**SECURITY AWARENESS PROGRAM ROLLOUT PLAN**

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| Document Title: | Security Awareness Program Rollout Plan |
| ISMS Reference: | ISMS-SAP-001 |
| Version: | 1.0 |
| Status: | Final |
| Date Created: | [Insert Date] |
| Last Reviewed: | [Insert Date] |
| Next Review Date: | [Insert Date – Typically Annual] |
| Document Owner: | Information Security Manager |
| Approved By: | Chief Information Security Officer (CISO) |

**PURPOSE**

This Security Awareness Program is designed to build a resilient, security-conscious culture across the organization by educating employees on current cyber threats, reinforcing secure behaviors, and ensuring compliance with regulatory frameworks such as SOC 2, ISO/IEC 27001, HIPAA, and NIST. The program includes a structured training content plan, role-based delivery cadence, behavioral metrics, control mappings, and an ongoing improvement process.

Through consistent, engaging, and targeted learning experiences, this initiative empowers staff to recognize, prevent, and report potential security risks—strengthening both human and technical defenses against evolving threats.

**TABLE OF CONTENTS:**

[Business Scenario & Program Objectives 2](#_Toc197258996)

[Target Audience Segmentation 2](#_Toc197258997)

[Step-by-Step Program Implementation (Detailed) 2](#_Toc197258998)

[Training Content Plan 4](#_Toc197258999)

[Delivery Cadence & Channels 4](#_Toc197259000)

[Behavior Metrics & KPIs 4](#_Toc197259001)

[Control Mappings & Risk Alignment 5](#_Toc197259002)

[Tools, Evidence Strategies, and Audit Readiness 5](#_Toc197259003)

[Roles & Responsibilities 5](#_Toc197259004)

[Continuous Improvement Plan 5](#_Toc197259005)

[Approval 6](#_Toc197259006)

## Business Scenario & Program Objectives

**Scenario:**The organization is scaling rapidly, handling sensitive customer data and undergoing audits for SOC 2 and ISO/IEC 27001 compliance. Security incidents traced to human error, weak password practices, and phishing attempts have highlighted the need for structured security awareness efforts.

**Objectives:**

* Reduce human-centric security risks
* Meet compliance obligations (SOC 2, ISO 27001, HIPAA)
* Increase reporting of suspicious activity and improve incident response
* Build long-term security awareness and accountability across all roles

## Target Audience Segmentation

|  |  |  |
| --- | --- | --- |
| **Group** | **Training Type** | **Frequency** |
| All Employees | Core Security Awareness | Quarterly |
| Managers | Role-Specific Security & Oversight | Semi-Annually |
| Developers/IT | Secure Coding, Cloud Security | Monthly |
| High-Risk Roles (e.g., Finance, HR) | Targeted Training (e.g., phishing, data handling) | Quarterly |
| New Hires | Security Onboarding Module | First Week |

## Step-by-Step Program Implementation (Detailed)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Step** | **Phase Name** | **Description** | **Key Outputs / Deliverables** | **Responsible Party** |
| 1 | **Define Scope & Objectives** | Align the program with business goals (e.g., audit readiness, culture change) and define measurable objectives (e.g., reduce phishing risk by 40%). | - Program Charter - Risk Register - Mapped Framework Controls | CISO / Security Program Manager |
| 2 | **Identify Risks & Target Roles** | Conduct a human risk assessment by reviewing past incidents, phishing click rates, audit findings, and employee roles (e.g., developers vs. HR staff). | - Human Risk Heatmap - Audience Segmentation Matrix | GRC Lead / IT Security / HR |
| 3 | **Select Delivery Platform** | Choose or configure an LMS and phishing simulation tool that supports SCORM content, role-based paths, and integrations (e.g., SSO, HRIS sync). | - Tool Procurement or Configuration Plan | IT / Learning & Development (L&D) |
| 4 | **Design Training Curriculum** | Develop or procure training modules aligned to risk and compliance frameworks. Ensure content includes videos, quizzes, simulations, and policy references. | - Annual Training Plan - Storyboards - SCORM Package or Licenses | Security Awareness Coordinator |
| 5 | **Pilot Training with Key Groups** | Soft launch to a small group (e.g., IT, Finance) to test user experience, clarity, and tech issues. Collect feedback and adjust before full deployment. | - Pilot Feedback Report - Issue Log | L&D / Security Trainer |
| 6 | **Company-Wide Rollout** | Launch with a kickoff campaign (email, Slack, posters), executive support, and clear deadlines. Rollout in phases if needed (e.g., by department). | - Rollout Schedule - Internal Comms Plan | Communications / HR / CISO |
| 7 | **Run Simulated Phishing Tests** | Schedule monthly or quarterly phishing simulations with varied themes (e.g., shipping alerts, HR requests). Provide just-in-time training after clicks. | - Phishing Reports - Remediation Training Paths | Red Team / Awareness Lead |
| 8 | **Collect Metrics & Feedback** | Track quiz scores, completion rates, click rates, and reporting behavior. Run annual security culture surveys and manager feedback sessions. | - Metrics Dashboard - Culture Survey Summary | GRC / HR |
| 9 | **Audit Evidence Collection** | Document training completions, phishing simulation results, and training revisions. Ensure access logs are retained and available for audits. | - LMS Export Files - Evidence Binder (manual or digital) | GRC / Compliance Analyst |
| 10 | **Annual Program Review** | Update the curriculum based on new threats, compliance changes, and behavioral trends. Integrate lessons learned into tabletop exercises and new policies. | - Updated Program Roadmap - Lessons Learned Report | CISO / Awareness Lead |

