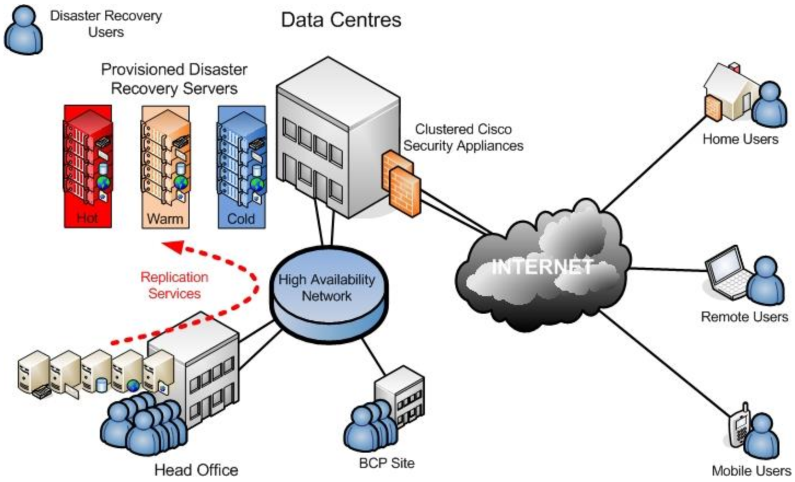
Hard Ware and Network Servicing

Level – 5

Based on December, 2024, Curriculum Version - II



Module Title: Disaster Recovery and Contingency Plan

Module code: -EIS HNS5 M07 1224

Nominal duration: -30 Hours

Prepared by: Ministry of Labor and Skill

December 2024
Addis Ababa, Ethiopia

Table of Contents

Contents

Acknowledgement

The Ministry of Labor and Skills (MoLS) would like to express its gratitude and appreciation to the teachers/trainers and experts from regional TVT bureaus, TVT colleges, and industry practitioners who contributed their expertise and experience in preparing this training module.

The ministry also expresses its deepest gratitude to the ……………………………….. for its invaluable support and collaboration in the module preparation. It is also thankful to MoLS staff members who coordinated the preparation and reviewing process of this training module.

Acronyms

DRCP	This Disaster Recovery and Contingency Plan
DRP	Disaster Recovery Plan
RPO	Recovery Point Objectives
ACP	Assessing Contingency Plans
RPOs	Define Recovery Point Objectives

Introduction to the Module

Preparing Disaster Recovery and Contingency Plan is described how to analyse the impact of the system on the organisation and carry out risk analysis, disaster recovery and contingency planning for the project.

This module covers the units:

- Impact and threat of system on business continuity
- Prevention and recovery strategy

Learning Objective of the Module

- Identify business critical functions and the security environment
- Identify critical data and software from documentation
- Assess potential business risk and threats impacts on IT systems
- Identify and evaluating statutory, commercial requirements and contingency possibilities
- Identify threats to the system
- Evaluate risk minimisation alternatives
- Evaluate prevention and recovery options for critical business functions
- Identify back-up methodologies
- Review Current operational procedures of risk safeguards and contingency plan
- Identify and documenting resources required for disaster recovery
- Identify cut-over criteria before initiating disaster plan

Module Instruction

For effective use these modules trainees are expected to follow the following module instruction:

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Perform Operation Sheets which were provided at the end of units
4. Do the “LAP test” giver at the end of each unit and
5. Read the identified reference book for Examples and exercise

Unit One: Impact and threat of system on business continuity

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Identifying critical functions, data and software from documentation
- Assessing potential business risk and threats impacts on IT systems

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this Training Module, you will be able to:

- Identify critical functions, data and software
- Evaluate Impact of system on business continuity
- Identify threats
- Perform risk minimisation

1.1 Identifying critical functions, data and software

Here are some ways to identify critical functions, data, and software

A. Analyzing business goals and objectives

The first step is to review business goals and objectives and determine how they align with mission, vision, and values. What are the main outcomes and benefits that deliver to customers, stakeholders, and partners? How do measure the performance and success? How do differentiate the organization from your competitors? These questions will help you identify the high-level functions that drive business value and purpose.

B. Mapping out business processes and dependencies

The next step is to map out the business processes that support the goals and objectives and identify the dependencies and interrelationships among them. A business process is a set of activities that transforms inputs into outputs, such as creating a product, delivering a service, or managing a project. A dependency is a condition or requirement that a process relies on to function, such as people, equipment, information, or suppliers. Use tools such as flowcharts, diagrams, or matrices to visualize business processes and dependencies and identify potential gaps, bottlenecks, or risks.

C. Assessing the impact and likelihood of disruptions

The third step is to assess the impact and likelihood of disruptions on your business processes and dependencies. A disruption is any event or situation that prevents or hampers your normal operations, such as a power outage, a fire, a strike, or a cyber attack. You can use tools such as impact analysis, risk assessment, or scenario planning to evaluate the potential consequences and probabilities of different types of disruptions and how they would affect your business processes and dependencies. You should consider factors such as financial losses, reputational damage, customer dissatisfaction, legal liabilities, or regulatory violations.

