Final Project: Designing a Compliance Framework for a startup

Groups of 2-4

Project Overview

Students will design a **compliance program** for a **hypothetical startup/organization**. Integrate the following regulatory and security frameworks if possible:

- **ISO 27001** (Information Security Management)
- **SOC 2** (Trust Services Criteria)
- **HIPAA** (Healthcare Data Privacy & Security)
- **SOX** (Financial Controls & Reporting)
- **NIST CSF** (Cybersecurity Risk Management)

Leverage **Common Controls Framework (CCF)** if applicable to your startup/organization

The project will involve:

- ❖ **Researching framework requirements**
- ❖ **Conducting a risk assessment & gap analysis**
- ❖ **Designing controls aligned to the frameworks & CCF**
- ❖ **Creating a high-level implementation roadmap**
- ❖ **Submitting a final report & presentation**

Objective 1: Understand compliance obligations and how CCF helps unify controls (if you are using the CCF).

Tasks:

- Identify **overlapping requirements** across frameworks.
- Develop a **compliance mapping table** aligning controls across frameworks using **CCF categories**.

Deliverable 1:

- Compliance Mapping Table (1-2 pages).

Objective 2: Conduct a **risk assessment** and identify compliance gaps.

Tasks:

- Identify **7-10 key risks**
- Conduct a **gap analysis** based on selected frameworks
- Develop a **risk matrix** (Likelihood, Impact, Existing Controls, Missing Controls).

Deliverable 2:

- **Risk Assessment Report (2-3 pages, including risk matrix)**.

Objective 3: Develop a **set of controls & policies** that address compliance gaps.

Tasks:

- Propose **controls aligned with the frameworks**
- Map controls to **CCF categories**.
- Create a **high-level implementation roadmap** (6-12 months).

Deliverable 3:

- **Compliance Framework Report (4-5 pages)**.

Objective 4: Present the compliance framework with findings & implementation plans.

Tasks:

- Compile a **detailed final report**.
- Prepare a strict **15-minute presentation (10-12 slides max)** summarizing key points.
  - Each team member has a role and presents
  - There will Q&A after the presentation and other students can also ask questions

Deliverables:

1. **Final Compliance Report (include deliverables 1-3 within it as well) - Due April 23rd**

2. **Presentation Slides - Presentation will be held in the last class on April 24th**

Grading Criteria:

- **Report Quality**: Well-researched, professional formatting.
- **Presentation Clarity**: Engaging and concise summary.
- **Professionalism**: Formatting, citations, and visual appeal.

Bonus section - Try to incorporate demos, charts, graphs, dashboards as applicable as well as real world use cases/case studies to support your deliverable