**Implementation Timeline Example (For Year 1)**

| **Month** | **Key Activities** |
| --- | --- |
| Month 1 | Kickoff planning, tool selection, stakeholder buy-in |
| Month 2–3 | Curriculum design, risk analysis, LMS configuration |
| Month 4 | Pilot training and phishing simulation |
| Month 5 | Organization-wide launch |
| Month 6+ | Monthly simulations, quarterly modules, feedback |
| Month 12 | Program review and re-alignment |

## Training Content Plan

**Core Topics (All Staff)**

* Password security & MFA
* Email & phishing awareness
* Secure device use (mobile and desktop)
* Remote work and VPN hygiene
* Reporting procedures and chain of escalation

**Role-Based Topics**

* **IT/Engineers**: Secure code, CI/CD, AWS IAM, S3 bucket permissions
* **HR/Finance**: Handling payroll data, email fraud prevention
* **Executives**: Risk prioritization, breach disclosure, governance duties

**Formats**

* LMS-based learning
* Microlearning videos (2–5 mins)
* Simulated phishing campaigns
* Security newsletters and posters
* Live Q&A during annual security week

## Delivery Cadence & Channels

|  |  |  |
| --- | --- | --- |
| **Cadence** | **Activity** | **Channel** |
| Monthly | Microlearning + Phishing Simulation | LMS + Email |
| Quarterly | Awareness Module + Knowledge Quiz | LMS |
| Annually | All-Hands Security Training Day | Live Event / Webinar |
| Onboarding | Security Essentials Course | LMS / HR Onboarding |

## Behavior Metrics & KPIs

|  |  |  |
| --- | --- | --- |
| **Metric Category** | **Measurement Type** | **Target Goal** |
| **Engagement** | Training completion % | ≥ 95% completion |
| **Phishing Resilience** | Failure rate in simulations | < 5% click-through |
| **Incident Reporting** | Reports of suspicious behavior | Quarterly increase |
| **Knowledge Retention** | Post-module quiz scores | ≥ 85% average |
| **Culture Maturity** | Security sentiment via annual surveys | Year-over-year growth |

## Control Mappings & Risk Alignment

|  |  |  |
| --- | --- | --- |
| **Framework** | **Control Reference** | **Program Coverage Area** |
| SOC 2 | CC1.2, CC2.2, CC4.1 | Security training, awareness, access & process reviews |
| ISO/IEC 27001:2022 | Clauses 6.2, 7.2, A.6.3 | Competence & awareness, training delivery |
| NIST SP 800-53 | AT-2, AT-3, PL-4 | Security training and tailored awareness |
| HIPAA | §164.308(a)(5)(i) | Workforce security awareness |
| PCI DSS v4.0 | Req. 12.6.1 | Employee education |
| COBIT | APO07, DSS06 | HR security and awareness initiatives |
| GDPR | Art. 39(b), 32(4) | Staff training and responsibilities |

## Tools, Evidence Strategies, and Audit Readiness

|  |  |  |
| --- | --- | --- |
| **Evidence Type** | **Tool/Source** | **Audit Use Case** |
| Training Completion Logs | LMS (e.g., KnowBe4, Curricula) | Proof of training fulfillment |
| Phishing Simulation Results | Cofense / Proofpoint / LMS plugin | Behavioral metrics & response rates |
| Surveys and Feedback | Google Forms / Microsoft Forms | Culture tracking & effectiveness rating |
| Quiz Results and Scoring Logs | LMS | Knowledge verification |
| Incident Reports & Trends | Jira / Zendesk / Ticketing platform | Reporting culture & employee vigilance |
| Annual Program Review Document | Confluence / Internal SharePoint | Evidence of continuous improvement |

## Roles & Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| **CISO / Security Lead** | Program design, metrics oversight, compliance integration |
| **HR / L&D** | LMS setup, onboarding integration, policy alignment |
| **Department Heads** | Reinforce adoption, review performance reports |
| **Employees** | Complete assigned trainings, report suspicious activity |

## Continuous Improvement Plan

* Annual review of training effectiveness
* Update topics based on threat intelligence, user feedback, audit findings
* Integrate learning into security policy updates and tabletop exercises
* Retire outdated materials and replace with interactive, modernized content

## Approval

| **Name** | **Title** | **Signature** | **Date** |
| --- | --- | --- | --- |
| [CISO Name] | Chief Information Security Officer | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Date] |
| [HR Lead Name] | ISMS Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Date] |