

WE Innovate Bootcamp

***GRC Final Exam***

***Documentation File***

**Scenario E: GreenFuel Logistics – Smart Fleet Management**

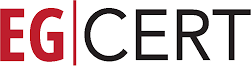
**GRC (Group2 – Team5)**

**Made by**

[Gasser Amr](https://www.linkedin.com/in/gasser-amr-a01111253/) Eldabaa

Mohamed Abed

Mohamed Ahmed



# Table of Contents

1. Business & Scope Brief

* 1.1 Mission Statement
* 1.2 Critical Services
* 1.3 Top Five Business Objectives
* 1.4 In-Scope Environments
* 1.5 Critical Processes
* 1.6 Stakeholders

2. Risk Assessment – GreenFuel Logistics

* 2.1 Risk Scoring Model (5×5 Matrix)
* 2.2 Risk Appetite Statement
* 2.3 Risk Register (8 Key Risks)
* 2.4 Risk Heatmap (Likelihood × Impact)

3. ISO 27001:2022 – Statement of Applicability (SoA) Excerpt

* 3.1 Risk-to-Control Mapping Table
* 3.2 Statement of Applicability – Summary

4. Secure Architecture & Segmentation

* 4.1 Target Architecture Design
* 4.2 Reference Diagram (Abstracted)
* 4.3 Minimal Inbound/Outbound Rules (Firewall / Segmentation Table)
* 4.4 Policy Snippets
* 4.4.1 Network Segmentation Policy
* 4.4.2 IoT Security Policy
* 4.4.3 Application Security Policy
* 4.4.4 Endpoint Security Policy
* 4.4.5 Monitoring & Logging Policy
* 4.4.6 Change & Configuration Management Policy
* 4.4.7 Access Control Policy

5. Compliance & Legal Alignment

* 5.1 Applicable Frameworks & Laws
* 5.1.1 PCI-DSS
* 5.1.2 GDPR (General Data Protection Regulation)
* 5.1.3 Egyptian Data Protection Law No. 151/2020
* 5.1.4 ISO/IEC 27001:2022
* 5.1.5 AWS Shared Responsibility Model
* 5.2 Compliance Matrix
* 5.3 Key Insights

5.4 Vendor Risk Management

* 5.4.1 Due Diligence (Pre-Onboarding)
* 5.4.2 Ongoing Vendor Monitoring
* 5.4.3 Exit Strategy

6. Training, Awareness & Governance

* 6.1 Purpose and Objectives
* 6.2 Security Training Program
* 6.3 Awareness Initiatives
* 6.4 Governance Structure
* 6.5 Incident Reporting & Escalation
* 6.6 Metrics and Continuous Improvement
* 6.7 Conclusion

**1.Business & Scope Brief**

## 1.1Mission Statement

GreenFuel Logistics, a subsidiary of GreenWatt Energy Solutions, supports the company’s mission of delivering **affordable, sustainable, and reliable clean energy**. Its specific role is to provide **smart fleet management and secure fuel card payment services** that optimize logistics operations, reduce operational costs, and enable real-time decision-making.

## 1.2. Critical Services

1. **Fleet Management System (FMS):** Real-time vehicle tracking, route optimization, and telemetry.
2. **Fuel Card Payment System:** Secure digital fuel transactions for fleet vehicles.
3. **IoT Telemetry Services:** Collection and processing of sensor data (location, fuel consumption, engine health).
4. **Mobile & Web Applications:** Access points for drivers (mobile app) and managers (dashboard).
5. **Cloud Telemetry Processing:** AWS IoT Core and DynamoDB supporting data collection, analysis, and reporting.

## 1.3. Top Five Business Objectives

|  |  |  |
| --- | --- | --- |
| Objective | Description | Strategic Value |
| Operational Efficiency | Optimize fleet routes, reduce fuel consumption, and minimize downtime. | Cost savings, sustainability. |
| Service Reliability | Ensure real-time fleet monitoring and 24/7 availability of critical systems. | Customer trust & satisfaction. |
| Data Security & Compliance | Protect sensitive vehicle, payment, and customer data under GDPR, PCI-DSS, Egyptian Privacy Law. | Legal compliance, risk reduction. |
| Sustainability Leadership | Reduce carbon footprint by integrating smart energy and transport practices. | Market leadership in green logistics. |
| Business Growth & Scalability | Expand services across regions while maintaining secure, efficient infrastructure. | Revenue growth & market expansion. |

