TechNova GRC Project

Author: Rahaf Alfehaidi

Date: August 2025

Executive Summary.

This project demonstrates a comprehensive Governance, Risk, and Compliance (GRC) assessment for TechNova, a small tech company. The assessment covers governance policies, risk evaluation, mitigation strategies, and compliance with regulations. The main findings indicate critical and medium-level risks, with recommended actions prioritized to strengthen the company’s risk management framework.

1. Company Overview (Governance) .

TechNova is a small software development company with 25 employees. The company operates:

Internal server

Customer database

Web application

Existing Policies:

Unique passwords for each employee

Daily backup of critical data

Governance Summary:

TechNova currently has basic governance in place, highlighting the need for structured risk management and compliance monitoring.

2. Scope of the Project (GRC) .

Governance:

Evaluate policies: access control, backups, password policies

Assess business continuity preparedness

Risk:

Identify potential cyber-attacks on web applications

Data loss of customer information

Human error or misuse of systems

Non-compliance with data protection regulations (GDPR)

Compliance:

Check adherence to security standards and regulations: GDPR, ISO 27001, NIST Cybersecurity Framework.

3. Risk Assessment .

Risk	Likelihood	Impact	Risk Level	Notes
Cyber-attack on web application	High	High	Critical	Requires Web Application Firewall (WAF) and regular updates
Loss of customer data	Medium	High	High	Daily backups and secure cloud storage
Human error	High	Medium	Medium	Employee training and role-based access controls
Non-compliance with regulations	Low	High	Medium	Periodic policy reviews and audits

4. Risk Mitigation & Controls.

Cybersecurity Controls:

Deploy Web Application Firewall (WAF)

Regular updates and patch management for servers and applications

Data Protection:

Daily backup to both local and secure cloud storage

Encrypt sensitive data (customer information)

Human Error Mitigation:

Employee cybersecurity awareness training

Implement role-based access controls (RBAC)

Compliance Actions:

Conduct quarterly audits of internal policies

Maintain documentation of all updates and corrective actions

5. Findings & Recommendations .

Findings:

Mix of critical and medium-level risks

Existing governance is basic, leaving gaps in cybersecurity, data protection, and compliance

Recommendations:

1.Prioritize mitigation of critical risks immediately (cyber-attacks and data loss)

2.Implement formal risk management and compliance monitoring procedures

3.Maintain continuous employee training and enforce role-based access policies

4.Develop dashboards for real-time monitoring of risks and compliance status

6. Dashboard Overview .

Tools: Excel / Power BI.

Visual Elements:

Risk Matrix: Likelihood vs Impact

Color-coded risk levels: Red (Critical), Orange (High), Yellow (Medium), Green (Low)

Progress tracker for mitigation actions.

Purpose:

Quickly identify top risks

Track status of mitigation efforts and compliance tasks