Maintaining Critical Services

INFO 6008 NEW Week 9 – July 02, 2019

FANSHAWE

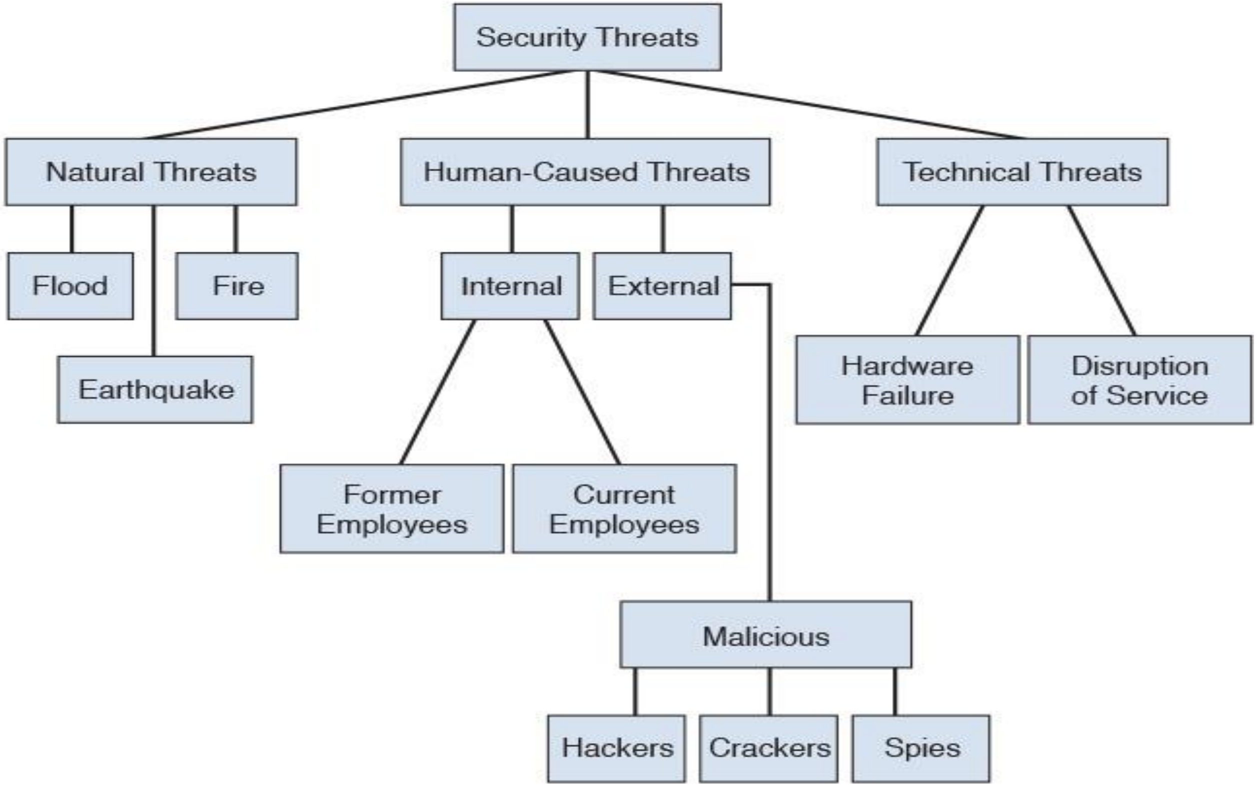
Maintaining Critical Services

- **We are covering the following topics:**
- **Threats to Business Operations:** Businesses face many threats and must have the proper controls and countermeasures to deal with them.
- **The Business Continuity Planning (BCP) Process:** One of the key activities of business continuity is the measurement of the performance of the program. Good governance presumes analysis of ongoing business processes to ensure that they are fulfilling company objectives.
- **Recovery Strategies:** Many different recovery strategies exist to deal with potential outages. An organization must choose the right one to ensure that critical activities can continue.
-

Maintaining Critical Services

- A company may not always update its plans as the company grows, changes, or modifies existing processes, even though the results of poor planning can be disastrous for the company.
- Some estimates indicate that only a small percentage of businesses are required by regulation to have a disaster recovery plan. Disaster recovery must compete for limited funds.
- Companies might be lulled into thinking that these funds might be better spent on more immediate needs. Some businesses might simply underestimate the risk and hope that adverse events don’t happen to them.
- Disaster recovery planning requires a shift of thinking from reactive to proactive.

Sources of Security Threats



Maintaining Critical Services

- There is no shortage of events that can endanger business operations. Such events can come from inside or outside the organization and are typically categorized as either human-caused, technical, or natural threats, as shown in the figure on the next slide.
- Natural threats are high on the list. In 2016, events such as Hurricane Matthew in the Caribbean, earthquakes in Ecuador, and catastrophic flooding in China topped the list. Such events highlight the need to be adequately prepared.
- Companies tend to seriously underestimate how long it would take to restore operations. In 2017, many companies were hit with ransomware because of flaws in their backup and offsite storage programs; other companies suffered because they had no workstation recovery plans for end users.

Maintaining Critical Services

- Many of us would prefer not to plan for disasters. Many see it as an unpleasant exercise or would just prefer to ignore it. Sadly, we all must deal with disasters and incidents. They are dynamic by nature.
- For example, mainframes face a different set of threats than distributed systems, just as users connected to free wireless networks face a different set of threats than those connected to wired networks inside an organization.
- This means that management must be dynamic and must be able to change with time.
- Regardless of the source of a threat, each one has the potential to cause an incident. Incident management and disaster recovery are closely related. Incidents might or might not cause disruptions to normal operations.

Maintaining Critical Services

- From the perspective of an auditor, a review of incident management should be performed to determine whether problems and incidents are **prevented, detected, analyzed, reported, and resolved in a timely manner.**
- This means the auditor should review existing incident response plans.
- The auditor also plays a critical role after an incident in that there should be a review of what worked and what did not so the plan can be optimized to be better prepared for the next incident.

- An organization needs to have a way to measure incidents and quantify their damage. The table on the next slide lists the incident classification and an auditor should have knowledge of problem and incident management practices.
- Note: disruptive incidents such as a crisis or major or minor events should be tracked and analyzed so that corrective actions can be taken to prevent these events from occurring in the future.

Incident Classification

Level	Description
Crisis	A crisis is considered a major problem. It is of sufficient impact that it adversely affects the organization’s ability to continue business functions.
Major	A major incident is of sufficient strength to negatively impact one or more departments, or it might even affect external clients.
Minor	Although these events are noticeable, they cause little or no damage.
Negligible	These detectable events cause no damage or have no longer-term effect.

THE BUSINESS CONTINUITY PLANNING (BCP) PROCESS

- The BCP process can be described as the process of creating systems of prevention and recovery to deal with potential threats to a company.
- One of the best sources of information about the BCP process is the Disaster Recovery Institute International (DRII), which you can find online at www.drii.org.
- The process that DRII defines for BCP is much broader in scope than the ISACA process. DRII breaks down the disaster recovery process into 10 domains:

THE BUSINESS CONTINUITY PLANNING (BCP) PROCESS

1. Project initiation and management
2. Risk evaluation and control
3. Business impact analysis
4. Developing business continuity management strategies
5. Emergency response and operations
6. Developing and implementing business continuity plans
7. Awareness and training programs
8. Exercising and maintaining business continuity plans
9. Crisis communications
10. Coordination with external agencies

THE BUSINESS CONTINUITY PLANNING (BCP) PROCESS

- The BCP process as defined by ISACA has a much narrower scope and focuses on the following seven steps:
- **1.** Project management and initiation
- **2.** Business impact analysis
- **3.** Development and recovery strategy
- **4.** Final plan design and implementation
- **5.** Training and awareness
- **6.** Implementation and testing
- **7.** Monitoring and maintenance

BCP - Project Management and Initiation

- Before the BCP process can begin, management must be on board.
- Management is ultimately responsible and must be actively involved in the process.
- Management sets the budget, determines the team leader, and gets the process started. The BCP team leader determines who will be on the BCP team.
- The team’s responsibilities include the following:

BCP - Project Management and Initiation

- Identifying regulatory and legal requirements
- Identifying all possible threats and risks
- Estimating the possibilities of these threats and their loss potential and ranking them based on the likelihood of the event occurring
- Performing a business impact analysis (BIA)
- Outlining which departments, systems, and processes must be up and running first
- Developing procedures and steps in resuming business after a disaster
- Assigning tasks to individuals that they should perform during a crisis situation
- Documenting, communicating with employees, and performing training and drills

BCP - Project Management and Initiation

One of the first steps the team is tasked with is meeting with senior management. The purpose of this meeting is to define goals and objectives, discuss a project schedule, and discuss the overall goals of the BCP process. This should give everyone present some idea of the scope of the final BCP policy.

It’s important for everyone involved to understand that the **BCP is the most important *corrective control*** the organization will have an opportunity to shape.

