**Disaster Recovery Solutions Seminar**

**Part A: Response to Questions**

**1. Vendor Lock-in Issues and Mitigation**

* According to Opara-Martins et al. (2014), vendor lock-in is a significant concern in cloud-based disaster recovery solutions. The issues include:
* Proprietary Systems: Cloud vendors often use unique proprietary technologies, making it difficult for organisations to switch providers or move data elsewhere.
* High Switching Costs: Organisations that attempt to migrate to a different vendor face increased costs and operational complexities.

**Mitigation Strategies:**

* Standardisation:Use standardised data formats and technologies to ensure interoperability across multiple platforms.
* Multi-cloud Strategy: Employ a multi-cloud approach to reduce dependency on a single vendor.
* Contractual Safeguards: Establish service-level agreements (SLAs) that facilitate data migration and clearly outline exit strategies.

**2. Security Concerns with Modern Cloud DR**

Morrow et al. (2021) identify key security concerns in modern cloud-based disaster recovery systems:

* Data Breaches: Sensitive data in transit and storage can be compromised.
* Insider Threats: Cloud environments increase the potential for insider misuse.
* Inadequate Encryption: Encryption standards often vary between vendors, leaving gaps in protection.

**Mitigation Strategies:**

* End-to-End Encryption: Implement robust encryption protocols during data transit and storage.
* Access Control Policies: Enforce strict access controls and multi-factor authentication (MFA) for all users.
* Regular Security Audits: Conduct frequent audits to identify and address vulnerabilities.

**Part B: High-Level DR Solution Design**

**A screenshot of a diagram

Description automatically generated**

**Scenario 1: RPO = 1 hr, RTO = 8 hrs, High Availability Required**

This scenario demands a highly available Active-Active architecture:  
**Design Features:**

* Redundant load balancers and active-active application and database servers.
* Synchronous data replication to ensure minimal data loss.
* Shared storage with real-time failover.

**Considerations:**

* Higher costs due to maintaining active infrastructure at all times.
* Applications must support active-active configurations.

**Scenario 2: RPO = 24 hrs, RTO = 72 hrs, No High Availability Required**

This scenario supports an Active-Passive or Warm Standby solution:  
 **Design Features:**

* Secondary systems are kept in a passive state and activated during failover.
* Asynchronous replication using snapshots or log shipping.
* Cost-effective due to minimal resource utilisation in standby mode.

**Considerations:**

* Recovery processes are slower and involve manual intervention.
* Risk of data corruption during replication delays.

**Scenario 3: RPO = 5 mins, RTO = 1 hr, High Availability Required**

A Cold Standby approach is appropriate for this low-criticality scenario:  
**Design Features:**

* Reserved instances and shared storage with periodic snapshots.
* Infrastructure deployment pipelines for manual activation during failover.
* Minimal upfront costs with increased recovery times.

**Considerations:**

* Requires extensive testing of deployment scripts.
* Manual processes may delay failover and recovery.

**Conclusion**

The designs proposed align with the requirements outlined for RPO and RTO. While high-availability systems offer immediate failover capabilities, they come at a higher cost. Active-passive and cold-standby solutions provide cost-effective options but require more manual intervention. Mitigating security and vendor lock-in challenges is critical across all scenarios through encryption, access control, and adopting multi-cloud strategies.

**References**

* Morrow, T., LaPiana, V., Faatz, D., Hueca, A. & Richmond, N. (2021). Cloud Security Best Practices Derived from Mission Thread Analysis. Carnegie-Mellon Univ Pittsburgh PA.
* Opara-Martins, J., Sahandi, R., & Tian, F. (2014). Critical Review of Vendor Lock-in and Its Impact on Adoption of Cloud Computing. In International Conference on Information Society (pp. 92-97). IEEE.