Course: IT RISK MANAGEMENT AND CONTROL

Week 10

Topic: Business Continuity and Disaster Recovery

Lecturer: Ninyikiriza Deborah Lynn

TODAYS outline

1. Review of week 9 Material
2. Business Continuity Planning (BCP)
3. Disaster Recovery Planning (DRP)
4. Testing and Maintaining BCP and DRP

Week 9 Review

1. Incident Management and Response

- Refers to the structured approach of detecting, responding to, managing, and recovering f rom IT-related incidents, particularly cybersecurity threats.

2. Incident Response Strategy

- Strategies are built around the assets of concern, thinking through risks and attacking sce narios likely to occur.

3. Incident response planning Goals for organizations;

- ✓ To protect the organization’s infrastructure, assets, & operations.
- ✓ To comply with federal, state, and local regulations.
- ✓ To minimize the potential for negative publicity.
- ✓ To prevent or minimize financial liabilities.
- ✓ To minimize customer disruptions

Week 9 Review

4. Roles and Responsibilities in incident response planning

- Involves various teams.
- The teams include, a group of legal and compliance members, IT lead ership members, external consultants, a group of senior management and external legal counsel.
- Each of the individuals on each team has a role in incident response.

5. Important terms

1. Triage: *The* process of quickly assessing and prioritizing incidents to d etermine the appropriate level of response

2. Escalation: The process of raising an incident to a higher level of aut hority or expertise when it requires additional attention, resources, or spe cialized knowledge.

Week 9 Review

6. Incident Response Planning phases

1. Intrusion detection

Enables early detection and accurate identification of incidents.

2. Containment

- The process of limiting the impact of the detected incident and pr eventing further spread.

- Short-term Containment: Involves immediate actions like discon necting infected systems from the network or temporarily blockin g specific services to prevent damage from escalation.

- Long-term Containment: Planning for a sustainable solution, suc h as removing affected systems from production and addressing vulnerabilities.

Week 9 Review

Incident Response Planning phases CONT…

3. Eradication

- Eradication involves the removal of the root cause of the incident to prevent recurrence.

4. Recovery

- Recovery aims at safely restoring and validating the affected syst ems to resume normal operations.

7. Incident detection and reporting

Incident Detection

- Incident Detection is the process of suing monitoring tools to iden tify and recognize events that may pose a risk to IT systems, dat a, or operations

Week 9 Review

8. Effective Incident detection involves activities like;

- Continuous Monitoring
- Automating Alerts
- Vulnerability Scanning and Penetration Testing
- User Reporting Mechanisms
- Automated Tools and Analytics

Week 9 Review

9. Incident Reporting

- Incident Reporting involves documenting and communicating incidents after detection to ensure a coo rdinated response and future prevention

The Incident Reporting process;

1. Incident Classification and Documentation
2. Notification Protocols
3. Root Cause Analysis
4. Incident Log and Tracking

10. Components of Effective Detection and Reporting

1. Incident Management System (IMS)
2. Collaboration Tools
3. Documentation and Knowledge Base

Week 9 Review

11. Best Practices in Incident Detection and Reporting

- Conduct regular employees training;
- Define Clear Metrics;
- Post-Incident Review:
- Ensure efficient incident detection and reporting

12. Managing and Recovering from Incidents

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication
5. Recovery
6. Perform Post-Incident Review (Lessons Learned)

Week 10: Business Continuity and Disaster Recovery

- Business Continuity (BC) and Disaster Recovery (DR) are essential elements in IT risk management and control that focus on minimizing disruptions in businesses and ensuring quick recovery of IT operations after an unexpected event.

Business Continuity (BC) in IT

- Business Continuity involves continuous planning to keep critical business functions running during and after a disruptive event, such as cyberattacks, natural disasters, or system failures.

Week 10: Business Continuity and Disaster Recovery

- Business continuity in IT means establishing policies and IT systems that support continuous operation, such as mechanisms for continuity, and strategic planning for resilience.

Need for “Business Continuity”

- Business Continuity aims to prevent interruptions to essential services, ensuring that any disruption causes minimal impact on business operations.

Key focus of Business Continuity

1. Risk Assessment and Business Impact Analysis;

- BC focuses on identifying risks and evaluating their potenti al impact on business operations.
- This helps to prioritize which systems are most critical for c ontinuity planning.