D. Prioritizing critical business functions

The fourth step is to prioritize your critical business functions based on the results of your impact and likelihood assessment. A critical business function is a business process or dependency that has a high impact and a high likelihood of disruption and that cannot be easily substituted or restored. Use tools such as ranking, scoring, or weighting to assign priority levels to your business functions and categorize them into critical, essential, important, or minor. You should also consider factors such as recovery time, recovery cost, recovery resources, or recovery alternatives.

E. Documenting and communicate critical business functions

The final step is to document and communicate your critical business functions and their priority levels in your continuity plan. You should include details such as the description, purpose, scope, owner, stakeholders, inputs, outputs, dependencies, risks, impacts, likelihoods, recovery objectives, recovery strategies, recovery actions, and recovery responsibilities of each critical business function. You should also communicate your critical business functions and their priority levels to your employees, customers, suppliers, and other relevant parties and ensure that they understand their roles and expectations in the event of a disruption.

By following these steps, you can identify your critical business functions and prioritize them in your continuity plan. This will help you protect your business value and purpose, meet your customer needs and expectations, and comply with your legal and regulatory obligations in the face of any disruption.

1.2 Assessing potential business risk and threats impacts on IT

This Disaster Recovery and Contingency Plan (DRCP) outline the strategies and procedures to minimize disruption and expedite recovery in the event of a network disaster. The primary objectives of this plan are to:

- **Protect Critical Data:** Safeguard essential data and prevent data loss.
- **Minimize Downtime:** Reduce the duration of network outages and service interruptions.
- **Ensure Business Continuity:** Maintain operational continuity and minimize business impact.
- **Facilitate Swift Recovery:** Streamline the recovery process and restore network functionality efficiently.

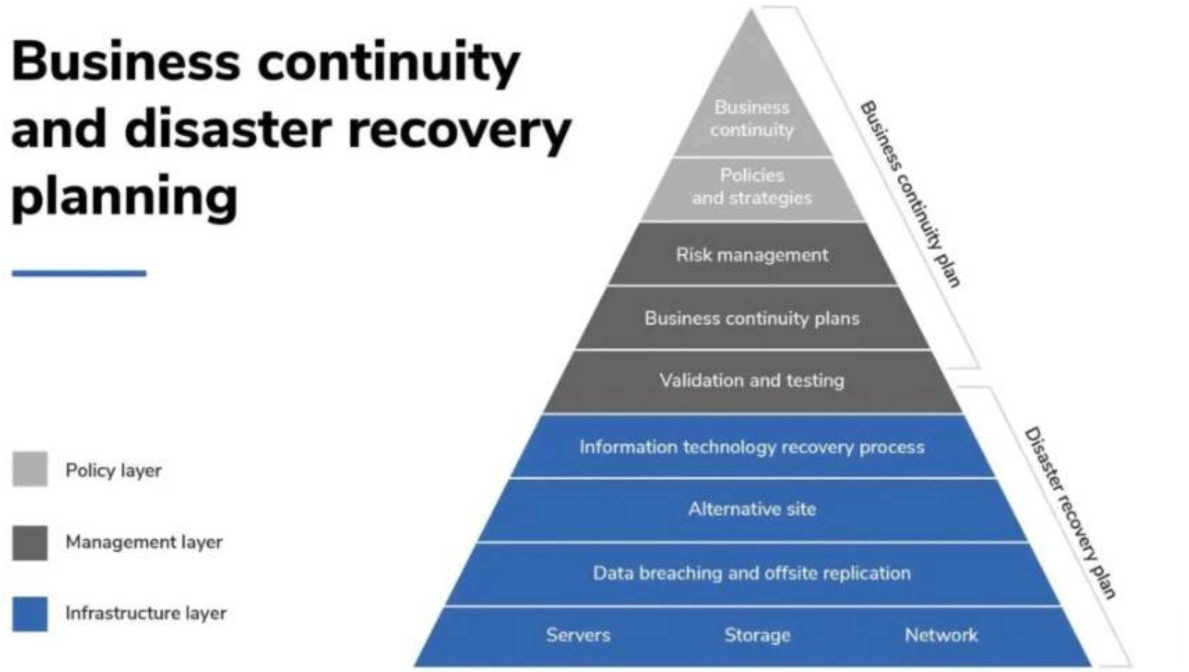


Figure 0-1 Business continuity and disaster recovery plan

Business continuity and disaster recovery have different overarching purpose. Business continuity aims to maintain the essential functions of an organization during and after a disruption, ensuring the continuation of critical processes and services. On the other hand, disaster recovery is primarily concerned with minimizing the downtime and data loss resulting from an IT-related disaster or failure. While their objectives may overlap to some extent, their ultimate purposes differ.

