Case Study: “Rivermount Energy & Utilities” (REU)

Company snapshot

- **Industry:** Regulated electric & gas utility (generation, transmission, distribution; growing wind/solar)
- **Workforce:** 9,200 employees; 40% field crews/contractors; multiple JV partners and OEM vendors
- **Data estate (high level):**
    - **Microsoft 365:** Exchange Online, SharePoint Online, OneDrive, Teams, Viva Engage, Power BI
    - **Azure:** ADLS Gen2 (smart-meter/telemetry landings & reports), Azure SQL (asset & work mgmt marts)
    - **Other clouds / on-prem:** AWS S3 (vendor engineering drops), on-prem file shares/NAS (as-built drawings, substation one-lines, project docs), ESRI ArcGIS
    - **OT/ICS:** SCADA/DCS historian networks (segmented; *not governed by Purview policies directly*)
- **Regulatory drivers: NERC CIP**, FERC/CEII, state PUC rules, PCI (bill pay), SOX (public company), OSHA/EPA retention, GDPR if EU vendors
- **Risk posture & pain points:**
    - Excess **anonymous/external links** to project sites with **CEII** (Critical Energy Infrastructure Information)
    - Customer PII (account/meter IDs) shows up in email/Teams during outage coordination
    - Contractors syncing engineering folders to personal cloud/USB
    - Inconsistent retention for engineering drawings, outage reports, and incident investigations
    - Limited visibility across multi-cloud where sensitive data actually resides
- **Recent fictional incidents:**

1. A substation **one-line diagram** shared via anonymous SharePoint link.

2. A planning analyst exported **AMI meter reads** to a personal Gmail to “model quickly.”

3. A Power BI dashboard with **customer addresses** shared to a vendor tenant.

- **Current controls (fragmented):**
  - Some **sensitivity labels** (no encryption); inconsistent label policies
  - **Standard Audit** only; short audit retention
  - No **Endpoint DLP**; no AWS scanning; ad-hoc eDiscovery (Standard)
- **Constraints & goals:**
  - Don’t slow field safety/outage restoration workflows
  - Phase controls with measurable risk reduction
  - Clear separation of duties across **CIP Compliance**, **Security**, **Legal**, **Data**
  - Build a unified governance operating model in 12 months

Your challenge (for students)

Design a 90-day rollout + 12-month roadmap using **Microsoft Purview** (compliance portal + governance portal) and adjacent Microsoft security. You must:

1. **Discover & map** sensitive data (CEII, customer PII, contracts) across M365, Azure, AWS, and on-prem file shares.
2. **Protect & govern** with minimal friction for field and project teams.
3. **Detect & investigate** exfiltration/misuse; enable incident response.
4. **Comply with retention & legal holds** (engineering, safety, regulatory).
5. **Measure success** with clear KPIs.

Deliverables: high-level architecture, role model, prioritized controls, 3–5 KPIs.

Discussion Prompts & Mini-Exercises (with what good answers include)

1) Discover & Map (Governance)

Prompt A: How will you identify where **CEII** and customer **PII** live (M365, Azure, AWS, on-prem)?
Good answers:

- **Purview governance portal**: register & **scan** ADLS Gen2, Azure SQL, Power BI, **AWS S3**, and file shares; organize with **Collections**; assign **Data Source Admin/Reader/Curator**.
- Use **built-in classifications** + custom rules for CEII terms (e.g., "one-line," "protection relay settings"); **Data Estate Insights** heatmaps; **Business Glossary** (e.g., "CEII—Substation One-Line").
- In **compliance portal**: **Content Explorer** for label/SIT distribution, **Activity Explorer** for label/DLP activity.
- Note **OT** is segmented; only derived/replicated data in IT zones is scanned.

Prompt B: What governance roles and separation of duties fit a NERC environment?
Good answers:

- Distinct governance roles (Collection Admin, Data Curator, Data Reader) and compliance roles (**Compliance Admin**, **eDiscovery Manager**, **Insider Risk**, **Communication Compliance**).
- Include **CIP Compliance Officer** as approver/auditor; least privilege throughout.

2) Labeling & Protection (Information Protection)

Prompt C: Propose a **sensitivity label taxonomy** with encryption decisions.
Good answers:

- **Public → Internal → Confidential-PII → Confidential-CEII → Restricted-Engineering**.
- Encrypt top tiers; scoped **label policies** to engineering, planning, and vendor groups; **auto-labeling** in Exchange/SPO/OneDrive for PII/CEII patterns; default labels in critical project sites.
- **Power BI**: label inheritance (dataset→report→dashboard) and user guidance.

Prompt D: How to roll out without breaking outage response?
Good answers:

- Pilot with **recommend** actions; watch **Activity Explorer**; then enforce for engineering repositories.

- **Mandatory labeling** for engineering sites; clear exception process and job aids; avoid blocking critical OT flows.

