SC-100 / SC-5007 Compliance Architecture Discussion Exercise

Scenario: "Project Atlas" – A FedRAMP Moderate Cloud Migration

Background

A U.S. federal civilian agency—**The Department of Infrastructure & Resilience (DIR)**—is modernizing its IT systems under a multi-year Zero Trust and cloud transformation initiative called **Project Atlas**.

DIR is migrating from an aging on-premises environment to a **multi-cloud architecture** anchored in **Microsoft 365 GCC High and Azure Government**, with several third-party SaaS platforms still in use for mission systems.

The agency must maintain **FedRAMP Moderate authorization**, comply with **FISMA**, **NARA records management requirements**, and internal **Inspector General (IG)** audit mandates.

The Data Reality (a.k.a. where things get spicy)

DIR handles a wide mix of data types:

- **Personally Identifiable Information (PII)**
    - Citizen complaints
    - Employee HR records
    - Contractor background investigations
- **Controlled Unclassified Information (CUI)**
    - Infrastructure vulnerability assessments
    - Critical facility diagrams
    - Incident response reports
- **Legal & Oversight Data**
    - Congressional correspondence
    - FOIA requests and responses
    - Litigation hold content
- **Operational Collaboration Data**

    - Teams chats during live incidents
    - SharePoint document libraries shared across agencies
    - Email with state and local government partners

Much of this data lives in:

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- A third-party case management SaaS platform
- Legacy file shares being migrated

The Tensions (These are intentional friction points)

1. Retention vs. Over-Retention

- NARA requires **specific retention schedules** for records.
- Program offices are afraid of deleting *anything*.
- Storage costs are increasing.
- Legal insists some data must be preserved for litigation readiness.

Tension:

"If we delete something we shouldn't, we're in trouble.
If we keep everything forever, we're also in trouble."

---

2. Data Loss vs. Mission Velocity

- Analysts routinely export data to Excel and share it via email.
- Teams chats include CUI during live incidents.
- External sharing is necessary with state/local partners—but risky.

Tension:

“We can’t slow down incident response—but we also can’t leak CUI.”

---

3. Visibility Gaps

- Security teams don’t know:
    - Where sensitive data actually lives
    - Who has access to it
    - Whether it’s being shared externally

Tension:

“We’re accountable for protecting data we can’t fully see.”

---

4. Audit & Compliance Readiness

- The IG is preparing a FedRAMP/FISMA audit.
- Auditors will ask:
    - How sensitive data is identified
    - How retention is enforced
    - How policy violations are detected and remediated

Tension:

“We can’t scramble every time there’s an audit.”

---

5. Hybrid & Tool Sprawl

- Not all compliance tooling is Microsoft.
- Some workloads remain on-prem.
- Leadership wants a **single compliance strategy**, not 15 disconnected ones.

Tension:

“Purview can’t do *everything*—but it has to anchor the strategy.”

Student Exercise: You Are the Cybersecurity Architecture Team

Your Mission

Design a **compliance-centric security architecture** that addresses DIR's risks while enabling mission operations.

You are **not required** to implement everything in Microsoft Purview—but your architecture **must clearly demonstrate Purview-aligned concepts**.

Deliverables

1. Data Classification Strategy

- How will the agency **identify and classify**:
    - PII?
    - CUI?
    - Sensitive operational data?
- What role do the following have:
    - Sensitive Information Types?
    - Auto-labeling?
    - Manual classification?

---

2. Retention & Records Management Approach

- How retention policies align with **NARA schedules**
- How records are:
    - Declared
    - Retained
    - Disposed of defensibly
- How litigation holds override normal retention

---

3. Data Loss Prevention (DLP) Strategy

- Where DLP policies are enforced (email, Teams, SharePoint, endpoints)
- How to:
    - Allow mission-critical sharing
    - Block risky behavior
    - Educate users (policy tips)

---

4. Visibility, Monitoring & Audit Readiness

- How leadership gets visibility into:
    - Data risk
    - Policy violations
    - Compliance posture
- How audit evidence is produced **without heroics**

---

5. Integration with Non-Microsoft Tools

- How Purview fits into a **broader compliance ecosystem**
- What stays outside Purview—and how consistency is maintained

---

SC-100 / SC-5007 Exam Alignment

This exercise reinforces:

- Designing solutions for data security & compliance
- Information protection & governance
- Risk management and regulatory compliance
- Microsoft Purview architecture & capabilities
- Tradeoff-based architectural thinking