1.2.1 Risk Identification

This section identifies potential risks that could impact the network infrastructure, including:

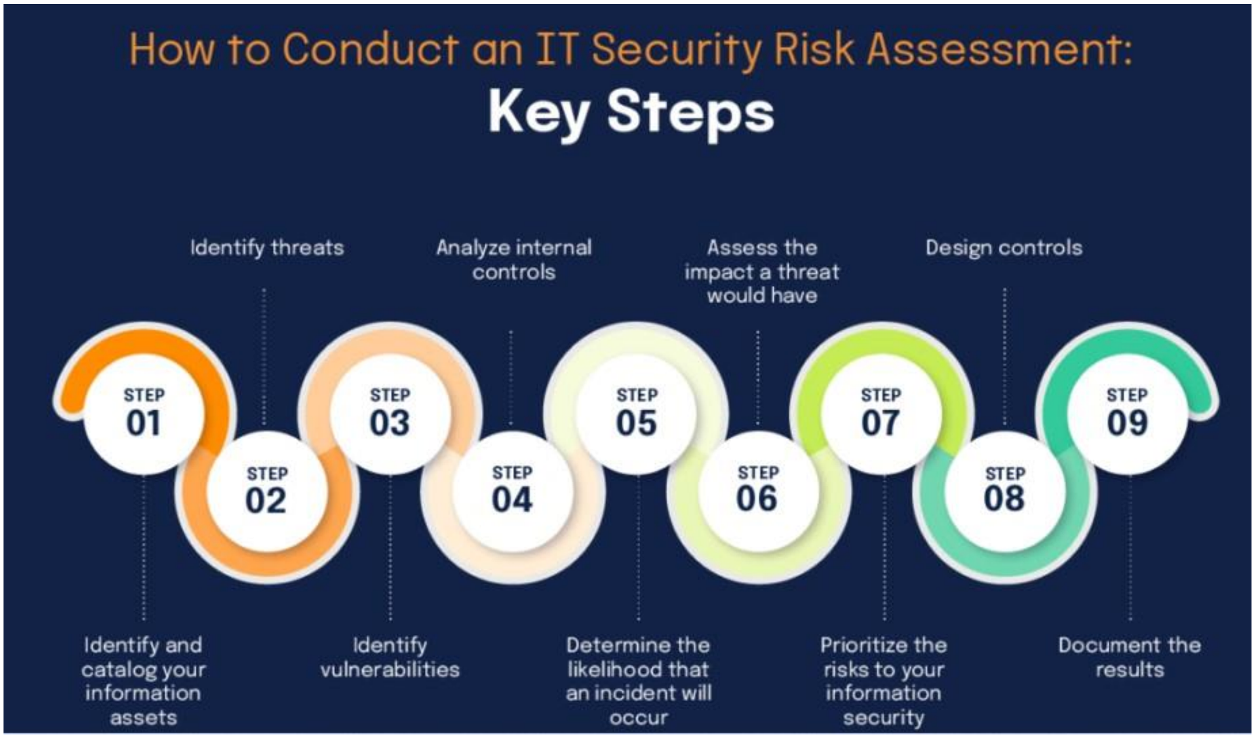
- **Natural Disasters:** Earthquakes, floods, hurricanes, fires
- **Cyber attacks:** Malware, ransom ware, DDoS attacks, phishing
- **Hardware Failures:** Server failures, storage device failures, network equipment failures
- **Human Error:** Accidental configuration changes, unauthorized access

IT risk assessments help organizations understand and manage potential threats to their information systems, networks, and data. They can also help inform decision-makers about how to implement risk management strategies.

1.2.2 Risk assessment

IT security risk assessments focus on identifying the threats facing your information systems, networks, and data and assessing the potential consequences you'd face should these adverse events occur. Risk assessments should be conducted on a regular basis (e.g., annually), and whenever major changes occur within your organization (e.g., acquisition, merger, re-organization, when a leader decides to implement new technology to handle a key business process, when employees suddenly move from working in an office to working remotely).

IT risk assessments are a crucial part of any successful security program. Risk assessments allow you to see how your organization's risks and vulnerabilities are changing over time, so decision-makers can put appropriate measures and safeguards in place to respond to risks appropriately.


