**Azure Disaster Recovery Plan (DRP) Template**

**1. Introduction**

**Purpose:**

This document outlines the Disaster Recovery Plan (DRP) for maintaining business continuity of critical services hosted in Azure. The plan ensures quick recovery from disasters like natural calamities, cyber-attacks, or hardware failures, minimizing operational downtime and data loss.

**Scope:**

The DRP covers all mission-critical applications, databases, and infrastructure deployed in Azure. This includes multi-region applications, databases, virtual machines (VMs), and networking configurations.

**2. Risk Assessment**

**Potential Risks**

1. **Regional Azure Outage:  
   *Example*:** An entire Azure region (e.g., East US) becomes unavailable due to a natural disaster or power outage.
   * Impact: Services in the affected region will be unavailable, impacting all hosted workloads.
   * Mitigation: Enable cross-region replication using Azure Site Recovery (ASR) and Geo-Redundant Storage (GRS).
2. **Cyberattacks:  
   *Example*:** A ransomware attack encrypts key databases and storage accounts.
   * Impact: Data and applications are inaccessible, potentially leading to compliance violations.
   * Mitigation: Implement encryption for data at rest, regular vulnerability scanning, and immutable backups.
3. **Human Errors:  
   *Example*:** Accidental deletion of production resources or misconfiguration of key services.
   * Impact: Service disruption or downtime due to configuration issues.
   * Mitigation: Use role-based access control (RBAC), soft delete for resources, and policy enforcement with Azure Policy.

**Impact Analysis Table**

| **Risk** | **Likelihood** | **Impact** | **Mitigation** |
| --- | --- | --- | --- |
| **Regional Outage** | **Medium** | **Critical** | **Cross-region replication and traffic routing policies.** |
| **Ransomware Attack** | **Low** | **High** | **Immutable backups, endpoint protection, and multi-factor authentication (MFA).** |
| **Human Error** | **High** | **Moderate** | **Role-based access control, auditing, and automated deployment pipelines.** |

**3. Recovery Objectives**

**Recovery Time Objective (RTO):**

Maximum acceptable downtime for critical services:

* Tier 1 Applications: 15 minutes
* Tier 2 Applications: 1 hour

**Recovery Point Objective (RPO):**

Maximum tolerable data loss:

* Databases: 5 minutes
* File Storage: 10 minutes

**4. Roles and Responsibilities**

**Key Stakeholders:**

* **Disaster Recovery Coordinator:** Oversees DR execution and testing.
* **IT Operations Team:** Executes failover and failback processes.
* **Support Team:** Communicates with customers and stakeholders during outages.
* **Security Team:** Ensures data integrity and compliance during recovery.

**5. Replication Strategy**

**Azure Services:**

* **Azure Site Recovery (ASR):**
  + Replicate Azure VMs across regions.
  + Replicate on-premises VMs to Azure.
* **Database Replication:**
  + SQL Database with active geo-replication.
  + Cosmos DB configured with multi-region writes.
* **Storage Replication:**
  + Enable Geo-Redundant Storage (GRS) for critical data.

**6. Failover and Failback Procedures**

**Failover Steps:**

1. Log into the Azure Portal.
2. Navigate to the Recovery Services Vault.
3. Select the replicated resource and trigger failover.
4. Verify service availability in the secondary region.

**Failback Steps:**

1. Restore primary region operations after the issue is resolved.
2. Reverse replicate resources to the primary region.
3. Validate data integrity and application performance.

**7. Backup Strategy**

**Azure Backup Policies:**

* **Daily Backups:**
  + Retain daily snapshots for 30 days.
* **Weekly Backups:**
  + Retain full weekly backups for 3 months.
* **Encryption:**
  + Use Azure Key Vault for backup encryption.

**8. Testing and Maintenance**

**Testing Schedule:**

* Conduct quarterly disaster recovery drills.
* Validate replication, failover, and failback processes.

**Post-Test Activities:**

* Review test outcomes with stakeholders.
* Update the DRP to address gaps or inefficiencies.

**9. Communication Plan**

**Stakeholder Updates:**

* Notify stakeholders within 15 minutes of a disaster declaration.
* Provide regular updates on recovery progress.

**Communication Channels:**

* Email, Teams, and SMS notifications.
* Public announcements through status pages.

**10. Compliance and Audit**

**Regulatory Standards:**

* Ensure compliance with GDPR, HIPAA, and other applicable regulations.

**Audit Checklist:**

* Are RTO and RPO defined and tested?
* Are backups encrypted and regularly validated?
* Is the DRP reviewed and updated annually?

**11. Appendices**

**Appendix A: Azure Resources Inventory**

* Resource Group 1: Application XYZ
  + VMs: VM1, VM2
  + Databases: SQL Database XYZ
  + Storage Accounts: StorageXYZ

