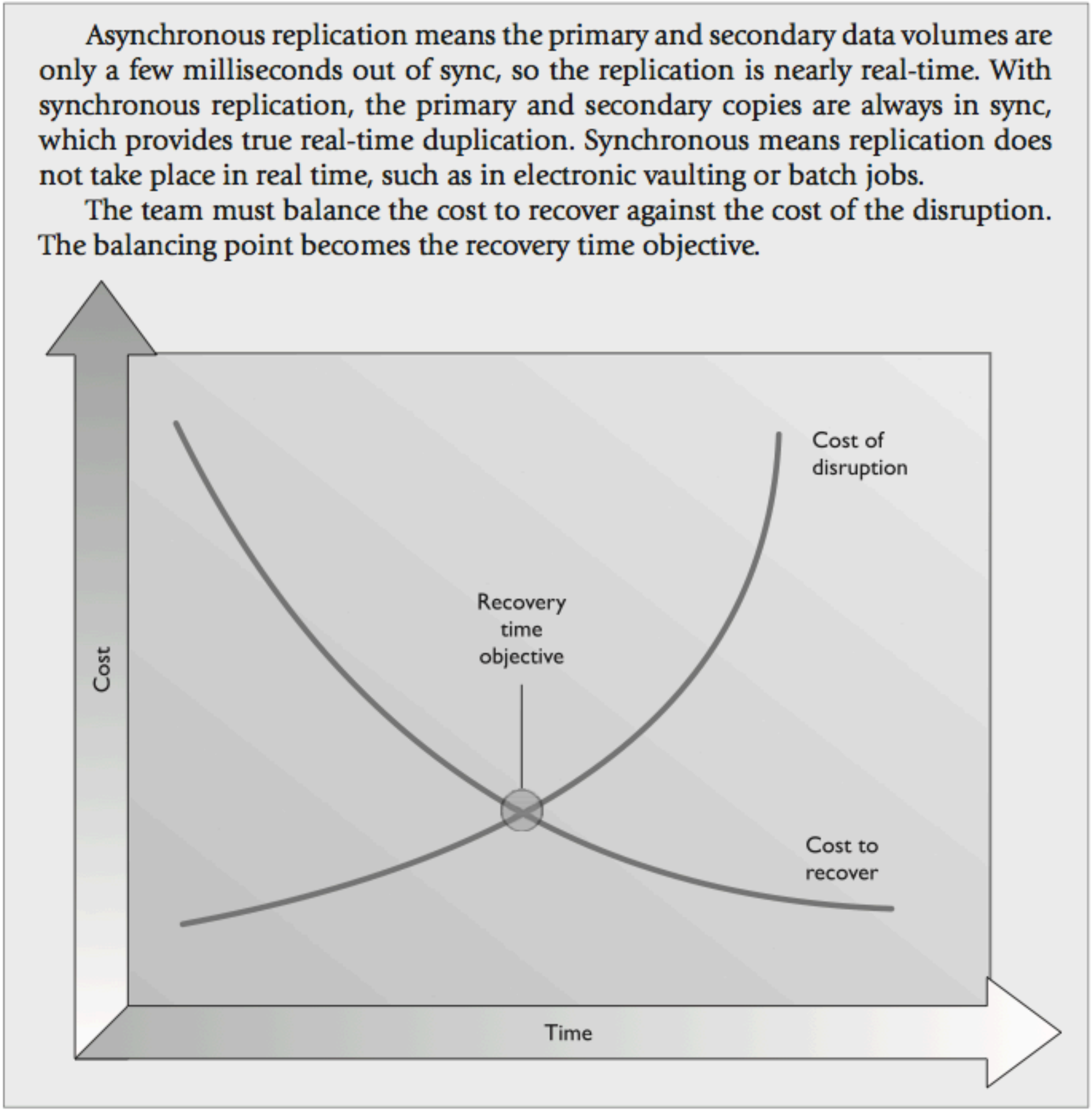
- Can the media be accessed in the necessary timeframe?
- Is the facility closed on weekends and holidays, and does it only operate during specific hours of the day?
- Are the access control mechanisms tied to an alarm and/or the police station?
- Does the facility have the capability to protect the 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.



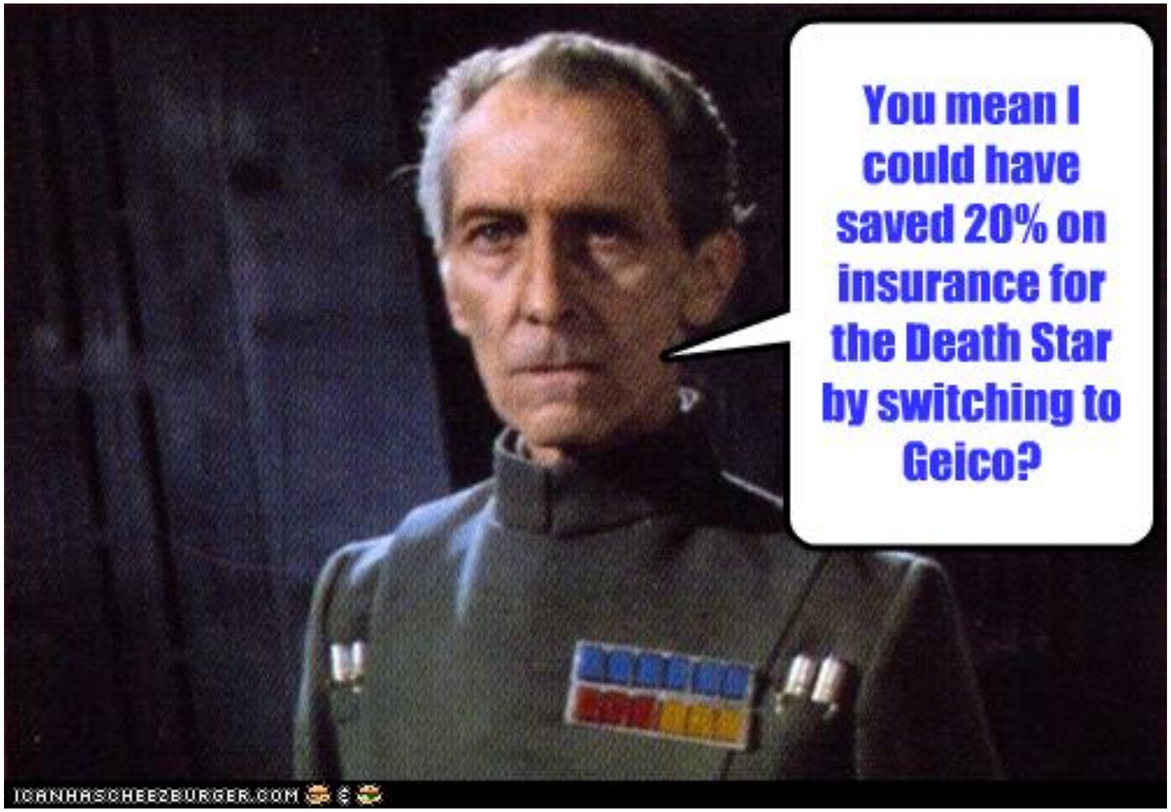


Asynchronous replication means the primary and secondary data volumes are only a few milliseconds out of sync, so the replication is nearly real-time. With synchronous replication, the primary and secondary copies are always in sync, which provides true real-time duplication. Synchronous means replication 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

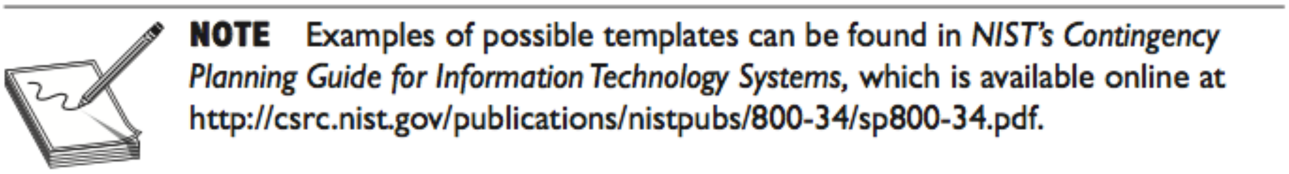
Restoration Teams

- 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.