## 1.4. In-Scope Environments

|  |  |  |
| --- | --- | --- |
| Environment | Assets / Systems | Notes |
| Production | Fleet Management System, Fuel Card Payment System, AWS IoT Core, DynamoDB, PostgreSQL DB | Core business operations. |
| Non-Production (Dev/Test) | Staging servers, test databases, UAT environments | For software updates, QA, and patches. |
| On-Premises | Windows Server 2016 (central management), PostgreSQL | Located at HQ, core data storage. |
| Cloud | AWS IoT Core + DynamoDB | IoT telemetry and real-time analytics. |
| Endpoints | 200 in-truck tablets (drivers), 50 desktops (offices) | User access points; critical risk surface. |
| SaaS Services | Potential third-party integrations (e.g., billing, notifications, GPS mapping APIs) | Must be secured under vendor management. |

## 1.5. Critical Processes

1. **Fleet Tracking & Monitoring** – Continuous real-time location and status reporting.
2. **Fuel Transaction Processing** – Secure authorization and logging of card payments.
3. **Data Collection & Analytics** – Aggregating IoT sensor data for reporting and optimization.
4. **User Access Management** – Authentication and authorization of drivers, managers, and admins.
5. **Incident Response & SOC Monitoring** – Continuous detection, logging, and response to threats.

## 1.6. Stakeholders

|  |  |  |
| --- | --- | --- |
| Stakeholder | Role | Responsibility |
| Business Owners (Executive Mgmt.) | Define objectives, approve budgets | Ensure alignment with sustainability and growth strategy. |
| Fleet Managers | Operational stakeholders | Oversee fleet performance, system usability, and efficiency. |
| IT Operations Team | Infrastructure management | Maintain servers, cloud integrations, and uptime. |
| Security Team (SOC, CISO) | Security & risk management | Ensure compliance, monitor threats, implement controls. |
| Compliance/Legal Officers | Regulatory alignment | Enforce GDPR, PCI-DSS, Egyptian Privacy Law adherence. |
| Drivers & End-Users | Operational users | Input data, interact with mobile app, and rely on service availability. |

[**file:///C:/Users/Gasser/Downloads/GRC%20final.html**](C://Users/Gasser/Downloads/GRC%20final.html)

**2. Risk Assessment – GreenFuel Logistics**

## 2.1 Risk Scoring Model (5×5 Matrix)

We adopt a **qualitative 5×5 scoring model** to assess risks:

|  |  |  |
| --- | --- | --- |
| Likelihood | Description | Score |
| Rare | Highly unlikely, <5% annual chance | 1 |
| Unlikely | Possible but not expected, ~10% | 2 |
| Possible | Could occur at least once in 3 years | 3 |
| Likely | Expected once per year | 4 |
| Almost Certain | Happens multiple times per year | 5 |
|  |  |  |
| Impact | **Description (business consequence)** | | **Score** |
| Insignificant | Negligible effect, no downtime, no regulatory issue | | 1 |
| Minor | Limited disruption (<4 hrs), small data exposure | | 2 |
| Moderate | Noticeable outage (1 day), reputational impact, small fines | | 3 |
| Major | Multi-day disruption, regulatory penalties, serious reputation | | 4 |
| Critical | Mission-critical failure, long downtime, large fines, lawsuits | | 5 |

**Risk Rating = Likelihood × Impact (1–25).**

* **Low (1–6)**: Acceptable.
* **Medium (7–12)**: Requires monitoring.
* **High (13–19)**: Mitigation or transfer required.
* **Critical (20–25)**: Must be treated immediately.

## 2.2 Risk Appetite Statement

GreenFuel Logistics has a **low risk appetite for operational disruptions, data breaches, and regulatory non-compliance** due to the safety-critical nature of fleet operations and financial transactions.

The organization tolerates **moderate risks in innovation and technology adoption** (e.g., cloud analytics, IoT telemetry) but has **zero tolerance for PCI-DSS violations, driver safety risks, or prolonged fleet downtime**.