3) Data Loss Prevention (DLP)

Prompt E: Design DLP for PII/CEII leaving via email, Teams, and endpoints.
Good answers:

- **M365 DLP** for Exchange, SharePoint, OneDrive, Teams (chat/channel).
- **Endpoint DLP** for USB/print/clipboard/sync on Windows/macOS; user prompts with business justification.
- Use built-in SITs (PII/PCI) + **custom SITs** (regex/keyword for substation names, project codes) + **EDM** for **customer/account/meter master**; alerts to SOC/Compliance.
- Stage: **Audit → Block with override → Block**; prioritize engineering project sites and outage channels.

Prompt F: When to use **EDM** or **trainable classifiers**?
Good answers:

- **EDM** for precise customer/account/meter IDs; reduces false positives.
- **Trainable classifiers** for documents like outage investigation narratives or engineering change notes.

4) Insider Risk & Adaptive Protection

Prompt G: Reduce contractor exfiltration before/after offboarding.
Good answers:

- **Insider Risk Management** with HR signals (contract end date), anomalous activity, exfil vectors (USB, personal cloud).
- **Adaptive Protection**: elevate user risk ⇒ stricter **DLP** automatically.
- Reviewer privacy controls, coaching messages, and case workflows.

5) Communication Compliance

Prompt H: A one-line diagram was posted in a public Teams channel. What now?
Good answers:

- **Communication Compliance** policy scanning Teams/Exchange/Viva Engage for CEII/PII; **reviewers** (CIP/Compliance), escalation rules, and coaching; documented remediation and education.

6) eDiscovery & Legal Holds

Prompt I: A regulator requests preservation for a blackout investigation (mail, Teams "war room," SharePoint project site, **ADLS telemetry**). Your plan?
Good answers:

- **eDiscovery (Premium)** case; **custodial** (mail, OneDrive, Teams of named users) + **non-custodial** locations (project SharePoint, shared mailboxes).
- Legal hold, **review sets**, analytics/dedupe/OCR; export with chain-of-custody.
- Coordinate with governance team to identify ADLS containers and document export paths.

7) Audit & Investigations

Prompt J: What telemetry would you pull to investigate the AMI export to Gmail?
Good answers:

- **Advanced Audit** (longer retention + richer events like item access/mailbox items accessed).
- Unified **audit log**: file access/sharing, label changes, DLP events; correlate with **Endpoint DLP** alerts and IRM signals; forward high-severity to SIEM.

8) Lifecycle: Retention & Records

Prompt K: Propose retention for engineering, outage, safety, and customer records.
Good answers:

- **Retention labels/policies** by BU/location; **event-based retention** (asset decommission, project close, incident closure).
- **Records Management** with disposition reviews; proof of deletion; legal hold precedence understood.

9) Operating Model & KPIs

Prompt L: What are your first-90-day KPIs?
Good answers:

- % of target data sources scanned/classified; % of engineering/project sites with labels; drop in anonymous links; DLP false-positive rate; MTTR for DLP incidents; reviewer SLA adherence.

Short “Answer-Key” Rubric (quick scoring)

- **Discovery & Governance (A–B):** Governance scans & Data Map, Collections/roles, Content/Activity Explorer, glossary; OT explicitly segmented.
- **Labels (C–D):** Tiered taxonomy with encryption; scoped publishing; phased rollout with metrics.
- **DLP (E–F):** M365 + Endpoint coverage; SITs + **EDM/trainables**; staged enforcement; alert routing & tuning loop.
- **Insider Risk (G):** HR signals, adaptive enforcement, reviewer privacy.
- **Comm Compliance (H):** Policies, reviewers, coaching, auditability.
- **eDiscovery (I):** Premium workflow; custodial/non-custodial holds; review sets; export; governance tie-in for ADLS.
- **Audit (J):** Advanced Audit value; correlation; evidence handling.
- **Retention (K):** Labels/policies, event triggers, records/disposition, hold interactions.
- **KPIs (L):** Measurable, risk-centric, time-bound.

---

20 Sample Quiz / Reflection Questions (energy-focused)

1. **Compliance vs governance portals—what goes where for REU?**
2. **Three ways to locate CEII in M365 content right now?**
3. **Why encrypt CEII but not “Internal” project comms?**
4. **Two scenarios where EDM outperforms regex for REU.**
5. **Where Endpoint DLP adds controls beyond M365 DLP in field operations.**
6. **How Adaptive Protection tightens DLP for expiring contractors.**
7. **Define custodial vs non-custodial locations for a blackout case.**

8. **How retention labels interact with legal holds during a FERC inquiry.**
9. **Example of event-based retention in energy (give the event).**
10. **When to choose Advanced Audit vs Standard Audit for investigations.**
11. **One change to reduce anonymous link sprawl without hurting collaboration.**
12. **Where to tune DLP to lower false positives (specific levers).**
13. **Reviewer workflow goals in Communication Compliance for CEII.**
14. **How Power BI labeling/inheritance protects operational reports.**
15. **How to scope label publishing to engineering and vendor JVs safely.**
16. **Two 90-day KPIs that demonstrate risk reduction for CIP stakeholders.**
17. **Which Purview capability exposes lineage across ADLS/Power BI?**
18. **Separation of duties you'd enforce for investigations and CIP oversight.**
19. **Escalation path when DLP blocks legitimate outage coordination.**
20. **Day-one end-user artifact you'd ship to engineering & field teams.**