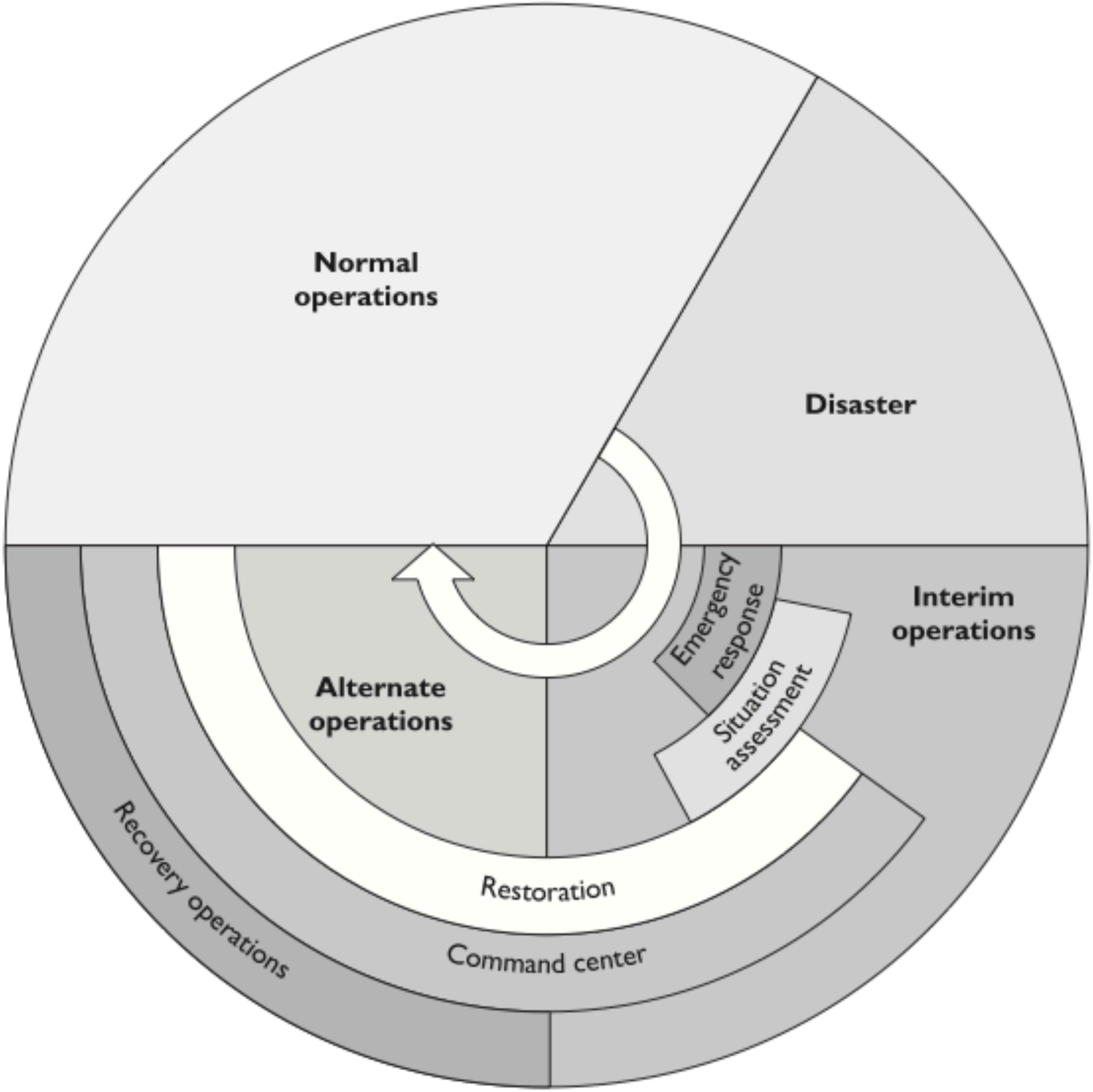
Reconstruction Issues

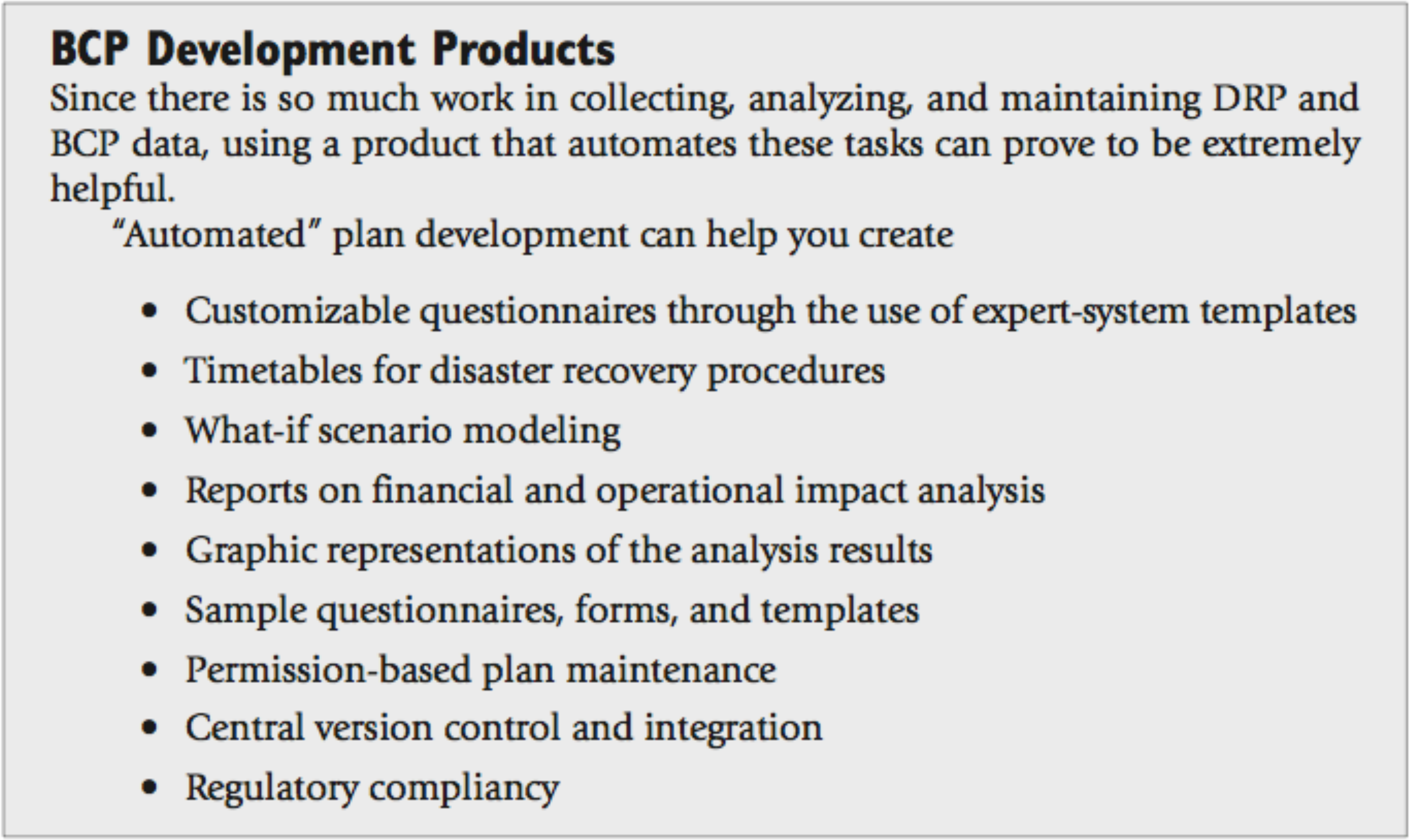
The following lists a few of these issues:

- 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.