## 2.3 Risk Register (8 Key Risks)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Risk Description | Likelihood | Impact | Inherent Risk | Residual Risk (after controls) | Owner | Treatment | Justification |
| R1 | Data breach of **Fuel Card Payment System** (PCI scope) | Likely (4) | Critical (5) | 20 (Critical) | 10 (Medium) | Compliance Officer | **Mitigate** | Implement PCI-DSS controls, tokenization, encryption, regular audits. |
| R2 | **IoT Gateway compromise** leading to fleet telemetry manipulation | Possible (3) | Major (4) | 12  (High) | 8 (Medium) | CISO | **Mitigate** | Strengthen VPN/mTLS, IDS for IoT, firmware patch mgmt. |
| R3 | **Ransomware attack** on HQ Windows Server 2016 (AD, identity) | Likely  (4) | Major (4) | 16  (High) | 9 (Medium) | IT Ops Lead | **Mitigate** | Patch mgmt, EDR, offline backups, phishing awareness. |
| R4 | **Driver mobile tablets** lost/stolen with cached fleet data | Almost Certain  (5) | Moderate (3) | 15  (High) | 6 (Low) | IT Security | **Mitigate** | MDM, EDR, remote wipe, enforced encryption. |
| R5 | **Cloud misconfiguration** (AWS IoT/DynamoDB exposed publicly) | Possible (3) | Critical (5) | 15  (High) | 9 (Medium) | Cloud Architect | **Mitigate** | IaC scans, CSPM, IAM hardening, least privilege. |
| R6 | **Service downtime** in Fleet Management System impacting logistics ops | Likely  (4) | Major (4) | 16  (High) | 12 (Medium) | Fleet Manager | **Mitigate/Transfer** | Redundancy + DR plan, cloud SLA with vendor. |
| R7 | **Insider threat** (fraudulent fuel card transactions) | Unlikely (2) | Major (4) | 8 (Medium) | 5  (Low) | Compliance & Finance | **Mitigate/Accept** | Transaction monitoring, segregation of duties, logging. |
| R8 | **Regulatory non-compliance** with GDPR/Egyptian Privacy Law | Possible (3) | Major (4) | 12 (High) | 7 (Medium) | Legal/Compliance | **Mitigate** | Updated privacy policy, DPO role, data subject rights process. |

## 2.4 Heatmap (Likelihood × Impact)

**[file:///C:/Users/Gasser/Downloads/HeatMap GRC final Assesment.html](file:///C:/Users/Gasser/Downloads/HeatMap GRC final Assesment.html  )**

3.ISO 27001:2022 – Statement of Applicability (SoA) Excerpt

### **Scope**

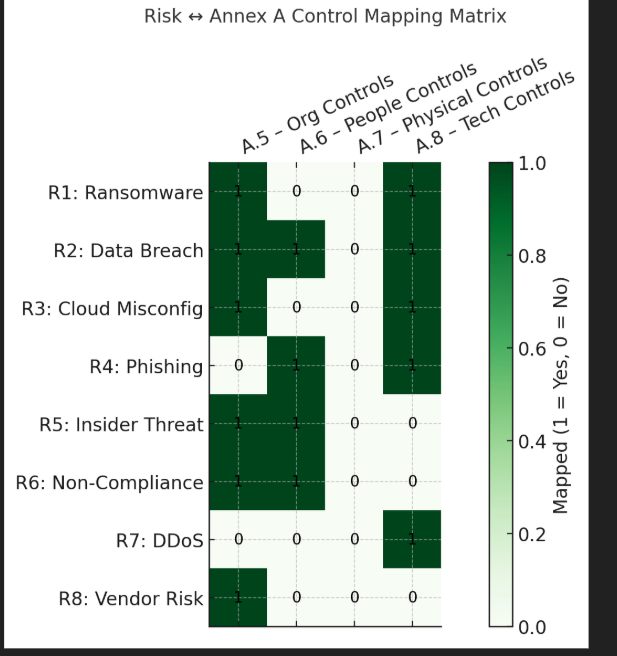
This SoA excerpt covers high-priority risks identified in the Risk Register (Ransomware, Data Breach, Cloud Misconfiguration, Phishing, Insider Threat, Regulatory Non-Compliance, DDoS, Vendor Risk).  
It maps these risks to **ISO/IEC 27001:2022 Annex A controls** and documents applicability, rationale, and implementation status.

