

Certificate in IT Disaster Recovery Planning (CITDRP)

Course outline

Module 1: Introduction to Disaster Recovery Planning

Module 1: Introduction to Disaster Recovery Planning is the first module of the Certificate in IT Disaster Recovery Planning (CITDRP) course. It provides an overview of the fundamentals of disaster recovery planning, including the importance of planning, the components of a disaster recovery plan, and the steps involved in developing a plan. It also covers the roles and responsibilities of key stakeholders in the disaster recovery process.

Lessons

- Overview of Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Disaster Recovery Strategies
- Disaster Recovery Technologies
- Disaster Recovery and Business Continuity
- Disaster Recovery and Data Protection
- Disaster Recovery and Cloud Computing
- Disaster Recovery and Security

After completing this module, students will be able to:

- Understand the fundamentals of disaster recovery planning and the importance of having a plan in place.
- Identify the key components of a disaster recovery plan and the steps involved in developing one.
- Develop an understanding of the different types of disasters and their potential impacts on an organization.
- Learn how to assess the risks associated with disasters and develop strategies to mitigate them.

Module 2: Risk Assessment and Business Impact Analysis

Module 2 of the Certificate in IT Disaster Recovery Planning (CITDRP) course focuses on risk assessment and business impact analysis. This module provides an overview of the risk assessment process, including identifying and assessing risks, developing risk mitigation strategies, and developing a business impact analysis. It also covers the importance of developing a comprehensive disaster recovery plan and the steps involved in creating one.

Lessons

- Understanding Risk Assessment and Business Impact Analysis
- Identifying and Assessing Risk Factors
- Developing Risk Mitigation Strategies
- Establishing Risk Management Policies
- Implementing Risk Management Processes
- Evaluating Risk Management Performance
- Developing Business Impact Analysis
- Establishing Business Continuity Plans
- Implementing Business Continuity Plans
- Testing and Maintaining Business Continuity Plans

After completing this module, students will be able to:

- Understand the importance of risk assessment and business impact analysis in IT disaster recovery planning.
- Develop an effective risk assessment and business impact analysis process.
- Identify potential risks and their impacts on the organization.
- Develop strategies to mitigate risks and reduce their impacts on the organization.

Module 3: Developing a Disaster Recovery Plan

Module 3 of the Certificate in IT Disaster Recovery Planning (CITDRP) course focuses on developing a comprehensive disaster recovery plan. It covers topics such as risk assessment, business continuity planning, data backup and recovery, and disaster recovery testing. Students will learn how to create a plan that meets the needs of their organization and how to implement it in the event of a disaster.

Lessons

- Understanding Disaster Recovery Planning
- Identifying Critical Systems and Data
- Developing a Risk Assessment
- Establishing Recovery Objectives
- Developing a Business Impact Analysis
- Developing a Disaster Recovery Strategy
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Implementing the Disaster Recovery Plan
- Evaluating the Disaster Recovery Plan

After completing this module, students will be able to:

- Understand the importance of developing a comprehensive disaster recovery plan.
- Identify the components of a disaster recovery plan and the steps necessary to create one.
- Develop a plan to ensure the continuity of operations in the event of a disaster.

- Implement strategies to test and maintain the disaster recovery plan.

Module 4: Testing and Maintenance of the Disaster Recovery Plan

Module 4 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the testing and maintenance of the Disaster Recovery Plan. It provides an overview of the different types of tests that can be used to evaluate the effectiveness of the plan, as well as the steps necessary to maintain the plan over time. The module also covers the importance of regularly reviewing the plan and making necessary updates to ensure that it remains up-to-date and effective.

Lessons

- Testing the Disaster Recovery Plan
- Maintenance of the Disaster Recovery Plan
- Documenting the Disaster Recovery Plan
- Evaluating the Disaster Recovery Plan
- Implementing the Disaster Recovery Plan
- Troubleshooting the Disaster Recovery Plan
- Monitoring the Disaster Recovery Plan
- Updating the Disaster Recovery Plan
- Auditing the Disaster Recovery Plan
- Training Staff on the Disaster Recovery Plan

After completing this module, students will be able to:

- Understand the importance of testing and maintaining a Disaster Recovery Plan.
- Develop a comprehensive testing and maintenance plan for a Disaster Recovery Plan.
- Identify and evaluate potential risks and threats to the Disaster Recovery Plan.
- Implement strategies to ensure the Disaster Recovery Plan is up-to-date and effective.