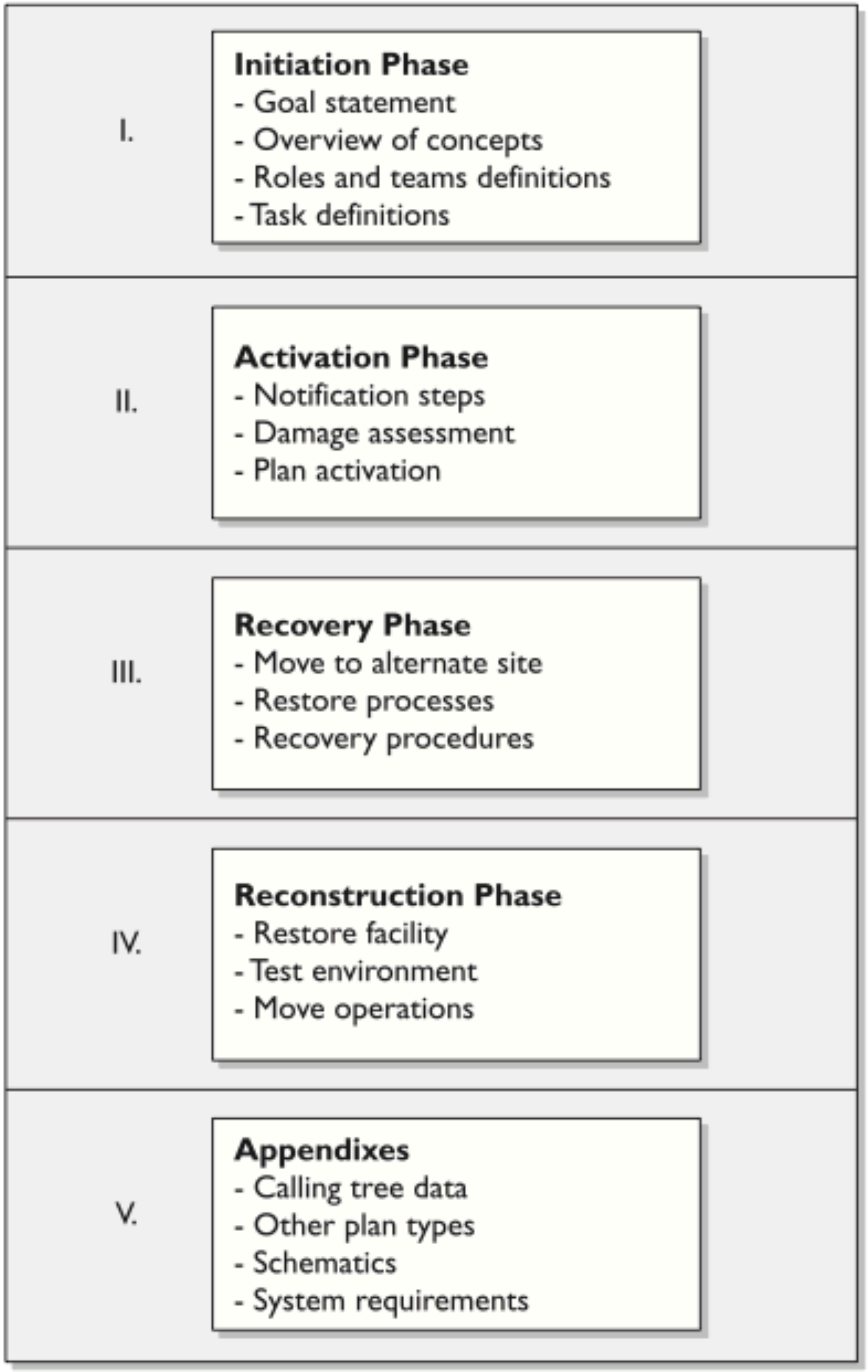
"Automated" plan development can help you create

- 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

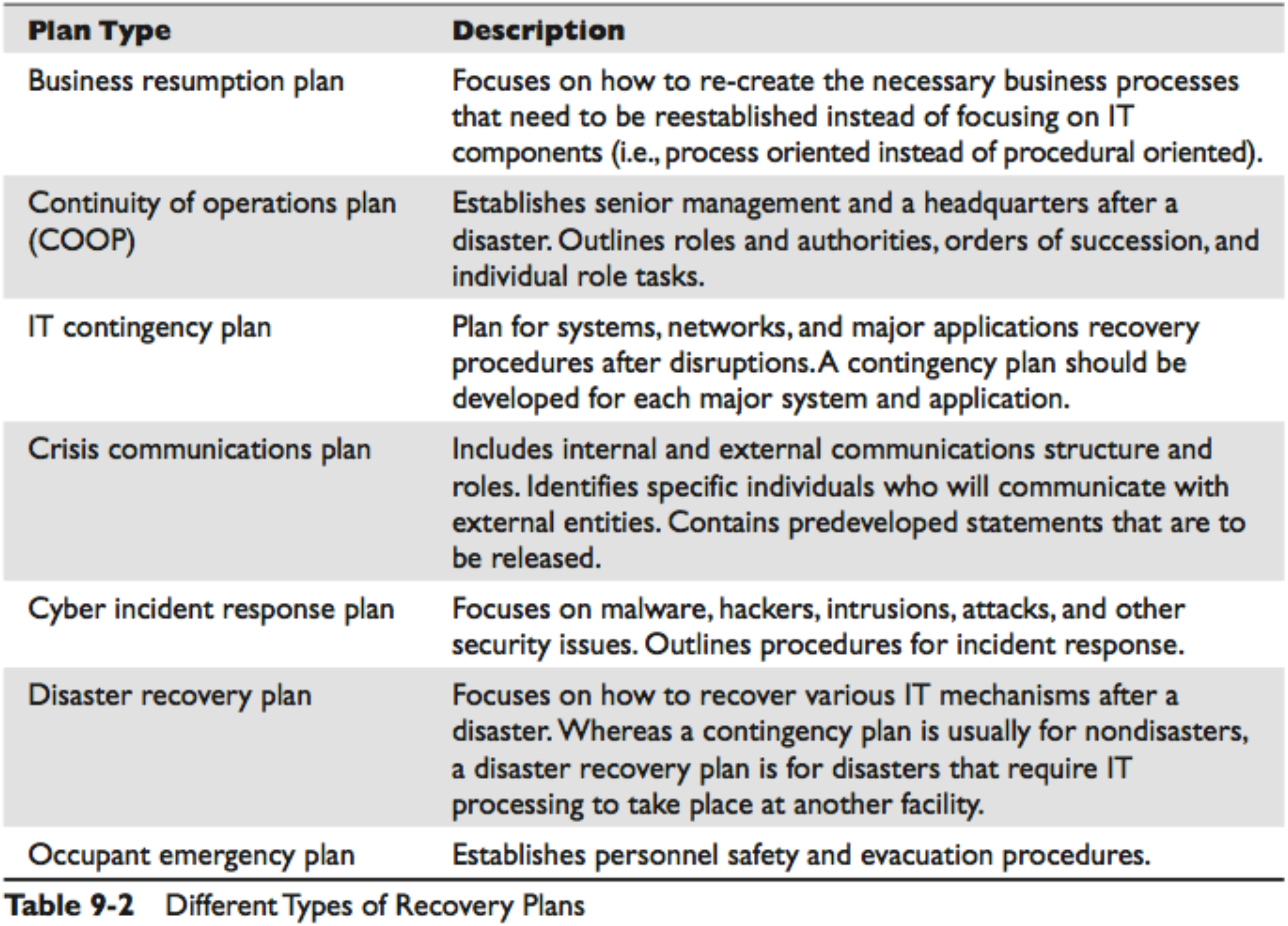
- Restore facility
- Test environment
- Move operations

V.

Appendixes

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

6. Testing



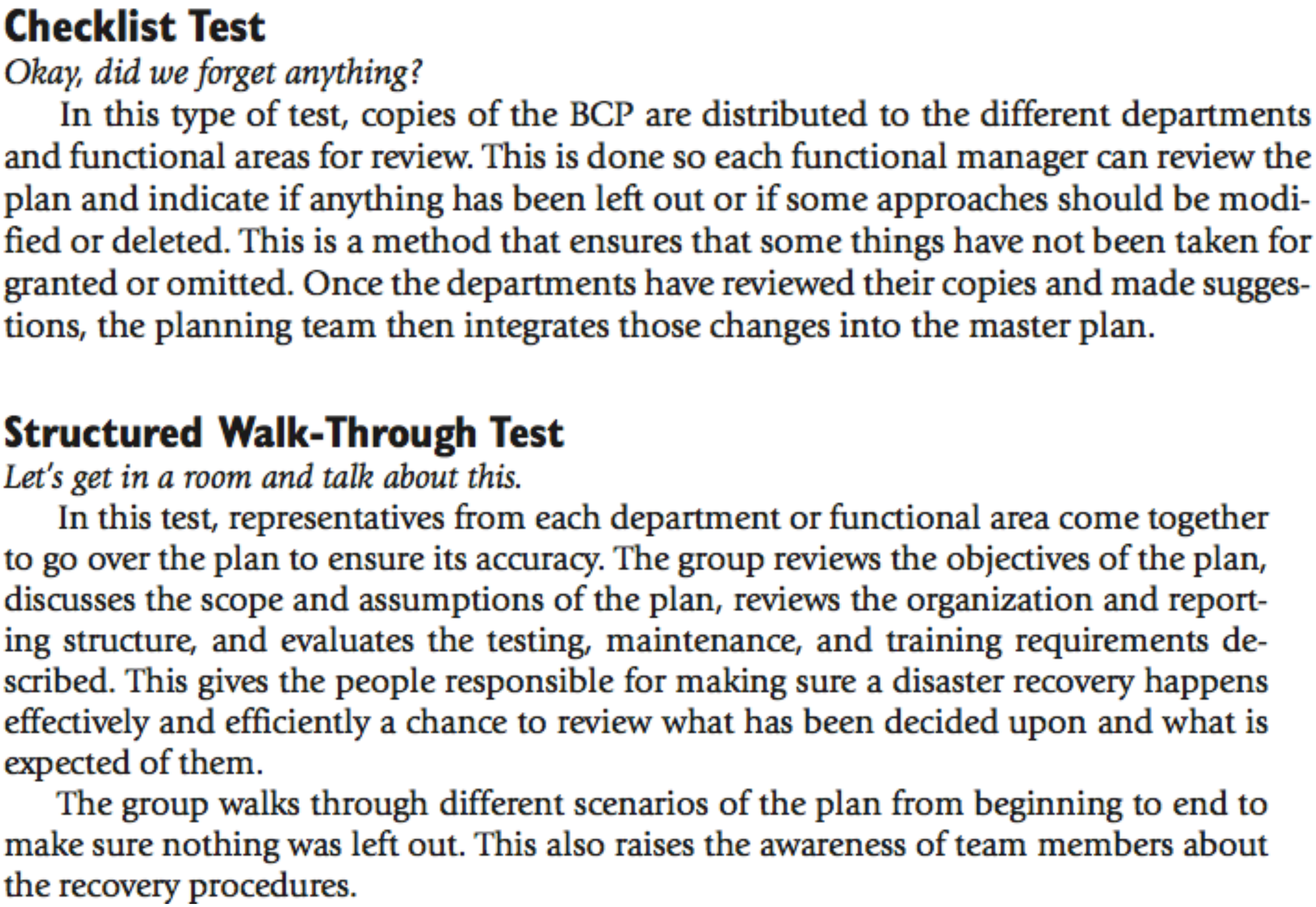
Plan Type	Description
Business resumption plan	Focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on IT components (i.e., process oriented instead of procedural oriented).
Continuity of operations plan (COOP)	Establishes senior management and 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.

