zero$ploit

WE Innovate Bootcamp – GRC Final Exam

8/17/2025

Table of Contents

Introduction

This final exam is designed to evaluate the knowledge and practical skills you have gained throughout the GRC Course. The exam is structured around realistic organizational scenarios that reflect the challenges security and compliance teams face in today's business environments.

Each team Assigned one scenario to work on. The scenario provides a detailed description of the organization, its objectives, operating environment, and the security and compliance challenges it faces. Based on this context, your team must complete a series of applied tasks that span the full GRC lifecycle, from governance and risk assessment to incident response and compliance.

The goal of this exam is not to recall definitions or provide short answers, but to apply your knowledge in practice by producing professional-level deliverables such as risk registers, and ISO 27001 control mappings. These deliverables should demonstrate both your technical understanding and your ability to think strategically about governance, compliance, and organizational objectives.

Instructions

1. Review the scenarios carefully.
2. Complete **all tasks** in the exact order provided, using your scenario's context.
3. Use the **templates provided in the Appendix** to structure your deliverables.
4. Ensure your work is **clear, well-structured, and justified**, explain not only *what* you recommend, but also *why*.
5. Your final submission should include diagrams, tables, and structured documentation where required.

Evaluation Criteria

Your submission will be assessed on the following dimensions:

- **Completeness & Logic (30%)** – All tasks addressed with clear traceability and logical flow.
- **Technical Depth (30%)** – Realistic, practical, and context-appropriate security and GRC practices.
- **Risk & Compliance Rigor (25%)** – Demonstrated ability to apply frameworks, standards, and laws.

Scenario E: GreenFuel Logistics (Smart Fleet Management)

GreenWatt Energy Solutions is a renewable energy company that manages solar farms and sells clean energy to businesses and households. Their goal is to become a leading provider of affordable and sustainable power.

Current Environment / Scope of Work

- **Core Systems:** Fleet Management System (real-time tracking) + Fuel Card Payment System.
- **Operating Systems:**
  - Windows Server 2016 for central management.
  - Linux (Debian 11) for IoT gateways.
- **Databases:** PostgreSQL 12 (vehicle data, routes, fuel consumption).
- **Applications:**
  - Mobile app for drivers.
  - Web dashboard for fleet managers.
  - Integration with GPS and IoT sensors in trucks.
- **Cloud Services:** AWS IoT Core + DynamoDB for telemetry.
- **Endpoints:** 200 tablets in trucks, 50 desktops in offices.
- **Security Controls:** VPN tunnels between IoT gateways and HQ, endpoint encryption, SOC monitoring.

Unified Task Pack (Complete these in order)

Deliver each task as a concise artifact (document, table, diagram). Use the **Appendix templates**.

1. Business & Scope Brief

- Summarize mission, critical services, and top 3 business objectives.
- Define in-scope environments (prod/non-prod, on-prem, cloud, endpoints, SaaS).
- Identify critical processes (min 3) and stakeholders (business owners, IT, Security, Compliance).
- Output: 1–2 pages brief.

2. Risk Assessment

- Define a 5×5 scoring model and the risk appetite statement.
- Build a Risk Register (min 5 risks) with likelihood, impact, inherent vs residual, owner, treatment.
- Select treatment plans (avoid/transfer/mitigate/accept) and justification.
- Output: Risk Register + heatmap.

3. ISO 27001 Control Mapping (Annex A:2022)

- Map each high risk to Annex A controls; include rationale.
- Produce a Statement of Applicability (SoA) excerpt, noting included/excluded.
- Output: SoA table.

4. Secure Architecture & Segmentation

- Propose target architecture (zones, gateways, WAF/reverse proxy, EDR, where relevant).
- Define minimal inbound/outbound rules between zones (tabular).
- Output: Reference diagram + policy snippets.

5. Compliance & Legal Alignment

- Identify applicable frameworks/laws per scenario (e.g., PCI-DSS, health privacy, data-protection laws, export controls).
- Map 3-5 requirements to existing/planned controls; document gaps and remediation plan.
- Outline vendor risk approach: due diligence, and ongoing monitoring.
- Output: Compliance matrix + vendor checklist.

6. Training, Awareness & Governance

- Define role-based training plan (who, what, frequency) tied to risks/incidents observed.
- Propose governance: ISMS scope, policy stack, committee cadence, and internal audit plan (next 2 quarters).
- Output: Training matrix + governance calendar.

Appendix & Templates

1. Risk Register

Risk ID	Risk Statement	Asset	Threat	Likelihood	Impact	Control	Owner	Treatment	Due Date

2. Statement of Applicability (SOA)

ID	ISO 27001: 2022 Controls			Applicable (Yes / No)	Remarks (Justification for exclusion)	Remarks (Overview of Implementation)	
	Section	Control No.	Control Title			Implemented	Reference

Address: 20 Al-Mathaf Al-Zeraie, Floor 06 apartments 61, Al-Agoza-Giza, Egypt.
Phone: +202 333 638 86