Lab: Data Resilience Evaluation & Policy Design

Module: Data & Cyber Resilience
Duration: 2.5 Hours

Overview

In this lab, you will act as a **data resilience and governance team** responsible for evaluating an organization's data resilience maturity and developing policies to strengthen it.
Your objective is to assess data protection strategies, identify weaknesses, and design policy recommendations that enhance availability, integrity, recoverability, and governance alignment.

This lab reinforces the **Data & Cyber Resilience** module and prepares you for **DRI International certifications (ABCP, CBCP, ACRP, CCRP)** by connecting **data resilience assessment, governance integration, and framework alignment** to business continuity practices.

Scenario

You are consultants for **Orion Health Systems**, a regional healthcare technology provider that manages patient records, analytics, and real-time medical device data.

Following a small data outage last month, Orion's leadership realized that while backups existed, the company **lacks a unified data resilience policy** and standardized approach across departments.

You've been brought in to:

1. **Evaluate** Orion's current data resilience readiness.

2. **Design** a set of policy recommendations to close identified gaps.

You have **2.5 hours total**:

- 1.5 hours to assess and design your policy framework.

- 1 hour to present your findings and recommendations.
  You may use **Google** or online references to research best practices and frameworks.

Your Task

Work in **teams of 3–4** to perform a **resilience maturity evaluation and policy design exercise**.
Your deliverable is a **Google Slides presentation** summarizing your assessment and recommendations for Orion Health Systems.

Your presentation must include:

1. Data resilience maturity evaluation (current state).
2. Key gaps and risk areas.
3. Policy recommendations and governance integration.
4. Framework alignment (ISO 27001, ISO 22301, DRI).
5. Metrics and improvement roadmap.

Step 1: Conduct a Data Resilience Evaluation

Assess Orion's existing data resilience posture using the following domains:

- **Availability:** Are systems and backups accessible when needed?
- **Integrity:** Are data validation and replication processes reliable?
- **Recoverability:** Are RTOs/RPOs defined and achievable?
- **Governance:** Are policies documented, owned, and enforced?

Rate each area (1–5) based on perceived maturity and justify your scoring.

Step 2: Identify Gaps and Risks

From your evaluation, identify top weaknesses such as:

- Inconsistent backup testing
- Lack of documented recovery metrics
- Single points of failure
- Over-reliance on third-party cloud providers
- Undefined data ownership or accountability

Summarize your findings in a short **Risk & Gap Table** with impact ratings.

Step 3: Draft Policy Recommendations

Design 3–5 core **data resilience policies** to improve maturity.
Your recommendations should address:

- **Backup and replication:** Frequency, testing, offsite copies
- **Encryption and access control:** Data protection and privacy
- **Governance and accountability:** Roles, documentation, reporting
- **Testing and improvement:** Scheduled validation and updates

Frame your policies in clear, actionable language that aligns with real-world governance frameworks.

Step 4: Map to Frameworks and Standards

Align your policy recommendations to:

- **ISO 27001:** Information Security Management
- **ISO 22301:** Business Continuity Management
- **NIST SP 800-34:** Contingency Planning

- **DRI Professional Practices:** Data protection and recovery

Show how these frameworks reinforce compliance, audit readiness, and resilience maturity.

Step 5: Define Metrics and Roadmap

Establish measurable indicators and next steps:

- **RTO / RPO targets** per system
- **Backup success rate (%)**
- **Testing completion frequency**
- **Audit compliance percentage**
- **Resilience Maturity Score (1–5)**

Outline a **12-month roadmap** for policy rollout, including short-term and long-term milestones.

Step 6: Present Your Recommendations

Deliver a **10-minute presentation** that summarizes:

- Orion's current state
- Key risk areas
- Your policy recommendations
- Framework alignment and metrics
- Expected business outcomes

Each team member should present a portion of the findings.

Evaluation Criteria

Category	Description	Points
Assessment Accuracy	Clear and realistic evaluation of data resilience maturity	25
Policy Design Quality	Strong, actionable, and standards-aligned recommendations	25
Framework Alignment	Integration of ISO, NIST, and DRI practices	25
Presentation & Teamwork	Clear communication, visuals, and collaboration	25

Total: 100 points

Expected Outcome

By the end of this lab, your team will have:

- Conducted a **practical data resilience maturity assessment**.
- Created a set of **policy recommendations** aligned with frameworks.
- Developed **metrics** to measure and improve organizational resilience.
- Strengthened your understanding of **governance-driven data protection**.

Key Takeaways

- Data resilience combines governance, technology, and process.
- Policies create accountability and structure for recovery readiness.
- Metrics enable continuous improvement and maturity tracking.
- Framework alignment builds trust, compliance, and audit confidence.