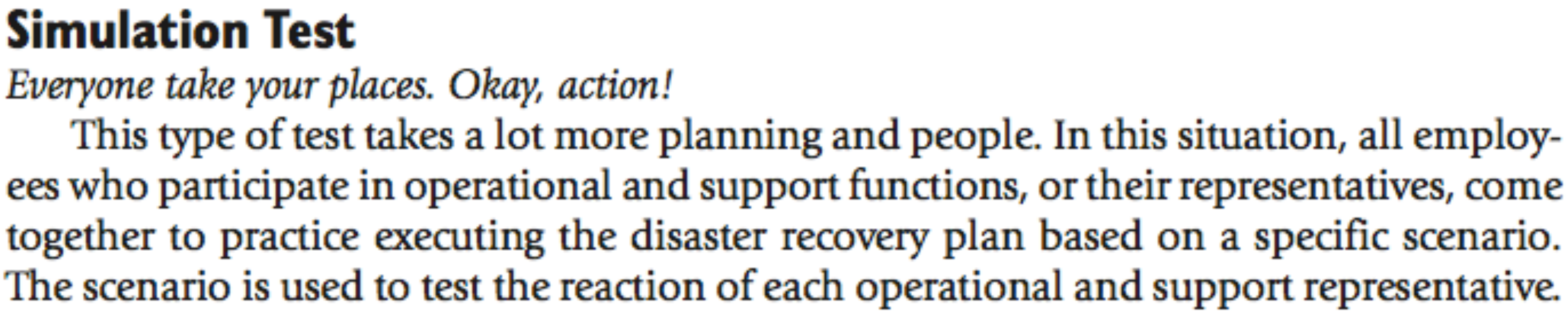
Structured Walk-Through Test

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.

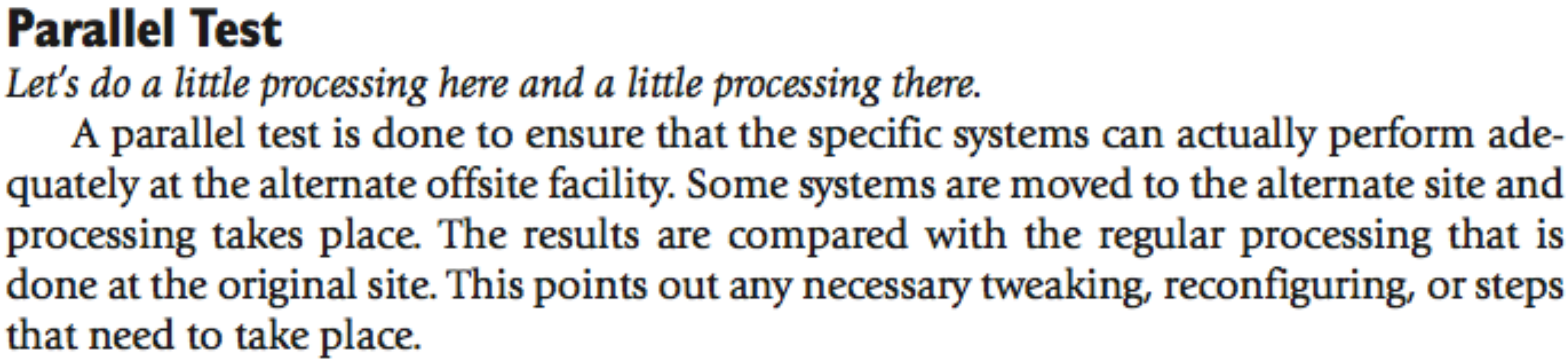
Types of tests (continued)



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.

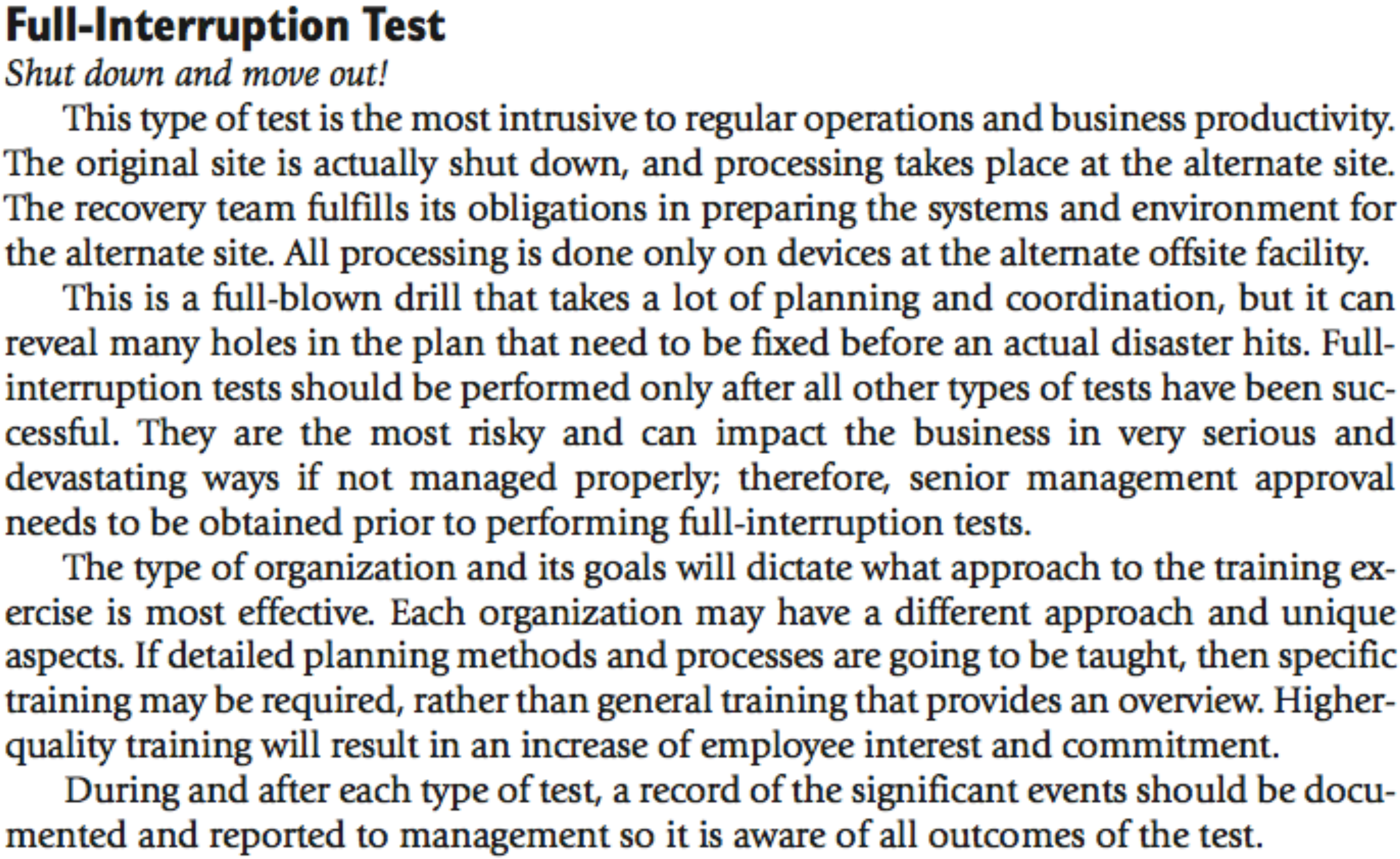


Parallel Test

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.