2. Redundancy and Resilience Measures;

- BC aims at implementing backups and redundant systems to prevent single points of failure, e.g, duplicate data center s or cloud solutions can support operational continuity.

3. Crisis Management Planning;

- BC aims at organizing a crisis response team and establish ing a communication plan to manage and mitigate disruptio ns efficiently.

Business Continuity and Disaster Recovery cont..

Disaster Recovery (DR) in IT

- Disaster Recovery is a subset of Business Continuity that focuses specifically on the restoration of IT syste ms after a disruption.
- DR aims to restore data access, applications, and infr astructure to their operational state as quickly as pos sible.
- It usually includes specific recovery procedures, such as backing up data, configuring recovery sites, and d efining the Recovery Time Objective (RTO) and Reco very Point Objective (RPO).

Business Continuity and Disaster Recovery cont..

RTO and RPO as Metrics in Business continuity

Recovery Time Objective (RTO) is the maximum accept able length of time that a system, application, or process can be down after a failure or disaster without causing si gnificant damage to the business.

- Purpose of RTO: It sets a target for how quickly syste ms should be restored.
- E.g, an RTO of 2 hours means that a system must be up and running within 2 hours after a disruption to mini mize business impact.

.

Business Continuity and Disaster Recovery cont..

RPO as a Metric in Business continuity

Recovery Point Objective (RPO) is the maximum accept able amount of data loss measured in time.

It indicates the point in time to which data must be resto red to resume acceptable operations.

- Purpose of RPO: It sets a target for how much data lo ss is tolerable, often dictating backup frequency.
- E.g, an RPO of 30 minutes means that backups shoul d occur at least every 30 minutes to prevent unaccept able data loss during an incident.

Key focus of Disaster Recovery

1. Performing data Backup and Recovery Solutions;

- DR focuses on performing regular backups (off-site or in the cloud) to ensure that data can quickly be restored.

2. Establishing Disaster Recovery Sites and Infrastructure;

- Focuses at establishing off-site DR locations where data and systems can be replicated, allowing operations to switch to the backup site if the primary systems fail.

3. Testing and Maintenance of DR Plans;

- Regularly tests DR procedures to identify gaps and update plans to ensure readiness for various disaster scenarios.

Off-site disaster recovery refers to the practice of storing critical data, backups, and IT infrastructure in a separate, physically distant location from the main business site.
The site acts as a backup environment, allowing an organization to restore operations after disaster.

Business Continuity Planning (BCP)

- The Business Continuity Planning (BCP) process in I T prepares organizations to maintain essential functi ons and recover critical systems quickly after a disru ption.
- In IT field, BCP focuses on ensuring that technology, data, and systems are resilient against potential thre ats and can be restored efficiently to minimize downti me.

Lets discuss the steps involved in the BCP process for IT in the next slide 

Steps of Business Continuity Planning in IT

1. Risk Assessment and Business Impact Analysis (BIA)

- *(a). Risk Assessment: Under risk assessment, we* Identify potential risks to IT infrastructure such as cyberattacks, har dware failures, natural disasters, or power outages.
- This assessment aims to evaluate the likelihood and potent ial impact of each threat on the organization's systems.
- *(b). Business Impact Analysis:* Determine the criticality of e ach IT system by analyzing the potential consequences of disruptions to the organization.

Steps of the BCP process in IT

2. Strategy Development

- (a) Determine Recovery Strategies: Based on BIA findings, identify specific strategies to recover and maintain IT operations. The strategies include;
- *Redundant Systems:* Set up failover servers or cloud-based backups to ensure critical applications remain available.
- *Data Backups:* Regularly back up data, ideally to off-site or cloud storage, and defining backup frequency based on RPO requirements.
- *Alternate Communication Channels:* Ensure alternative methods for team communication during disruptions, such as dedicated phone lines or satellite communication.

(b) Identify Resource Requirements:

- List the necessary hardware, software, and personnel needed to support the recovery strategy.
- This ensures quick deployment and minimizes resource shortages during the actual event.

Steps of the BCP process in IT

3. Plan Development

(a) Create a Business Continuity Document Plan:

- The BCP document plan details specific steps for respondi ng to different types of incidents.