Although the BCP process is primarily corrective, it also has the following elements:

- **Preventive:** Controls to identify critical assets and develop ways to prevent outages
- **Detective:** Controls to alert the organization quickly in case of outages or problems
- **Corrective:** Controls to return to normal operations as quickly as possible

BCP - Business Impact Analysis

Chance and uncertainty are part of the world we live in. We cannot predict what tomorrow will bring or whether a disaster will occur—but this doesn't mean we cannot plan for it.

For eg. the city of Galveston, Texas, is in an area prone to hurricanes. Just because the possibility of a hurricane in winter in Galveston is extremely low doesn't mean that planning can't take place to reduce the potential negative impact of such an event actually occurring.

This is what BIA is about. Its purpose is to think through all possible disasters that could take place, assess the risk, quantify the impact, determine the loss, and develop a plan to deal with the incidents that seem most likely to occur.

BCP - Business Impact Analysis

As a result, BIA should present a clear picture of what is needed to continue operations if a disaster occurs.

The individuals responsible for BIA must look at the organization from many different angles and use information from a variety of inputs.

For a BIA to be successful, the BIA team must know what the key business processes are. Questions the team must ask when determining critical processes might include the following:

- **Does the process support health and safety?**
- **Does the loss of the process have a negative impact on income?**
- **Does the loss of the process violate legal or statutory requirements?**
- **How does the loss of the process affect users?**

BCP - Business Impact Analysis

- Performing BIA is no easy task. It requires not only knowledge of business processes but also a thorough understanding of the organization. This includes IT resources and individual business units, as well as the interrelationships between these pieces.
- This task requires the support of senior management and the cooperation of IT personnel, business unit managers, and end users. The general steps of BIA are as follows:

1. Determine data-gathering techniques.
2. Gather business impact analysis data.
3. Identify critical business functions and resources.
4. Verify completeness of data.
5. Establish recovery time for operations.
6. Define recovery alternatives and costs

BCP - Business Impact Analysis

- BIA typically includes both quantitative and qualitative components:
- ***Quantitative analysis*** **deals with numbers and dollar amounts.** It involves attempting to assign a monetary value to the elements of risk assessment and to place dollar amounts on the potential impact, including both loss of income and expenses. Quantitative impacts can include all associated costs, including these:
- Lost productivity
- Delayed or canceled orders
- Cost of repair
- Value of the damaged equipment or lost data
- Cost of rental equipment
- Cost of emergency services
- Cost to replace the equipment or reload data

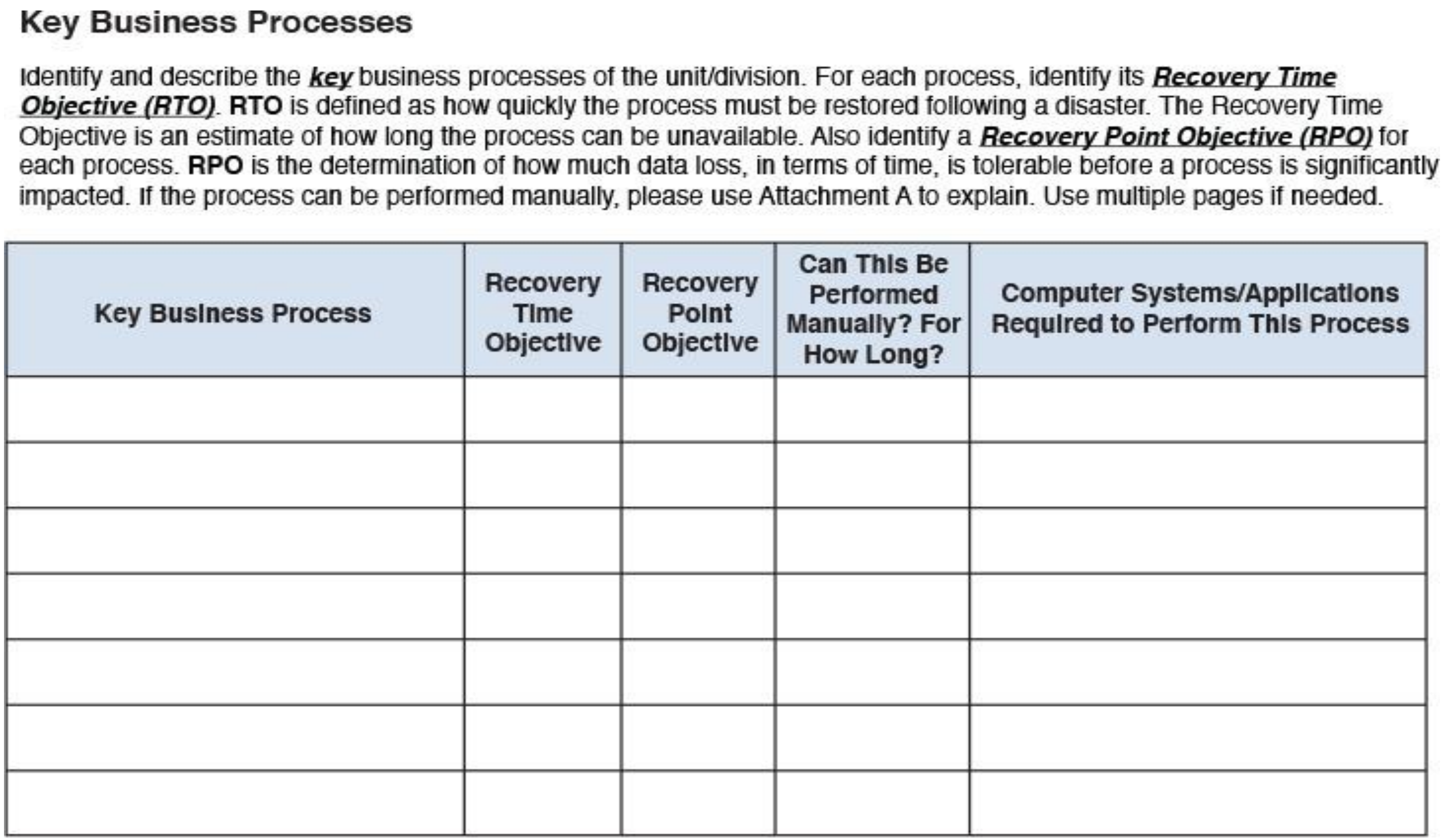
BCP - Business Impact Analysis

- BIA typically includes both quantitative and qualitative components:
- ***Quantitative analysis* deals with numbers and dollar amounts.** It involves attempting to assign a monetary value to the elements of risk assessment and to place dollar amounts on the potential impact, including both loss of income and expenses. Quantitative impacts can include all associated costs, including these:
- Lost productivity
- Delayed or canceled orders
- Cost of repair
- Value of the damaged equipment or lost data
- Cost of rental equipment
- Cost of emergency services
- Cost to replace the equipment or reload data

BCP - Business Impact Analysis

- *Qualitative assessment* is scenario driven and does not involve assigning dollar values to components of the risk analysis. A qualitative assessment ranks the seriousness of impacts into grades or classes, such as low, medium, and high. These are usually associated with items to which no dollar amount can be easily assigned:
- **Low:** Minor inconvenience; customers might not notice.
- **Medium:** Some loss of service; might result in negative press or cause customers to lose some confidence in the organization.
- **High:** Will result in loss of goodwill between the company and a client or an employee; negative press also reduces the outlook for future products and services.
- Although different approaches for calculating loss exist, one of the most popular methods of acquiring data is using a questionnaire. A team may develop a questionnaire for senior management and end users and might hand it out or use it during an interview process. This form might include items such as the recovery point objective (RPO), the recovery time objective (RTO), or even the mean time to recover (MTTR).

BCP – BIA Questionnaire



Key Business Processes

Identify and describe the ***key*** business processes of the unit/division. For each process, identify its ***Recovery Time Objective (RTO)***. **RTO** is defined as how quickly the process must be restored following a disaster. The Recovery Time Objective is an estimate of how long the process can be unavailable. Also identify a ***Recovery Point Objective (RPO)*** for each process. **RPO** is the determination of how much data loss, in terms of time, is tolerable before a process is significantly impacted. If the process can be performed manually, please use Attachment A to explain. Use multiple pages if needed.

Key Business Process	Recovery Time Objective	Recovery Point Objective	Can This Be Performed Manually? For How Long?	Computer Systems/Applications Required to Perform This Process

BCP - Business Impact Analysis

- The questionnaire can even be used in a round-table setting. This method of performing information gathering requires the BIA team to bring the required key individuals into a meeting and discuss as a group what impact specific types of disruptions would have on the organization.
- **Auditors play a key role because they might be asked to contribute information such as past transaction volumes or the impact to the business of specific systems becoming unavailable.**
- The BIA must typically determine criticality, downtime estimates, and resource requirements.
- **Criticality** can be determined by performing risk calculations such as annualized loss and its impact.
- **Downtime** estimates can be evaluated by examining the RTO. Determining the resource requirements requires an analysis of the inputs and outputs of systems.