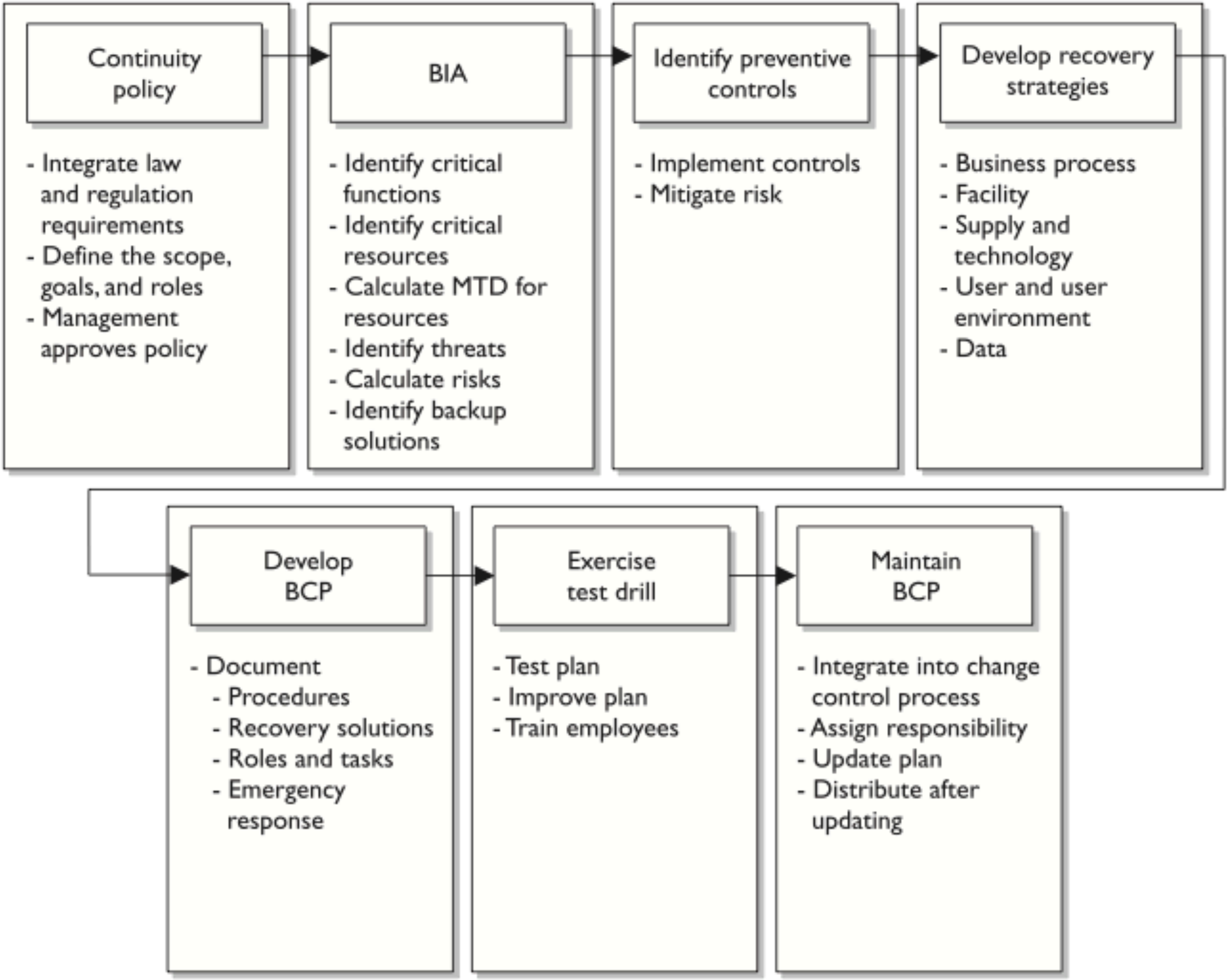
Procedure: Personnel Evacuation Description	Location	Names of Staff Trained to Carry Out Procedure	Date Last Carried Out
Each floor within the building must have two individuals who will ensure that all personnel have been evacuated from the building after a disaster. These individuals are responsible 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

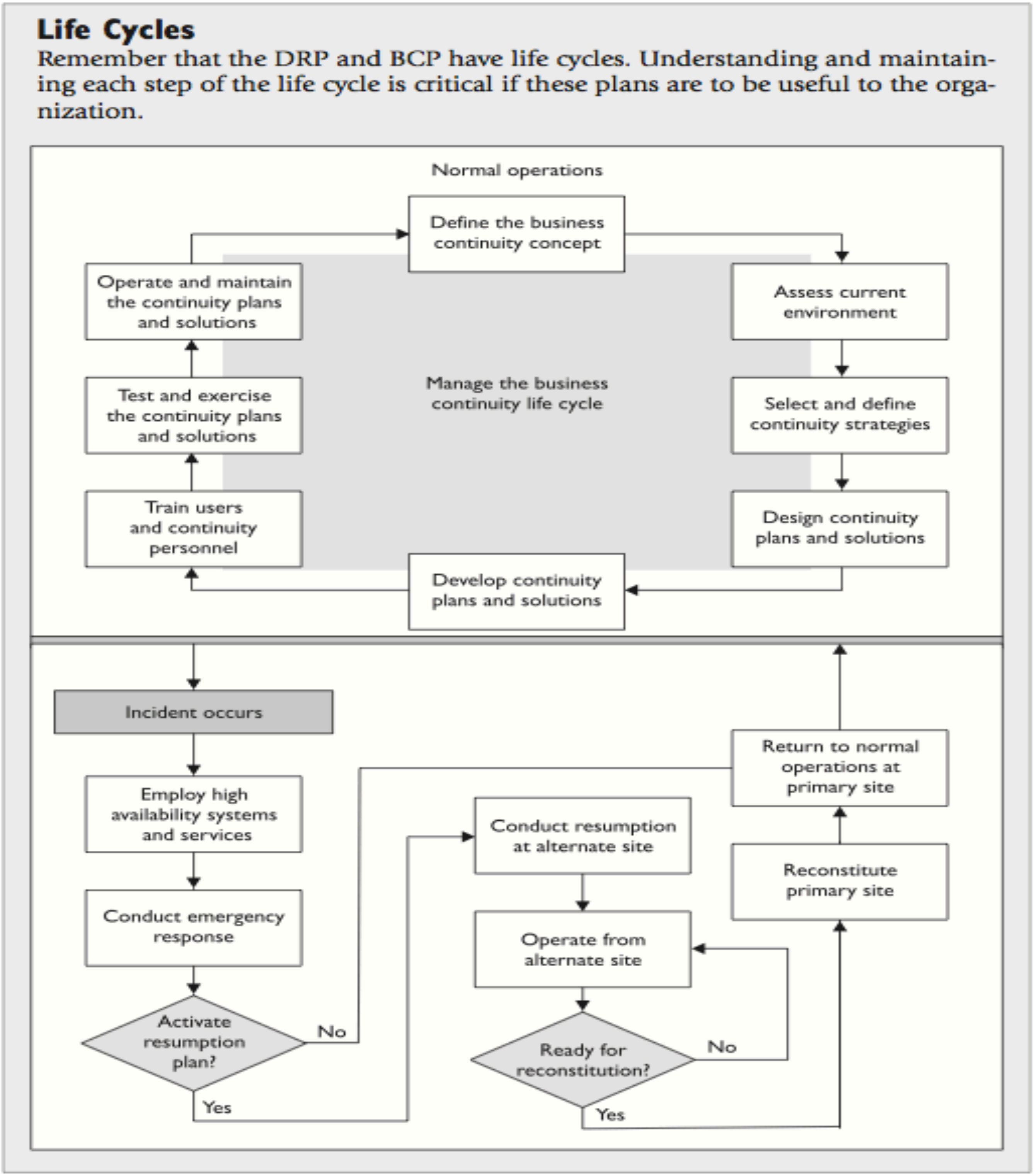
- Document
  - Procedures
  - Recovery solutions
  - Roles and tasks
  - Emergency response

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.

