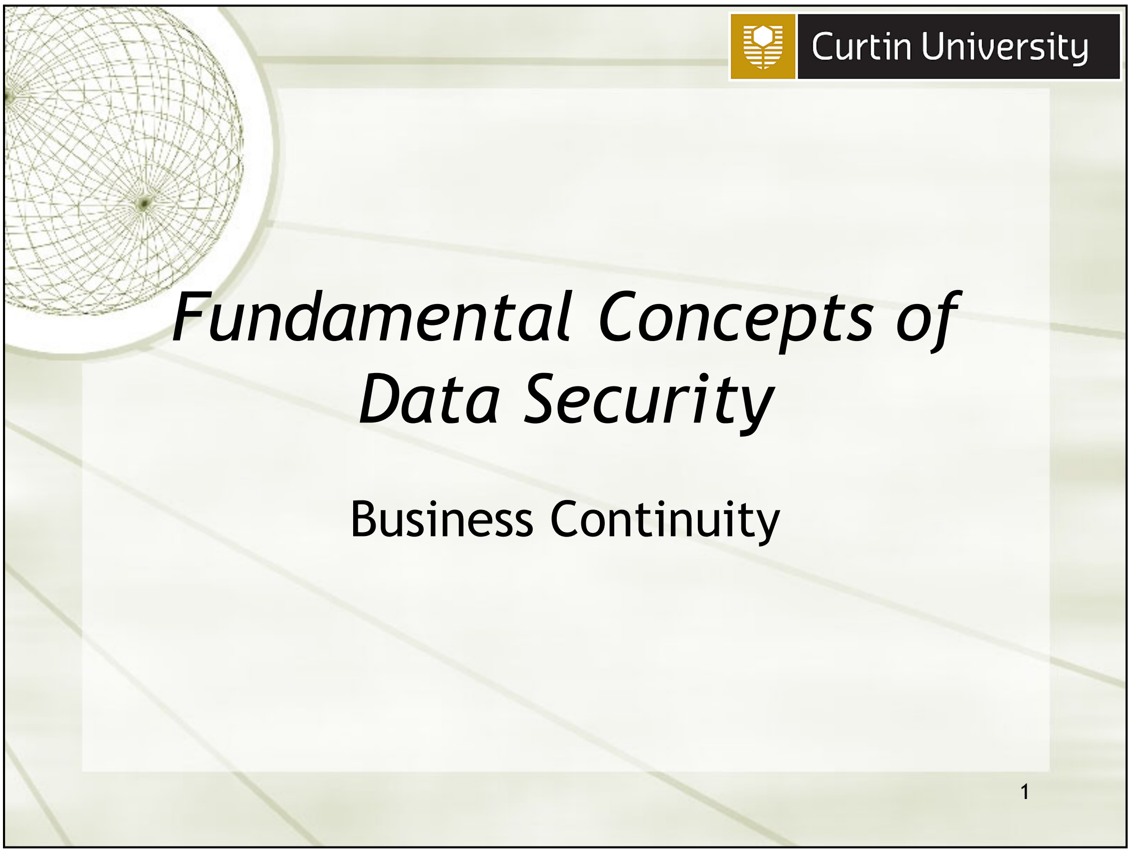


Curtin University

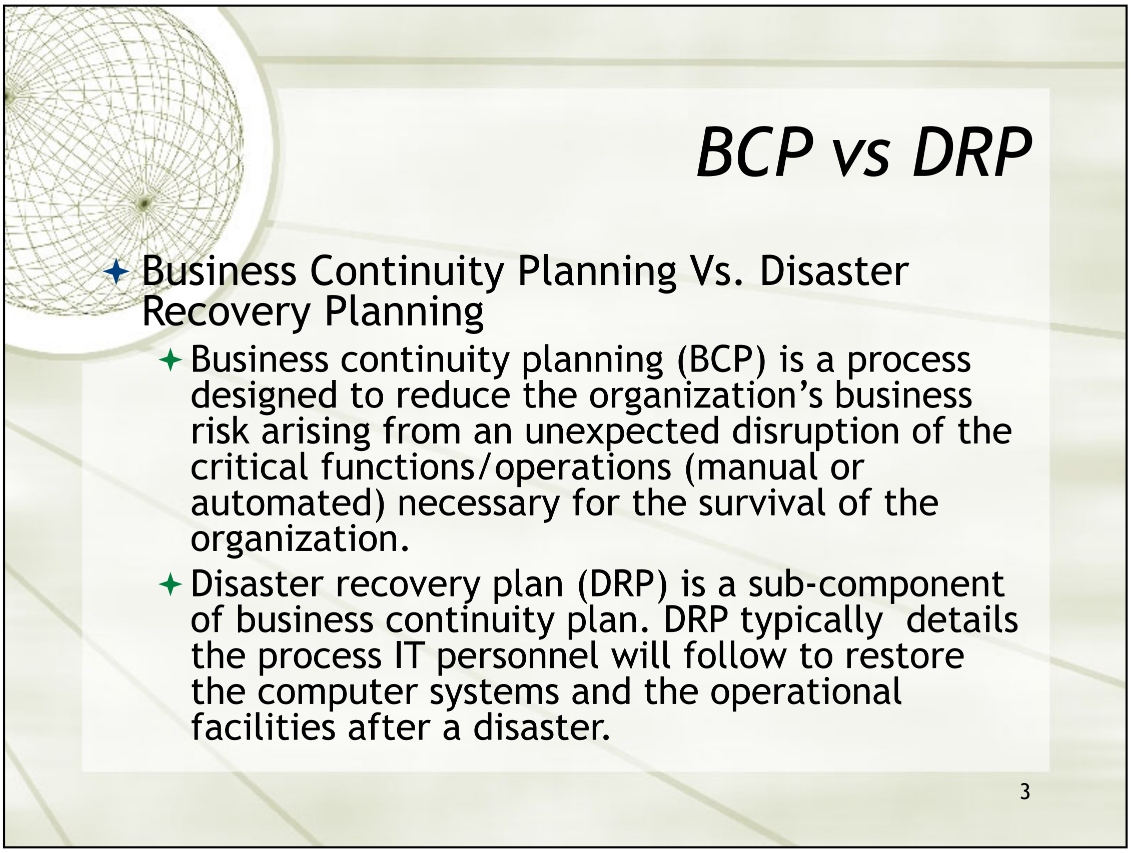
Fundamental Concepts of Data Security

Business Continuity

1

Comprehensive approach to business continuity plan

- Prevention: risk management plan (this lecture) – what to do to prevent incidents
- Preparedness: business impact analysis – if incidents do happen, what would be the impact
- Response: incident response plan – what to do when incidents happen
- Recovery: recovery plan – how to recover after an incident/disaster



BCP vs DRP

- Business Continuity Planning Vs. Disaster Recovery Planning
  - Business continuity planning (BCP) is a process designed to reduce the organization’s business risk arising from an unexpected disruption of the critical functions/operations (manual or automated) necessary for the survival of the organization.
  - Disaster recovery plan (DRP) is a sub-component of business continuity plan. DRP typically details the process IT personnel will follow to restore the computer systems and the operational facilities after a disaster.

An emergency is a potentially life-threatening situation, usually occurring suddenly and unexpectedly. Emergencies may be the result of natural and/or human causes.

Preparing for emergencies involves planning, practicing, evaluating, and adjusting.

An immediate response is critical in emergencies.

The Emergency Planning and Community Right-to-Know Act has the following four main components: emergency planning, emergency notification, information requirements, and toxic chemical release reporting.

For proper coordination of the internal emergency response, it is important that one person be in charge and that everyone involved knows who that person is.

Since there is no way to predict when first aid might be needed, part of preparing for emergencies should include training employees to administer first aid. In certain cases, OSHA requires that companies have at least one employee on-site who has been trained in first aid.