BCP - Business Impact Analysis

- **Criticality Analysis**
- How do you classify systems and resources according to their value or order of importance? You determine the estimated loss in the event of a disruption and calculate the likelihood that the disruption will occur. The quantitative method for this process involves three steps:

1. Estimate potential losses (SLE): This step involves determining the single loss expectancy (SLE), which is calculated as follows:

- Single loss expectancy = Asset value × Exposure factor
- Items to consider when calculating the SLE include the physical destruction of human-caused events, the loss of data, and threats that might cause a delay or disruption in processing. The exposure factor is the measure or percentage of damage that a realized threat would have on a specific asset.

BCP - Business Impact Analysis

- **Criticality Analysis**

2. Conduct a threat analysis (ARO): The purpose of a threat analysis is to determine the likelihood that an unwanted event will happen. The goal is to estimate the annual rate of occurrence (ARO). Simply stated, how many times is this event expected to happen in one year?

3. Determine annual loss expectancy (ALE): This third and final step of the quantitative assessment seeks to combine the potential loss and rate/year to determine the magnitude of the risk. This is expressed as annual loss expectancy (ALE). ALE is calculated as follows:

- Annualized loss expectancy (ALE) =
- Single loss expectancy (SLE) × Annualized rate of occurrence (ARO)

BCP - Business Impact Analysis

- **Criticality Analysis**
- For example, suppose that the potential loss due to a hurricane on a business based in Tampa, Florida, is $1 million.
- An examination of previous weather patterns and historical trends reveals that there has been an average of one hurricane of serious magnitude to hit the city every 10 years, which translates to 1/10, or 0.1% per year.
- This means the assessed risk that the organization will face a serious disruption is $100,000 (= $1 million × 0.1) per year.
- That value is the annualized loss expectancy and, on average, is the amount per year that the disruption will cost the organization. Placing dollar amounts on such risks can aid senior management in determining what processes are most important and should be brought online first. Qualitatively, these items might be categorized not by dollar amount but by a risk-ranking scale.

BCP – BIA - System Classification

Classification	Description
Critical	These extremely important functions cannot be performed with duplicate systems or processes. These functions are extremely intolerant to disruptions, and any disruption is very costly.
Vital	Although these functions are important, they can be performed by a backup manual process—but not for a long period of time. These systems can tolerate disruptions for typically five days or less.
Sensitive	Although these tasks are important, they can be performed manually at a reasonable cost. However, this is inconvenient and requires additional resources or staffing.
Noncritical	These services are not critical and can be interrupted. They can be restored later with little or no negative effects.

BCP - Business Impact Analysis

- After addressing all these questions, the BCP team can start to develop recommendations and look at some potential recovery strategies.
- The BCP team should report these findings to senior management as a prioritized list of key business resources and the order in which restoration should be processed. The report should also offer potential recovery scenarios.
- Before presenting the report to senior management, however, the team should distribute it to the various department heads. These individuals were interviewed, and the plan affects them and their departments; therefore, they should be given the opportunity to review it and note any discrepancies.
- The BIA information must be correct and accurate because all future decisions will be based on those findings.
- **Interdependencies can make criticality analysis very complex. For example, you might have two assets that on their own are noncritical but in certain contexts or situations become critical!**

BCP - Development and Recovery Strategy

- At this point, the team has completed both the project initiation and BIA. Now it must determine the most cost-effective recovery mechanisms to be implemented based on the critical processes and threats determined during the BIA.
- An effective recovery strategy should apply preventive, detective, and corrective controls to meet the following objectives:
    - ❖Remove identified threats.
    - ❖Reduce the likelihood of identified risks.
    - ❖Reduce the impact of identified risks.
- The recovery strategies should specify the best way to recover systems and processes in case of interruption.
- Operations can be interrupted in several different ways:

BCP - Development and Recovery Strategy

- **Data interruptions:** Caused by the loss of data. Solutions to data interruptions include backup, offsite storage, and remote journaling.
- **Operational interruptions:** Caused by the loss of equipment. Solutions to this type of interruption include hot sites, redundant equipment, and redundant array of independent disks (RAID).
- **Facility and supply interruptions:** Caused by interruptions due to fire, loss of inventory, transportation problems, HVAC problems, and telecommunications. Solutions to this type of interruption include redundant communication and transporting systems.
- **Business interruptions:** Caused by interruptions due to loss of human resources, strikes, critical equipment, supplies, and office space. Solutions to this type of interruption include redundant sites, alternate locations, and temporary staff.

BCP - Development and Recovery Strategy

- The selection of a recovery strategy is based on several factors, including cost, criticality of the systems or process, and the time required to recover. To determine the best recovery strategy, follow these steps:

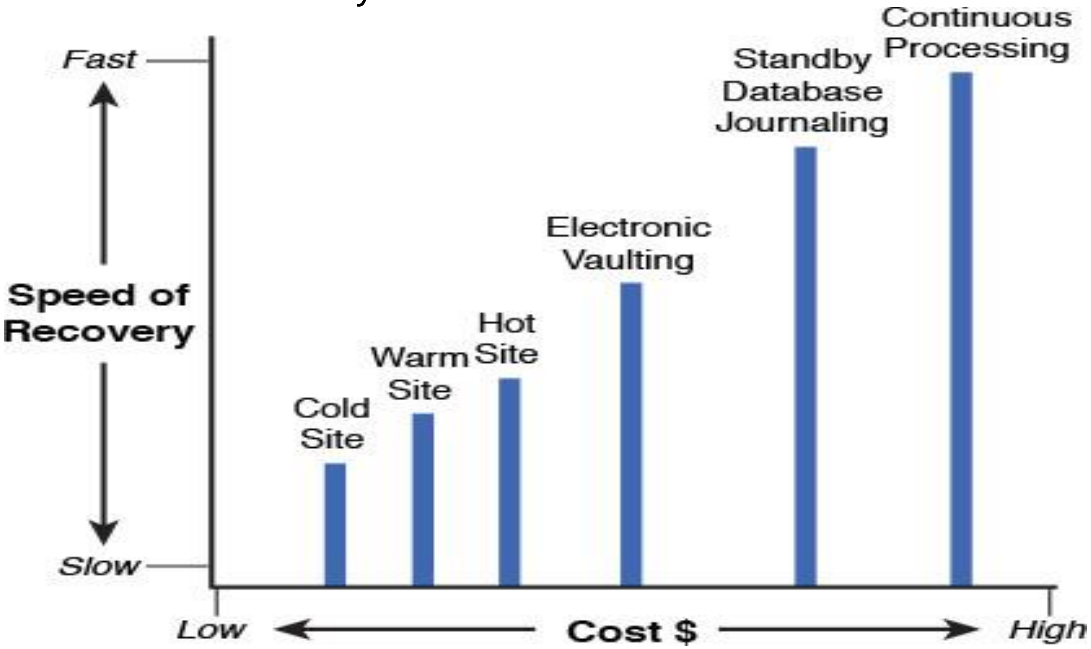
1. Document all costs for each possible alternative.
2. Obtain cost estimates for any outside services that might be needed.
3. Develop written agreements with the chosen vendor for such services.
4. Evaluate what resumption strategies are possible if there is a complete loss of the facility.
5. Document your findings and report your chosen recovery strategies to management for feedback and approval.

BCP - Development and Recovery Strategy

- Normally, any IT system that runs a mission-critical application needs a recovery strategy. There are many to choose from; the appropriate choice is based on the impact to the organization of the loss of the system or process. Recovery strategies include the following:
  - ❖Continuous processing
  - ❖Standby processing
  - ❖Standby database shadowing
  - ❖Remote data journaling
  - ❖Electronic vaulting
  - ❖Mobile site
  - ❖Hot site
  - ❖Warm site
  - ❖Cold site
  - ❖Reciprocal agreements

BCP - Development and Recovery Strategy

- The following figure gives a better idea of how each of these options compares to the cost of implementation. It is important to realize that there must be a balance between the level of service needed and the recovery method.