How to Conduct an IT Security Risk Assessment:
Key Steps
STEP 01
Identify and catalog your information assets
STEP 02
Identify threats
STEP 03
Identify vulnerabilities
STEP 04
Analyze internal controls
STEP 05
Determine the likelihood that an incident will occur
STEP 06
Assess the impact a threat would have
STEP 07
Prioritize the risks to your information security
STEP 08
Design controls
STEP 09
Document the results

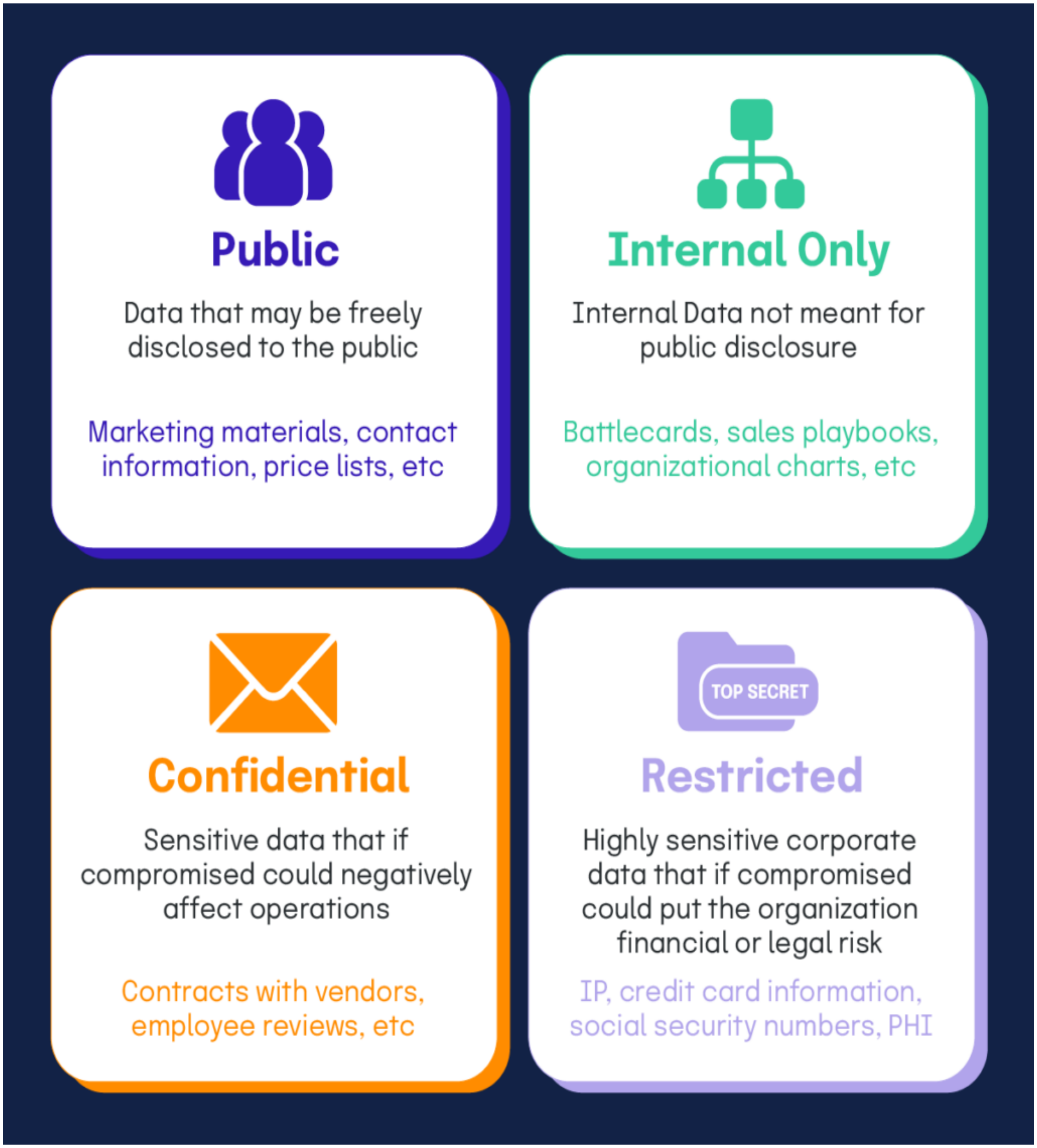
a. Identifying and catalog information assets

The first step in a risk assessment is to make sure that you have a comprehensive list of your informational assets. It’s important to remember that different roles and different departments will have different perspectives on what the most important assets are, so you should get input from more than one source here. The most important information asset for salespeople might be your company’s CRM. At the same time, IT likely sees the servers they maintain as a higher priority, while HR’s most important information asset is confidential employee information.

Once you have identified all of your information assets and key stakeholders within all departments, you’ll need to classify these data assets based on their sensitivity level as well as the strategic importance of the asset to the organization. To get accurate and complete information, you’ll need to talk to the administrators of all major systems across all departments.

Below is a sample data classification framework.

Once you have your data classified, you can zero in on the most sensitive data and see how it is being handled.



Public

Data that may be freely disclosed to the public

Marketing materials, contact information, price lists, etc

Internal Only

Internal Data not meant for public disclosure

Battlecards, sales playbooks, organizational charts, etc

Confidential

Sensitive data that if compromised could negatively affect operations

Contracts with vendors, employee reviews, etc

Restricted

Highly sensitive corporate data that if compromised could put the organization financial or legal risk

IP, credit card information, social security numbers, PHI

b. Identifying threats

When thinking about threats to data security, hackers are usually top of mind, but threats to your business's information security come in many different forms. hackers exploiting weaknesses in a business' firewalls or website security programs has been very common. You need to take into account many different threat types when compiling a list of all the unique threats your business faces.