In addition to providing first aid training, it is important to have well-stocked first aid kits readily available, have personal protective devices available, post emergency telephone numbers, and keep all employees informed.

The OSHA standard for evacuation planning is 29 CFR 1910.38. This standard requires a written plan for evaluating the facility in the event of an emergency. Critical elements of the plan are as follows: marking of exit routes, communications, outside assembly, and training.

A company's emergency action plan should be a collection of small plans for each anticipated emergency. These plans should have the following components: procedures, coordination, assignments/responsibilities, accident prevention strategies, and schedules.

EAPs should be customized so that they are location-specific by including a map, an organization chart, local coordination information, and local training schedules.

An emergency response team is a special team to handle general and localized emergencies to facilitate evacuation and shutdown, protect and salvage company property, and work with civil authorities.

An emergency response network is a network of emergency response teams that covers a designated geographical area.

Computers can help simplify some of the complications brought by advances in technology. Expert systems mimic human thought processes in making decisions on an if-then basis regarding emergency responses.

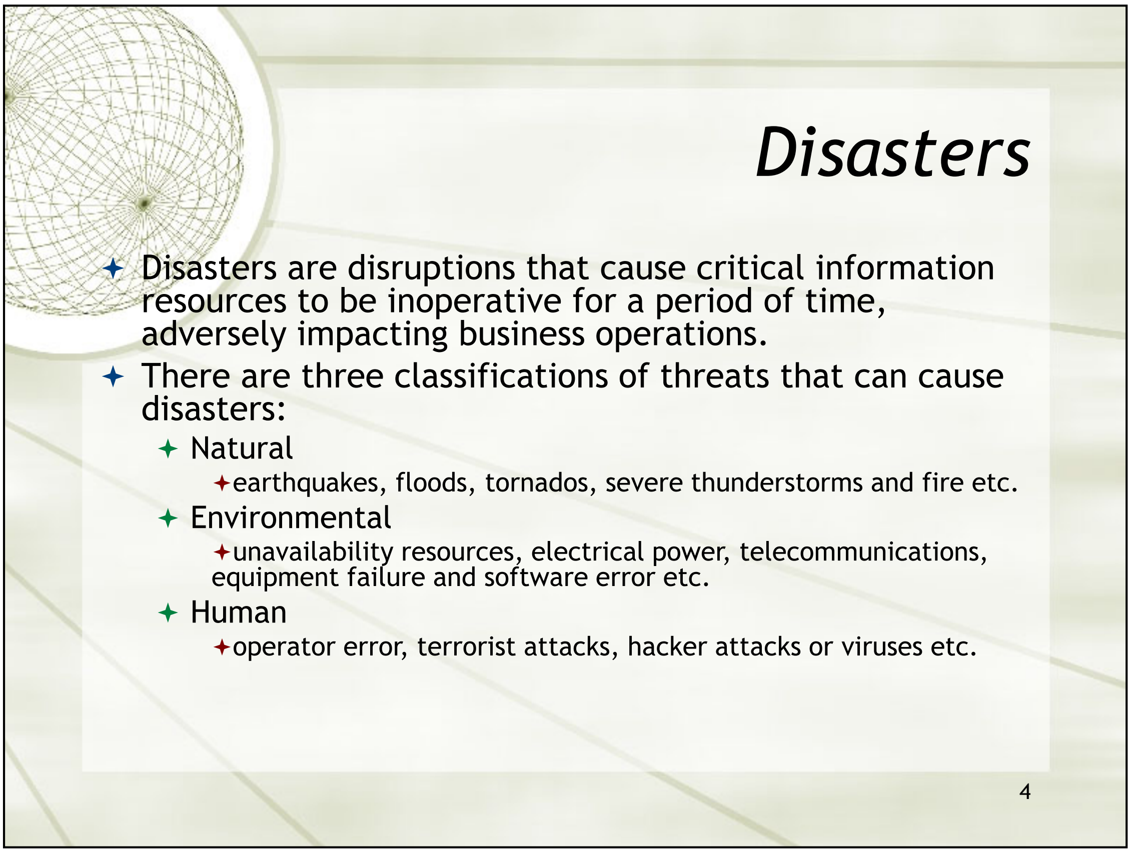
Trauma is psychological stress. It typically results from exposure to a disaster or emergency so shocking that it impairs a person's sense of security or well being. Trauma left untreated can manifest itself as post-traumatic stress disorder. This disorder is characterized by intrusive thoughts, flashbacks, paranoia, concentration difficulties, rapid heartbeat, and irritability.