BCP - Final Plan Design and Implementation

- In the final plan design and implementation phase, the team prepares and documents a detailed plan for recovering critical business systems.
- This plan should be based on information gathered during the project initiation, the BIA, and the recovery strategies phase. The plan should be a guide for implementation and should address factors and variables such as:

  - ❖ Selecting critical functions and priorities for restoration
  - ❖ Determining support systems that critical functions need
  - ❖ Estimating potential disasters and calculating the minimum resources needed to recover from the catastrophe
  - ❖ Determining the procedures for declaring a disaster and under what circumstances this will occur
  - ❖ Identifying individuals responsible for each function in the plan
  - ❖ Choosing recovery strategies and determining what systems and equipment will be needed to accomplish the recovery
  - ❖ Determining who will manage the restoration and testing process
  - ❖ Calculating what type of funding and fiscal management is needed to accomplish these goals

BCP - Final Plan Design and Implementation

- In the final plan design and implementation phase, the team prepares and documents a detailed plan for recovering critical business systems.
- This plan should be based on information gathered during the project initiation, the BIA, and the recovery strategies phase. The plan should be a guide for implementation and should address factors and variables such as:
  - ❖ Selecting critical functions and priorities for restoration
  - ❖ Determining support systems that critical functions need
  - ❖ Estimating potential disasters and calculating the minimum resources needed to recover from the catastrophe
  - ❖ Determining the procedures for declaring a disaster and under what circumstances this will occur
  - ❖ Identifying individuals responsible for each function in the plan
  - ❖ Choosing recovery strategies and determining what systems and equipment will be needed to accomplish the recovery
  - ❖ Determining who will manage the restoration and testing process
  - ❖ Calculating what type of funding and fiscal management is needed to accomplish these goals

BCP - Final Plan Design and Implementation

- The plan should be written in easy-to-understand language that uses common terminology that everyone will understand.
- The plan should detail how the organization will interface with external groups such as customers, shareholders, the media, and community, region, and state emergency services groups during a disaster.
- Important teams should be formed so that training can be performed.
- The final step of the phase is to combine all this information into the business continuity plan and then interface it with the organization’s other emergency plans.

Note

- **Copies of the business continuity plan should be kept both onsite and offsite**.

BCP - Training and Awareness

- The goal of training and awareness is to make sure all employees know what to do in case of an emergency.
- Employees need to know where to call or how to maintain contact with the organization if a disaster occurs.
- Therefore, the organization should design and develop training programs to make sure each employee knows what to do and how to do it.
- Training can include a range of specific programs, such as CPR, fire drills, crisis management, and emergency procedures.
- Employees assigned to specific tasks should be trained to carry out needed procedures. Cross-training of team members should occur, if possible, so that team members are familiar with a variety of recovery roles and responsibilities.
- **Know that the number-one priority of any business continuity plan or disaster recovery plan is to protect the safety of employees.**

BCP - Process Responsibilities

Person or Department	Responsibility
Senior management	Project initiation, ultimate responsibility, overall approval and support
Middle management or business unit managers	Identification and prioritization of critical systems
BCP committee and team members	Planning, day-to-day management, implementation, and testing of the plan
Functional business units	Plan implementation, incorporation, and testing
IT audit	Business continuity plan review, test results evaluation, offsite storage facilities, alternate processing contracts, and insurance coverage

BCP - Implementation and Testing

- During the implementation and testing phase, the BCP team ensures that the previously agreed-upon steps are implemented.
- No demonstrated recovery exists until a plan has been tested. Before examining the ways in which the testing can occur, look at some of the teams that are involved in the process:
- **Incident response team:** Team developed as a central clearinghouse for all incidents.
- **Emergency response team:** The first responders for the organization. They are tasked with evacuating personnel and saving lives.
- **Emergency management team:** Executives and line managers who are financially and legally responsible. They must also handle the media and public relations.
- **Damage assessment team:** The estimators. They must determine the damage and estimate the recovery time.

BCP - Implementation and Testing

- **Salvage team:** Those responsible for reconstructing damaged facilities. This includes cleaning up, recovering assets, creating documentation for insurance filings or legal actions, and restoring paper documents and electronic media.
- **Communications team:** Those responsible for installing communications (data, voice, phone, fax, radio) at the recovery site.
- **Security team:** Those who manage the security of the organization during a time of crisis. They must maintain order after a disaster.
- **Emergency operations team:** Individuals who reside at the alternative site and manage systems operations. They are primarily operators and supervisors who are familiar with system operations.
- **Transportation team:** Those responsible for notifying employees that a disaster has occurred. They are also in charge of providing transportation, scheduling, and lodging for those who will be needed at the alternative site.

BCP - Implementation and Testing

- **Coordination team:** Those tasked with managing operations at different remote sites and coordinating the recovery efforts.
- **Finance team:** Individuals who provide budgetary control for recovery and accurate accounting of costs.
- **Administrative support team:** Individuals who provide administrative support and also handle payroll functions and accounting.
- **Supplies team:** Individuals who coordinate with key vendors to maintain needed supplies.
- **Relocation team:** Those in charge of managing the process of moving from the alternative site to the restored original location.
- **Recovery test team:** Individuals deployed to test the business continuity plan/disaster recovery plan and determine their effectiveness.

BCP - Implementation and Testing

- The last team – the Recovery Team consists of individuals who test the business continuity plan; this should be done at least once a year.
- Testing helps bring theoretical plans into reality. To build confidence, the BCP team should start with easier parts of the plan and build to more complex items.
- The initial tests should focus on items that support core processing and should be scheduled during a time that causes minimal disruption to normal business operations.
- Tests should be observed by an auditor who can witness the process and record accurate test times. Having an auditor is not the only requirement: Key individuals who would be responsible in a real disaster must play a role in the testing process.

BCP - Implementation and Testing

- Testing methods vary among organizations and range from simple to complex. Regardless of the method or types of testing performed, the idea is to learn from the practice and improve the process each time a problem is discovered.
- The three different types of BCP testing, as defined by the ISACA:

1. Paper tests
2. Preparedness tests
3. Full operation tests

BCP - Implementation and Testing
Paper Tests

- The most basic method of BCP testing is the *paper test*. Although it is not considered a replacement for a full interruption or parallel test, it is a good start.
- A paper test is an exercise that can be performed by sending copies of the plan to different department managers and business unit managers for review. Each of these individuals can review the plan to make sure nothing has been overlooked and that everything that is being asked of them is possible.
- A paper test can also be performed by having the members of the team come together and discuss the business continuity plan. This is sometimes known as *walk-through testing*.

BCP - Implementation and Testing
Paper Tests

- The plans are laid out across the table so that attendees have a chance to see how an actual emergency would be handled.
- By reviewing the plan in this way, some errors or problems should become apparent.
- With either method—sending the plan around or meeting to review the plan—the next step is usually a **preparedness test**.

BCP - Implementation and Testing Preparedness Tests

- A *preparedness test* is a simulation in which team members go through an exercise that re-enacts an actual outage or disaster.
- This type of test is typically used to test a portion of the plan. The preparedness test consumes time and money because it is an actual test that measures the team’s response to situations that might someday occur.
- This type of testing provides a means of incrementally improving the plan.

BCP - Implementation and Testing Preparedness Tests

- During preparedness tests, team leaders might want to use the term *exercise* because the term *test* denotes passing or failing, which can add pressure on team members and can be detrimental to the goals of continual improvement.
- For example, during one disaster recovery test, the backup media was to be returned from the offsite location to the primary site. When the truck arrived with the media, it was discovered that the tapes had not been properly secured, and they were scattered around the bed of the truck. Even though the test could not continue, it was not a failure because it uncovered a weakness in the existing procedure.

BCP - Implementation and Testing
Full Operation Tests

- The *full operation test* is as close to an actual service disruption as you can get.
- The team should have performed paper tests and preparedness tests before attempting this level of interruption.
- This test is the most detailed, time-consuming, and thorough of all the tests discussed.
- **A full interruption test mimics a real disaster**, and all steps are performed to start up backup operations.
- It involves all the individuals who would be involved in a real emergency, including internal and external organizations.

BCP - Implementation and Testing
Full Operation Tests

- Goals of a full operation test include the following:
- Verifying the business continuity plan
- Evaluating the level of preparedness of the personnel involved
- Measuring the capability of the backup site to operate as planned
- Assessing the ability to retrieve vital records and information
- Evaluating the functionality of equipment
- Measuring overall preparedness for an actual disaster

The disaster recovery and continuity plan should be *tested at least once yearly*. Environments change; each time the plan is tested, more improvements might be uncovered.

BCP - Monitoring and Maintenance

- When the testing process is complete, individuals tend to feel that their job is done. If someone is not made responsible for this process, the best plans in the world can start to become outdated in six months or less.
- Don’t be surprised to find out that no one really wants to take on the task of documenting procedures and processes.
- The responsibility of performing periodic tests and maintaining the plan should be assigned to a specific person.
- While you might normally think of change-management practices being used to determine whether changes made to systems and applications are adequately controlled and documented, these same techniques should be used to address issues that might affect the business continuity plan.

BCP - Monitoring and Maintenance

- A few additional items must be done to finish the business continuity plan.
- The primary remaining item is to put controls in place to maintain the current level of business continuity and disaster recovery.
- This is best accomplished by implementing change-management procedures.
- If changes to the approved plans are required, you will then have a documented structured way to accomplish this.
- A centralized command and control structure will ease this burden.
- **Life is not static, and the organization’s business continuity plans shouldn’t be either.**

BCP - Understanding BCP Metrics

- Reviewing the results of the information obtained is the next step of the BIA process. During this step, the BIA team should ask questions such as these:
- **Are the systems identified critical?** All departments like to think of themselves as critical, but that is usually not the case. Some departments can be offline longer than others.
- **What is the required recovery time for critical resources?** If the resource is critical, costs will mount the longer the resource is offline. Depending on the service and the time of interruption, these times will vary.

