Milestone 6: Backup, Restore, and Disaster Recovery

Objective:

The purpose of backup and restore systems in an enterprise environment is to protect critical data and ensure business continuity in the event of data loss, system failures, disasters, or human error. Some key reasons for having such a system include:

1. Data protection and recovery
2. Business continuity
3. Compliance and legal requirements
4. Disaster recovery
5. Version control and historical data
6. Protection against ransomware and cyberattacks
7. Peace of mind and risk mitigation
8. System upgrades and migrations

Disaster recovery is of paramount importance for organizations of all sizes and types. It refers to the process and set of strategies and procedures put in place to recover and restore critical business operations after a significant disruptive event, such as a natural disaster, cyberattack, equipment failure, power outage, or any other event that can cause significant data loss or downtime. The importance of disaster recovery can be summarized as follows:

Disaster recovery is not just a reactive measure; it is a proactive strategy that enables organizations to prepare for unforeseen events, protect their assets, and ensure business continuity in the face of adversity. It is a crucial component of a comprehensive risk management and business continuity plan.

Instructions:

It is recommended that you consult with a TA to ensure that your policy meets the requirements.

Step 1: Backup Policy

If you already have a backup policy that covers the points below, you can go to step 2. If not create or update it to cover all the points. Make sure to also justify your decisions/ reasoning

1. Data retention
2. Frequency of backups
3. Backup types
4. Storage media
5. Off-site backups
6. Encryption and security
7. Testing and verification
8. Backup automation

9. Monitoring and alerts
10. Documentation and documentation review
11. Scalability and growth
12. Compliance and regulatory requirements
13. Disaster recovery planning
14. Regular review and testing

Remember, a well-defined backup policy should align with your organization's needs and risk tolerance. It should strike a balance between data protection, cost, and operational efficiency while considering any industry-specific requirements.

Step 2: Implementation

Designate one or more of your servers as the backup server that will contain the backups of all other VMs.

Some of the solutions you may want to consider are:

There are several open-source and free enterprise backup solutions available that can meet your backup needs. Here are a few popular options:

1. Bacula
2. Amanda
3. Duplicati
4. Veeam Backup & Replication Community Edition
5. Clonezilla
6. UrBackup
7. Bareos

These solutions vary in terms of features, scalability, and complexity, so it's important to evaluate them based on your specific requirements. Additionally, make sure to review the licensing terms and any potential limitations or restrictions that may apply.

Step 3 - Disaster Recovery Plan

A comprehensive Disaster Recovery (DR) plan should address various aspects of an organization's operations to ensure business continuity in the event of a disaster. Here is a list of key elements that should be included in a well-rounded DR plan:

1. Risk Assessment and Business Impact Analysis
2. Recovery Objectives and Priorities
3. Roles and Responsibilities
4. Contact Information
5. Data Backup and Restoration Procedures
6. Disaster Recovery Site
7. Hardware and Software Inventory
8. Network Infrastructure

9. Application Recovery Procedures
10. Testing and Maintenance
11. Training and Awareness
12. Vendor and Supplier Contingency Plans
13. Financial and Legal Considerations
14. Emergency Response Procedures
15. Incident Reporting and Escalation
16. Communication Plan
17. Post-Recovery Evaluation

Remember that each organization's DR plan will vary based on its specific needs, industry, size, and the criticality of its operations. Regular updates and reviews of the plan are essential to ensure its relevance and effectiveness in addressing potential threats and disasters.

Submission Requirements

- [ ] 30 Points - A backup policy that contains all 14 points
- [ ] 40 Points - You can backup and restore your machines to the specifications in your policy
- [ ] 30 Points - Disaster Recovery Plan