For example, you also have to take into account not just malicious human interference, but also accidental human interference, such as employees accidentally deleting information or clicking on a malware link. Depending on the quality of your hardware and your information systems, you might also need to account for the risk of system failure.

Finally, things such as natural disasters and power failures can wreak as much havoc as humans can, so you need to account for any of those kinds of threats as well. After you've completed this step, you should have a thorough list of the threats to your assets.

c. Identifying vulnerabilities

Vulnerability is a weakness in your system or processes that might lead to a breach of information security. For example, if your company stores customers' credit card data but isn't encrypting it or testing that encryption process to ensure it's working properly, that's a significant vulnerability. Allowing weak passwords, failing to install the most recent security patches on software, and failing to restrict user access to sensitive information are behaviors that will leave your business's sensitive information vulnerable to attack.

Another vulnerability you may face during the coronavirus health crisis is the lack of staff. Security controls are at risk of not being performed as IT security staff are working remotely or worse, sick themselves.

You can find vulnerabilities through audits, penetration testing, security analyses, automated vulnerability scanning tools, or the NIST vulnerability database.

It's also important to consider potential physical vulnerabilities. For example, suppose your employees work with hard copies of sensitive information or use company electronics outside of the office. In that case, this can lead to the misuse of information, just like vulnerabilities in your software and electronic systems

d. Analyzing internal controls

After identifying the vulnerabilities in the systems and processes, the next step is to implement controls to minimize or eliminate the vulnerabilities and threats. This could be either control to eliminate the vulnerability itself or control to address threats that can't be totally eliminated.

Controls can be technical, such as computer software, encryption, or tools for detecting hackers or other intrusions, or non-technical, such as security policies or physical controls. Controls can also be broken down into preventive or detective controls, meaning that they either prevent incidents or detect when an incident is occurring and alert you.

Creating effective controls requires experience and skills. Suppose your firm does not have security and compliance subject matter experts on staff. In that case, it is crucial to seek out assistance from professional services firms that have deep expertise in addressing IT security issues.

e. Determining the likelihood

Using all the information you have gathered – your assets, the threats those assets face, and the controls you have in place to address those threats – you can now categorize how likely each of the vulnerabilities you found might actually be exploited. Many organizations use the categories of high, medium, and low to indicate how likely a risk is to occur.

So, if, for example, a core application you use to run your business is out-of-date and there's no process for regularly checking for updates and installing them, the likelihood of an incident involving that system would probably be considered high.

On the other hand, if you handle a large volume of personal health information, have automated systems for encrypting and anonymizing it, and regularly test and check the effectiveness of those systems, the likelihood of an incident could be considered low. You will need to use your knowledge of the vulnerabilities and the implementation of the controls within your organization to make this determination.

f. Assessing the impact a threat

This step is known as impact analysis, and it should be completed for each vulnerability and threat you have identified, no matter the likelihood of one happening. Your impact analysis should include three things:

1. The mission of the system, including the processes implemented by the system
2. The criticality of the system is determined by its value and the value of the data to the organization
3. The sensitivity of the system and its data

If possible, you should consider both the quantitative and qualitative impacts of an incident to get the full picture. Depending on the three factors above, you can determine whether a threat would have a high, medium, or low impact on your organization. Taken together with how likely an incident is to occur, this impact analysis will help you to prioritize these risks in the next step.

g. Prioritizing the risks

Prioritizing security risks will help you determine which ones warrant immediate action, where you should invest your time and resources, and which risks you can address at a later time.

For this step, it might help to utilize a simple risk matrix that helps you use the information you already have about each vulnerability/threat pair you've identified and plot it on the matrix. Risks that are both likely to happen and would have severe consequences would be mapped as a high priority, while risks that are unlikely to happen and would have marginal consequences would be mapped as the lowest priority, with everything else falling somewhere in between.

Make a risk matrix as simple or as complex as is helpful to you. If you're a large organization with a lot of risks competing with each other for time and attention, a more in-depth 5×5 risk matrix will likely be helpful; smaller organizations with fewer risks to prioritize can probably utilize a simple 3×3 matrix and still get the same benefit.

Self-check 1.1

Directions: Answer all the questions listed below.

Part I: Say true or false

----------------1. A Business Impact Analysis (BIA) helps identify critical systems and their impact on business operations in the event of a disruption.

----------------2. Recovery Time Objective (RTO) defines the maximum amount of data loss that can be tolerated before significant business impact occurs.

----------------3. Redundancy measures, such as redundant servers and network connections, are not crucial for effective disaster recovery.

----------------4. Regular testing of the disaster recovery plan is unnecessary as long as the plan is well-documented.

----------------5. A cold site is a fully equipped and operational facility that can be quickly brought online in the event of a disaster.