BCP - Understanding BCP Metrics

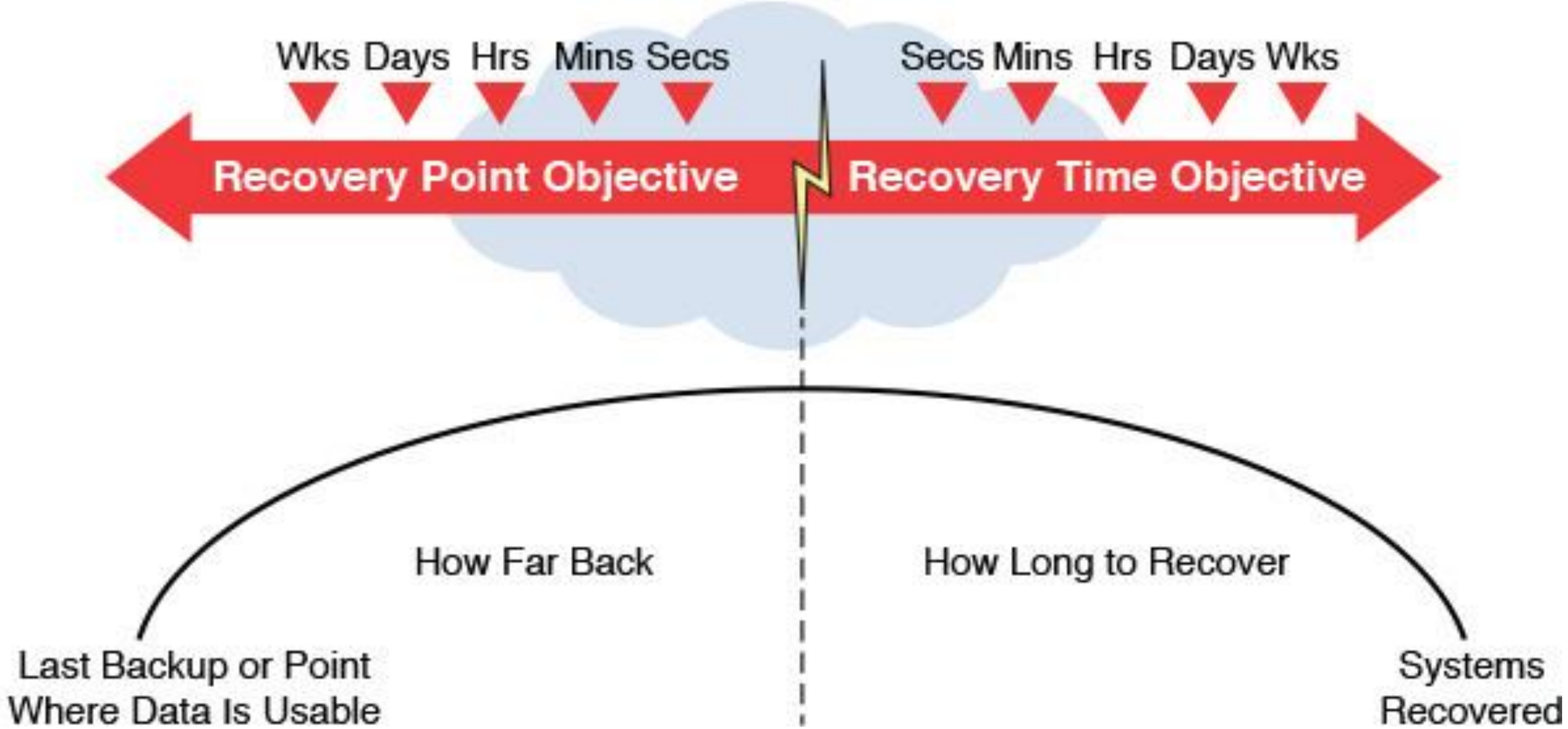
- All this information is needed because at the core of the BIA are two critical items:
- **Recovery point objective (RPO):** The RPO defines how current the data must be or how much data an organization can afford to lose. The greater the RPO, the more tolerant the process is to interruption.
- **Recovery time objective (RTO):** The RTO specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored.

BCP - Understanding BCP Metrics

- The lower the time requirements are, the higher the cost will be to reduce loss or restore the system as quickly as possible.
- For example, most banks have a very low RPO because they cannot afford to lose any processed information.
- Think of the recovery strategy calculations as being designed to meet the required recovery time frames:
- Maximum tolerable downtime (MTD) = RTO + Work recovery time (WRT). (The WRT is the remainder of the MTD used to restore all business operations.)
- The following figure represents an overview of how RPO and RTO are related.

BCP – RPO vs RTO

The RTO specifies the maximum elapsed time to recover an application at an alternate site. The greater the RTO, the longer the process can take to be restored



BCP - Understanding BCP Metrics

- These items must be considered in addition to RTO and RPO:
- **Maximum acceptable outage:** This value is the time that systems can be offline before causing damage. This value is required in creating RTOs and is also known as maximum tolerable downtime (MTD).
- **Work recovery time (WRT):** The WRT is the time it takes to get critical business functions back up and running once the systems are restored.
- **Service delivery objective (SDO):** This defines the level of service provided by alternate processes while primary processing is offline. This value should be determined by examining the minimum business need.

BCP - Understanding BCP Metrics

- **Maximum tolerable outages:** This is the maximum amount of time the organization can provide services at the alternate site. This value can be determined using contractual values.
- **Core processes:** These activities are specifically required for critical processes and produce revenue.
- **Supporting processes:** These activities are required to support the minimum services needed to generate revenue.
- **Discretionary processes:** These include all other processes that are not part of the core or supporting processes and that are not required for any critical processes or functions.

BCP - RECOVERY STRATEGIES

- Recovery alternatives are the choices an organization has for restoring critical systems and the data in those systems. Recovery strategies can include the following:
- Alternate processing sites
- Hardware recovery
- Software and data recovery
- Backup and restoration
- Telecommunications recovery

BCP - RECOVERY STRATEGIES

- The goal is to create a recovery strategy that balances the cost of downtime, the criticality of the system, and the likelihood of occurrence.
- As an example, if you have an RTO of less than 12 hours and the resource you are trying to recover is a mainframe computer, a cold-site facility would never work—because you can't buy a mainframe, install it, and get the cold site up and running in less than 12 hours.
- Therefore, although cost is important, so are criticality and the time to recover. The total outage time that the organization can endure is referred to as *maximum tolerable downtime* (MTD).
- The table on the next slide shows some MTDs used by many organizations:

BCP - Required Recovery Times

Item	Required Recovery Time
Critical	Minutes to hours
Urgent	24 hours
Important	72 hours
Normal	7 days
Nonessential	30 days

BCP - Alternate Processing Sites

- For disasters that have the potential to affect the primary facility, plans must be made for a backup process or an alternate site.
- Some organizations might opt for a *redundant processing site*. Redundant sites are equipped and configured just like the primary site. They are owned by the organization, and their cost is high.
- After all, the company must spend a large amount of funds to build and equip a complete, duplicate site. Although the cost might seem high, it must be noted that organizations that choose this option have done so because they have a very short (if any) RPO.

BCP - Alternate Processing Sites

- A loss of services for even a very short period of time would cost the organization millions.
- The organization might also be subject to regulations that require it to maintain redundant processing.
- Before choosing a location for a redundant site, it must be verified that the site is not subject to the same types of disasters as the primary site.
- Regular testing is also important to verify that the redundant site still meets the organization’s needs and that it can handle the workload to meet minimum processing requirements.

BCP - Alternate Processing Options

- *Mobile sites* are another processing alternative. Mobile sites are usually tractor-trailer rigs that have been converted into data-processing centers. They contain all the necessary equipment and can be transported to a business location quickly.
- They can be chained together to provide space for data processing and can provide communication capabilities. Used by the military and large insurance agencies, mobile sites are a good choice in areas where no recovery facilities exist.
- Another type of recovery alternative is *subscription services,* such as hot sites, warm sites, and cold sites.

BCP - Alternate Processing Options

- A *hot site* facility is ready to go. It is fully configured and equipped with the same system as the production network. It can be made operational within just a few hours.
- A hot site merely needs staff, data files, and procedural documentation. Hot sites are a high-cost recovery option, but they can be justified when a short recovery time is required.
- Because a hot site is typically a subscription-based service, a range of fees is associated with it, including a monthly cost, subscription fees, testing costs, and usage or activation fees.