## 3.1 Risk-to-Control Mapping Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Annex A Control(s)** | **Control Name (2022)** | **In/Out of Scope** | **Rationale / Implementation Decision** |
| **R1: Ransomware Attack** | A.5.23, A.8.16, A.8.28 | Information security for use of cloud services; Logging & monitoring; Secure coding | **Included** | Endpoint detection, regular patching, centralized monitoring applied. Critical for ensuring resilience. |
| **R2: Data Breach (Customer PII exposure)** | A.5.12, A.5.15, A.5.34 | Data protection & privacy; Access control; Information deletion | **Included** | Regulatory driver (GDPR). Strong identity & access management (IAM), data loss prevention (DLP), and retention policies enforced. |
| **R3: Cloud Misconfiguration** | A.5.23, A.5.30, A.5.36 | Cloud security; Secure configuration; Secure development lifecycle | **Included** | Use of CSPM (Cloud Security Posture Management) to scan/alert misconfigurations. Control must be applied due to reliance on SaaS/IaaS. |
| **R4: Phishing & Social Engineering** | A.6.3, A.6.4, A.6.8 | Awareness, training, and education; Threat intelligence; Anti-malware defenses | **Included** | Users are first line of defense; mandatory awareness campaigns and phishing simulations applied. |
| **R5: Insider Threat** | A.6.2, A.6.6, A.6.9 | Employment lifecycle; Segregation of duties; Monitoring activities | **Included** | Segregation of duties reduces single point abuse; insider monitoring & HR onboarding/offboarding processes active. |
| **R6: Regulatory Non-Compliance** | A.5.1, A.5.2, A.5.34 | Policies for ISMS; IS roles & responsibilities; Compliance with legal/contractual requirements | **Included** | Legal/regulatory adherence mandatory. ISMS documentation maintained and reviewed annually. |
| **R7: DDoS Attack** | A.8.16, A.8.22 | Logging & monitoring; Resilience against attacks | **Included** | Technical controls (WAF, CDN, rate-limiting) in place. Accept residual risk within defined appetite. |
| **R8: Vendor/Supply Chain Risk** | A.5.19, A.5.20 | Supplier relationship security; Supplier monitoring | **Included** | Vendor due diligence and SLA security clauses mandatory. Regular supplier audits scheduled. |

## 3.2 Statement of Applicability – Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Annex A Clause** | **Control** | **Applicability** | **Justification** |
| A.5 – Organizational Controls | Policies, IS roles, compliance, supplier security | **Included** | Essential for governance, regulatory adherence, and third-party assurance. |
| A.6 – People Controls | Awareness, employment lifecycle, segregation of duties | **Included** | High relevance due to phishing & insider risks. |
| A.7 – Physical Controls | Physical entry, equipment security | **Excluded** | Most infrastructure cloud-hosted; physical hosting outsourced to CSP. Only office access controls handled separately. |
| A.8 – Technological Controls | Logging, monitoring, secure coding, resilience | **Included** | Directly addresses ransomware, data breach, DDoS, and misconfiguration risks. |

****

**4. Secure Architecture & Segmentation**

## 4.1 Target Architecture Design

### **Segmentation Principles**

* **Zone-based segmentation**: Business-critical systems separated into **zones** with only minimal, justified traffic flows.
* **Defense-in-Depth**: Each layer (IoT, cloud, on-prem, endpoints) is shielded with **gateways, reverse proxies, and firewalls**.
* **Least privilege**: Inbound and outbound rules restricted to required services only.
* **Zero trust extension**: Authentication & encryption at every interface (TLS/mTLS, VPN).

### **Proposed Zones**

* **External Zone**: Internet, third-party SaaS (maps, payment).
* **DMZ (Demilitarized Zone)**:
  + Web Application Firewall (WAF) / Reverse Proxy (filters driver mobile app & fleet manager dashboard).
  + API Gateway (validates tokens, rate-limits requests).
* **Application Zone**:
  + Fleet Management System (FMS), Fuel Card Payment System, Web Dashboard.
  + Middleware/API services.
* **Data Zone**:
  + PostgreSQL (HQ), DynamoDB (AWS).
  + Telemetry storage (IoT Core).
* **IoT Zone**:
  + IoT gateways in trucks (Debian 11).
  + Enforced VPN tunnels to HQ/Cloud.
* **User Zone**:
  + Driver tablets (MDM-enrolled).
  + Office desktops (EDR-protected).
* **Security Zone**:
  + SOC/SIEM, IDS/IPS, log servers, monitoring.