----------------6. Cyberattacks are a significant threat to network services and should be considered in a comprehensive risk assessment.

---------------7. Employee training on disaster recovery procedures is not essential for the success of the plan.

----------------8. Cloud computing can offer cost-effective and scalable solutions for data backup and disaster recovery.

----------------9. Relying solely on physical security measures is sufficient for protecting network infrastructure from all threats.

---------------10. A well-defined disaster recovery plan helps minimize downtime, reduce financial losses, and maintain business continuity.

Answer

1. **True**
2. **False:** RTO defines the **timeframe** for restoring systems, not data loss.

3. **False:** Redundancy is crucial for minimizing single points of failure and ensuring continued operations.
4. **False:** Regular testing is essential to identify and address any weaknesses in the plan.
5. **False:** A cold site is a basic facility with minimal equipment that requires time to be made operational.
6. **True**
7. Employee training is crucial to ensure that everyone understands their roles and responsibilities in the event of a disaster.
8. **True**
9. **False:** Physical security is important, but it's only one aspect of a comprehensive security strategy.
10. **True**

Part I: Fill in the blank space

1. A comprehensive disaster recovery plan should include a thorough _______________ to identify potential threats and their impact.

- **Risk Assessment**

2. _______________ define the maximum amount of data loss that can be tolerated in the event of a disaster.

- **Recovery Point Objectives (RPO)**

3. _______________ define the timeframe within which critical systems and processes must be restored after a disaster.

- **Recovery Time Objectives (RTO)**

4. _______________ involves creating duplicate components or systems to minimize the impact of failures**.**

- **Redundancy**

5. A _______________ site is a fully equipped and operational facility that can be quickly brought online in the event of a disaster.

- **Hot Site**

6. Regular _______________ of the disaster recovery plan are essential to ensure its effectiveness.

- **Testing**

7. _______________ is crucial for protecting network infrastructure from cyber attacks and unauthorized access.

- **Network Security**

Unit Two: Prevention and recovery strategy

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Evaluating prevention and recovery options
- Reviewing Current operational procedures of risk safeguards and contingency plan
- Submitting Disaster recovery and prevention strategy for approval

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this Training Module, you will be able to:

- Evaluate prevention and recovery options for critical business functions
- Review Current operational procedures of risk safeguards and contingency plan
- prepare Disaster recovery and prevention strategy

2.1. Evaluating prevention and recovery options

Evaluating prevention and recovery options for network services involves systematically assessing strategies to mitigate potential issues, ensure continuity, and restore functionality after disruptions. Here's how to approach this evaluation

a. **Prevention Strategies**

- **Redundancy:** Implement failover systems such as backup servers and redundant network paths to avoid single points of failure.
- **Monitoring Tools:** Use advanced network monitoring tools to detect anomalies and predict issues before they escalate.
- **Security Measures:** Strengthen firewalls, intrusion detection systems, and endpoint protection to prevent cyber attacks.
- **Regular Maintenance:** Schedule routine updates and inspections for hardware and software to ensure reliability.

b. **Recovery Planning**

- **Disaster Recovery Plan (DRP):** Develop a detailed plan for restoring network services, specifying roles, processes, and timelines.
- **Backups:** Ensure regular data and configuration backups, stored securely and easily accessible during a recovery.
- **Alternative Solutions:** Set up temporary solutions (e.g., mobile networks or cloud services) to maintain service during recovery.

c. **Testing and Validation**

- Regularly test prevention and recovery mechanisms, such as simulating outages and running penetration tests.
- Evaluate the effectiveness of failover systems and recovery speed during mock drills.
- Document lessons learned from tests to refine strategies.

d. Continuous Improvement

- Analyze past incidents to identify gaps in prevention and recovery efforts.
- Incorporate feedback from stakeholders to improve response protocols.
- Stay updated on new technologies and methods for network security and recovery.

2.2. **Reviewing Current operational procedures**

Reviewing current operational procedures for risk safeguards and contingency plans involves a systematic approach to evaluate their effectiveness, identify gaps, and recommend improvements.

a. Understand Objectives and Scope

Define Objectives: Clarify what you aim to achieve with the review, such as identifying vulnerabilities or ensuring compliance with regulations.

Determine Scope: Decide which areas, operations, or risks will be reviewed. Include key risk safeguards and contingency plans.

b. Gathering Documentation and Information

Collect Policies and Procedures: Obtain all relevant documents, including risk management policies, operational procedures, and contingency plans.

Understand Context: Learn about the organization's risk appetite, key threats, and critical operations.

Review Past Incidents: Analyze reports from previous incidents or audits to identify recurring issues.

C. Engaging Key Stakeholders

Interview Staff: Discuss processes with those responsible for implementing safeguards and contingency plans.

Collaborate with Experts: Engage risk managers, compliance officers, and IT specialists for technical insights.

d. Analyzing Safeguards

Evaluate Preventative Measures: Check whether current safeguards adequately mitigate identified risks.

