Energy & Utilities – Multi-Framework Compliance Tracker
Project Type: Compliance Tracking & Renewal Management
Industry: Energy & Utilities
Role: GRC / Cybersecurity Governance Practitioner

1. Executive Summary

An energy and utilities organization needed to manage compliance across several frameworks and certifications, including **PCI DSS, SOC 2, ISO 27001 and key vendor certifications**. Compliance activities were scattered across emails, spreadsheets and shared drives, making it hard to see what was due, who owned it and whether evidence was ready for audits.

I designed a **centralized compliance tracker** that brought all obligations, renewal dates, owners and evidence into a single, simple view. The goal was to reduce missed renewals, improve audit readiness and give leadership a quick way to see overall compliance health.

2. Context & Problem

The main issues were:

- No single place to see **all compliance obligations and expiry dates**
- Different teams tracking their own tasks in separate files
- Last-minute rushes when audits or renewals approached
- No clear owner for some requirements or certificates
- Leadership had to ask multiple people just to answer “Are we on track?”

The organization needed a tool that was **simple enough to use in Excel**, but structured enough to support audits and internal reporting.

3. Objectives

I set four clear objectives:

1. **Centralize** all compliance items in one tracker.
2. **Assign ownership** and due dates for each item.
3. **Track status** of tasks and evidence (Not Started, In Progress, Complete).
4. Enable **quick reporting** to management and auditors.

4. Approach

4.1 Define Compliance Scope

I listed all key compliance areas:

- PCI DSS (for payment-related systems)
- SOC 2 (for service reliability and security)
- ISO 27001 (for information security)
- Vendor certifications (e.g., cloud provider, payment gateway, key partners)

Each compliance item was treated as a record in the tracker.

4.2 Design the Tracker Structure

I designed an **Overview sheet** with columns such as:

- Framework / Certification
- Requirement or Obligation
- Owner
- Frequency (annual, quarterly, ad-hoc)
- Next Due Date
- Status (Not Started / In Progress / Complete)

Then I added a **Detailed sheet** for each major framework with:

- Requirement ID or description
- Issue date / expiry date
- Link to evidence location
- Notes and dependencies

4.3 Status & Automation Basics

I used simple formulas to:

- Calculate **days until expiry**
- Flag items as **Due Soon** or **Overdue** using conditional formatting
- Roll up counts of items by status to provide a quick summary (e.g., “5 items due in the next 30 days”)

4.4 Roles & Process

I defined a basic process:

- Owners update status and evidence links regularly
- A GRC or compliance lead reviews the tracker **monthly**
- Ahead of audits, the tracker is used to confirm which items are fully ready

5. Key Deliverables

- **Compliance Tracker – Overview Sheet** (all frameworks in one view)
- **Framework-Specific Tabs** (PCI DSS, SOC 2, ISO 27001, vendor certifications)
- **Status & Summary View** for leadership and audit prep
- Simple **process description** for how and when to update the tracker

---

6. Outcomes

In this scenario, the tracker:

- Reduced the risk of **missed renewals** and expired certificates
- Made audit preparation more predictable and less last-minute
- Gave leadership a **single source of truth** for compliance status
- Helped clarify who was responsible for what, and when it was due

---

7. My Role

In this project, I:

- Designed the tracker structure and fields
- Defined the update process and ownership model
- Built formulas and status indicators
- Aligned the layout with the needs of both **individual owners** and **leadership reporting**