DESIGNING A GRC FRAMEWORK FOR TECHSTART INNOVATIONS

Student Name: Oluwatimilehin Oluwagbemi

Reg. No: 2025/GRC/10712

Date: 24/07/2025

SOLUTION TO ASSIGNMENT TASKS

Task 1.1 Business Objectives and Compliance Impact

1. **Goal 1 – Expand into the German Market**: this goal drives the need for governance, risk management and compliance to be integrated into TechStart as it requires full compliance with the General Data Protection Regulation (GDPR). GDPR sets out detailed requirements for organizations and businesses of all sizes on collecting, storing, and managing personal data. TechStart being a data collection organization must fully comply with the GDPR if they want to expand their market to Germany. To fully expand to the German market, there is need for governance frameworks such as data classification policies, ongoing risk assessments and technical controls aligned with GDPR Articles 5, 30, and 32 to ensure data protection and legal readiness for cross-border operations.
2. **Goal 2 – Raise $10M Series B Investment**: to boost the confidence of Investors, TechStart must demonstrate credible governance and ensure that their system is secure. This can be achieved by adopting frameworks like SOC 2 and ISO 27001 which ensures security of Information Systems and how it's being managed. This compliance with SOC 2 and ISO 27001 will validate TechStarts approach to asset management, access controls, incident response and vendor risk management. As Investors will demand for a robust risk management practice, it is essential for TechStart to integrate formal GRC program.
3. **Goal 3 – Reduce Security Incidents by 60%**: achieving this goal drives the need for proper and structured risk management including real-time monitoring, regular updates / patching, and awareness training for employees. TechStart need to be ISO 27001 compliance to stay off attack radar as data protection and supply chain risks are important. There is need for TechStart to be ISO 27001 certified, this will provide them a risk-based framework and ISMS that will help proactively secure data, meet regulatory standards and customer requirements. ISO 27001 enforces preventive and detective controls under clause A.8.8 for updating systems and clause A.6.3 for employee training which is crucial for security incidents reduction. Human are the first line of defence, hence the need for employee training.

Task 1.2 Asset Inventory Table

Asset Category	Specific Asset	Owner	Related Compliance Rule	Importance Level
Data	Customer's Record / Database	CTO	GDPR Article 30	High
Process	Banking Activities / Credit Card Issuing	CFO	PCI-DSS Requirement 3	Critical
Technology	Salesforce	DevOps	ISO 27001 clause A.8.28 and A.8.9	High

Task 1.3 Stakeholder Alignment Roleplay

As our CFO, I am aware that you are concerned with investor confidence and financial performance, which are both dependent upon having a strong asset inventory. This will increase transparency into our business's motivations and areas of risk by cataloguing our critical information, systems, and procedures. This is a strategic move that supports our GDPR and PCI-DSS obligations, improves audit readiness, and reassures investors that we have firm control over our assets which is more than just a compliance checkbox.

Task 2 Inherent Risk Assessment

Inherent Risk = Threat Likelihood x Impact

Given: Threat Likelihood = 25% (0.25) and Impact = $2,000,000

Therefore, Inherent Risk = Threat Likelihood x Impact

= 0.25 x $2,000,000

= $500,000

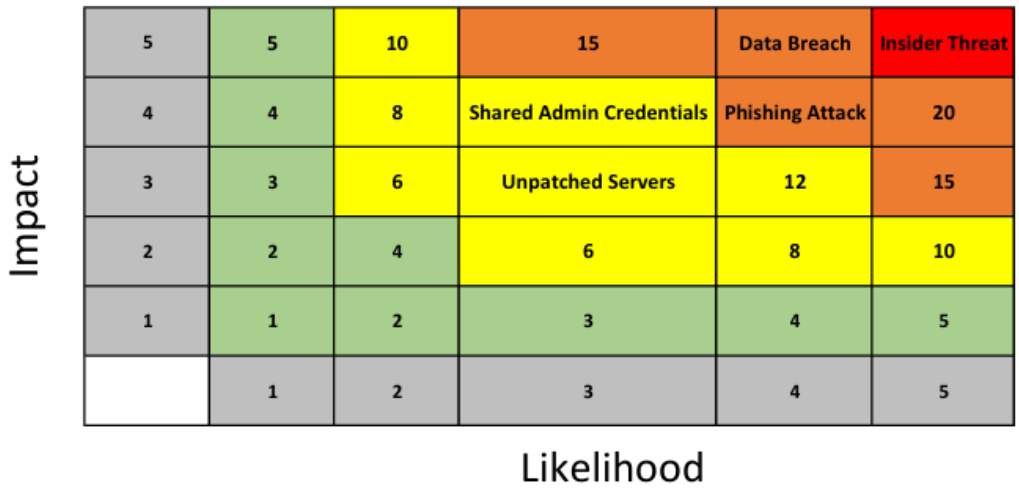
Inherent Risk = $500,000

Based on current gaps in TechStart, they are likely to face Inherent Risk that costs $500,000 if nothing is done to close the gaps.