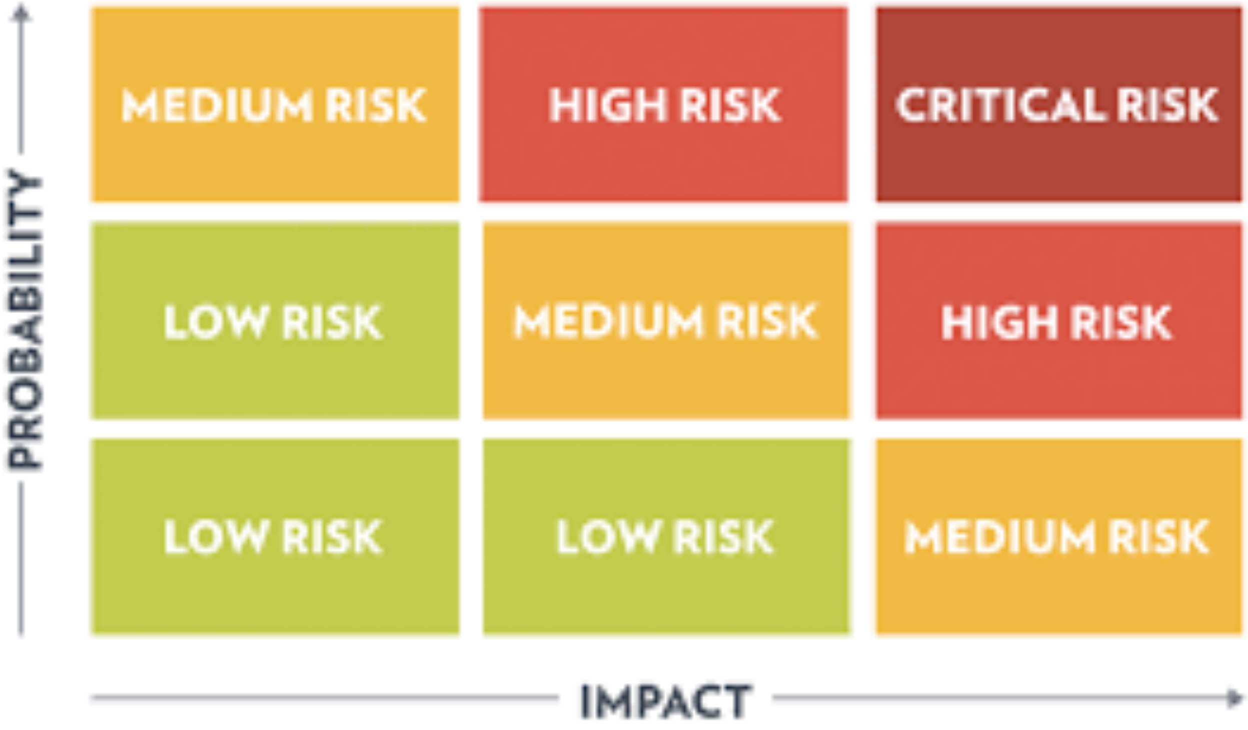
Normal operations
Define the business continuity concept
Assess current environment
Select and define continuity strategies
Design continuity plans and solutions
Develop continuity plans and solutions
Train users and continuity personnel
Test and exercise the continuity plans and solutions
Operate and 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.

Criticality Analysis (CA)

- **Performed after Business Impact Analysis**
  - **Identifyfies those business processes that are most important and how quickly they need to be recovered during and after any disaster scenario.**



MEDIUM RISK	HIGH RISK	CRITICAL RISK
LOW RISK	MEDIUM RISK	HIGH RISK
LOW RISK	LOW RISK	MEDIUM RISK

Contingency Plans

- Develop contingency plan – procedures and guidelines for how the organization can still stay functional in a crippled state
- Discuss current contingency plan with necessary parties
- Explain contingency plan
- Monitor contingency plan training
- Propose contingency plan
- Summarize contingency plan

Contingency Plans

- Direct implementation of contingency plan
  - Object-to-task mapping
  - Resource-to-task mapping
  - Milestones
  - Budget estimates
  - Success factors
  - Deadlines
- Direct operation of contingency plan
- Influence management on importance of having properly trained SA/staff to perform contingency plan on mission critical systems
- Test contingency plan – highlights deficiencies in the plan

Contingency Plans

- Verify current contingency plan is available and accuracy
- Verify that necessary parties understand contingency plan and where it is maintained, parties include:
  - Business units
  - Senior management
  - IT department
  - Security department
  - Communications department
  - Legal department
- Write contingency plan

Plans
Post-incident Activities and Investigation

Domain 4:
Information Security Incident Management

Connecticut Eradication and Recovery

- Eradication actions for specific incident type
- Follow change management procedures
- Perform recovery procedures
- System verification
- Remove malicious code/virus
- Assess the impact on operating systems
- Harden the operating systems
- Remove dormant user ID’s
- Tighten access rights
- Shut down and restart systems/services for DoS
- Software/Hardware configuration changes
- Restoration from previous backup
- Re-installation.

Connecticut Resume Operation

- Once eradication and recovery have been completed successfully, normal operations can resume.
- Appropriate agency and interagency communication will occur at this time.

Connecticut Post Incident Review

- **The IT security Division focuses on analyzing patterns of activity across the enterprise.**
  - **They support comprehensive tracking, recording, and dissemination of information to the enterprise.**
  - **By consolidating the information collected, the team is better able to identify similar attacks, artifacts, exploits, trends and patterns.**
  - **Potential new threats to the enterprise can also be identified.**
  - ***Your Agency* will focus on patterns of activity within the LAN and agency applications.**
  - **In this model, it is important that the team have expertise or familiarity with all platforms and operating systems used in the organization.**
  - **If this does not exist within the centralized team component, then there must be mechanisms in place to collaborate with the distributed team members or other organizational experts who can provide the required knowledge.**

Connecticut Post Incident Activities

- Based on the results of the analysis of any vulnerability or artifact information, the IT security Division coordinates the release of remediation, detection, and recovery steps throughout the enterprise as required.
- <u>Post Incident Activity</u> – The IMT and response team(s) will attend a debriefing meeting and an After Action Report (AAR) of the incident from start to conclusion is developed which will include an improvement plan.
- Documentation of any permanent changes to systems as a result of the incident are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

Connecticut Follow Up

- Specific follow up activities include:
  - Monitor affected systems
  - Update incident log
  - Perform post-mortem
  - Incident documentation
  - Media-Handling
  - Update incident response procedures

Reconstitution

- Discuss current reconstitution plan with necessary parties to ensure they understand their respective reconstitution roles and responsibilities
- Explain reconstitution plan – plan for handling the situation when an organization moves to a new site or returns to the original site
- Explain restoration – placing information onto the new site through the use of proper protection, detection, and reaction capabilities defined in the plan
- Monitor reconstitution plan training
- Monitor restoration/reconstitution
- Summarize restoration/reconstitution plan

Reconstitution

- Verify that necessary parties understand restoration/reconstitution plans and where they are maintained
- Develop restoration/reconstitution plan
  - Ensuring adequate environment and necessary equipment and supplies are present and functional
  - Proper communications, connectivity and testing procedures
  - Backup data from alternate site to new site
- Direct implementation of reconstitution plan – facility restoration, environment testing, and moving of operations
- Direct operation of reconstitution plan
- Implement and maintain recovery procedures
- Implement recovery procedures

Reconstitution

- Implement testing and assessment
  - Checklist test – has anything been forgotten?
  - Structured walk-through test – all parties meet and talk through scenarios step by step
  - Simulation test – drills are done to practice executing disaster recovery plans
  - Parallel test – ensures that specific systems can run at the alternate offsite facility
  - Full-Interruption test – original site is shutdown and offsite is used
- Implement training
- Influence management on importance of having properly trained SA/staff to perform reconstitution plan on mission critical systems
- Propose reconstitution plan

Reconstitution

- Test/exercise restoration/reconstitution plan
- Verify current restoration/reconstitution plan is available and accurate
- Write restoration/reconstitution plan
- Evaluate test/execution of reconstitution plan

Recovery

- Address recovery procedures with SA/staff
- Develop recovery plan
  - Business process recovery
  - Facility recovery
  - Supply and technology recovery
  - User environment recovery
  - Data recovery
- Direct SA/staff to use recovery plan during recovery
- Discuss current recovery plan with necessary parties
- Explain recovery plan
- Monitor recovery plan training

