**Training, Awareness & Governance**

Role-based training tied to risks (e.g., insider threats from HUM-001, phishing from human error).

**Training Matrix**

| **Role/Stakeholder** | **Training Content** | **Frequency** | **Tied to Risks/Incidents** |
| --- | --- | --- | --- |
| All Employees (incl. HR) | General security awareness, phishing, data handling. | Annual + quarterly refreshers | Human error, insider leaks (HUM-001/002). |
| IT & Infrastructure Teams | Patch management, vulnerability scanning. | Bi-annual | Legacy system exploits (PHYS-001/002). |
| Security Teams | Incident response, logging/monitoring. | Quarterly | Data breaches (SW-001, INT-001). |
| Compliance & Risk Management | GDPR/PCI DSS compliance, PII protection. | Annual | Regulatory non-compliance (DB-004). |
| Business Owners | Risk oversight, vendor due diligence. | Annual | Overall business continuity. |

**Governance Calendar**

ISMS Scope: Covers all assets/processes in hybrid environment for ISO 27001 certification. Policy Stack: Information Security Policy, Access Control Policy, Incident Response Policy. Committee: GRC Committee (monthly meetings with stakeholders). Internal Audit Plan:

| **Quarter** | **Activity** | **Responsible** |
| --- | --- | --- |
| Q3 2025 | Internal ISMS audit, policy review. | Compliance Team |
| Q4 2025 | Vendor risk assessment, training effectiveness review. | Security & Risk Mgmt |
| Q1 2026 | Penetration testing follow-up, gap remediation audit. | IT & Security Teams |
| Q2 2026 | Full compliance audit (PCI/GDPR), committee report. | All Stakeholders |