Test Controls: Perform drills or simulations to assess the effectiveness of physical, procedural, and technical safeguards.

Check Alignment: Ensure safeguards align with organizational goals and industry standards.

e. Assessing Contingency Plans(ACP)

Review Plan Content: Verify that contingency plans address key risks, identify roles, and provide clear instructions.

Check Accessibility: Confirm that the plans are readily available and understood by relevant personnel.

Conduct Testing: Simulate scenarios to test the functionality and practicality of contingency measures.

Evaluate Recovery Times: Ensure the plans meet recovery time objectives (RTOs) and recovery point objectives (RPOs).

f. Identify Gaps and Risks

Analyze Gaps: Identify areas where safeguards or plans are incomplete, outdated, or ineffective.

Document Risks: Record any risks that are not adequately addressed.

g. Benchmark and Compare

Use Best Practices: Compare your procedures against industry standards and regulatory requirements.

Assess Against Competitors: Benchmark against similar organizations if data is available.

h. Provide Recommendations

Short-Term Fixes: Identify quick wins for immediate improvement.

Long-Term Strategies: Suggest comprehensive solutions to address systemic issues.

Prioritize Actions: Rank recommendations based on impact and urgency.

i. Report Findings

Prepare a Comprehensive Report: Include an executive summary, detailed findings, identified risks, and recommendations.

Communicate Clearly: Use clear language and visuals to ensure the report is understandable.

j. Implement and Monitor Improvements

Develop an Action Plan: Assign responsibilities and timelines for implementing recommendations.

Monitor Progress: Regularly review the implementation of improvements and adjust as needed.

2.3 Preparing Disaster recovery and prevention strategy

Preparing a disaster recovery and prevention strategy involves developing a comprehensive framework to safeguard on the organization from potential disasters and ensure business continuity. Below is a step-by-step guide:

1. Assess Risks and Vulnerabilities

Identify Potential Disasters: Consider natural disasters, cyber attacks, power failures, human errors, and supply chain disruptions.

- Conduct Risk Assessments: Evaluate the likelihood and impact of each potential disaster.
- Pinpoint Vulnerabilities: Identify weaknesses in your infrastructure, systems, and processes.

2. Define Objectives and Scope

- Set Goals: Determine key priorities, such as minimizing downtime, protecting data, and ensuring employee safety.
- Determine Scope: Decide which operations, systems, and assets are critical to include in the strategy.

3. Build a Disaster Prevention Plan

Mitigation Measures:

- Implement firewalls, antivirus software, and regular system updates for cyber threats.

Install backup power supplies (e.g., generators or UPS systems).

- Ensure facilities comply with safety standards for natural disasters (e.g., flood barriers, fire suppression systems).

Training and Awareness:

- Educate employees about disaster risks and their roles in prevention.
- Conduct drills to reinforce preparedness.

Supplier and Vendor Collaboration:

- Work with vendors to ensure they have robust disaster prevention measures.
- Establish alternative suppliers to mitigate supply chain risks.

4. Develop the Disaster Recovery Plan

Inventory Critical Assets:

- Document key systems, applications, and data.
- Identify dependencies among systems and operations.

Data Backup Strategy:

- Establish regular backups, including offsite and cloud storage.
- Ensure backups are tested and easily accessible during an emergency.

Recovery Objectives:

- Define Recovery Time Objectives (RTOs): Maximum acceptable downtime.
- Define Recovery Point Objectives (RPOs): Maximum data loss tolerable.

Create Recovery Procedures:

- Specify step-by-step actions for restoring operations.
- Identify recovery team roles and responsibilities.

Designate Alternate Locations:

- Arrange for backup office locations or remote work capabilities.

5. Create a Communication Plan

Internal Communication:

- Develop protocols for notifying employees, management, and other stakeholders.
- Use multiple communication channels (email, SMS, intranet, etc.).

External Communication:

- Prepare templates for communicating with customers, suppliers, and media.
- Assign spokespersons for public relations.

6. Test and Validate the Strategy

Conduct Simulations:

- Perform disaster recovery drills for various scenarios.
- Test system failovers and data recovery procedures.

Evaluate Effectiveness:

- Review drill outcomes to identify weaknesses.
- Update the strategy based on lessons learned.

7. Document the Plan

Create a Comprehensive Manual:

- Include risk assessments, preventive measures, recovery procedures, and contact lists.

Make it Accessible:

- Store copies securely in both digital and physical formats.
- Ensure authorized personnel can access the plan when needed.

8. Establish Governance and Maintenance

Assign Ownership:

- Appoint a disaster recovery team or manager to oversee implementation and updates.

Regular Reviews:

- Reassess risks and update the strategy annually or after significant changes.

Monitor Compliance:

- Ensure the strategy aligns with industry standards and regulatory requirements.

9. Leverage Technology

Automation:

- Use automation tools for backups, system monitoring, and incident alerts.