Module 5: Disaster Recovery Strategies

Module 5 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the strategies and techniques for disaster recovery planning. It covers topics such as risk assessment, business continuity planning, disaster recovery planning, and testing and implementation. It also provides an overview of the different types of disaster recovery strategies and how to select the most appropriate one for a given organization.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Disaster Recovery Strategies
- Disaster Recovery Technologies
- Disaster Recovery and Business Continuity

- Disaster Recovery and Cloud Computing
- Disaster Recovery and Data Backup
- Disaster Recovery and Data Security

After completing this module, students will be able to:

- Develop a comprehensive disaster recovery plan that meets the organization's specific needs.
- Identify and assess potential risks and threats to the organization's IT infrastructure.
- Implement strategies to protect the organization's data and systems from disasters.
- Evaluate the effectiveness of the disaster recovery plan and make necessary adjustments.

Module 6: Backup and Recovery Solutions

Module 6 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of backup and recovery solutions. It provides an overview of the different types of backup and recovery solutions available, as well as the best practices for implementing them. It also covers the importance of testing and validating backups, and how to develop a comprehensive backup and recovery plan.

Lessons

- Understanding Backup and Recovery Strategies
- Types of Backup and Recovery Solutions
- Planning and Implementing Backup and Recovery Solutions
- Testing and Validating Backup and Recovery Solutions
- Troubleshooting Backup and Recovery Solutions
- Disaster Recovery Planning and Backup and Recovery Solutions
- Cloud Backup and Recovery Solutions
- Automating Backup and Recovery Solutions
- Security Considerations for Backup and Recovery Solutions
- Best Practices for Backup and Recovery Solutions

After completing this module, students will be able to:

- Understand the importance of backup and recovery solutions in IT disaster recovery planning.
- Develop strategies for implementing backup and recovery solutions.
- Analyze the different types of backup and recovery solutions available.
- Implement backup and recovery solutions to ensure data protection and business continuity.

Module 7: Data Protection and Security

Module 7 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers data protection and security. It provides an overview of the different types of data protection and security measures that can be implemented to protect data and systems from malicious attacks. It also covers topics such as encryption, authentication, access control, and data backup and recovery. The module also provides an introduction to the legal and regulatory requirements for data protection and security.

Lessons

- Introduction to Data Protection and Security
- Understanding Data Protection Regulations
- Risk Assessment and Management
- Data Encryption and Access Control
- Network Security and Firewalls
- Disaster Recovery Planning
- Business Continuity Planning
- Data Backup and Recovery
- Auditing and Monitoring
- Incident Response and Management

After completing this module, students will be able to:

- Understand the importance of data protection and security in IT disaster recovery planning.
- Develop strategies to protect data from unauthorized access and malicious attacks.
- Implement data security measures to ensure the integrity and confidentiality of data.
- Monitor and audit data security systems to ensure compliance with industry standards and regulations.

Module 8: Cloud Computing and Disaster Recovery

Module 8 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of cloud computing and disaster recovery. It provides an overview of cloud computing, its benefits and challenges, and how it can be used to create a disaster recovery plan. It also covers the different types of cloud services, cloud security, and how to develop a cloud-based disaster recovery plan.

Lessons

- Introduction to Cloud Computing
- Cloud Computing Security
- Cloud Computing Architecture
- Cloud Computing Services
- Cloud Computing Deployment Models
- Disaster Recovery Planning
- Disaster Recovery Strategies
- Disaster Recovery Testing
- Disaster Recovery Implementation
- Disaster Recovery Automation
- Disaster Recovery as a Service
- Business Continuity Planning
- Business Impact Analysis
- Risk Management
- Data Backup and Recovery
- Cloud Backup Solutions
- Cloud Disaster Recovery Solutions
- Cloud Migration Strategies

- Cloud Security Best Practices
- Cloud Compliance and Auditing

After completing this module, students will be able to:

- Understand the fundamentals of cloud computing and its various components.
- Develop a comprehensive disaster recovery plan for cloud-based systems.
- Implement best practices for cloud-based disaster recovery.
- Analyze the risks associated with cloud-based disaster recovery and develop strategies to mitigate them.

Module 9: Network and System Recovery

Module 9 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of network and system recovery. It provides an overview of the different types of network and system recovery strategies, as well as the tools and techniques used to implement them. It also covers the steps involved in planning and executing a successful recovery process.