# 4.2 Reference Diagram (Abstracted)

## 4.3 Minimal Inbound/Outbound Rules (Firewall / Segmentation Table)

|  |  |  |  |
| --- | --- | --- | --- |
| Source Zone | Destination Zone | Allowed Service/Ports | Justification |
| Internet | DMZ (WAF) | HTTPS (443) | Secure entry point for apps |
| DMZ (WAF) | APP (FMS/Dashboard) | HTTPS (443) | Forward filtered requests |
| APP (FMS) | DATA (PostgreSQL) | TCP 5432 | FMS queries DB |
| APP (FMS) | DATA (DynamoDB) | HTTPS (443) | Cloud telemetry access |
| IoT Gateways | DMZ (API Gateway) | MQTT/TLS 8883 | Telemetry ingestion |
| User Tablets | DMZ (WAF) | HTTPS (443) | Mobile app access |
| Desktops | APP (Dashboard) | HTTPS (443) | Fleet manager dashboard |
| SOC/IDS | All Zones | Syslog (514/TCP/UDP) | Security monitoring |
| MDM | Tablets/Desktops | HTTPS (443), MDM agent | Device control and patching |

## 4.4 Policy Snippets

**4.4.1 Network Segmentation Policy**

**Objective:** Ensure that network traffic is restricted, monitored, and controlled between security zones to reduce attack surface.

**Policy Statements:**

1. All environments (On-Prem, Cloud, IoT, Endpoints, Security, External) must be **segmented into distinct network zones**.
2. A **default-deny rule** must be enforced on all firewalls: traffic is denied unless explicitly authorized.
3. Inbound traffic to internal systems must only pass through a **DMZ layer** (e.g., WAF, reverse proxy, API gateway).
4. Inter-zone communication must follow the **minimal inbound/outbound rule set**, updated annually or when systems change.
5. **No direct Internet access** is allowed to the Data Zone or Application Zone.

**4.4.2 IoT Security Policy**

**Objective:** Protect IoT gateways and telemetry flows from compromise.

**Policy Statements:**

1. All IoT gateways must establish **VPN tunnels using mTLS** (mutual TLS) to HQ or Cloud IoT Core.
2. Only **MQTT over TLS (port 8883)** and management channels are permitted outbound from IoT devices.
3. IoT gateways must implement **secure boot, OS hardening, and signed firmware updates**.
4. IoT traffic must be monitored by **IDS/IPS sensors** positioned at the IoT-Cloud interface.
5. Compromised or anomalous devices must be **isolated immediately** by the SOC.

**4.4.3 Application Security Policy**

**Objective:** Safeguard web, mobile, and payment systems against cyberattacks.

**Policy Statements:**

1. All public-facing applications must sit behind a **Web Application Firewall (WAF)** and use **TLS 1.2+ encryption**.
2. All API endpoints must use **OAuth2/JWT authentication** with role-based access control (RBAC).
3. The **Fuel Card Payment System** must comply with **PCI DSS requirements**, and no cardholder data may be stored unencrypted.
4. Vulnerability scans and **secure code reviews** must be conducted before release into production.
5. A **staging/UAT environment** must exist; production deployments require formal approval from IT + Compliance.

**4.4.4 Endpoint Security Policy**

**Objective:** Secure user devices (driver tablets, office desktops) to prevent compromise.

**Policy Statements:**

1. All endpoints must be **enrolled in Mobile Device Management (MDM)** or Endpoint Detection & Response (EDR) before accessing systems.
2. Devices must enforce **disk encryption, screen lock, and remote wipe capabilities**.
3. Outbound connections are restricted to:
   * **HTTPS (443)** for apps and cloud services.
   * **MDM/EDR servers** for updates and compliance checks.
4. Drivers’ tablets are limited to **fleet applications only** (kiosk mode).
5. All desktops must run **anti-malware software with daily signature updates**.

**4.4.5 Monitoring & Logging Policy**

**Objective:** Ensure visibility across all zones through centralized monitoring.

**Policy Statements:**

1. All systems (IoT, Applications, Endpoints, Databases) must forward logs to a centralized **SOC/SIEM** over **TLS-secured channels**.
2. Logs must include at minimum: **authentication events, privilege changes, data access, system errors, and network flows**.
3. Logs must be retained for a minimum of **12 months** for compliance (PCI DSS, GDPR, Egyptian law).
4. IDS/IPS must monitor traffic at **IoT → Cloud**, **DMZ → App**, and **App → Data** boundaries.
5. SOC analysts must perform **daily monitoring, weekly correlation reviews, and monthly compliance reports**.

