**Project Overview: Cloud Data Migration & Analytics Platform**

**Project Name:** Project Aurora  
**Duration:** 12 months  
**Sponsor:** Chief Data Officer  
**Objective:**  
Migrate on-premise SQL Server databases and legacy ETL jobs into a modern Azure-based data platform to improve analytics capabilities, scalability, and integration with downstream Power BI dashboards. The platform will serve multiple business units including Finance, Operations, and Customer Experience.

**Scope:**

* Implement Azure Data Lake Gen2 for centralized data storage.
* Migrate 50+ SQL databases and 200 ETL pipelines to Azure Data Factory.
* Deploy Azure Synapse Analytics for enterprise reporting.
* Integrate data governance and metadata management via Microsoft Purview.
* Decommission legacy on-prem servers and retire redundant ETL scripts.

**Key Stakeholders:**

* Data Engineering Team
* Cybersecurity & Compliance Office
* Business Unit Data Stewards
* Cloud Infrastructure Team

**Architecture Summary:**  
Data ingestion will occur through Azure Data Factory pipelines, transforming and loading datasets into a curated Synapse layer. Authentication will rely on Azure AD with role-based access. Backup and recovery mechanisms will use Azure Recovery Vault and cross-region replication.

**Potential Risk Areas**

**📋 Compliance & Governance Risks**

* Migration may expose personal or financial data during transfer, risking non-compliance with **Australian Privacy Principles (APPs)** and **GDPR** if not encrypted in transit and at rest.
* Insufficient **data classification** or lineage tracking could lead to inaccurate reporting or breach of **corporate data retention policies**.
* Misaligned access control policies between on-prem and cloud environments may result in unauthorized data exposure.
* Lack of clear governance roles (data owner vs. steward) could weaken accountability for data quality and regulatory reporting.
* Policy documentation may lag behind rapid system changes, leading to audit findings during compliance reviews.

**🔄 Business Continuity Risks**

* Inadequate disaster recovery testing could result in prolonged downtime during major outages or ransomware events.
* Over-reliance on a single Azure region may expose operations to regional disruptions.
* Insufficient versioning or replication of critical datasets might hinder recovery point objectives (RPO/RTO) during failure scenarios.
* Legacy system decommissioning before verifying new platform stability could disrupt business-critical reporting.
* Missing incident response procedures or inadequate monitoring might delay detection of system failures or data loss.