Lessons

- Understanding Network and System Recovery Strategies
- Developing a Network and System Recovery Plan
- Implementing Network and System Recovery Procedures
- Testing Network and System Recovery Plans
- Troubleshooting Network and System Recovery Issues
- Managing Network and System Recovery Resources
- Evaluating Network and System Recovery Performance
- Documenting Network and System Recovery Processes
- Developing Network and System Recovery Policies
- Understanding Network and System Recovery Technologies

After completing this module, students will be able to:

- Understand the principles of network and system recovery, including the importance of backup and recovery strategies.
- Develop a plan for recovering a network and system in the event of a disaster.
- Implement a network and system recovery plan, including the use of backup and recovery tools.
- Monitor and evaluate the effectiveness of the network and system recovery plan.

Module 10: Disaster Recovery for Virtualized Environments

Module 10 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for virtualized environments. It provides an overview of the different types of virtualization technologies, the challenges associated with disaster recovery in virtualized environments, and best practices for designing and implementing a successful disaster recovery plan. The module also covers the importance of testing and monitoring the disaster recovery plan, as well as the different types of backup and recovery strategies available.

Lessons

- Understanding Disaster Recovery Strategies for Virtualized Environments
- Developing a Disaster Recovery Plan for Virtualized Environments
- Implementing Backup and Recovery Solutions for Virtualized Environments
- Testing and Validating Disaster Recovery Plans for Virtualized Environments
- Managing Disaster Recovery for Virtualized Environments
- Automating Disaster Recovery for Virtualized Environments
- Disaster Recovery for Cloud-Based Virtualized Environments
- Disaster Recovery for Hybrid Virtualized Environments
- Disaster Recovery for Containers and Serverless Computing
- Disaster Recovery for Multi-Tenant Virtualized Environments

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning for virtualized environments.
- Develop a comprehensive disaster recovery plan for virtualized environments.
- Implement a disaster recovery plan for virtualized environments.
- Monitor and maintain a disaster recovery plan for virtualized environments.

Module 11: Disaster Recovery for Mobile Devices

Module 11 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for mobile devices. It covers topics such as mobile device backup and recovery, mobile device security, and mobile device management. It also provides an overview of the different types of mobile devices and their associated risks. Finally, it provides guidance on how to develop a comprehensive disaster recovery plan for mobile devices.

Lessons

- Understanding Mobile Device Disaster Recovery Strategies
- Developing a Mobile Device Disaster Recovery Plan
- Implementing Mobile Device Disaster Recovery Procedures
- Testing and Evaluating Mobile Device Disaster Recovery Plans
- Managing Mobile Device Disaster Recovery Resources
- Troubleshooting Mobile Device Disaster Recovery Issues
- Best Practices for Mobile Device Disaster Recovery
- Mobile Device Disaster Recovery in the Cloud
- Mobile Device Disaster Recovery in the Enterprise
- Mobile Device Disaster Recovery in the Home Environment

After completing this module, students will be able to:

- Understand the importance of mobile device disaster recovery planning and the steps involved in the process.
- Develop a comprehensive mobile device disaster recovery plan that meets the needs of the

organization.

- Implement a mobile device disaster recovery plan that is tailored to the organization's specific needs.
- Monitor and evaluate the effectiveness of the mobile device disaster recovery plan on an ongoing basis.

Module 12: Disaster Recovery for Databases

Module 12 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for databases. It provides an overview of the different types of databases, the importance of database backups, and the steps necessary to ensure successful recovery of databases in the event of a disaster. It also covers the different strategies for database recovery, such as replication, clustering, and log shipping.

Lessons

- Understanding Database Disaster Recovery Planning
- Database Backup Strategies
- Database Replication and High Availability
- Database Recovery Techniques
- Database Recovery Testing
- Database Recovery Planning and Documentation
- Database Recovery Automation
- Database Recovery in the Cloud
- Database Recovery in Virtualized Environments
- Database Recovery in Multi-site Environments
- Database Recovery in Hybrid Environments
- Database Recovery in Containers
- Database Recovery in DevOps Environments
- Database Recovery in Big Data Environments
- Database Recovery in IoT Environments
- Database Recovery in AI/ML Environments
- Database Recovery in Blockchain Environments
- Database Recovery in Edge Computing Environments
- Database Recovery in Multi-Cloud Environments
- Database Recovery in Hybrid Cloud Environments

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning for databases.
- Develop a comprehensive disaster recovery plan for databases.
- Implement a disaster recovery plan for databases.
- Monitor and test the disaster recovery plan for databases.