**4.4.6 Change & Configuration Management Policy**

**Objective:** Ensure secure and controlled changes across environments.

**Policy Statements:**

1. Any firewall, routing, or segmentation change must undergo **Change Advisory Board (CAB) review**.
2. Configuration baselines must be enforced using **IaC (Infrastructure as Code)** templates (e.g., Terraform, Ansible).
3. Unauthorized changes must trigger **alerts in SIEM** and be escalated to Security.
4. Network and system configurations must be **audited quarterly**.

**4.4.7 Access Control Policy**

**Objective:** Enforce least privilege and secure authentication between zones.

**Policy Statements:**

1. All privileged access to servers, DBs, and cloud consoles must use **MFA (multi-factor authentication)**.
2. **Role-based access controls (RBAC)** must be applied for Fleet Managers, Drivers, IT Ops, and Compliance staff.
3. Direct SSH/RDP access from Internet is prohibited; all remote admin must go through a **bastion host + VPN**.
4. API keys and credentials must be stored only in **secure vaults (e.g., AWS Secrets Manager, HashiCorp Vault)**.
5. **Compliance & Legal Alignment**

GreenFuel operates in a highly regulated environment due to its involvement with payment processing (Fuel Card System), personal data handling (drivers, fleet managers, customers), and cloud services (AWS IoT Core, DynamoDB). Compliance is not just about avoiding penalties, it directly impacts customer trust, operational continuity, and brand reputation.

# Applicable Frameworks & Laws

## PCI-DSS (Payment Card Industry Data Security Standard)

* + - Mandatory for any entity processing cardholder data.
    - Covers access control, encryption, vulnerability management, and monitoring.
    - Directly impacts Fuel Card Payment System.

## GDPR (General Data Protection Regulation, EU)

* + - Relevant if GreenFuel manages data of EU drivers/customers.
    - Covers lawful processing, user consent, data subject rights, breach notification (72 hours).
    - Non-compliance fines: up to €20M or 4% of global turnover.

## Egyptian Data Protection Law No. 151/2020

* + - National equivalent of GDPR.
    - Requires registration with the regulator, lawful consent, cross-border transfer controls, breach notification.
    - Applies to driver and employee personal data stored in HQ systems.

## ISO/IEC 27001:2022

* + - Best-practice framework for ISMS (Information Security Management System).
    - Provides structured governance, risk treatment, continuous improvement.
    - GreenFuel is aligning operations with Annex A controls to manage cyber risks.

## AWS Shared Responsibility Model

* + - AWS secures infrastructure (physical, hypervisors, networking).
    - GreenFuel secures data, applications, identity access, configurations.
    - Misconfigurations (e.g., open S3 buckets, weak IAM roles) remain GreenFuel’s

responsibility.

1. **Compliance Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Framework / Law** | **Requirement** | **Existing / Planned Control** | **Gap** | **Remediation Plan** | **Why It Matters** |
| **PCI-DSS** | Strong authentication for cardholder data environments | VPN +  encryption in place | No MFA for payment system access | Implement **MFA + centralized identity management** | Prevents fraud and ensures PCI certification |
| **PCI-DSS** | Encrypt cardholder data in transit & at rest | TLS 1.2+, DB  encryption enabled | No **key management lifecycle** | Adopt **AWS KMS with rotation & access logging** | Protects against insider abuse and theft |
| **GDPR / Egypt Law** | Data subject rights (access, deletion, portability) | Logs exist in DB | No **formal DSAR (Data Subject Access Request) workflow** | Develop **request portal + compliance team training** | Avoids fines and builds customer trust |
| **GDPR / Egypt Law** | Breach notification within 72 hours | SOC  monitoring in place | No **documented incident response playbook** | Establish **IR plan with escalation matrix & regulator templates** | Ensures timely compliance with legal deadlines |
| **ISO 27001** | ISMS governance (policies, audits, risk mgmt) | Some policies exist | No **formal ISMS scope/policy stack** | Define ISMS scope, implement policy framework, conduct **quarterly ISMS audits** | Creates structured, repeatable governance |
| **AWS Shared Responsibility** | Secure cloud configuration (IAM, encryption, monitoring) | IAM roles & VPC security groups | No **continuous monitoring** for misconfigs | Deploy **CSPM (Cloud Security Posture Mgmt) tool** + AWS Config | Prevents cloud breaches due to misconfigurations |

**3.vendor risk management**



# Key Insights

* **Compliance is proactive, not reactive** → Building controls in early avoids expensive

retrofits.