Five Potential Risks:

- Phishing Attack
- Shared Admin Credentials
- Insider threats
- Data Breach
- Unpatched Production Servers.

The Screenshots below represents the Simple Risk Heatmap created using Excel for the potential risks TechStart might face,



Risk Type	Likelihood (L)	Impact (I)	Risk Magnitude (L x I)
Phishing Attack	4	4	16
Shared Admin Credentials	3	4	12
Insider Threat	5	5	25
Data Breach	4	5	20
Unpatched Servers	3	3	9

Key

Impact	1	2	3	4	5
	Negligible	Low	Medium	High	Very High

Likelihood	1	2	3	4	5
	Unlikely	Remote	Fairly Likely	Likely	Very Likely

Risk Impact vs Likelihood

5 and Below	Green
6 - 12	Yellow
13 - 20	Orange
25	Red

Task 3 Map Controls to ISO 27001

ISO 27001 Control Mapping Table

Issue Identified	ISO 27001 Control	Sprinto Feature
No employee training	**A.6.3**	**Automated Security Awareness Training Modules, Tracking and Monitoring Training Completion**
Shared Admin Passwords	**A.5.16**	**Role-based access control, Integration with Identity and access management system (IAM)**
Servers not Updated	**A.8.8**	**Integration with Vulnerability Scanner**

Issue Identified: No Employee Training

- Who is responsible: The Management is responsible for awareness training of employees according to ISO 27001 clause A.6.3 standard. They are to ensure all personnel such as employees and contractors receive necessary training, tailored to their specific roles and responsibilities in the organization. ISO 270001 clause A.6.3 emphasizes the need for the management to develop a security awareness culture within their organization. They must ensure all employees have understanding of information security threats, vulnerabilities and controls relevant to their roles in the organization.
- What steps need to be taken: management must ensure all employees receives adequate awareness education and training which must be relevant, practical and understandable on a regular basis. They must ensure regular updates about the organization's policies and procedures regarding information security to the employees. Management must develop a suitable set of procedures for labelling and handling information and it must be implemented in alignment with the organization's chosen classification scheme. Management should:
    - Define the need for training to employees by identifying the gaps facing the organization security posture.
    - Develop training materials which will cover the organization's relevant policies and procedures, security best practices and how to detect threats and vulnerabilities.
    - Conduct the training based on employee's role and responsibilities, document the training conducted and also make training materials accessible to staffs and employees.
    - Evaluate the effectiveness of the training by getting feedbacks from their employee, track security incidents to see if the training have positive impact on the employee.
- What tools can be used to fill this gap:
    - Phishing Simulations: this will test the ability of the employees in recognizing and responding to Phishing emails. Using real-world simulation attacks, it will give them insights to how security conscious they should be in handling emails, that not all emails are genuine.
    - E-learning platforms: there are many e-learning platforms with comprehensive modules on security awareness training for organizations which can be used to train their employees, example is KnowBe4.
    - Conducting Regular Security Training and Awareness: this should not be a one-time thing, it must be continuous, campaigns about security awareness should be done regularly through newsletters, blog posts, articles, emails for employees to stay aware and abreast of security threats and vulnerabilities.

Task 4 GRC Strategy

https://docs.google.com/presentation/d/1h3_rLuh5bYxPW-7LFm39utldoC3gYwaENL_QqQW6w7U/edit?usp=sharing

Bonus Task:

Evidence Collection Simulation:

Logs or reports I would collect from AWS to demonstrate GDPR Article 30 compliance **are:**

Records of Processing Activities such as:

- Written documentation and overview of procedures by which personal data are processed.
- Significant Information about data processing such as:
    - Data Categories
    - The group of Data subjects
    - The purpose of the processing
    - The Data recipients.