BCP - Alternate Processing Options

- Contracts for hot sites need to be closely examined; some might charge extremely high activation fees to prevent users from utilizing the facility for anything less than a true disaster.
- Regardless of what fees are involved, the hot site needs to be periodically tested.
- Tests should evaluate processing abilities as well as security. The physical security of a hot site should be at the same level or greater than the physical security at the primary site.
- Finally, it is important to remember that the hot site is intended for short-term use only. With a subscriber service, other companies might be competing for the same resource. The organization should have a plan to recover primary services quickly or move to a secondary location.
- Hot sites should not be externally identifiable to decrease the risk of sabotage and other potential disruptions.

BCP - Examples of Functions and Recovery Times

Process	Recovery Time
Database	15 minutes to 1 hour
Applications	12–24 hours
Help desk	24–48 hours
Purchasing	24–48 hours
Payroll	1–3 days
Asset inventory	5–7 days
Nonessential services	30 days
Emergency services (for example, for companies that need to set up operations quickly in areas that have been hit by disasters, such as insurance companies, governmental agencies, military, and so on)	Hours to a few days

BCP - Alternate Processing Options

- ***With reciprocal agreements***, two organizations pledge assistance to one another in the event of a disaster.
- These agreements are carried out by sharing space, computer facilities, and technology resources. On paper, this appears to be a cost-effective solution because the primary advantage is its low cost. However, reciprocal agreements have drawbacks and are infrequently used.
- The parties to such an agreement must trust each other to aid in the event of a disaster. However, the nonvictim might be hesitant to follow through if such a disaster occurs, based on concerns such as the realization that the damaged party might want to remain on location for a long period of time or that the victim company's presence will degrade the helping company's network services.

BCP - Alternate Processing Options

- Even concerns about the loss of competitive advantage can drive this hesitation.
- The issue of confidentiality also arises: The damaged organization is placed in a vulnerable position and must entrust the other party with confidential information.
- Finally, if the parties to the agreement are near each other, there is always the danger that disaster could strike both parties and thereby render the agreement useless.
- The legal departments of both firms need to look closely at such an agreement. ISACA recommends that organizations considering reciprocal agreements address the following concerns before entering into them:

BCP - Alternate Processing Options

  - ❖What amount of time will be available at the host computer site?
  - ❖Will the host site’s employees be available for help?
  - ❖What specific facilities and equipment will be available?
  - ❖How long can emergency operations continue at the host site?
  - ❖How frequently can tests be scheduled at the host site?
  - ❖What type of physical security is available at the host site?
  - ❖What type of logical security is available at the host site?
  - ❖Is advance notice required for using the site? If so, how much?
  - ❖Are there any blocks of time or dates when the facility is not available?
- Although reciprocal agreements are not usually appropriate for organizations with large databases, some organizations, such as small banks, have been known to sign reciprocal agreements for the use of a shared hot site.

BCP - Alternate Processing Options

- When reviewing alternative processing options, subscribers should look closely at any agreements and at the actual facility to make sure it meets the needs of the organization.
- One common problem is oversubscription. If situations such as Hurricane Harvey occur, there could be more organizations demanding a subscription service than the vendor can supply.
- The subscription agreement might also dictate when the organization may inhabit the facility.
- Thus, even though an organization might be in the path of a deadly storm, it might not be able to move into the facility yet because the area has not been declared a disaster area.

BCP - Alternate Processing Options

- Procedures and documentation should also be kept at the offsite location, and backups must be available.
- It’s important to note that backup media should be kept in an area that is not subject to the same type of natural disaster as the primary site.
- For example, if the primary site is in a hurricane zone, the backup needs to be somewhere less prone to those conditions. If backup media is at another location, agreements should be in place to ensure that the media will be moved to the alternate site so it is available for the recovery process.
- **A final item is that organizations must also have prior financial arrangements to procure needed equipment, software, and supplies during a disaster.** This might include emergency credit lines, credit cards, or agreements with hardware and software vendors.

BCP – Hardware Recovery

- Recovery alternatives are just one of the items that must be considered to cope with a disaster. Hardware recovery is another.
- Remember that an effective recovery strategy involves more than just corrective measures; it is also about prevention.
- Hardware failures are some of the most common disruptions that can occur. It is therefore important to examine ways to minimize the likelihood of occurrence and to reduce the effect if it does occur.
- This process can be enhanced by making well-informed decisions when buying equipment.
- At purchase time, you should know three important items associated with the reliability:

BCP – Hardware Recovery

- **Mean time between failures (MTBF):** The MTBF calculates the expected lifetime of a device that can be repaired. A higher MTBF means the equipment should last longer.
- **Mean time to failure (MTTF):** The MTTF calculates the expected lifetime of a one-time-use item that is typically not repaired.
- **Mean time to repair (MTTR):** The MTTR estimates how long it would take to repair the equipment and get it back into use. For MTTR, lower numbers mean the equipment takes less time to repair and can be returned to service sooner.
- For critical equipment, an organization might consider some form of service level management. This is simply an agreement between an IT service provider and a customer.

BCP – Hardware Recovery

- The most common example is a *service level agreement* (*SLA*), which is a contract with a hardware vendor that provides a certain level of protection. For a fee, the vendor agrees to repair or replace the equipment within the contracted time.
- **Fault tolerance** can be used at the server level or the drive level.
- At the server level is *clustering*, technology that groups several servers together yet allows them to be viewed logically as a single server. Users see the cluster as one unit, although it is actually many.
- The advantage is that if one server in the cluster fails, the remaining active servers will pick up the load and continue operation.

Redundant Array of Independent Disks

- **Fault tolerance on the drive level** is achieved primarily with *redundant array of independent disks (RAID)*, which is used for hardware fault tolerance and/or performance improvements and is achieved by breaking up the data and writing it to multiple disks.
- RAID has humble beginnings that date back to the 1980s at the University of California.
- To applications and other devices, RAID appears as a single drive. Most RAID systems have *hot-swappable disks*, which means the drives can be removed or added while the computer systems are running.
- If a RAID system uses parity and is fault tolerant, the parity date is used to rebuild the newly replaced drive. RAID used today:

Redundant Array of Independent Disks

- Another RAID technique is *striping*, which means the data is divided and written over several drives.
- Although write performance remains almost constant, read performance drastically increases.
- According to ISACA, these are the most common levels of RAID used today:

❖ RAID 0

❖ RAID 3

❖ RAID 5

Redundant Array of Independent Disks

- **RAID 0: Striped disk array without fault tolerance:** Provides data striping and improves performance **but provides no redundancy**.
- **RAID 1: Mirroring and duplexing:** Duplicates the information on one disk to another. It provides twice the read transaction rate of single disks and the same write transaction rate as single disks yet effectively cuts disk space in half.
- **RAID 2: Error-correcting coding:** *Rarely used* because of the extensive computing resources needed. It stripes data at the bit level instead of the block level.
- **RAID 3: Parallel transfer with parity:** Uses byte-level striping with a dedicated disk. Although it provides fault tolerance, it is rarely used.

Redundant Array of Independent Disks

- **RAID 4: Shared parity drive:** Similar to RAID 3 but provides block-level striping with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. Its primary disadvantage is that the parity disk can create write bottlenecks.
- **RAID 5: Block interleaved distributed parity:** Provides data striping of both data and parity. Level 5 has good performance and fault tolerance. It is a popular implementation of RAID. It requires at least three drives.
- **RAID 6: Independent data disks with double parity:** Provides high fault tolerance with block-level striping and parity data distributed across all disks.
- **RAID 10: A stripe of mirrors:** Known to have very high reliability. It requires a minimum of four drives.

Redundant Array of Independent Disks

- **RAID 0+1: A mirror of stripes:** Not one of the original RAID levels. RAID 0+1 uses RAID 0 to stripe data and creates a RAID 1 mirror. It provides high data rates.
- **RAID 15:** Creates mirrors (RAID 1) and distributed parity (RAID 5). This is not one of the original RAID levels.
- One final drive-level solution worth mentioning is *just a bunch of disks (JBOD).* JBOD is similar to RAID 0 but offers few of the advantages. What it does offer is the capability to combine two or more disks of various sizes into one large partition. It also has an advantage over RAID 0: In case of drive failure, only the data on the affected drive is lost; the data on surviving drives remains readable.
- This means that **JBOD has no fault tolerance**. JBOD does not provide the performance benefits associated with RAID 0.

Software and Data Recovery

- Because data processing is essential to most organizations, having the software and data needed to continue this operation is critical to the recovery process.
- The objectives are to back up critical software and data and be able to restore them quickly. Policy should dictate when backups are performed, where the media is stored, who has access to the media, and what its reuse or rotation policy is.
- Backup media can include tape reels, tape cartridges, removable hard drives, disks, and cassettes. The organization must determine how often backups should be performed and what type of backup should be performed.