* **PCI-DSS and Law 151 are mandatory** → non-compliance directly risks **legal penalties**

## and loss of payment partnerships.

* **AWS misconfigurations are a leading cloud risk** → GreenFuel must invest in **continuous monitoring tools** (CSPM, GuardDuty, Security Hub).
* **Vendor governance is as important as internal governance** → third-party failures can

directly affect GreenFuel’s customers and brand.

**6.Training, Awareness & Governance**

# Purpose and Objectives

The objective of this program is to ensure that GreenFuel Logistics’ workforce, management, and governance structures actively contribute to the protection of critical assets, compliance obligations, and business continuity. Training, awareness, and governance form the human and organizational layer of defense, complementing technical controls.

# Security Training Program

Training must be structured, role-specific, and mandatory.

## General Staff (All Employees):

* + - Core cybersecurity hygiene (passwords, MFA, phishing).
    - Data classification and secure handling of sensitive information.
    - Incident reporting responsibilities.

## Drivers & Operations Staff:

* + - Safe use of mobile fleet applications.
    - Avoiding SMS/email-based scams targeting drivers.
    - Steps to follow in case of lost or stolen devices.

## Technical Teams (IT, Developers, Cloud Administrators):

* + - Secure coding practices and cloud security (OWASP, AWS shared responsibility).
    - System hardening, patch management, and monitoring.
    - Incident response procedures and red/blue team exercises.

## Management & Leadership:

* + - Compliance awareness (PCI DSS, GDPR, Egypt Law 151/2020).
    - Governance duties under ISO 27001.
    - Escalation and decision-making in crisis scenarios.

## Delivery & Frequency:

* + Induction training for all new hires.
  + Annual mandatory refresher programs.
  + Quarterly technical workshops for IT staff.
  + E-learning modules, supported by simulations and case studies.

# Awareness Initiatives

Awareness must extend beyond formal training and be embedded into daily culture.

* + **Phishing Simulations:** Regular campaigns to test resilience and reinforce learning.
  + **Internal Communications:** Monthly security newsletters, quick tips, and alerts on emerging threats.
  + **Visual Campaigns:** Posters and reminders in depots, offices, and driver hubs.
  + **Recognition Programs:** Incentives for employees who proactively report phishing or security incidents.

This approach promotes **continuous reinforcement**, ensuring staff remain alert between formal training cycles.

# Governance Structure

To embed accountability, GreenFuel should adopt a formal security governance framework aligned with ISO 27001.

## Information Security Steering Committee (ISSC):

* Chaired by CIO or CISO.
* Includes representatives from IT, Operations, Compliance, and HR.
* Meets monthly to review incidents, training completion, audit findings, and regulatory updates.

## Policy Framework:

* **Information Security Policy** – overarching principles.
* **Acceptable Use Policy** – governs systems, devices, and internet use.
* **Data Protection & Handling Policy** – addresses classification, storage, and disposal.
* **Incident Response Policy** – formalizes reporting and escalation paths.

## Accountability:

Training completion rates and awareness campaign outcomes form part of annual performance reviews for staff and managers.

# Incident Reporting & Escalation

A clear reporting chain ensures timely response:

1. Employee identifies a potential incident (phishing, lost laptop, unauthorized access).
2. Incident reported via a **dedicated hotline or online portal**.
3. IT Security Team conducts triage and initial response.
4. Severe incidents escalated to ISSC and senior management within predefined SLAs.
5. Post-incident review integrated into future training and awareness activities.

This process ensures that employees are **empowered to act quickly** and that governance structures maintain oversight.

# Metrics and Continuous Improvement

Governance effectiveness is measured through defined Key Performance Indicators (KPIs):

* + Training completion rate (target: ≥ 95%).
  + Reduction in phishing click-through rates per quarter.
  + Average time taken to report incidents.
  + Percentage of policies reviewed and updated annually.

Results are reviewed by ISSC and feed into a **continuous improvement cycle** to align with evolving threats and regulatory changes.

# Conclusion

By embedding structured training, ongoing awareness, and a robust governance framework, GreenFuel Logistics ensures that its workforce becomes a **proactive defense layer** against cyber threats. Governance mechanisms formalize accountability, awareness initiatives reinforce vigilance, and training builds competence—together strengthening resilience, compliance, and business continuity.