  The BCP plan must include;

- *Activation Procedures:* Must have the criteria and instructio ns for when and how to activate the BCP.
- *Step-by-Step Recovery Procedures*: It should have detaile d processes for recovering each critical system, including i nstructions for data restoration, server recovery, and applic ation access.
- *Roles and Responsibilities*: It must assign specific roles to staff, such as IT managers, data recovery specialists, and c ommunications personnel.

(b) Vendor Coordination: Identify key vendors and partners critical to IT operations, such as cl oud providers or telecommunications companie s, and outline communication channels for imm ediate response during incidents.

Steps of the BCP process in IT

4. Testing and Training

(a) Plan testing:

- Conduct regular testing to verify the effectiveness of the BCP.

  Common tests performed include;

- *Tabletop Exercises:* Simulated discussions with key personnel to tes t their actions in incident scenarios.

- *Full Drills:* Testing actual procedures in a controlled environment to v erify that all systems can be restored within RTO and RPO targets.

(b) Employee training

- Ensure all relevant personnel are aware of the BCP and trained in th eir specific roles.

- Regularly update training to ensure readiness as systems or roles c hange within the organization.

Steps of the BCP process in IT

5. Maintenance and Review

- *(a). Do continuous Updates;*
- Regularly update the BCP to reflect changes in the IT environment, such as new applications, updated hardware, or revised recovery requirements.
- *(b). Post-Incident Review;*
- After any disruption, review the plan’s effectiveness and adjust based on lessons learned to strengthen the approach for future incidents;

Steps of the BCP process in IT

To be noted;

- ✓ Each stage in the BCP process enhances an organization's ability to withstand and recover from IT disruptions, aligning with industry best practices to safeguard data integrity, minimize downtime and maintain operational continuity.
- ✓ By regularly testing and updating these plans, businesses ensure that their IT resilience evolves with emerging risks and changing technological landscapes.

Disaster Recovery Planning (DRP)

- Disaster Recovery Planning (DRP) in IT is a focused part of Business Continuity Planning (BCP), concentrating on r estoring IT infrastructure, systems, and data access after a disruption.
- A robust DRP allows organizations to minimize downtime and resume critical operations promptly.

Steps of the Disaster Recovery Planning process in IT:

1. Identify the Risk and Impact Analysis

- **(a)** *Risk Assessment:* Identify the range of potential risks t hat could impact IT infrastructure, such as natural disaster s, cyberattacks, system failures, or power outages.
- This step assesses the likelihood and potential impact of each threat on IT systems.

Disaster Recovery Planning (DRP)

- *(b) Business Impact Analysis (BIA):* Evaluate the impa ct of disruptions on different systems and processes.

  This includes determining:

- *Recovery Time Objective (RTO):* The maximum accep table downtime for each system, guiding how quickly each component needs to be restored.
- *Recovery Point Objective (RPO):* The maximum data l oss in terms of time, informing the frequency of backu ps needed to keep data losses within an acceptable li mit.

Steps of the DRP process in IT

2. Setting Recovery Strategies

- **(a) Define Recovery Priorities:** Based on RTO and RPO values, prioritize systems by criticality, starting with essential applications and data.
- Systems that impact customer-facing services or essential operations typically receive the highest priority.
- **(b) Perform Backup and Data Replication**
- *Regular Backups*: Scheduling regular data backups, considering storage at secure off-site or cloud locations to protect against site-specific disasters.
- *Real-Time Replication:* For high-priority systems, employ real-time replication or continuous data protection, ensuring the most recent data is available for recovery.

Steps of the DRP process in IT

3. Develop the Disaster Recovery Plan Document

- *Define Step-by-Step Recovery Procedures:* Create detailed instructions for restoring systems and data.
- Include steps for system booting, configuration, data restoration, and verification which IT teams can follow to avoid missing critical steps.
- *Set Roles and Responsibilities:* Define specific responsibilities for key personnel involved in the recovery process.
- This includes assigning primary and backup roles to ensure coverage during the recovery phase.

Steps of the DRP process in IT

Develop the Disaster Recovery Plan Document cont..

- *Define Communication Protocols:* Establish clear internal and external communication guidelines such as whom to notify and who has the authority to activate the DRP.
- *Carry out Vendor and Partner Coordination*: Document contact information and procedures for essential vendors (e.g. Cloud providers, backup services) to streamline coordination during a recovery.