Recovery

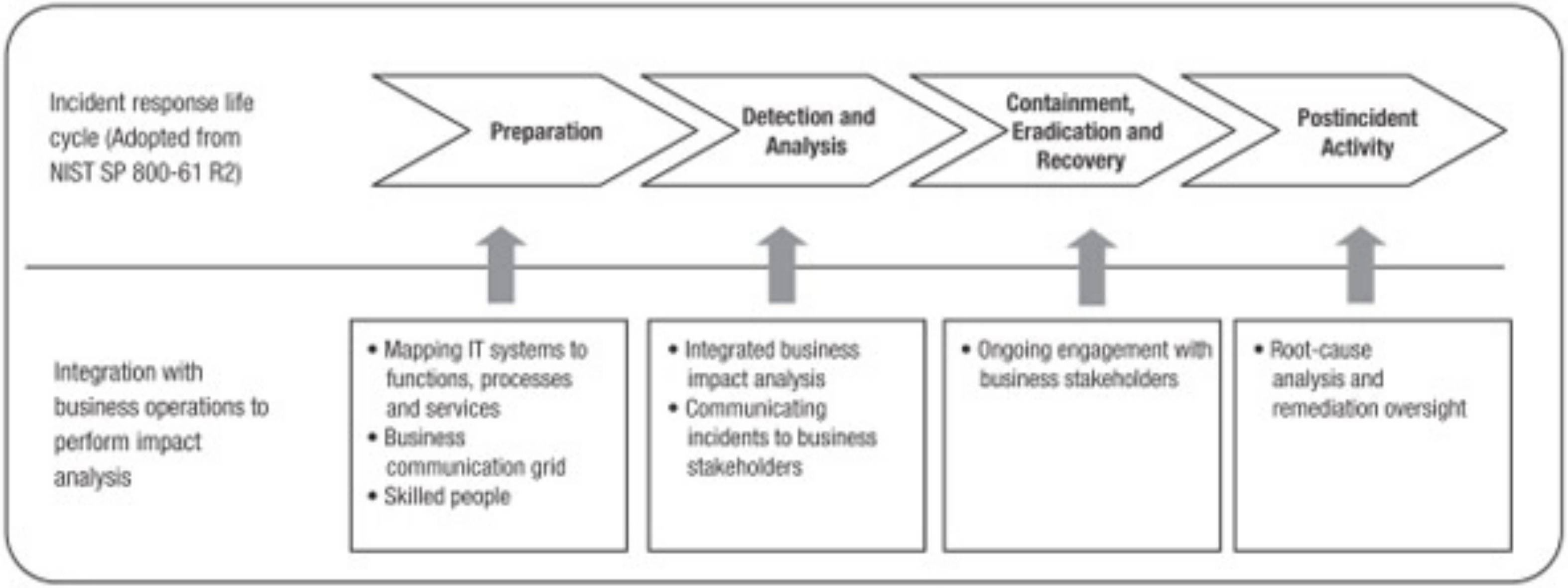
- Summarize recovery plan
- Verify that necessary parties understand recovery plan and where it is maintained
- Direct implementation of recovery plan
- Direct operation of recovery plan
  - Move to alternate site
  - Restore processes
  - Recovery procedures
- Influence management on importance of having properly trained SA/staff to perform recovery plan on mission critical systems
- Propose recovery plan

Recovery

- Test recovery plan
- Verify current recovery plan is available and accurate
- Verify SA understands rules for restoring files
- Write recovery plan
  - Required roles
  - Required resources
  - Input and output mechanisms
  - Workflow steps
  - Required time for completion
  - Interfaces with other processes

Incident Response Lifecycle and Business Integration

Figure 1—Incident Response Life Cycle and Business Integration



Incident response life cycle (Adopted from NIST SP 800-61 R2)

Preparation

Detection and Analysis

Containment, Eradication and Recovery

Postincident Activity

Integration with business operations to perform impact analysis

- Mapping IT systems to functions, processes and services
- Business communication grid
- Skilled people

- Integrated business impact analysis
- Communicating incidents to business stakeholders

- Ongoing engagement with business stakeholders

- Root-cause analysis and remediation oversight

Source: Hari Mukundhan. Reprinted with permission.

Source: https://www.isaca.org/Journal/archives/2015/volume-6/ Pages/a-business-integrated-approach-to-incident-response.aspx

Communications Grid

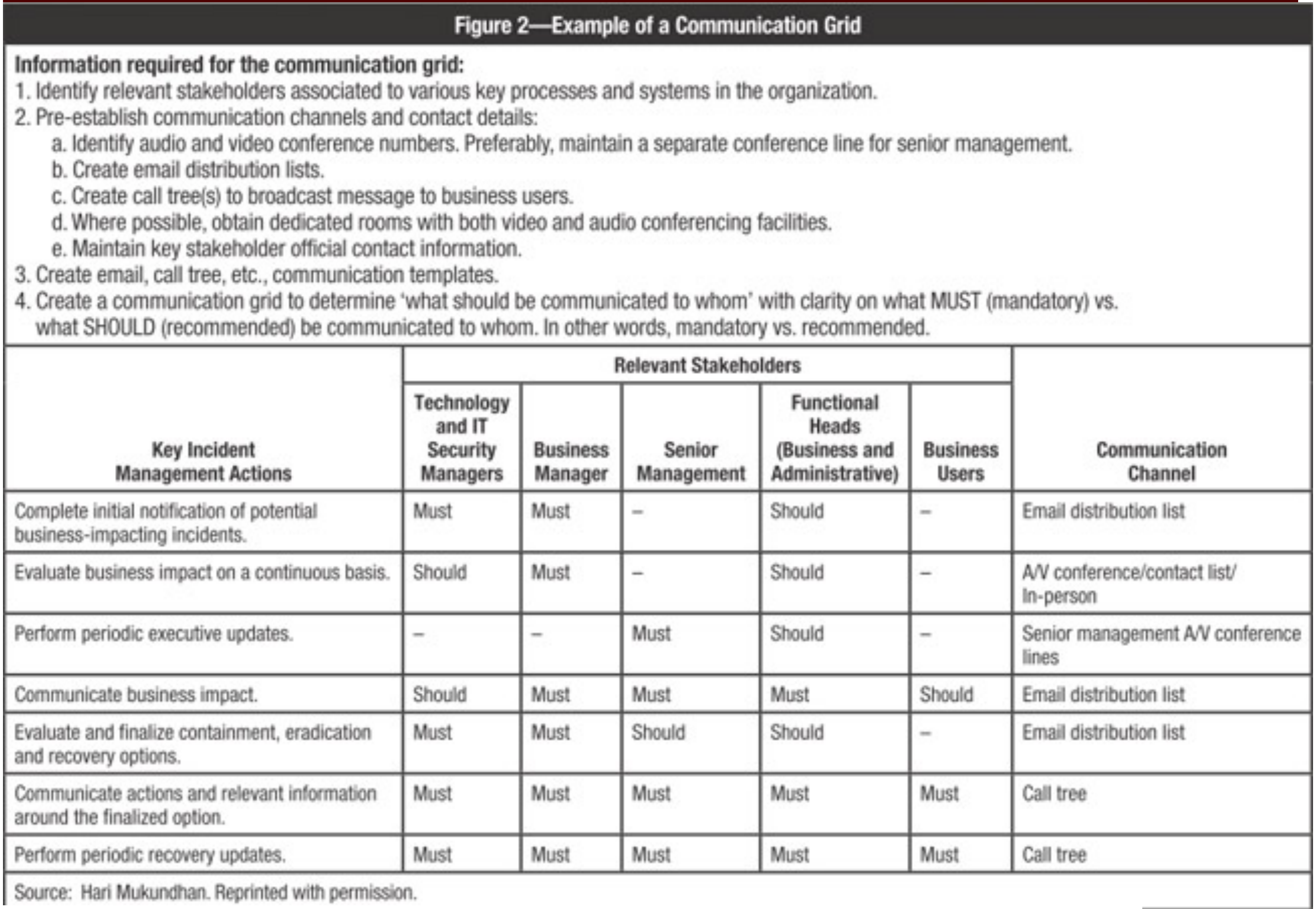


Figure 2—Example of a Communication Grid

Information required for the communication grid:

1. Identify relevant stakeholders associated to various key processes and systems in the organization.
2. Pre-establish communication channels and contact details:
   a. Identify audio and video conference numbers. Preferably, maintain a separate conference line for senior management.
   b. Create email distribution lists.
   c. Create call tree(s) to broadcast message to business users.
   d. Where possible, obtain dedicated rooms with both video and audio conferencing facilities.
   e. Maintain key stakeholder official contact information.
3. Create email, call tree, etc., communication templates.
4. Create a communication grid to determine 'what should be communicated to whom' with clarity on what MUST (mandatory) vs. what SHOULD (recommended) be communicated to whom. In other words, mandatory vs. recommended.

	Relevant Stakeholders					
Key Incident Management Actions	**Technology and IT Security Managers**	**Business Manager**	**Senior Management**	**Functional Heads (Business and Administrative)**	**Business Users**	**Communication Channel**
Complete initial notification of potential business-impacting incidents.	Must	Must	–	Should	–	Email distribution list
Evaluate business impact on a continuous basis.	Should	Must	–	Should	–	A/V conference/contact list/ In-person
Perform periodic executive updates.	–	–	Must	Should	–	Senior management A/V conference lines
Communicate business impact.	Should	Must	Must	Must	Should	Email distribution list
Evaluate and finalize containment, eradication and recovery options.	Must	Must	Should	Should	–	Email distribution list
Communicate actions and relevant information around the finalized option.	Must	Must	Must	Must	Must	Call tree
Perform periodic recovery updates.	Must	Must	Must	Must	Must	Call tree

Source: Hari Mukundhan. Reprinted with permission.