Module 13: Disaster Recovery for Applications

Module 13 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals

of disaster recovery for applications. It provides an overview of the different types of application disaster recovery strategies, including backup and restore, replication, and high availability. It also covers the steps involved in planning and implementing an effective application disaster recovery plan.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Disaster Recovery Strategies for Applications
- Disaster Recovery Strategies for Databases
- Disaster Recovery Strategies for Network Infrastructure
- Disaster Recovery Strategies for Storage
- Disaster Recovery Strategies for Virtualization
- Disaster Recovery Strategies for Cloud Computing
- Disaster Recovery Strategies for Mobile Applications
- Disaster Recovery Strategies for Web Applications
- Disaster Recovery Strategies for Security
- Disaster Recovery Strategies for Compliance
- Disaster Recovery Strategies for Business Continuity
- Disaster Recovery Strategies for Data Protection
- Disaster Recovery Strategies for System Monitoring
- Disaster Recovery Strategies for Automation
- Disaster Recovery Strategies for Automated Testing
- Disaster Recovery Strategies for Automated Deployment

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning and the importance of having a comprehensive plan in place.
- Develop a strategy for recovering applications and data in the event of a disaster.
- Identify the key components of a disaster recovery plan and the steps necessary to implement it.
- Utilize best practices for testing and maintaining a disaster recovery plan.

Module 14: Disaster Recovery for Storage

Module 14: Disaster Recovery for Storage is a module in the Certificate in IT Disaster Recovery Planning (CITDRP) course. It covers the fundamentals of storage disaster recovery planning, including the different types of storage, the importance of data protection, and the steps to take to ensure successful recovery. It also covers the different types of storage technologies, the importance of data replication, and the different strategies for storage disaster recovery.

Lessons

- Understanding Disaster Recovery Strategies for Storage
- Developing a Disaster Recovery Plan for Storage
- Implementing Disaster Recovery Solutions for Storage

- Testing and Maintaining Disaster Recovery for Storage
- Disaster Recovery for Cloud Storage
- Disaster Recovery for Virtual Storage
- Disaster Recovery for SAN Storage
- Disaster Recovery for Tape Storage
- Disaster Recovery for Object Storage
- Disaster Recovery for RAID Storage

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning for storage systems.
- Develop strategies for protecting data stored on storage systems.
- Implement backup and recovery procedures for storage systems.
- Monitor and test storage system disaster recovery plans.

Module 15: Disaster Recovery for Networks

Module 15 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for networks. It provides an overview of the different types of network disasters, the steps to take to prepare for them, and the strategies for recovering from them. It also covers the importance of having a comprehensive disaster recovery plan in place and the different components of such a plan.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Network Design for Disaster Recovery
- Network Security and Disaster Recovery
- Network Backup and Recovery Strategies
- Network Monitoring and Testing
- Disaster Recovery Testing and Documentation
- Disaster Recovery Strategies for Cloud Computing
- Disaster Recovery Strategies for Virtualization
- Disaster Recovery Strategies for Mobile Devices
- Disaster Recovery Strategies for VoIP
- Disaster Recovery Strategies for Storage Area Networks
- Disaster Recovery Strategies for Wide Area Networks
- Disaster Recovery Strategies for Local Area Networks

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning and the importance of having a comprehensive plan in place.
- Develop a strategy for recovering from a network disaster, including identifying critical systems and data, and determining the best methods for restoring them.

- Implement a network disaster recovery plan, including testing and validating the plan.
- Monitor and maintain the disaster recovery plan to ensure it is up-to-date and effective.

Module 16: Disaster Recovery for Business Continuity

Module 16 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for business continuity. It provides an overview of the different types of disasters, the importance of having a disaster recovery plan, and the steps necessary to create and implement a successful plan. It also covers the different types of recovery strategies, the roles and responsibilities of the disaster recovery team, and the tools and techniques used to ensure a successful recovery.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Disaster Recovery Strategies
- Disaster Recovery Technologies
- Disaster Recovery and Business Continuity
- Disaster Recovery and Cloud Computing
- Disaster Recovery and Data Backup
- Disaster Recovery and Data Security
- Disaster Recovery and Network Security
- Disaster Recovery and System Security
- Disaster Recovery and Network Design
- Disaster Recovery and System Administration
- Disaster Recovery and Data Center Management
- Disaster Recovery and Business Continuity Planning

After completing this module, students will be able to:

- Develop a comprehensive disaster recovery plan for an organization.
- Identify and assess potential risks and threats to an organization's IT infrastructure.
- Implement strategies to ensure business continuity in the event of a disaster.
- Evaluate the effectiveness of disaster recovery plans and make necessary adjustments.

Module 17: Disaster Recovery for Cloud Computing

Module 17 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for cloud computing. It provides an overview of the different types of cloud computing, the risks associated with cloud computing, and the strategies and best practices for disaster recovery in the cloud. The module also covers the importance of data backup and recovery, as well as the different types of cloud-based disaster recovery solutions.