Steps of the DRP process in IT

4. Testing and Training

- **(a) Perform Regular DR Testing:**
  - *Tabletop Exercises*: These are scenario-based discussi ons with relevant staff on how they would respond to dis asters, helping teams to understand their roles and resp onsibilities.
  - *Simulated Drills:* Conduct full or partial recovery simulati ons, such as data recovery exercises or failover drills to test the readiness of the DRP, validating its effectivenes s in restoring systems within acceptable RTO and RPO.

Steps of the DRP process in IT

5. Testing and Training con't…

- *(b) Perform Staff Training:* Train IT staff and relevant employees on their roles and recovery procedures.
- This training ensures everyone is familiar with the DRP, understands their responsibilities, and can act efficiently during the attack of actual incidents.

Steps of the DRP process in IT

5. Continuous Improvement and Maintenance

- *Regular Plan Updates:* As IT infrastructure, applications, or bu siness processes evolve, update the DRP to incorporate these changes.
- For example, adding new applications, implementing security updates, or modifying system configurations may require revis ions.
- *Post-Incident Review:* After any incident where the DRP is acti vated, conduct a review to identify what worked well and what needs to be improved.
- This feedback loop helps to refine the DRP based on real-worl d challenges and strengthens future response readiness.

Testing and Maintaining BCP and DRP

- Testing and Maintaining Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) are ess ential activities to ensure that these plans are effect ive and up-to-date.
- This helps in preparing organizations to respond pr omptly and effectively to disruptions.
- In IT risk management, regular testing and mainten ance of BCP and DRP enable resilience, adaptabilit y, and reliability of IT systems.

Goals of Testing the BCP and DRP

- *To validate Assumptions:* Testing helps to confirm whether assumptions in the BCP and DRP (like the availability of a lternate sites or the sufficiency of backups) are accurate.
- *To assess Recovery Time and Recovery Point Objectives* (RTO/RPO): Testing ensures that the recovery processes meet the targeted RTO and RPO, limiting downtime and d ata loss to acceptable levels.
- *To enhance Preparedness and Confidence:* Testing builds confidence and ensures that staff are trained, equipped, a nd ready to execute their roles effectively during a real inci dent.

Testing and Maintaining BCP and DRP

1. Testing BCP and DRP in IT

- Testing is a structured process to validate that BCP and DRP w ill perform as expected during an actual disruption.
- Regular testing helps to identify gaps, ensures that responsible teams are prepared, and refines the plans over time.

Types of Tests;

- *Tabletop Exercises:* These involve a simulation in which key st aff members discuss their responses to a disaster scenario wit hout any real system involvement.
- This low-cost approach clarifies roles, improves understanding, and refines the communication processes.

Walkthroughs: In walkthrough tests, e mployees go through the plan step-by-step to ensure they understand each p art and identify missing elements or pro cedural issues.

Testing and Maintaining BCP and DRP

Types of tests con't….

- *Simulation Drills:* These involve simulating specific disaster sc enarios (like cyberattacks or server failures) to test recovery s trategies.
- Teams perform tasks, such as system failover or data recover y, validating the DRP's effectiveness in restoring operations w ithin acceptable limits of (RTO and RPO).
- *Full-Scale Testing:* Full-scale tests involve testing all or major parts of the BCP and DRP, including backup sites, alternate c ommunication channels, and recovery of critical systems.
- These are complex and resource-intensive but they provide a comprehensive assessment of readiness for any disruption.

Testing and Maintaining BCP and DRP

2. Maintaining BCP and DRP in IT

- Maintaining BCP and DRP involves regularly updati ng the Business Continuity and Disaster Recovery pl ans to align with changes in IT infrastructure, busine ss processes, or external factors.
- This ensures the plans remain relevant and effective over time.

Maintaining BCP and DRP in IT

2 (a) Maintenance Activities include;

- *Review and Update Procedures:*
- IT systems, applications, and infrastructure evolve ove r time, necessitating periodic reviews to integrate new components, configurations, or processes into the Busi ness Continuity and Disaster Recovery Plans.
- *Incorporate Organizational Changes:*
- As roles, responsibilities, and personnel change within the organization, the BCP and DRP must be updated t o reflect current team structures and responsibilities.

Testing and Maintaining BCP and DRP

2 (a) Maintenance Activities cont….