A disaster recovery plan should have at least the following components: recovery coordinator, recovery team, recovery analysis and planning, damage assessment and salvage operations, recovery communications, and employee support and assistance.

Employers can help decrease the likelihood of a terrorist attack on their facilities by taking the following actions: run a safe and caring operation, listen to employees, train employees, communicate, know your personnel, empower personnel, harden the site against external threats and restrict access, remove any barriers to clear visibility around the facility, have and enforce parking and delivery regulations, make sure that visitors can be screened from a distance, keep all unstaffed entrance doors locked from the outside and alarmed, make air intakes and other utilities inaccessible to all but designated personnel, ensure contractors and visitors wear badges, have an emergency response plan and practice it on a regular basis, be cautious of what information is placed on your company’s website, keep up to date with the latest safety and security strategies, protect the integrity of your facility’s key system.

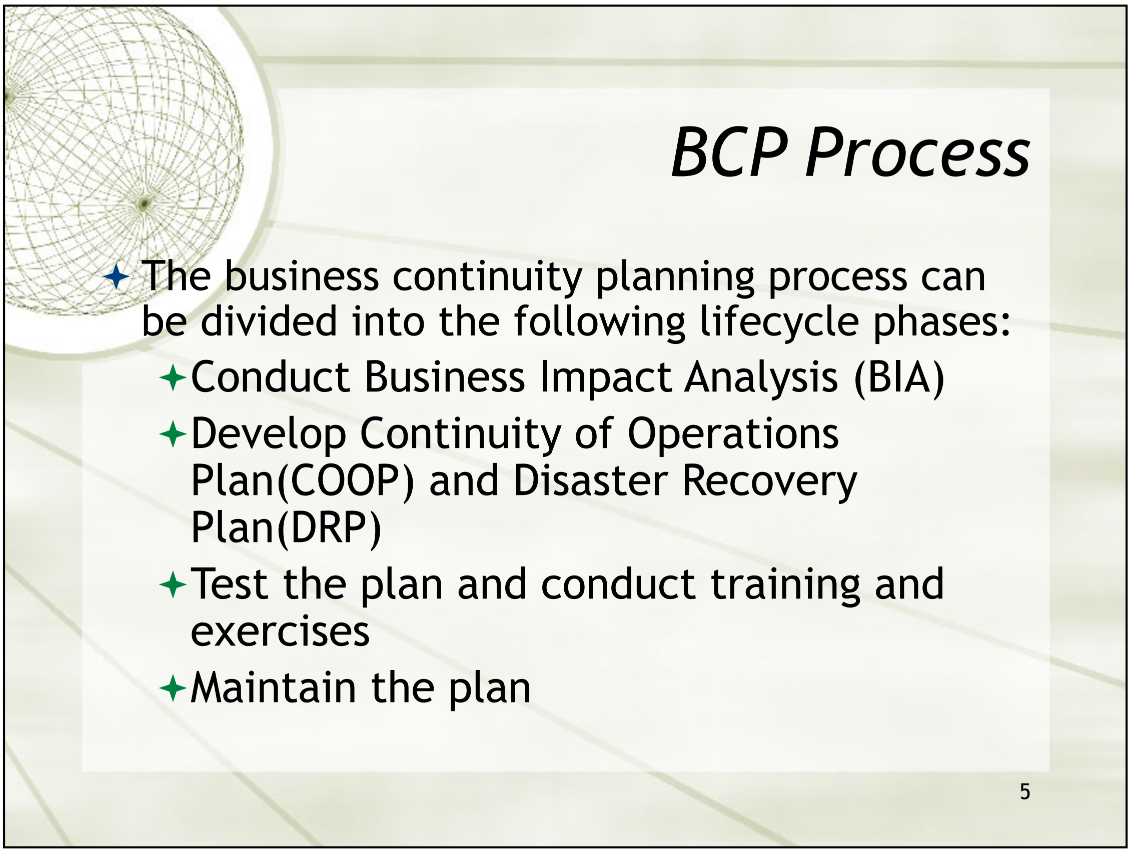
Secure hazardous materials so that terrorists cannot gain access to them for use in making bombs and other weapons of mass destruction. A hazmat security plan should have two components: personnel security and physical security.

All systems, conditions, and potential hazards should be checked and corrected as appropriate before resuming business after a disaster.



Disasters

- Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting business operations.
- There are three classifications of threats that can cause disasters:
  - Natural
    - earthquakes, floods, tornados, severe thunderstorms and fire etc.
  - Environmental
    - unavailability resources, electrical power, telecommunications, equipment failure and software error etc.
  - Human
    - operator error, terrorist attacks, hacker attacks or viruses etc.