Software and Data Recovery

- These operations will vary depending on the cost of the media, the speed of the restoration needed, and the time allocated for backups. Typically, the following **four** backup methods are used:
- **Full backup**: All data is backed up. No data files are skipped or bypassed. All items are copied to one tape, set of tapes, or backup medium. If restoration is needed, only one tape or set of tapes is needed. A full backup requires the most time and space on the storage medium but takes the least time to restore.
- **Differential backup**: A full backup is done typically once a week, and a daily differential backup is done only to those files that have changed since the last full backup. If you need to restore, you need the last full backup and the most recent differential backup. This method takes less time per backup but takes longer to restore because both the full and differential backups are needed.

Software and Data Recovery

- **Incremental backup**: This method backs up only those files that have been modified since the previous incremental backup. An incremental backup requires additional backup media because the last full backup, the last incremental backup, and any additional incremental backups are required to restore the media.
- **Continuous backup:** Some backup applications perform a *continuous backup* that keeps a database of backup information. These systems are useful because if a restoration is needed, the application can provide a full restore, a point-in-time restore, or a restore based on a selected list of files.

Software and Data Recovery

- Tape continues to be a viable option for backup. One current backup format is linear tape-open (LTO). LTO provides high-capacity storage, and in its latest iteration, LTO-6, it offers 2.5TB of storage per tape cartridge. If compression is used an enterprise can store up to 6.25TB of data on a single tape. That said 96% or more of today’s backups are incremental backups – and incremental backups are fundamentally incompatible with modern tape drives.
- Although tape and optical systems still have significant market share for backup systems, hardware alternatives and cloud based options are making inroads. One of these technologies is massive array of inactive disks (MAID).

Software and Data Recovery

- MAID offers a hardware storage option for the storage of data and applications. It was designed to reduce the operational costs and improve long-term reliability of disk-based archives and backups.
- MAID is similar to RAID, except that it provides power management and advanced disk monitoring. The MAID system powers down inactive drives, reduces heat output, reduces electrical consumption, and increases the drive’s life expectancy. This represents real progress over using hard disks to back up data.
- Storage area networks (SANs) are another alternative. SANs are designed as a subnetwork of high-speed, shared storage devices.
- Cloud backup is gaining in popularity as it offers several benefits. These value-added functions include geographical redundancy, advanced search, content management and automatic offsite storage.

Software and Data Recovery

- The reality is that in order to provide recovery of every data set, system, and application, in the face of each possible disaster from which you wish to protect your enterprise, you’re going to need a hybrid mix of on-premise and cloud-based storage and recovery options.
- Putting the cloud up on a high pedestal is probably warranted with the capabilities available today in backup and recovery. But don’t count out on-premises; it has a place in your protection strategy, ensuring your enterprise always has the best coverage possible.

Backup and Restoration

- Where backup media are stored can have a big impact on how quickly data can be restored and brought back online.
- The media should be stored in more than one physical location to reduce the possibility of loss.
- A tape librarian should manage these remote sites by maintaining the site, controlling access, rotating media, and protecting this valuable asset. Unauthorized access to the media is a huge risk because it could impact the organization’s ability to provide uninterrupted service.
- Encryption can help mitigate this risk.
- Transportation to and from the remote site is also an important concern. Consider the following important items:
- Secure transportation to and from the site must be maintained.

Backup and Restoration

- Delivery vehicles must be bonded.
- Backup media must be handled, loaded, and unloaded in an appropriate way.
- Drivers must be trained on the proper procedures to pick up, handle, and deliver backup media.
- Access to the backup facility should be 24×7 in case of emergency.
- *Offsite storage* should be contracted with a known firm that has control of the facility and is responsible for its maintenance.
- Physical and environmental controls should be equal to or better than those of the organization’s facility.
- A letter of agreement should specify who has access to the media and who is authorized to drop off or pick up media.

Backup and Restoration

- There should also be an agreement on response time that is to be met in times of disaster.
- *Onsite storage* should be maintained to ensure the capability to recover critical files quickly.
- Backup media should be secured and kept in an environmentally controlled facility that has physical control sufficient to protect such a critical asset.
- This area should be fireproof, with controlled access so that anyone depositing or removing media is logged.
- Although most backup media is rather robust, it will not last forever and will fail over time. This means tape rotation is another important part of backup and restoration.
- Backup media must be periodically tested. Backups will be of little use if they malfunction during a disaster. Common media-rotation strategies include the following:

Backup and Restoration

- **Simple**: A simple backup rotation scheme is to use one tape for every day of the week and then repeat the next week. One tape can be for Mondays, one for Tuesdays, and so on. You would add a set of new tapes each month and then archive the monthly sets. After a predetermined number of months, you would put the oldest tapes back into use.
- **Grandfather-father-son**: This rotation method includes four tapes for weekly backups, one tape for monthly backups, and four tapes for daily backups. It is called *grandfather-father-son* because the scheme establishes a kind of hierarchy. Grandfathers are the one monthly backup, fathers are the four weekly backups, and sons are the four daily backups.

Backup and Restoration

- **Tower of Hanoi:** This tape-rotation scheme is named after a mathematical puzzle. It involves using five sets of tapes, each set labeled A through E. Set A is used every other day; set B is used on the first non-A backup day and is used every fourth day; set C is used on the first non-A or non-B backup day and is used every eighth day; set D is used on the first non-A, non-B, or non-C day and is used every 16th day; and set E alternates with set D.
- An organization’s backups are a complete mirror of the organization’s data. Although most backups are password protected, this really offers only limited protection.
- If attackers have possession of the backup media, they are not under any time constraints and have ample time to crack passwords and access the data. Encryption can offer an additional layer of protection and help protect the confidentiality of the data.

Backup and Restoration

- **Tower of Hanoi:** This tape-rotation scheme is named after a mathematical puzzle. It involves using five sets of tapes, each set labeled A through E. Set A is used every other day; set B is used on the first non-A backup day and is used every fourth day; set C is used on the first non-A or non-B backup day and is used every eighth day; set D is used on the first non-A, non-B, or non-C day and is used every 16th day; and set E alternates with set D.
- An organization’s backups are a complete mirror of the organization’s data. Although most backups are password protected, this really offers only limited protection.
- If attackers have possession of the backup media, they are not under any time constraints and have ample time to crack passwords and access the data. Encryption can offer an additional layer of protection and help protect the confidentiality of the data.

Backup and Restoration

- Storage Area Networks (SANs) are an alternative to traditional backup.
- SANs support disk mirroring, backup and restore, archival and retrieval of archived data, and data migration from one storage device to another. SANs can be implemented locally or can use storage at a redundant facility.
- Another option is a *virtual SAN*(*VSAN*), a SAN that offers isolation among devices that are physically connected to the same SAN fabric. A VSAN is sometimes called *fabric virtualization*.

Backup and Restoration

- Traditionally, SANs used Small Computer System Interface (SCSI) for connectivity, but there are more current options in use today. One is iSCSI, which is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate.
- Fiber Channel over Ethernet (FCoE) is another SAN interface standard. FCoE is similar to iSCSI; it can operate at speeds of 10Gbps and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is nonroutable.
- One important issue with SAN and backups is location redundancy. This is the concept that content should be accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.

Backup and Restoration

- Another important item is security of the backups. This is where secure storage management and replication are important. The idea is that systems must be designed to allow a company to manage and handle all corporate data in a secure manner, with a focus on the confidentiality, integrity, and availability of the information. The replication service allows for the data to be duplicated in real time so that additional fault tolerance is achieved.
- When you need to make point-in-time backups, you can use SAN snapshots. SAN snapshot software is typically sold with a SAN solution and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to physical disk and make a point-in-time backup copy.

Backup and Restoration

- If budget is an issue, an organization can opt for ***electronic vaulting*****,** which involves transferring data by electronic means to a backup site, as opposed to physical shipment.
- With electronic vaulting, an organization contracts with a vaulting provider. The organization typically loads a software agent onto systems to be backed up, and the vaulting service accesses these systems and copies the selected files. Moving large amounts of data can slow WAN service.
- Another backup alternative is *standby database shadowing*. A standby database is an exact duplicate of a database maintained on a remote server. In case of disaster, it is ready to go. Changes are applied from the primary database to the standby database to keep records synchronized.

Backup and Restoration

- As an alternative to traditional backup techniques, using cloud services for backup may offer a cost-saving alternative. These services should be carefully evaluated, as there are many concerns when using them. Cloud backups can be deployed in a variety of configurations—for example, as an on-premises private cloud or as an offsite public or private cloud.