- *Perform Vendor and Partner Coordination:*
- For organizations relying on third-party vendors e.g cloud storage or communication services, maintain up-to-date contact informatio n and verify the vendor’s disaster recovery capabilities.
- *Post-Incident Review and Lessons Learned*:
- After any incident where the BCP or DRP is activated, conducting a review identifies successful actions and areas for improvement.
- Lessons learned can be incorporated to enhance future response effectiveness.

Testing and Maintaining BCP and DRP

2(b) Frequency of Maintenance

- *Regularly Scheduled Updates:* Many organizations schedule BCP and DRP reviews annually or semi-annually, especially after significant organizational or IT changes.
- *After Significant Changes*: Major IT changes, like new software deployments or infrastructure upgrades, often trigger updates to ensure the plans reflect current systems.
- *Following Each Test or Real Incident*: Tests or real-world incidents provide practical insights into the plan’s effectiveness and should prompt reviews and updates as needed.

Benefits of Testing and Maintaining BCP and DRP

- *Preparedness:* Regular testing and maintenance ensure that staff are ready and aware of their responsibilities, minimizing confusion during real incidents.
- *Plan Effectiveness:* Testing validates whether the BCP and D RP will work as intended, while maintenance ensures they re main aligned with current operational needs.
- *Regulatory Compliance:* Regularly updated and tested BCP a nd DRP enable organizations to comply with industry regulati ons, ensuring data protection and business continuity.
- Together, testing and maintenance are critical for keeping BC P and DRP practical, actionable, and aligned with an organiz ation’s evolving IT and operational landscape.

Week 10 Summary

1. Business Continuity and Disaster Recovery

(a) Business Continuity (BC) in IT

- Involves continuous planning to keep critical business functions ru nning during and after a disruptive event, such as cyberattacks, nat ural disasters, or system failures.

(b) Key focus of Business Continuity

1. Risk Assessment and Business Impact Analysis;

- BC focuses on identifying risks and evaluating their potential impac t on business operations.

2. Redundancy and Resilience Measures;

- BC aims at implementing backups and redundant systems to preve nt single points of failure.

3. Crisis Management Planning;

- BC aims at organizing a crisis response team and establishing co mmunication.

Week 10 Summary

1. Business Continuity and Disaster Recovery

(a) Disaster Recovery (DR) in IT

- Disaster Recovery is a subset of Business Continuity that focuses specifically on the restoration of IT systems after a disruption.

(b) Key focus of Disaster Recovery

1. Performing data Backup and Recovery Solutions;

- DR focuses on performing regular backups (off-site or in the cloud) to ensure that data can quickly be restored.

2. Establishing Disaster Recovery Sites and Infrastructure;

- Focuses at establishing off-site DR locations where data and systems can be replicated, allowing operations to switch to the backup site if the primary systems fail.

3. Testing and Maintenance of DR Plans;

- Regularly tests DR procedures to identify gaps and update plans to ensure readiness for various disaster scenarios.

4. Off-site disaster recovery

Refers to the practice of storing critical data, backups, and IT infrastructure in a separate, physically distant location from the main business site.

Week 10 summary

2. RTO and RPO as Metrics in Business continuity

(a) Recovery Time Objective (RTO)

- The maximum acceptable length of time that a system, application, or process can be down after a failure or disaster without causing signifi cant damage to the business.
- Purpose of RTO: It sets a target for how quickly systems should be re stored.

(b) Recovery Point Objective (RPO)

- The maximum acceptable amount of data loss measured in time.
- It indicates the point in time to which data must be restored to resume acceptable operations.
- Purpose of RPO: It sets a target for how much data loss is tolerable, often dictating backup frequency.

Week 10 Summary

3. Business Continuity Planning (BCP)

- A process in IT that prepares organizations to maintain essential f unctions and recover critical systems quickly after a disruption.
- **Steps of Business Continuity Planning in IT**

1. Risk Assessment and Business Impact Analysis (BIA)

- *(a). Risk Assessment:* Identify potential risks to IT infrastructure su ch as cyberattacks, hardware failures, natural disasters, or power outages.
- *(b). Business Impact Analysis:* Determine the criticality of each IT system by analyzing the potential consequences of disruptions to t he organization.

