**Integrated Training, Awareness & Governance (T.A.G) Plan**

Investing in **secure infrastructure** is only half of the equation. The other, more critical half is building a "human firewall" capable of using these technologies and responding to threats effectively. This plan is the foundation that connects your technical assets (like **SIEM** and **EDR**) with the human element to ensure maximum possible protection.

**Part 1: The Awareness & Training Program**

The goal of this program is to build a security culture where every employee understands their role in protecting the company. The content is tailored to specific job roles and the risks they face.

**1.1. Strategic Program Objectives**

* **Build a Security Culture:** Instill security awareness across all levels of the company as part of every employee's daily responsibility.
* **Reduce Human Risk:** Decrease the number of security incidents resulting from human error, such as phishing attacks.
* **Enable Response:** Empower employees to recognize and report threats quickly, in accordance with the Incident Response Policy.
* **Ensure Compliance:** Ensure all individuals understand the data protection policies and regulatory requirements like **PCI DSS** and **GDPR**.

**1.2. Targeted Training Modules by Role**

Each job role receives specialized training designed for its specific risks and responsibilities.

* **For All Employees (Including HR):**
  + **"Digital Security Fundamentals" Module:** Covers basic concepts like the importance of strong passwords, securely handling personal devices, and recognizing fraudulent emails.
  + **"Data Handling" Module:** Focuses on how to securely handle sensitive customer data, especially the personally identifiable information (PII) stored in the database.
  + **"Incident Reporting" Module:** Provides practical steps for reporting any suspicious activity, from a questionable email to strange system behavior.
* **For IT & Infrastructure Teams:**
  + **"Patch Management" Module:** Teaches how to follow a schedule for applying security updates to all systems to prevent the exploitation of vulnerabilities in legacy systems.
  + **"Cloud Infrastructure Security" Module:** Covers security best practices in the **GCP** environment, including firewall management and access control.
* **For Security Teams (SOC) & Security Analysts:**
  + **"Incident Response" Module:** Hands-on training for responding to complex attack scenarios, such as ransomware, including how to isolate infected machines and identify the source of the attack.
  + **"Forensic Analysis" Module:** Training on how to use **SIEM** logs and **EDR** data to conduct digital forensic investigations after an incident.

**1.3. Training Methodology & Measurement**

We will use a mix of tools and metrics to ensure training effectiveness.

| Methodology | Frequency | Target Audience | Success Metrics |
| --- | --- | --- | --- |
| **E-learning Modules** | Annually for all employees, and upon hiring | All Employees | Completion rates, scores on final quizzes. |
| **Phishing Simulations** | Quarterly | All Employees | Phishing click-through rate, reporting rate. |
| **Interactive Workshops** | Bi-annually | IT & Security Teams | Performance in practical exercises, such as successfully isolating a server in a test environment. |
| **Periodic Policy Review** | Quarterly | All Employees | Digital signatures on policy documents, to ensure they have been read and understood. |

**Part 2: The Governance Framework**

This section ensures that security awareness translates into actionable policies and procedures that are consistently applied and reviewed.

**2.1. Governance Structure**

* **ISMS Scope:** The ISMS covers all assets in the hybrid cloud environment, from servers in **GCP** to on-premise endpoints, to ensure compliance with the **ISO 27001** standard.
* **GRC Committee:**
  + **Members:** Executive Sponsor, CFO, CISO, COO, and a representative from Legal/Compliance.
  + **Responsibilities:** Overseeing risk, reviewing security policies, and assessing business continuity readiness.

**2.2. The Policy Management Lifecycle**

1. **Development & Approval:** Policies are drafted based on identified risks and objectives, then submitted to the GRC Committee for formal approval.
2. **Dissemination & Communication:** Policies are published internally and are integrated into the annual training program to ensure they are understood.
3. **Enforcement & Monitoring:** Policies are mandatory. Compliance is monitored via internal audits and **SIEM logs**.
4. **Regular Review:** All policies are reviewed at least annually, or when significant changes occur in technology or regulations.

**2.3. The Detailed Compliance and Audit Plan**

| Quarter | Key Activities | Responsible Team | Expected Outcomes |
| --- | --- | --- | --- |
| **Q3 2025** | **Focus:** Internal ISMS audit and policy review. | Compliance & Risk Team. | An audit report identifying gaps between current procedures and company policies, along with a corrective action plan. |
| **Q4 2025** | **Focus:** Human awareness testing and vendor risk assessment. | Security Team, Risk Management. | A report detailing the phishing click-through rate, and an updated list of risks from external vendors and partners. |
| **Q1 2026** | **Focus:** Penetration test follow-up and vulnerability remediation audit. | IT Team, Security Team. | A report confirming that all security vulnerabilities discovered during the penetration test have been fully remediated. |
| **Q2 2026** | **Focus:** Full compliance audit (PCI & GDPR) and final report generation. | All Stakeholders (led by Compliance Team). | A comprehensive report on compliance status to ensure the company is ready for external audits and avoids fines. |