BCP Process

- The business continuity planning process can be divided into the following lifecycle phases:
  - Conduct Business Impact Analysis (BIA)
  - Develop Continuity of Operations Plan(COOP) and Disaster Recovery Plan(DRP)
  - Test the plan and conduct training and exercises
  - Maintain the plan

Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology (NIST) is responsible for developing best practices and standards as they pertain to U.S. government and military environments. NIST outlines the following steps in its Special Publication 800-34, Continuity Planning Guide for Information Technology Systems:

1. *Develop the continuity planning policy statement.* Write a policy that provides the guidance necessary to develop a BCP, and that assigns authority to the necessary roles to carry out these tasks.

2. *Conduct the business impact analysis (BIA).* Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.

3. *Identify preventive controls.* Once threats are recognized, identify and implement controls and countermeasures to reduce the organization's risk level in an economical manner.

4. *Develop recovery strategies.* Formulate methods to ensure systems and critical functions can be brought online quickly.

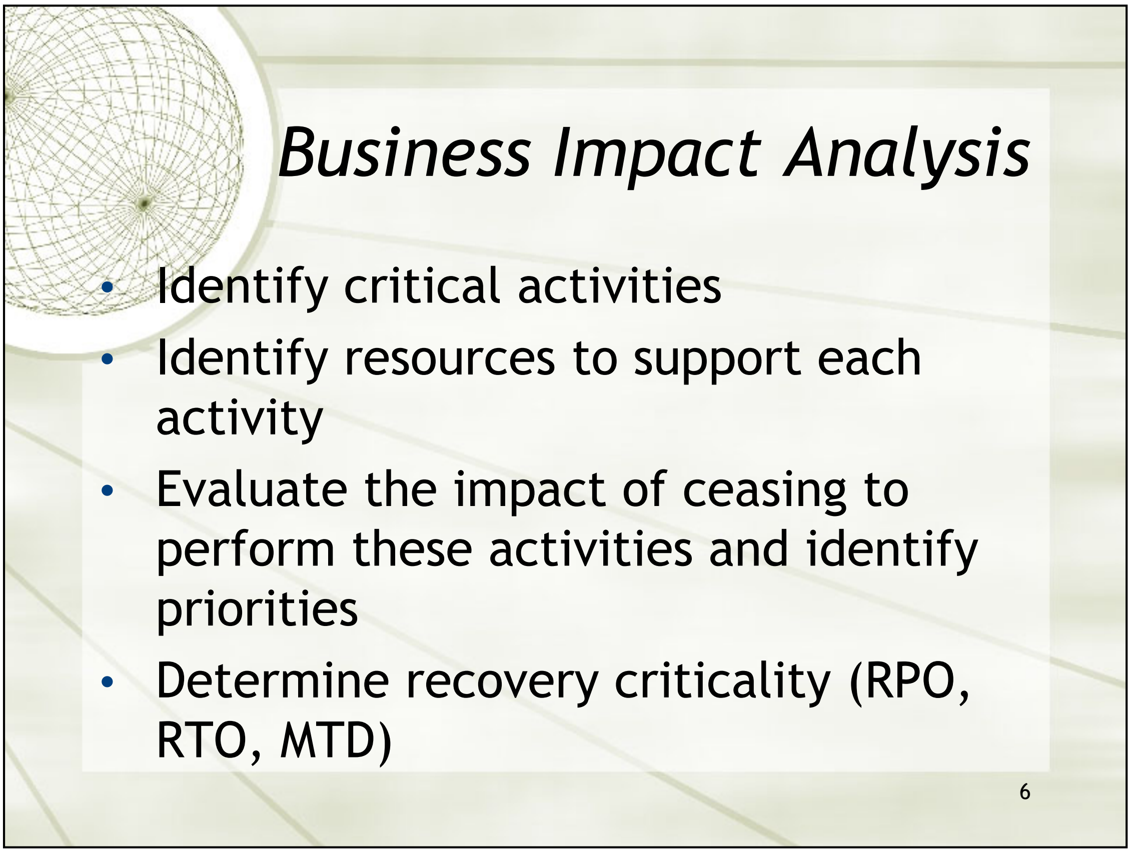
5. *Develop the contingency plan.* Write procedures and guidelines for how the organization can still stay functional in a crippled state.

6. *Test the plan and conduct training and exercises.* Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.

7. *Maintain the plan.* Put in place steps to ensure the BCP is a living document that is updated regularly.

The BCP effort has to result in a sustainable, long-term program that serves its purpose—assisting the organization in the event of a disaster. The effort must be well thought out and methodically executed. It must not be perceived as a mere “public relations” effort to make it simply appear that the organization is concerned about disaster response. The initiation process for BCP might include the following:

- Setting up a budget and staff for the program before the BCP process begins. Dedicated personnel and dedicated hours are essential for executing something as labor-intensive as a BCP.
- Setting up the program would include assigning duties and responsibilities to the BCP coordinator and to representatives from all of the functional units of the organization.
- Senior management should kick off the BCP with a formal announcement or, better still, an organization-wide meeting to demonstrate high-level support.
- Awareness-raising activities to let employees know about the BCP program and to build internal support for it.
- Establishment of skills training for the support of the BCP effort.
- The start of data collection from throughout the organization to aid in crafting various continuity options.
- Putting into effect “quick wins” and gathering of “low-hanging fruit” to show tangible evidence of improvement in the organization’s readiness, as well as improving readiness.