**Appendix B: Contact List**

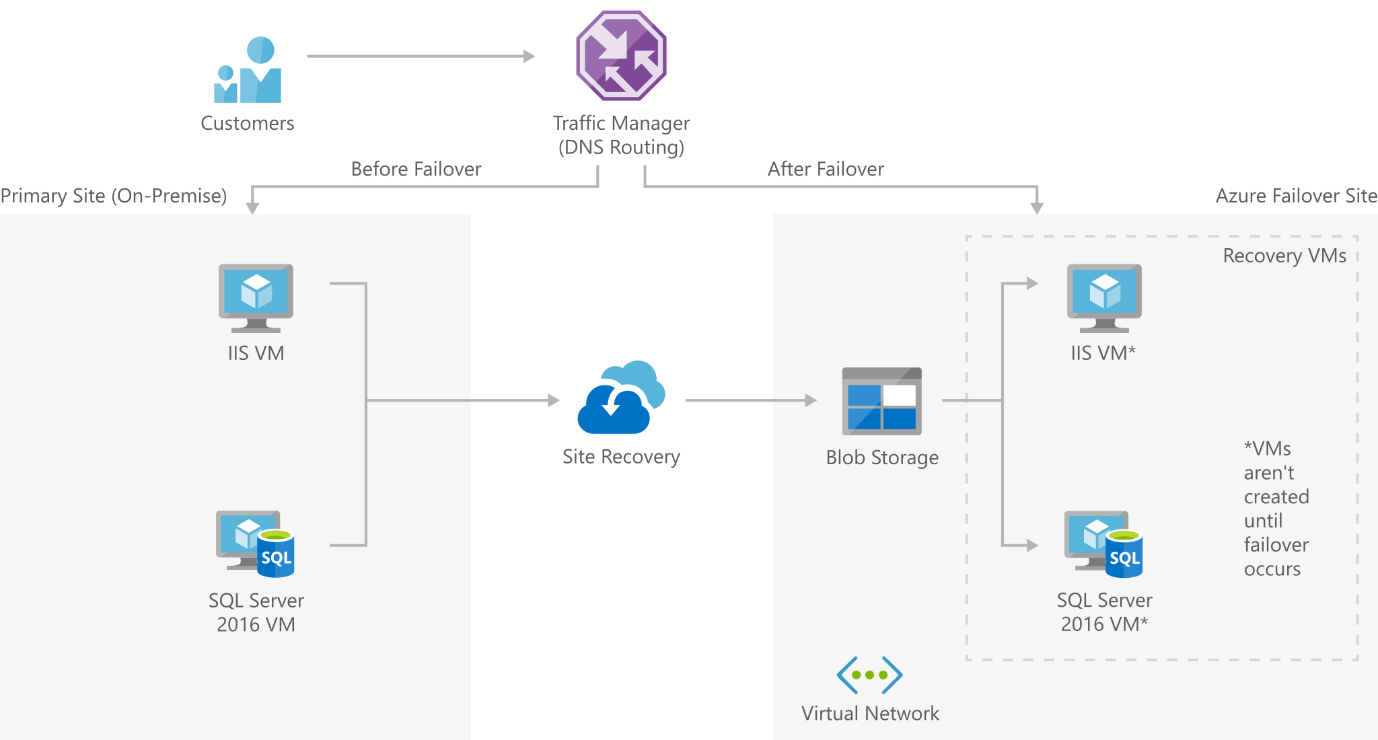
* Disaster Recovery Coordinator: Name, Email, Phone
* IT Operations Lead: Name, Email, Phone
* Security Team Lead: Name, Email, Phone

**Architecture**

**Two Solution Architectures**

**1. SMB Disaster Recovery in Azure**

Small businesses can implement disaster recovery in the cloud at low cost using partner solutions such as Double Take DR, which is based on Azure Traffic Manager, Azure Virtual Network, and Site Recovery – services that run in a patched, supported, high-availability environment. The solution architecture is illustrated below.



**Here is how the solution works:**

Traffic Manager routes DNS traffic, which can move traffic between sites based on policies that you define.

Azure Site Recovery orchestrates machine replication and manages your failback procedures’ configuration.

Virtual Network is the location of the failover site to be created during a disaster.

Blob storage allows you to store replica images of all your Site Recovery-protected machines.

**2. Enterprise-scale Disaster Recovery in Azure**

Large organizations might need to build disaster recovery capabilities for systems like SharePoint, Linux, and Dynamics CRM web servers in an on-premise datacenter. Azure provides a solution that enables failover of a complex environment to Azure infrastructure.

The solution rests on Traffic Manager, Azure Active Directory, Site Recovery, Virtual Network, and VPN Gateway. These services can run in high-availability environments that are supported and patched by Azure. The solution architecture is illustrated below.

A diagram of a software process

Description automatically generated

* **Traffic Manager** routes DNS traffic, moving traffic between sites based on policies your organization defines.
* **Azure Site Recovery** orchestrates machine replication and handles the configuration of your disaster recovery process.
* **Blob storage** contains replica images of every machine protected by Site Recovery.
* **Azure Active Directory** is a replica of your on-premise Azure Active Directory service that allows companies to authenticate and authorize cloud applications.
* **VPN Gateway** achieves communication between on-premises and cloud networks, while keeping them secure and private.
* **Virtual Network** is where a failover site is created in the event of a disaster.

**Best Practices for Azure Disaster Recovery**

**Azure Disaster Recovery Plan**

The first step is to build a disaster recovery plan, test it fully to verify its effectiveness, and then implement it. Remember to include all relevant people, technologies, and processes required to restore functionality within your service-level agreement (SLA).

Here are tips to help you create and test your disaster recovery plan:

* **Evaluation**—before creating a plan, you must evaluate the business impact of an application failure and build your recovery plan around the most critical applications and data. Determine and specify a role to own the disaster recovery plan, someone who can oversee all aspects, including testing and automation.
* **Support**—clearly define and write a process for contacting your support services and instructions for escalating issues. This document can help prevent prolonged downtime that occurs simply because the team tries to work out a recovery process on the fly. Use cross-region recovery for your mission-critical applications.
* **Automate**—your plan must include a backup strategy covering all transactional and reference data. You should test the backup restoration processes regularly. Document all processes, including manual steps, and automate as many tasks as possible.
* **Monitor**—configure alerts for all Azure services consumed by the application. Train the relevant staff to execute the plan and perform regular disaster recovery simulations to verify and improve your plan.