Week 10 Summary

Steps of Business Continuity Planning in IT cont…

2. Strategy Development

- **(a) Determine Recovery Strategies:** Based on BIA findings, identify sp ecific strategies to recover and maintain IT operations. The strategies in clude;
- *Redundant Systems:* Set up failover servers or cloud-based backups to ensure critical applications remain available.
- *Data Backups:* Regularly back up data, ideally to off-site or cloud storag e, and defining backup frequency based on RPO requirements.
- *Alternate Communication Channels:* Ensure alternative methods for tea m communication during disruptions, such as dedicated phone lines or s atellite communication.
- **(b) Identify Resource Requirements:**
- List the necessary hardware, software, and personnel needed to suppor t the recovery strategy to ensure quick deployment and minimize resour ce shortages.

Week 10 Summary

Steps of Business Continuity Planning in IT cont…

3. Plan Development

(a) Create a Business Continuity Document Plan:

- The BCP document plan details specific steps for responding to differ ent types of incidents.

  The BCP plan must include;

- *Activation Procedures:* Must have the criteria and instructions for whe n and how to activate the BCP.
- *Step-by-Step Recovery Procedures*: It should have detailed processes for recovering each critical system,
- *Roles and Responsibilities*: It must assign specific roles to staff, such as IT managers, data recovery specialists, etc

(b) Vendor Coordination:

- Identify key vendors and partners critical to IT operations, such as clo ud providers or telecommunications.

Week 10 Summary

Steps of Business Continuity Planning in IT cont…

4. Testing and Training

(a) Plan testing:

- Conduct regular testing to verify the effectiveness of the BCP e.g;
- *Tabletop Exercises:* Simulated discussions with key personnel to te st their actions in incident scenarios.
- *Full Drills:* Testing actual procedures in a controlled environment to verify that all systems can be restored within RTO and RPO targets.

(b) Employee training

- Ensure all relevant personnel are aware of the BCP and trained in t heir specific roles.
- Regularly update training to ensure readiness as systems or roles c hange within the organization..

Week 10 Summary

Steps of Business Continuity Planning in IT cont…

5. Maintenance and Review

- *(a). Do continuous Updates;*
- Regularly update the BCP to reflect changes in the IT environment, such as new applications, updated hardware, or revised recovery requirements.
- *(b). Post-Incident Review;*
- After any disruption, review the plan's effectiveness and adjust based on lessons learned to strengthen the approach for future incidents.

Week 10 Summary

4. Disaster Recovery Planning (DRP)

- A focused part of Business Continuity Planning (BCP) in IT that co ncentrates on restoring IT infrastructure, systems, and data acces s after a disruption.
- **Steps of the Disaster Recovery Planning process in IT:**

1. Identify the Risk and Impact Analysis

- **(a)** *Risk Assessment:* Identify the range of potential risks that coul d impact IT infrastructure, such as natural disasters, cyberattacks, system failures, or power outages.
- This step assesses the likelihood and potential impact of each thre at on IT systems.

Week 10 Summary

Steps of the Disaster Recovery Planning process in IT cont..

Step 1 cont….Risk and Impact Analysis continued…

- *(b) Business Impact Analysis (BIA):* Evaluate the impact of disru ptions on different systems and processes by determining the;
- *Recovery Time Objective (RTO):* The maximum acceptable dow ntime for each system, guiding how quickly each component ne eds to be restored.
- *Recovery Point Objective (RPO):* The maximum data loss in ter ms of time, informing the frequency of backups needed to keep data losses within an acceptable limit.

Week 10 Summary

Steps of Disaster Recovery in IT cont…

2. Setting Recovery Strategies

- **(a) Define Recovery Priorities:** Based on RTO and RPO values, p rioritize systems by criticality, starting with essential applications an d data.
- **(b) Perform Backup and Data Replication**
- *Regular Backups*: Schedule regular data backups, considering stor age at secure off-site or cloud locations to protect against site-speci fic disasters.
- *Real-Time Replication:* For high-priority systems, employ real-time replication or continuous data protection, ensuring the most recent data is available for recovery.

Week 10 Summary

Steps Disaster Recovery Planning in IT cont…

3. Develop the Disaster Recovery Plan Document

- *Define Step-by-Step Recovery Procedures:*
- Create detailed instructions for restoring systems and data.
- *Set Roles and Responsibilities:* Define specific responsibilities for key personnel involved in the recovery process.
- *Define Communication Protocols:* Establish clear internal and exte rnal communication guidelines.
- *Carry out Vendor and Partner Coordination*: Document contact inf ormation and procedures for vendors (e.g. Cloud providers.