Disaster Recovery as a Service (DRaaS):

- Consider cloud-based solutions for faster and more reliable recovery.

Monitoring Tools:

- Use real-time monitoring to detect and prevent potential disasters.

10. Build a Culture of Resilience

Promote Awareness:

- Regularly communicate the importance of disaster recovery and prevention.

Encourage Feedback:

- Involve employees in refining the strategy.

Foster Adaptability:

- Prepare the organization to adapt quickly to unforeseen challenges.

Self-check 1.1

Directions: Answer all the questions listed below.

Part-I: Choose the correct answer from the given alternatives

1. **Which of the following best defines Recovery Time Objective (RTO)?**

   a) The maximum tolerable downtime for a system or application after a disaster.

   b) The maximum amount of data loss that can be tolerated.

   c) The process of restoring systems and data after a disaster.

   d) The cost associated with recovering from a disaster.

2. **Which of the following is NOT a key component of a comprehensive disaster recovery plan (DRP)?**

   a) Risk Assessment

   b) Business Impact Analysis (BIA)

   c) System Documentation

   d) Employee Benefits Package

3. **A "cold site" for disaster recovery typically refers to:**

   a) A fully operational facility with all necessary hardware and software pre-installed.

   b) A facility with basic infrastructure (power, cooling) but lacking hardware and software.

   c) A cloud-based solution for data backup and recovery.

   d) A redundant system within the same location as the primary site.

4. **Which of the following is NOT a common redundancy technique for network infrastructure?**

   a) Load Balancing

   b) Data Deduplication

   c) Redundant Power Supplies

   d) Multiple Internet Connections

5. **Which of the following is a crucial step in ensuring the effectiveness of a disaster recovery plan?**

   a) Regular backups

   b) System documentation

   c) Regular testing and maintenance

   d) All of the above

6. **Which of the following is NOT a primary goal of network security in the context of disaster recovery?**

   a) Preventing data breaches

   b) Ensuring business continuity

   c) Minimizing downtime

   d) Increasing network bandwidth

7. **What is the primary purpose of a Business Impact Analysis (BIA)?**

   a) To identify and prioritize critical systems and processes.

   b) To determine the cost of implementing a disaster recovery plan.

   c) To train staff on emergency procedures.

   d) To select a suitable disaster recovery site.

8. **Which of the following is NOT a common threat to network services?**

   a) Natural disasters (e.g., earthquakes, floods)

   b) Cyberattacks (e.g., malware, DDoS attacks)

   c) Hardware failures (e.g., server crashes, network equipment malfunctions)

   d) Increased network traffic

9. **Which of the following statements about disaster recovery plans is TRUE?**

   a) DRPs should be static and rarely updated.

b) DRPs should be regularly tested and updated to reflect changes in the business environment.

c) DRPs are primarily concerned with restoring hardware, not data.

d) DRPs are only necessary for large organizations.

10. **What is the primary purpose of conducting regular security audits?**

a) To improve network performance.

b) To identify and address network vulnerabilities.

c) To comply with industry regulations. d) To reduce operating costs.

Operation Sheet 2.1

Operation Title: Prepare Disaster Recovery and Contingency Plan

Purpose: To Know how to Prepare Disaster Recovery and Contingency Plan

Equipment Tools and Materials:

- ✓ Computer

Quality Criteria: Assured performing of all the activities according to the procedures

Information: Under this project, you are expected to identify the systems impact on the business, identify the threats of the system, develop disaster recovery plan, and develop a disaster recovery and contingency planning checklist.

Assume you are working in a certain financial institution, say **Click International Bank**, as head of IT technicians responsible for the smooth functioning of the core banking system. The core banking system is a web-based information system installed in the bank's private network, which enables the bank to perform transactions across all branches.

The bank has many branches in Addis Ababa, in regions and in neighboring African countries. Each branch is connected through a Virtual Private Network (VPN), can access the centralized database and the transactions are finally send to the central database.

The bank repeatedly suffers network interruption and transactions are often aborted in the middle of the process.

Instruction: - Under this project you are expected to perform the following four tasks based on the information provided**:-**

Task 1: Identify the potential impacts of the core banking system on the continuity of the bank's business.

Task 2: Identify the major internal and external threats to the core banking system.

Task 3: Develop disaster recovery plan for the system.

Task 4: Develop a disaster recovery and contingency planning checklist for the core banking system.

Developers Profile

No	Name	Qualification	profession	Organization	Mobile No	E-mail
1	Abel G/Egziabher	MSc	IT	MOls	0911776728	ab.smart99@gmail.com
2	Zerihun Abate	MSc	ITM	Sebeta PTC	0911858358	zedoabata2017@gmail.com
3	Abebe Mintefa	MSc	ITM	Ambo TVT	0929362458	tolabula@gmail.com
4	Mohammed Bekele	BSc	CS	MoLS	0941267468	mbelela@gmai.com