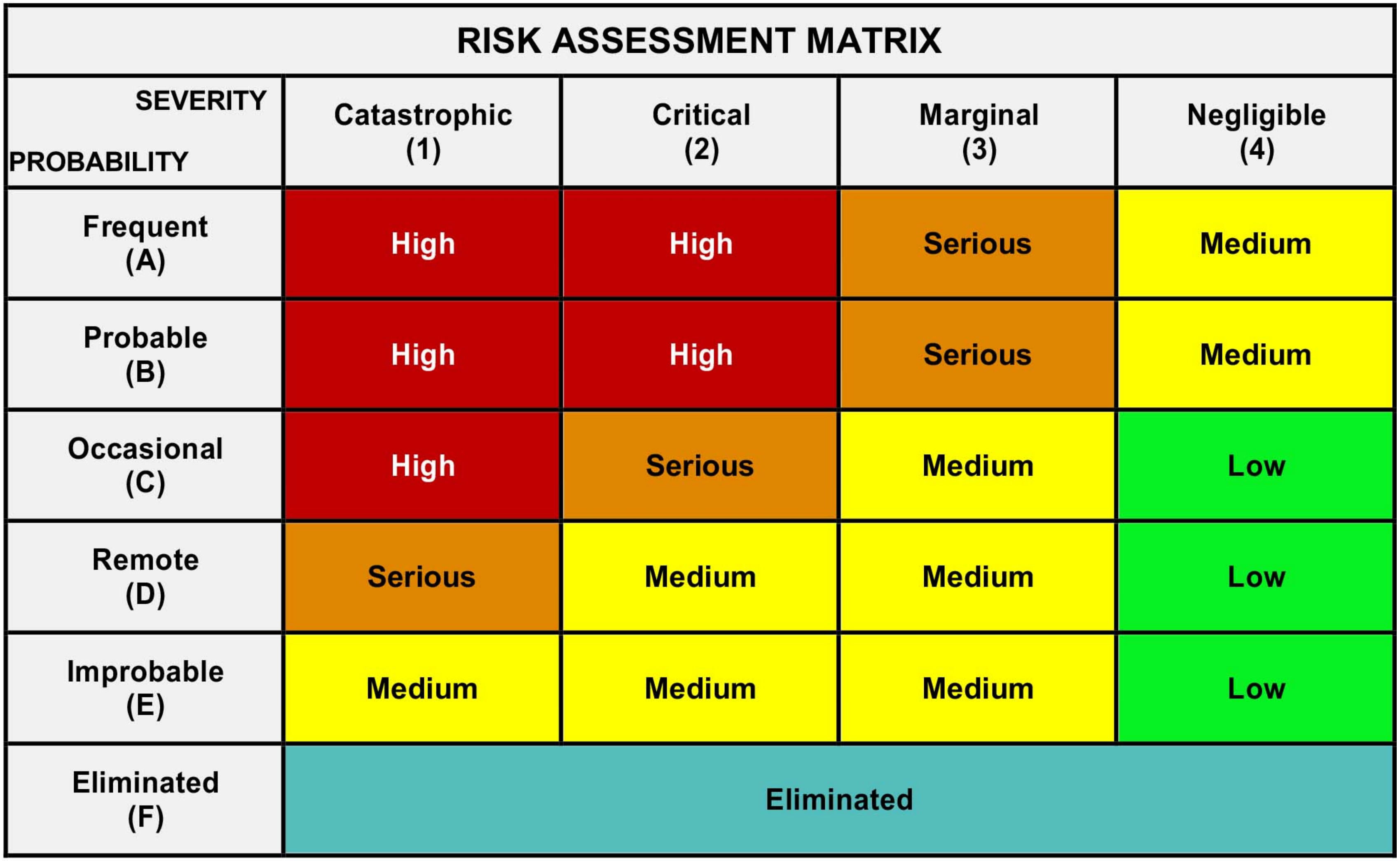
Source: https://www.isaca.org/Journal/archives/2015/volume-6/Pages/a-business-integrated-approach-to-incident-response.aspx

MIL-STD-882E System Safety

SEVERITY CATEGORIES		
Description	**Severity Category**	**Mishap Result Criteria**
Catastrophic	**1**	Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.
Critical	**2**	Could result in one or more of the following: permanent partial disability,injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M.
Marginal	**3**	Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M.
Negligible	**4**	Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K.

PROBABILITY LEVELS			
Description	**Level**	**Specific Individual Item**	**Fleet or Inventory**
Frequent	**A**	Likely to occur often in the life of an item.	Continuously experienced.
Probable	**B**	Will occur several times in the life of an item.	Will occur frequently.
Occasional	**C**	Likely to occur sometime in the life of an item.	Will occur several times.
Remote	**D**	Unlikely, but possible to occur in the life of an item.	Unlikely, but can reasonably be expected to occur.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item.	Unlikely to occur, but possible.
Eliminated	**F**	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.	Incapable of occurence. This level is used when potential hazards are identified and later eliminated.

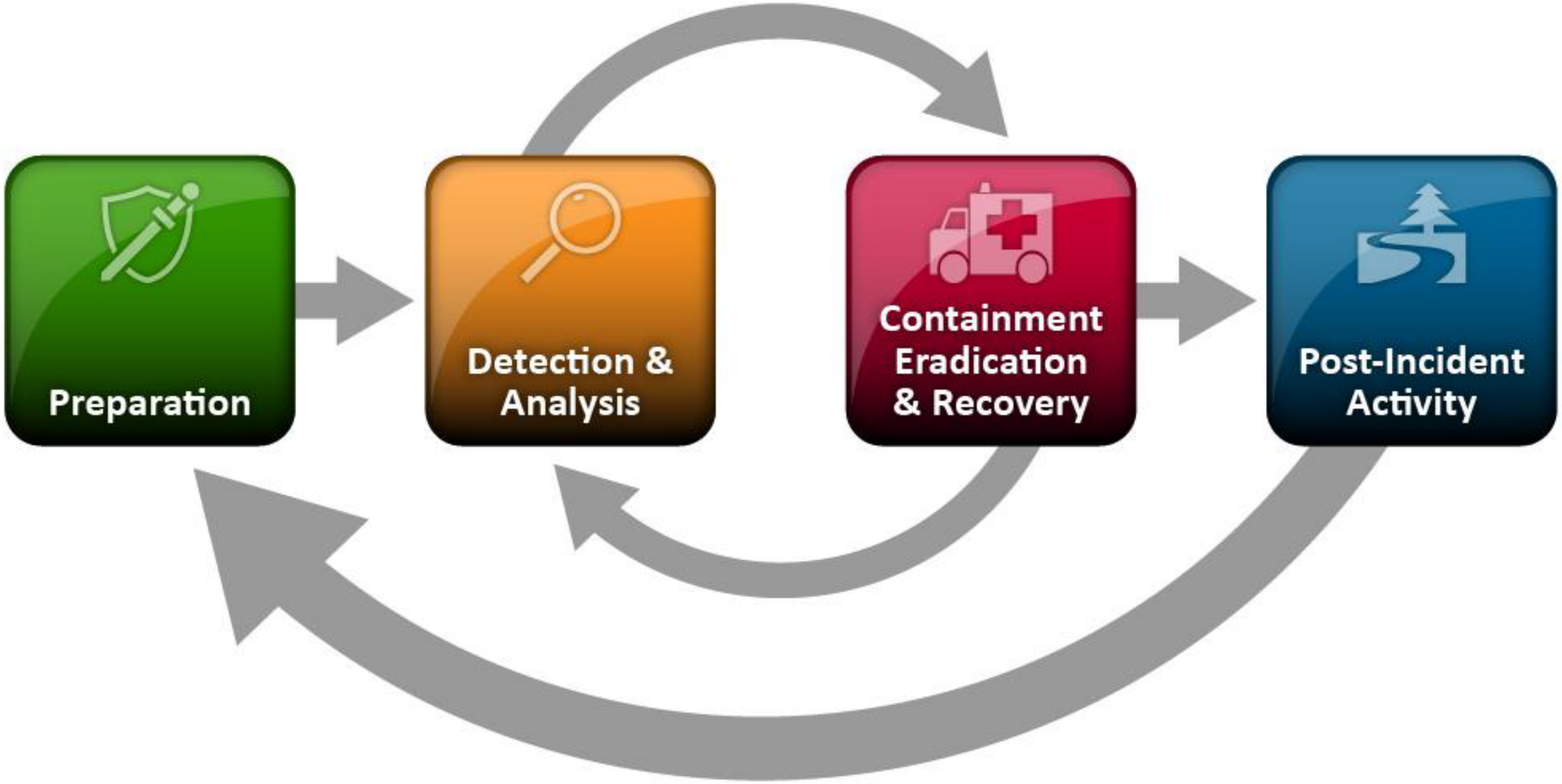
MIL-STD-882E Risk Assessment



RISK ASSESSMENT MATRIX

SEVERITY PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

NIST Incident Response Life Cycle



Certified Information System Management

- The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs. CISM is the leading credential for information security managers.
- The recent quarterly *IT Skills and Certifications Pay Index* (ITSCPI) from Foote Partners ranked CISM among the most sought-after and highest-paying IT certifications.
- DoD 8140 compliant
- DoD 8570 Level III IAM

J. A. "Drew" Hamilton, Jr., Ph.D.

Chair, NSA Cyber Operations Community of Practice

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

This work funded by NSA Contract #H98230-19-1-0291

CCI
2 Research Blvd.
Starkville, MS 39759

Voice: (662) 325-2294
Fax: (662) 325-7692
drew@drew-hamilton.com