Business Impact Analysis

- Identify critical activities
- Identify resources to support each activity
- Evaluate the impact of ceasing to perform these activities and identify priorities
- Determine recovery criticality (RPO, RTO, MTD)

6

Three steps are typically involved in accomplishing the BIA:

1. Determine mission/business processes and recovery criticality. Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.

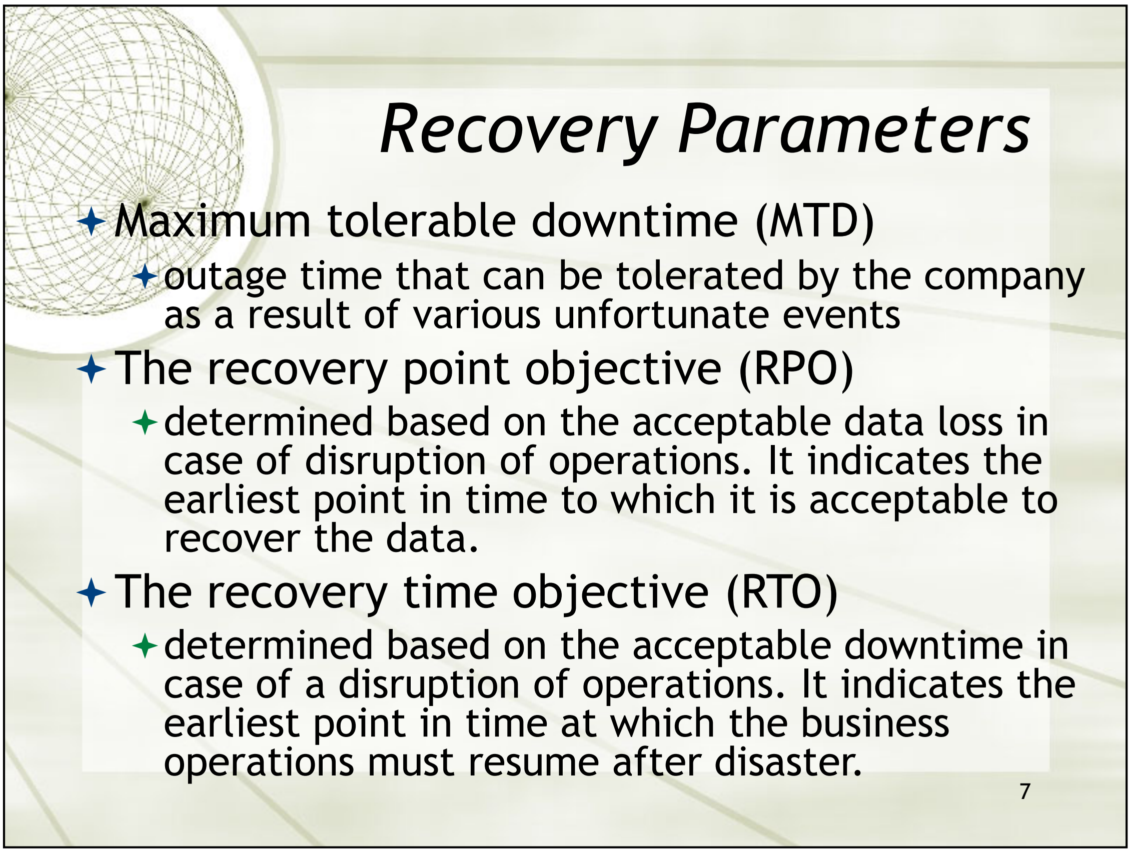
2. Identify resource requirements. Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. Identify recovery priorities for system resources. Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

- **Maximum Tolerable Downtime (MTD)**. The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.
- **Recovery Time Objective (RTO)**. RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
- **Recovery Point Objective (RPO)**. The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.



Recovery Parameters

- Maximum tolerable downtime (MTD)
  - outage time that can be tolerated by the company as a result of various unfortunate events
- The recovery point objective (RPO)
  - determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time to which it is acceptable to recover the data.
- The recovery time objective (RTO)
  - determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume after disaster.

7

The BIA identifies which of the company's critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the ***maximum tolerable downtime (MTD)*** or ***maximum period time of disruption (MPTD)***

The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit:

- **Nonessential** 30 days
- **Normal** 7 days
- **Important** 72 hours
- **Urgent** 24 hours
- **Critical** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

