Title: Designing a GRC Framework for TechStart Innovations

Overview

In this assignment, you will simulate the role of a GRC analyst for a fast-growing financial technology (fintech) company. You are expected to use your knowledge from **Week 1** to assess a real-world business scenario, identify security and compliance risks, and suggest solutions using Governance, Risk, and Compliance (GRC) best practices.

This assignment is designed to help you apply theoretical concepts to real-world use cases, preparing you for industry expectations.

Assignment Duration

Time Allotted: 90 minutes
Work Mode: Individual or in pairs (maximum of 2 students)
Submission Format: Typed PDF

Scenario: TechStart Innovations

TechStart Innovations is a fintech startup with 50 employees. The company recently raised a Series A investment and is preparing for further funding. The company's core operations involve handling sensitive data such as:

- **Banking details** of users (must comply with PCI-DSS),
- **Personal data** of customers from the European Union (must comply with GDPR),
- **Internal source code and algorithms** (considered intellectual property and business secrets).

Technology Stack in Use:

- AWS Cloud for hosting
- GitHub for software development
- SaaS tools such as Slack and Salesforce

Current Challenges:

- TechStart has no formal GRC program.
- They are preparing for ISO 27001 certification.
- A recent phishing attempt nearly succeeded.
- Their audit highlighted weak access controls and lack of documentation.

Your role is to help TechStart build a strong foundation for their GRC framework using Week 1 concepts.

Assignment Tasks

Task 1: Establish the Business and Risk Context

Purpose: Understand how business goals influence compliance and risk decisions. Every GRC program begins with understanding what the business is trying to achieve and what assets are critical to its operations.

1.1 Business Objectives and Compliance Impact

TechStart's three main goals are:

Business Goal	What It Means	Related Compliance Requirement
Expand into the German market	Must comply with European privacy laws	GDPR
Raise $10M Series B investment	Requires secure systems and investor confidence	SOC 2
Reduce security incidents by 60%	Needs better threat detection and response	ISO 27001

Your Task:
For each of the above goals, explain in 2–3 sentences how that goal drives the need for proper governance, risk management, and compliance. Refer to your lecture notes and frameworks discussed in Week 1.

1.2 Create an Asset Inventory Table

Purpose: Before implementing controls, the company must know what data and systems are critical to its operations. This is called **Asset Inventory**.

Fill out a table like the one below. You must list at least **three (3)** assets and classify their importance.

Asset Category	Specific Asset	Owner	Related Compliance Rule	Importance Level
Data	EU Customer Database	CTO	GDPR Article 30	High
Process	Payment Processing Flow	CFO	PCI-DSS Requirement 3	Critical
Technology	AWS Production Servers	DevOps	ISO 27001 Clause A.14	High

1.3 Stakeholder Alignment Roleplay

Purpose: Many GRC initiatives fail because internal stakeholders (e.g., CFO, CTO) do not see the value. You must be able to explain why each GRC activity is important to the business.

Your Task:
Write a short paragraph or dialogue where you (as a GRC lead) try to convince the CFO why completing the asset inventory is necessary. Mention benefits such as investor confidence, regulatory compliance, audit readiness, and risk visibility.

Task 2: Perform Inherent Risk Assessment

Purpose: Use the **FAIR methodology** to calculate the level of risk TechStart is facing based on current gaps.

Scenario:

- A former employee still has access to GitHub.
- There is no Single Sign-On (SSO) enforcement.
- If the source code is stolen, it could cause $2 million in damage.

Your Task:
Calculate the **Inherent Risk** using the formula from your Week 1 notes:

Inherent Risk = Threat Likelihood × Impact

- Threat Likelihood = 25% (0.25)
- Impact = $2,000,000

Show your calculation and final value.

Bonus (Optional): Create a Risk Heatmap

List five potential risks TechStart might face (e.g., phishing, insider threats, data breaches, unpatched systems) and plot them on a **simple risk heatmap** based on likelihood and impact. You can draw this manually or use Excel.

Task 3: Map Controls to ISO 27001

Purpose: Fix the identified problems using ISO 27001 controls. This task helps you apply the knowledge of **control mapping** and **gap analysis** discussed in Week 1.

Your Task:
Match each gap with the appropriate ISO 27001 control and the relevant feature in a GRC tool (e.g., Sprinto). Then, pick one issue and write how you would close the gap.

Problem Identified	ISO 27001 Control	Sprinto Feature
No employee training	A.7.2.2	Auto-assigned training modules
Shared admin passwords	A.9.2.3	Role-based access control
Servers not updated	A.12.6.1	Real-time monitoring alerts

Select one of the above issues and explain:

- Who is responsible
- What steps need to be taken
- What tools can be used to fix the gap

Task 4: Present Your GRC Strategy

Purpose: Present your work as if you are briefing company leadership. This task helps you practice your communication skills and align GRC activities with business needs.

Create a 3-slide presentation (maximum):

- **Slide 1:** Why GRC Matters
  Link GRC efforts to TechStart's business goals, such as expansion, investment readiness, and risk reduction.
- **Slide 2:** Tool Recommendation
  Compare **Sprinto** vs **Secureframe** based on their suitability for a fintech startup. Use features, automation, cost, and ease of implementation as criteria.
- **Slide 3:** Overcoming Resistance
  Propose strategies for dealing with resistance to change (e.g., training, showing ROI, using quick wins).

You can use PowerPoint, Google Slides, or create this in your report as clearly separated sections or upload the ppt to the drive and attached the link to it, ensure to make it accessible to anyone with the link

Optional Bonus Tasks (Extra Credit)

If you complete the main tasks early or wish to earn extra marks, you can complete one or more of the following:

1. **Evidence Collection Simulation:**
   Identify what logs or reports you would collect from AWS to demonstrate GDPR Article 30 compliance.
2. **Workflow Diagram:**
   Create a simple workflow showing:
   New employee → Access request → Approval → Automated provisioning → Audit trail generated
3. **Budget Estimation:**
   Estimate how much GRC implementation might cost using the $20,000–$80,000 range. Justify your answer by considering:
   - ✓ Number of employees
   - ✓ Number of frameworks
   - ✓ Level of automation and tooling

Grading Rubric (Total: 20 Marks)

Section	Max Marks	What Will Be Assessed
Business Context & Inventory	4 marks	Relevance, clarity, and connection to compliance goals
Risk Calculation	4 marks	Correct use of FAIR model and logic
Control Mapping	4 marks	Accurate ISO 27001 linkage and realistic control plan
GRC Presentation	4 marks	Clear communication, creativity, and practical strategy
Bonus Tasks (Optional)	4 marks	Shows deeper understanding and real-world application

Final Notes

- All required knowledge comes from **Week 1 materials**: no outside research is required.
- Be clear, concise, and explain your reasoning.
- Use diagrams, charts, or screenshots if it helps make your ideas clearer.
- Practical thinking and alignment with business needs are more important than perfection.