Telecommunications Recovery

- Telecommunications recovery should play a key role in recovery. After all, the telecommunications network is a critical asset and should be given a high priority for recovery.
- Although these communications networks can be susceptible to the same threats as data centers, they also face some unique threats.
- Protection methods include redundant WAN links and bandwidth on demand.
- Whatever the choice, the organization should verify capacity requirements and acceptable outage times.
- The following are the primary methods for telecommunications network protection:

Telecommunications Recovery

- **Redundancy**: This involves exceeding what is required or needed. Redundancy can be added by providing extra capacity, providing multiple routes, using dynamic routing protocols, and using failover devices to allow for continued operations.
- **Diverse routing**: This is the practice of routing traffic through different cable facilities. Organizations can obtain both diverse routing and alternate routing, but the cost is not low. Most of these systems use facilities that are buried, and they usually emerge through the basement and can sometimes share space with other mechanical equipment. This adds risk. Many cities have aging infrastructures, which is another potential point of failure.

Telecommunications Recovery

- **Alternate routing**: This is the ability to use another transmission line if the regular line is busy or unavailable. This can include using a dial-up connection in place of a dedicated connection, a cell phone instead of a land line, or microwave communication in place of a fiber connection.
- **Long-haul diversity**: This is the practice of having different long-distance communication carriers. This recovery facility option helps ensure that service is maintained; auditors should verify that it is present.
- **Last-mile protection**: This is a good choice for recovery facilities in that it provides a second local loop connection and can add to security even more if an alternate carrier is used.
- **Voice communication recovery:** Many organizations are highly dependent on voice communications. Some of these organizations have started making the switch to VoIP because of the cost savings. Some land lines should be maintained to provide recovery capability.

Telecommunications Recovery

- **Alternate routing**: This is the ability to use another transmission line if the regular line is busy or unavailable. This can include using a dial-up connection in place of a dedicated connection, a cell phone instead of a land line, or microwave communication in place of a fiber connection.
- **Long-haul diversity**: This is the practice of having different long-distance communication carriers. This recovery facility option helps ensure that service is maintained; auditors should verify that it is present.
- **Last-mile protection**: This is a good choice for recovery facilities in that it provides a second local loop connection and can add to security even more if an alternate carrier is used.
- **Voice communication recovery:** Many organizations are highly dependent on voice communications. Some of these organizations have started making the switch to VoIP because of the cost savings. Some land lines should be maintained to provide recovery capability.

Telecommunications Recovery

- Recovery strategies have historically focused on computing resources and data. Networks are susceptible to many of the same problems, but often they are not properly backed up. This can be a real problem because there is a heavy reliance on networks to deliver data when needed.

Verification of Disaster Recovery and Business Continuity Process Tasks

- As an auditor, you will be tasked with understanding and evaluating business continuity/disaster recovery strategy.
- An auditor should review a plan and make sure it is current and up-to-date.
- The auditor should also examine last year’s test to verify the results and look for any problem areas.
- The business continuity coordinator is responsible for maintaining previous tests. Upon examination, an auditor should confirm that a test met targeted goals or minimum standards.
- The auditor should also inspect the offsite storage facility and review its security, policies, and configuration.

Verification of Disaster Recovery and Business Continuity Process Tasks

- This should include a detailed inventory that includes checking data files, applications, system software, system documentation, operational documents, consumables, supplies, and a copy of the business continuity plan.
- Contracts and alternative processing agreements should also be reviewed.
- Any offsite processing facilities should be audited, and the owners should have a reference check.
- All agreements should be made in writing.

Verification of Disaster Recovery and Business Continuity Process Tasks

- The offsite facility should meet the same security standards as the primary facility and should have environmental controls such as raised floors, HVAC controls, fire prevention and detection, filtered power, and uninterruptible power supplies (UPSs).
- A UPS allows a computer to keep running for at least a short time when the primary power source is lost.
- If the location is a shared site, the rules that determine who has access and when they have access should be examined.
- Another area of concern is the business continuity plan itself. An auditor must make sure the plan is written in easy-to-understand language and that users have been trained. This can be confirmed by interviewing employees.

Verification of Disaster Recovery and Business Continuity Process Tasks

- Finally, insurance should be reviewed. An auditor should examine the level and types of insurance the organization has purchased. Insurance can be obtained for each of the following items:
- IS equipment
- Data centers
- Software recovery
- Business interruption
- Documents, records, and important papers
- Errors and omissions
- Media transportation

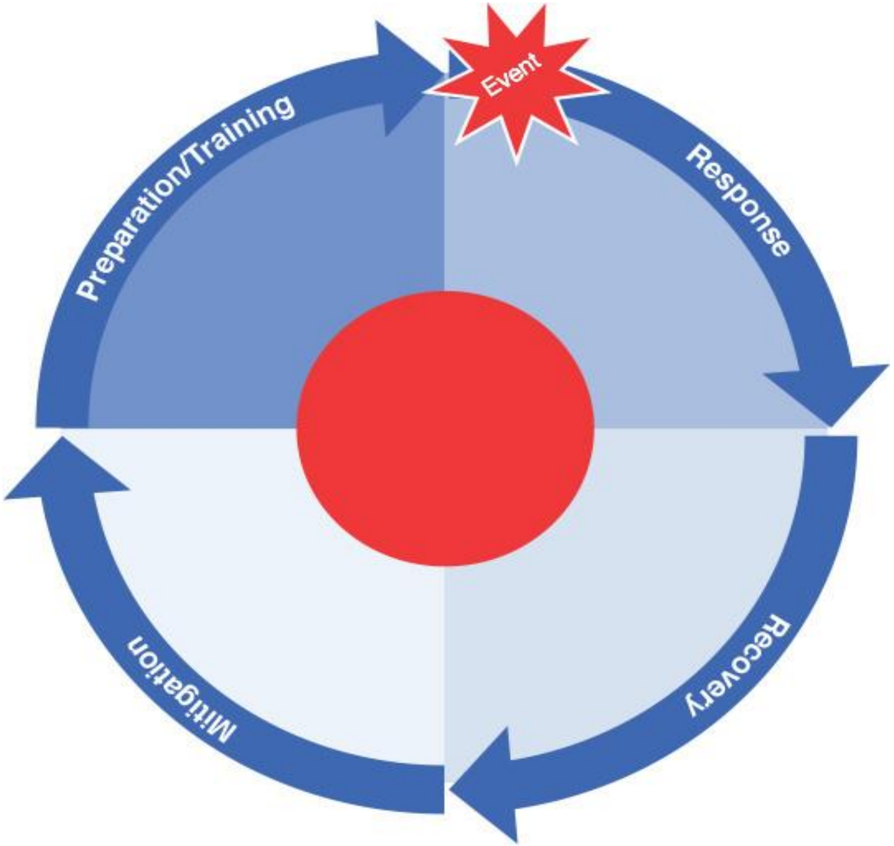
Verification of Disaster Recovery and Business Continuity Process Tasks

- Insurance is not without drawbacks, which include high premiums, delayed claim payouts, denied claims, and problems proving financial loss.
- Finally, most policies pay for only a percentage of actual loss and do not pay for lost income, increased operating expenses, or consequential loss.
- The purpose of disaster recovery is to get a damaged organization restarted so that critical business functions can resume. When a disaster occurs, the process of progressing from the disaster back to normal operations includes the following:

Verification of Disaster Recovery and Business Continuity Process Tasks

- Crisis management
- Recovery
- Reconstitution
- Resumption
- An auditor should be concerned with all laws, mandates, and policies that govern the organization in a disaster situation. As an example, federal and state government entities typically use a Continuity of Operations (COOP) site, which is designed to take on operational capabilities when the primary site is not functioning.
- The length of time the COOP site is active and the criteria used to determine when the COOP site is enabled depend on the business continuity and disaster recovery plans.

The Disaster Life Cycle



The Disaster Life Cycle

- Both governmental and nongovernmental entities typically use a checklist to manage continuity of operations. The table on the next slide shows a sample disaster recovery checklist.

Disaster Recovery Checklist

Time	Activity
When disaster occurs	Notify disaster recovery manager and recovery coordinator
Under 2 hours	Assess damage, notify senior management, and determine immediate course of action
Under 4 hours	Contact offsite facility, recover backups, and replace equipment as needed
Under 8 hours	Provide management with updated assessment and begin recovery at updated site
Under 36 hours	Re-establish full processing at alternative site and determine a timeline for return to the primary facility

The Disaster Life Cycle

- An auditor should verify that the disaster recovery manager directs short-term recovery actions immediately following a disaster and has the approval and resources to do so.
- **Protection of life is a priority while working to mitigate damage**. The areas impacted the most need attention first. Recovery from a disaster entails sending personnel to the recovery site.
- Individuals responsible for emergency management need to assess damage and perform triage.
- When employees and materials are at the recovery site, interim functions can resume operations. This might require installing software and hardware.

The Disaster Life Cycle

- Backup data or copies of configurations might need to be loaded, and systems might require setup.
- When operations are moved from the alternative operations site back to the restored site, the efficiency of the new site must be tested.
- **In other words, processes should be sequentially returned from least critical to most critical.**
- In the event that a few glitches need to be worked out in the new facility, you can be confident that your most critical processes are still in full operation at the alternative site.
- When those processes are complete, normal operations can resume.