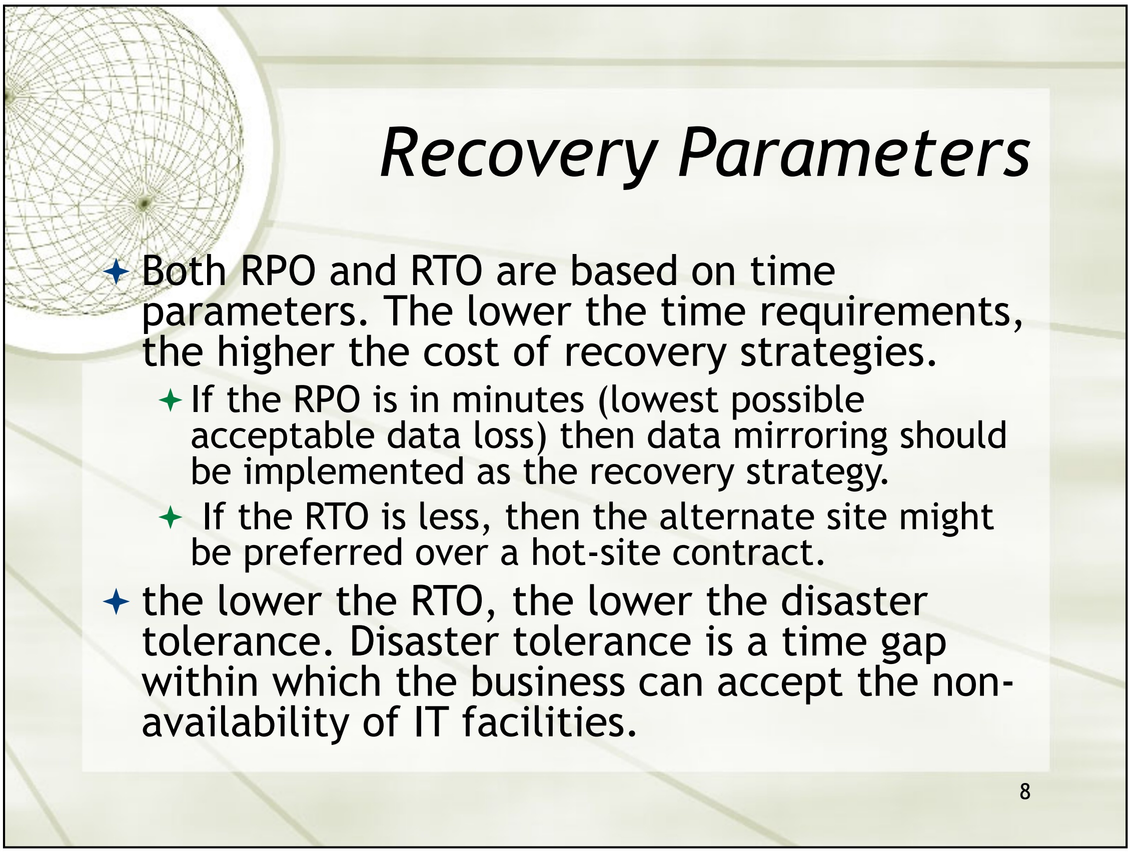
For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line could be considered Critical and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor's service level agreement (SLA), which may promise to have it back online in eight days.

Sometimes the MTD will depend in large measure on the type of business in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

The ***Recovery Time Objective (RTO)*** is the earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in business continuity. The RTO value is smaller than the MTD value, because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization's reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of production for a certain period of time (RTO) and still get back on its feet. But if the company cannot get production up and running within the MTD window, the company is sinking too fast to properly recover.

The ***Work Recovery Time (WRT)*** is the remainder of the overall MTD value. RTO usually deals with getting the infrastructure and systems back up and running, and WRT deals with restoring data, testing processes, and then making everything "live" for production purposes.

The ***Recovery Point Objective (RPO)*** is the acceptable amount of data loss measured in time. This value represents the earliest point in time at which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster.



Recovery Parameters

- Both RPO and RTO are based on time parameters. The lower the time requirements, the higher the cost of recovery strategies.
  - If the RPO is in minutes (lowest possible acceptable data loss) then data mirroring should be implemented as the recovery strategy.
  - If the RTO is less, then the alternate site might be preferred over a hot-site contract.
- the lower the RTO, the lower the disaster tolerance. Disaster tolerance is a time gap within which the business can accept the non-availability of IT facilities.