Week 10 Summary

Steps of Disaster Recovery Planning in IT cont…

4. Testing and Training

- **(a) Perform Regular DR Testing:**
  - *Tabletop Exercises*: Scenario-based discussions with relevant staff on how they would respond to disasters, helping teams to understand their roles and responsibilities.
  - *Simulated Drills:* Conduct full or partial recovery simulations, such as data recovery exercises or failover drills to test the readiness of the DRP.
- **(b) Perform Staff Training:** Train IT staff and relevant employees on their roles and recovery procedures.

Week 10 Summary

Steps of Disaster Recovery Planning in IT cont…

5. Continuous Improvement and Maintenance

- *Regular Plan Updates:* Update the DRP to incorporate IT changes e.g, adding new applications, implementing security updates, or m odifying system configurations may require revisions.
- *Post-Incident Review:* Conduct a review to identify what worked w ell and what needs to be improved after any incident.

Week 10 Summary

5. Testing and Maintaining Business Continuity Plans (BCP)

- Testing and Maintaining Business Continuity Plans (BCP) and Dis aster Recovery Plans (DRP) are essential activities to ensure that these plans are effective and up-to-date.

6. Goals of Testing the BCP and DRP

- *To validate Assumptions:* Testing helps to confirm whether assum ptions in the BCP and DRP are accurate.
- *To assess Recovery Time and Recovery Point Objectives* ensures that the recovery processes meet the targeted RTO and RPO
- *To enhance Preparedness and Confidence: B*uilds confidence and ensures that staff are trained, equipped, and ready to act during a real incident.

Week 10 Summary

7. Testing BCP and DRP in IT

- A structured process to validate that BCP and DRP will perform as expected during an actual disruption.

Types of Tests;

- *Tabletop Exercises;* Involve a simulation in which key staff members discuss their responses to a disaster scenario.
- *Walkthroughs: E*mployees go through the plan step-by-step to ensure they understand each part and identify missing elements or procedural issues.
- *Simulation Drills:* simulating specific disaster scenarios (like cyber attacks or server failures) to test recovery strategies.
- *Full-Scale Testing:* Full-scale tests involve testing all or major parts of the BCP and DRP, including backup sites, alternate communication channels, and recovery of critical systems.

Week 10 Summary

8. Maintaining BCP and DRP in IT

- Involves regularly updating the Business Continuity and Disaster Recovery plans to ensures the plans remain relevant and effective over time.

Maintenance Activities include;

- *Review and Update Procedures:* IT systems, applications, and infr astructure evolve over time, necessitating periodic reviews
- *Incorporate Organizational Changes* update the BCP and DRP to reflect current team structures and responsibilities.
- *Perform Vendor and Partner Coordination:* maintain up-to-date co ntact information and verify the vendor's disaster recovery capabili ties.
- *Post-Incident Review and Lessons Learned*:, lessons learned afte r BCP or DRP is activated can be incorporated to enhance future r esponse effectiveness.

Week 10 Summary

9. Frequency of Maintenance

- *Regularly Scheduled Updates:*
- *After Significant Changes*.
- *Following Each Test or Real Incident*:

10. Benefits of Testing and Maintaining BCP and DRP

- *Preparedness:*
- *Plan Effectiveness:*
- *Regulatory Compliance:*

References

- *"Business Continuity and Disaster Recovery Planning for IT Professionals" (2nd Edition) by Susan Snedaker, published by Syngress in 2014.*
- *"Disaster Recovery and Business Continuity" (3rd Edition) by Thejendra BS, also published by O'Reilly in 2014.*
- *Business Continuity and Disaster Recovery for InfoSec Managers" by John Rittinghouse and James Ransome, published by Butterworth-Heinemann in 2011.*
- *Principles of Business Continuity and Disaster Recovery" by Philip Jan Rothstein, published by Rothstein Publishing in 2020.*
- *IT Disaster Recovery Planning for Dummies" by Peter H. Gregory, published by For Dummies in 2010*

End of Week 10

NEXT LECTURE we will look @

Week 11: Compliance and Regulatory Issues

See u There!