Lessons

- Understanding Cloud Computing Disaster Recovery
- Developing a Cloud Computing Disaster Recovery Plan
- Implementing Cloud Computing Disaster Recovery Strategies
- Testing and Evaluating Cloud Computing Disaster Recovery Plans
- Managing Cloud Computing Disaster Recovery
- Business Continuity Planning for Cloud Computing
- Risk Management for Cloud Computing Disaster Recovery
- Security Considerations for Cloud Computing Disaster Recovery
- Cloud Computing Disaster Recovery Best Practices
- Troubleshooting Cloud Computing Disaster Recovery Issues

After completing this module, students will be able to:

- Understand the fundamentals of disaster recovery planning for cloud computing environments.
- Develop a comprehensive disaster recovery plan for cloud computing environments.
- Implement and test disaster recovery plans for cloud computing environments.
- Monitor and maintain disaster recovery plans for cloud computing environments.

Module 18: Disaster Recovery for Security

Module 18 of the Certificate in IT Disaster Recovery Planning (CITDRP) course focuses on disaster recovery for security. It covers topics such as security threats, risk assessment, security policies, and security controls. It also provides guidance on how to develop a comprehensive security plan for disaster recovery.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Disaster Recovery Strategies
- Disaster Recovery and Business Continuity
- Security Considerations for Disaster Recovery
- Disaster Recovery and Cloud Computing
- Disaster Recovery and Data Backup
- Disaster Recovery and Data Protection

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning and the importance of security in the process.
- Develop a comprehensive disaster recovery plan that includes security measures.
- Implement security measures to protect data and systems from potential disasters.
- Monitor and test the disaster recovery plan to ensure its effectiveness.

Module 19: Disaster Recovery for Compliance

Module 19 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of disaster recovery for compliance. It provides an overview of the legal and regulatory requirements for disaster recovery planning, as well as best practices for developing and implementing a compliant disaster recovery plan. The module also covers the importance of testing and monitoring the plan, and how to ensure that the plan is kept up to date.

Lessons

- Understanding Disaster Recovery Regulations and Compliance Requirements
- Developing a Disaster Recovery Plan
- Implementing Disaster Recovery Procedures
- Testing and Maintaining Disaster Recovery Plans
- Disaster Recovery Strategies for Business Continuity
- Risk Management and Disaster Recovery Planning
- Disaster Recovery Planning for Cloud Computing
- Disaster Recovery Planning for Virtualization
- Disaster Recovery Planning for Mobile Devices
- Disaster Recovery Planning for Databases
- Disaster Recovery Planning for Network Infrastructure
- Disaster Recovery Planning for Storage Systems
- Disaster Recovery Planning for Applications
- Disaster Recovery Planning for Security
- Disaster Recovery Planning for Business Processes
- Disaster Recovery Planning for Human Resources
- Disaster Recovery Planning for Financial Systems
- Disaster Recovery Planning for Telecommunications
- Disaster Recovery Planning for Third-Party Vendors
- Disaster Recovery Planning for Regulatory Compliance

After completing this module, students will be able to:

- Understand the legal and regulatory requirements for disaster recovery planning.
- Develop a comprehensive disaster recovery plan that meets the requirements of the applicable regulations.
- Implement and test the disaster recovery plan to ensure its effectiveness.
- Monitor and update the disaster recovery plan to ensure it remains compliant with the applicable regulations.

Module 20: Disaster Recovery for Auditing

Module 20 of the Certificate in IT Disaster Recovery Planning (CITDRP) course covers the fundamentals of auditing for disaster recovery. It provides an overview of the different types of audits, the audit process, and the importance of auditing for disaster recovery. It also covers the different types of audit reports and how to interpret them. Finally, it provides guidance on how to develop an effective audit plan and how to use audit results to improve disaster recovery planning.

Lessons

- Understanding Disaster Recovery Planning
- Risk Assessment and Business Impact Analysis
- Developing a Disaster Recovery Plan
- Testing and Maintaining the Disaster Recovery Plan
- Auditing the Disaster Recovery Plan
- Disaster Recovery Strategies
- Disaster Recovery Technologies
- Disaster Recovery and Business Continuity
- Disaster Recovery and Data Protection
- Disaster Recovery and Cloud Computing

After completing this module, students will be able to:

- Understand the principles of disaster recovery planning and the importance of auditing.
- Develop an understanding of the different types of disasters and their impact on IT systems.
- Identify the key components of a disaster recovery plan and the steps necessary to implement it.
- Develop the skills to audit a disaster recovery plan and identify areas of improvement.