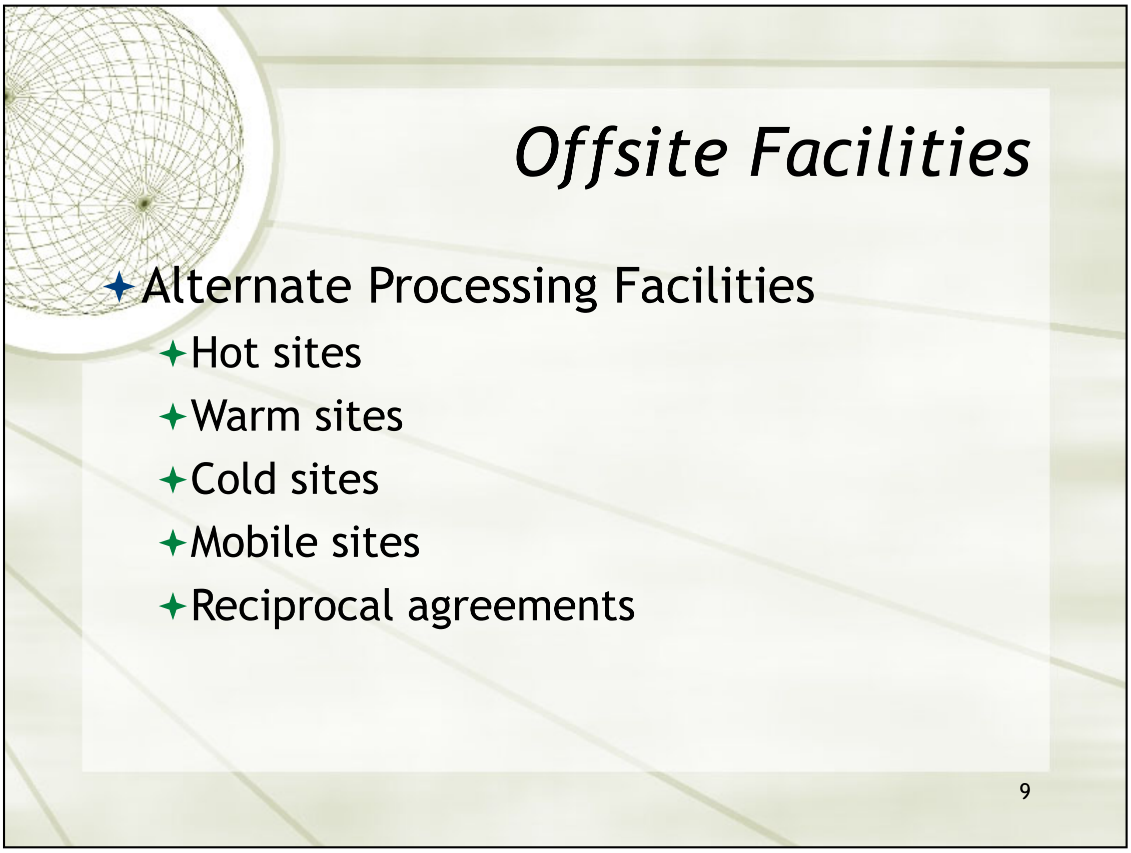
8

The RTO, RPO, and WRT values are critical to understand because they will be the basic foundational metrics used when determining the type of recovery solutions a company must put into place, so let’s dig a bit deeper into them. RTO is the duration of time and a service level that a business process must be restored to in order to ensure that unacceptable consequences associated with a disaster are not endured. Let’s say a company has determined that if it is unable to process product order requests for 12 hours, the financial hit will be too large for it to survive. So the company develops methods to ensure that orders can be processed manually if their automated technological solutions become unavailable. But if it takes the company 24 hours to actually stand up the manual processes, the company could be in a place operationally and financially where it can never fully recover. So RTO deals with “how long do we have to get everything up and working again?”

Now let’s say that the same company experienced a disaster and got its manual processes up and running within two hours, so it met the RTO requirement. But just because business processes are back in place, we still might have a critical problem. The company has to restore the data it lost during the disaster. It does no good to restore data that is a week old. The employees need to have access to the data that was being processed right before the disaster hit. If the company can only restore data that is a week old, then all the orders that were in some stage of being fulfilled over the last seven days could be lost. If the company makes an average of

$25,000 per day in orders and all the order data was lost for the last seven days, this can result in a loss of $175,000 and a lot of unhappy customers. So just getting things up and running (RTO) is part of the picture. Getting the necessary data in place so that business processes are up to date and relevant (RPO) is just as critical.

The actual MTD, RTO, and RPO values are derived during the BIA. The impact analysis is carried out to be able to apply criticality values to specific business functions, resources, and data types. The company must have data restoration capabilities in place to ensure that mission-critical data is never older than one minute. The company cannot rely on something as slow as backup tape restoration, but must have a high-availability data replication solution in place. The RTO value for mission-critical data processing is two minutes or less. This means that the technology that carries out the processing functionality for this type of data cannot be down for more than two minutes. The company may choose to have a cluster technology in place that will shift the load once it notices that a server goes offline.



Offsite Facilities

- Alternate Processing Facilities
  - Hot sites
  - Warm sites
  - Cold sites
  - Mobile sites
  - Reciprocal agreements

9

For larger disasters that affect the primary facility, an offsite backup facility must be accessible. Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need, and then incurs an activation fee when the facility actually has to be used. In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution, not a long-term solution.

It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company’s locale. On, and subsequent to, September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor not to sites located in New Jersey (which were already full), but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to unplanned locations.

Companies can choose from three main types of leased or rented offsite facilities:

- ***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. Some facilities, for a fee, store data backups close to the hot site. 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 of readiness. This is the most expensive of the three types of offsite facilities. It can pose 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, such as HVAC, and foundational infrastructure components, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment such as communication equipment and servers. 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. Drawbacks, however, are that much of the equipment has to be procured, delivered to, and configured at the warm site after the fact, and the annual testing available with hot-site contracts is not usually available with warm-site contracts. 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. A cold site is essentially an empty data center. 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. However, it 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, as the systems and software must be delivered, tweaked, and configured. Cold sites are often used as backups for call centers, manufacturing plants, and other services that can be moved lock, stock, and barrel in one shot.

Most companies use *warm sites,* which have some devices such as disk drives, tape drives, and controllers, but very little else. These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental. A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a *cold site* must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring.

The following provides a quick overview of the differences between offsite facilities:

Hot Site Advantages

- Ready within hours for operation
- Highly available
- Usually used for short-term solutions, but available for longer stays
- Annual testing available

Hot Site Disadvantages

- Very expensive
- Limited on hardware and software choices

Warm and Cold Site Advantages

- Less expensive
- Available for longer timeframes because of the reduced costs
- Practical for proprietary hardware or software use

Warm and Cold Site Disadvantages

- Operational testing not usually available
- Resources for operations not immediately available

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.

Reciprocal Agreements

Another approach to alternate offsite facilities is to establish a ***reciprocal agreement*** with another company, usually one in a similar field or that that has similar technological infrastructure. This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability. To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. Whether it can assist the other company while tending effectively to its own business is an open question. The stress of two companies working in the same environment could cause tremendous levels of tension. If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare. Does the other company upgrade to new technology and retire old systems and software? If not, one company's systems may become incompatible with that of the other company?

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?

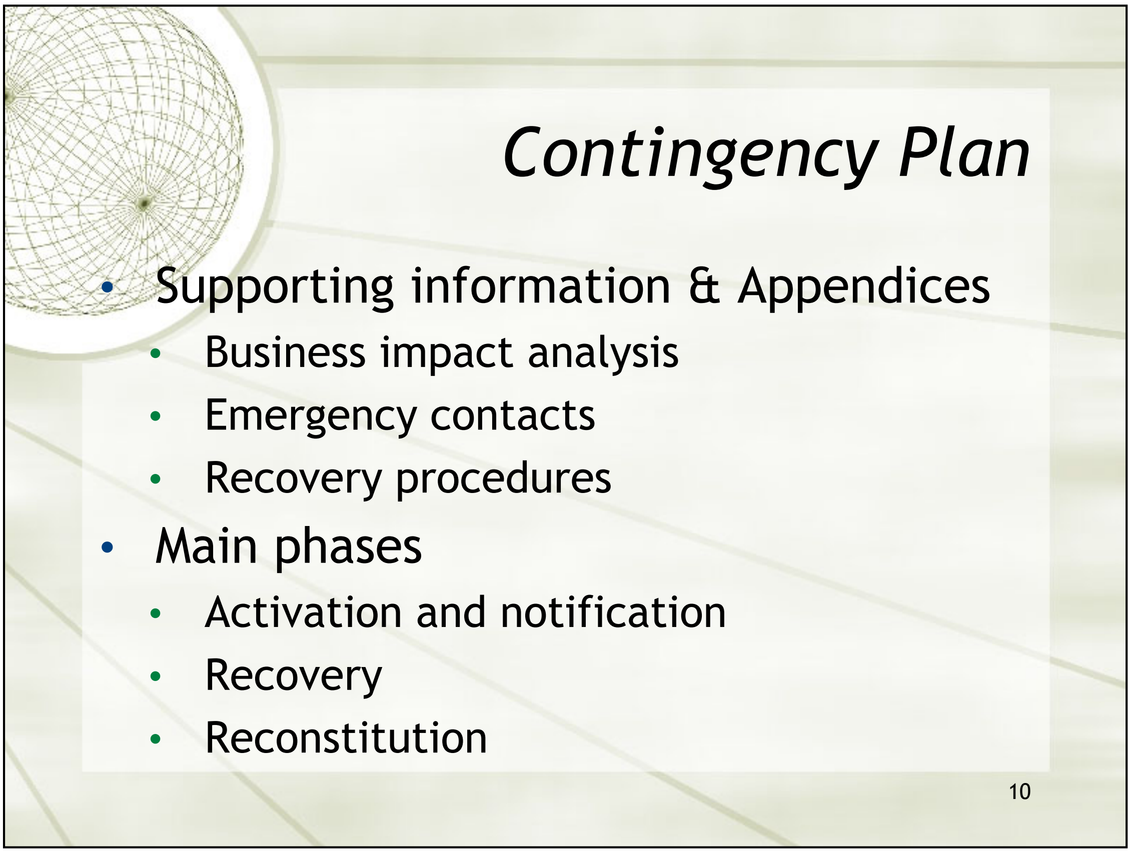
Offsite Location

When choosing a backup facility, it should be far enough away from the original site so that 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 5 miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50 to 200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Redundant Sites

Some companies choose to have ***redundant sites***, or mirrored sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment. The business-processing capabilities between the two sites can be completely synchronized. These sites are owned by the company and are mirrors of the original production environment. A redundant site has clear advantages: it has full availability, is ready to go at a moment's notice, and is under the organization's complete control. This is, however, one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site.

But expensive is relative here. If the company would lose a million dollars if it were out of business for just a few hours, the loss potential would override the cost of this option. Many organizations are subjected to regulations that dictate they must have redundant sites in place, so expense is not an issue in these situations.



Contingency Plan

- Supporting information & Appendices
  - Business impact analysis
  - Emergency contacts
  - Recovery procedures
- Main phases
  - Activation and notification
  - Recovery
  - Reconstitution

10

According to NIST SP800-34r1:

There are five main components of the information system contingency plan (ISCP). The supporting information and plan appendices provide essential information to ensure a comprehensive plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency.

Supporting information and Appendices

The supporting information component includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

This section may contain the roles and responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.

Activation and Notification Phase

The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

Activation criteria: The ISCP should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan

Notification procedures: An outage or disruption may occur with or without prior notice. For example, advance notice is often given that a hurricane is predicted to affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. Notification procedures should be documented in the plan for both types of situation. The procedures should describe the methods used to notify recovery personnel during business and non business hours. Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash. Following the outage or disruption, notification should be sent to the Outage Assessment Team so that it may determine the status of the situation and appropriate next steps. When outage assessment is complete, the appropriate recovery and system support personnel should be notified.

Outage assessment: To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption. Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation

Recovery Phase

Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.

Sequence of Recovery Activities: The sequence of activities should reflect the system's MTD to avoid significant impacts to related systems. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner. If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendices, such as equipment lists or vendor contact information, should be made in the plan where necessary. Procedures should clearly describe requirements to package, transport, and purchase materials required to recover the system.

Recovery Procedures: To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic area;
- Notifying internal and external business partners associated with the system;
- Obtaining necessary office supplies and work space;
- Obtaining and installing necessary hardware components;
- Obtaining and loading backup media;
- Restoring critical operating system and application software;
- Restoring system data to a known state;
- Testing system functionality including security controls;
- Connecting system to network or other external systems; and
- Operating alternate equipment successfully.

Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly.

Recovery Escalation and Notification: Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action. Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources. Procedures should be included to establish a clear set of events, actions and results, and should be documented for teams or individuals as appropriate.

Reconstitution Phase

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.

Validation of recovery typically includes these steps:

-*Concurrent Processing*. Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

-*Validation Data Testing*. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

-*Validation Functionality Testing*. Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

At the successful completion of the validation testing, ISCP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. The ISCP Coordinator must determine if the system has undergone significant change and will require reassessment and reauthorization.

Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

- *Notifications*. Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.
- *Cleanup.* Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.
- *Offsite Data Storage*. If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.
- *Data Backup*. As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for

future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

- *Event Documentation*. All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts.

An after-action report with lessons learned should be documented and included for updating the ISCP. Once all activities and steps have been completed and documentation has been updated, the ISCP can be formally deactivated. An announcement with the declaration should be sent to all business and technical contacts.