Security Awareness Program Development Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's dynamic threat landscape, traditional security technology is no longer enough; the human element is now the primary attack vector, with over 85% of breaches involving a human factor. Security Awareness Program Development Training Course is designed to transition security efforts from a "check-the-box" compliance exercise to building a robust Human Firewall. You will master the strategic development of a security awareness program that goes beyond simple instruction, leveraging behavioral science principles and data-driven metrics to foster a sustainable Security Culture. Learn to implement sophisticated Phishing Simulation programs and create engaging, customized content that truly changes employee behavior, transforming your workforce into the organization's strongest line of defense and significantly enhancing overall Cyber Resilience.

This hands-on program equips security, HR, and compliance professionals with the complete framework from needs assessment to Continuous Improvement required to develop and manage a high-impact Security Awareness Program. We focus on integrating your program with your organization's Governance, Risk, and Compliance (GRC) strategy, ensuring every training initiative directly contributes to Risk Mitigation and demonstrates Measurable ROI. Participants will gain the skills to perform audience-specific profiling, select the most effective delivery methods, and use key metrics to prove program value to leadership. By the end, you'll possess a comprehensive, actionable blueprint for embedding a positive, proactive Security Culture that dramatically reduces organizational susceptibility to all forms of Social Engineering attacks.

Programme Curriculum

Security Awareness Program Development Training Course

Introduction

In today's dynamic threat landscape, traditional security technology is no longer enough; the human element is now the primary attack vector, with over 85% of breaches involving a human factor. Security Awareness Program Development Training Course is designed to transition security efforts from a "check-the-box" compliance exercise to building a robust Human Firewall. You will master the strategic development of a security awareness program that goes beyond simple instruction, leveraging behavioral science principles and data-driven metrics to foster a sustainable Security Culture. Learn to implement sophisticated Phishing Simulation programs and create engaging, customized content that truly changes employee behavior, transforming your workforce into the organization's strongest line of defense and significantly enhancing overall Cyber Resilience.

This hands-on program equips security, HR, and compliance professionals with the complete framework from needs assessment to Continuous Improvement required to develop and manage a high-impact Security Awareness Program. We focus on integrating your program with your organization's Governance, Risk, and Compliance (GRC) strategy, ensuring every training initiative directly contributes to Risk Mitigation and demonstrates Measurable ROI. Participants will gain the skills to perform audience-specific profiling, select the most effective delivery methods, and use key metrics to prove program value to leadership. By the end, you'll possess a comprehensive, actionable blueprint for embedding a positive, proactive Security Culture that dramatically reduces organizational susceptibility to all forms of Social Engineering attacks.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Strategically Align the security awareness program with organizational GRC and business objectives.
2. Conduct a comprehensive Human Risk Assessment to identify and prioritize critical behavioral gaps.
3. Design and execute realistic Phishing Simulation and Social Engineering testing campaigns.
4. Develop engaging, targeted content utilizing principles of Behavioral Science for maximum impact.
5. Establish and track Security Awareness KPIs to demonstrate Measurable ROI to executive leadership.
6. Implement Role-Based Training to address specific risks for executives, developers, and high-risk users.
7. Integrate awareness programs with New Hire Onboarding and annual Compliance Training.
8. Master the creation of a positive Security Culture that encourages proactive incident reporting.
9. Develop a Communication Strategy that maintains a continuous security dialogue, not just an annual event.
10. Analyze recent Threat Intelligence to keep training content current and highly relevant.
11. Secure Executive Buy-in and allocate an appropriate budget for long-term program sustainability.
12. Establish processes for Program Maturity and Continuous Improvement using feedback loops and metrics.
13. Address evolving risks like Remote Work Security and the safe use of Generative AI Tools.

Target Audience

1. Information Security Managers/Officers
2. GRC (Governance, Risk, & Compliance) Professionals
3. IT/Cybersecurity Training & Development Specialists
4. Human Resources (HR) & Organizational Development (OD) Leads
5. Audit and Internal Control Staff
6. Business Continuity and Disaster Recovery Managers

7. Data Protection Officers (DPO)
8. IT Operations Managers

Course Modules

Module 1: Foundational Strategy and GRC Alignment

- The Case for Change
- Defining the Security Awareness Framework
- Integrating the program with GRC objectives and regulatory Compliance
- Securing Executive Buy-in and establishing a dedicated budget and governance structure.
- Case Study: A financial institution's failure to train on insider threat protocols leads to a large data exfiltration, highlighting the need for GRC integration.

Module 2: The Human Factor and Behavioral Science

- Identifying and profiling key Target Audiences
- Behavioral Change Models for security adoption.
- Shifting the culture from blame to Positive Reinforcement and security champions.
- Analyzing common cognitive biases that lead to security errors
- Case Study: A healthcare provider uses gamification and micro-learning to achieve a 40% reduction in unsafe practices, demonstrating effective behavioral science.

Module 3: Needs Assessment and Risk Prioritization

- Conducting a Risk-Based Assessment driven by organizational threat intelligence.
- Leveraging Vulnerability Scanning and past incident data to pinpoint weak areas.
- Developing and deploying effective Security Culture Surveys.
- Mapping high-priority threats to specific learning objectives.
- Case Study: A manufacturing firm uses spear-phishing results to tailor training content specifically for their most vulnerable department.

Module 4: Content Design and Delivery Channels

- Designing content for retention.
- Creating a multi-channel Communication Strategy
- The "What, Why, and How" of core topics.
- Role-Based Training content for developers and remote workers.
- Case Study: A tech company moves from annual training to continuous, 3-minute video modules, resulting in a 25% improvement in quiz scores.

Module 5: Phishing, Social Engineering, and Incident Reporting

- Developing a multi-tiered Phishing Simulation Program lifecycle.
- Training staff on advanced Social Engineering tactics
- Establishing clear, simple, and rewarded Incident Reporting Procedures.
- Utilizing simulation data to drive targeted re-training and remediation.
- Case Study: A mid-sized logistics company uses a simulated ransomware-delivery phishing attack to test and improve their reporting and response time.

Module 6: Emerging Threats and Advanced Topics

- Training for Cloud Security Awareness and data classification in SaaS environments.
- Mitigating the risk of Generative AI Tools.
- Implementing Remote Work Security Best Practices
- Content for Physical Security Awareness
- Case Study: An enterprise deploys new training on safe AI use following an internal audit revealing staff inputting sensitive IP into public LLMs.

Module 7: Implementation and Program Launch

- Developing an annual Awareness Training Calendar and deployment schedule.
- Integrating the program into the New Hire Onboarding process.
- Selecting and leveraging a Security Awareness Platform
- The importance of localization, accessibility, and mandatory training enforcement.
- Case Study: An international NGO successfully launches a global program by localizing content into three languages and gaining full regional manager support.

Module 8: Measurement, ROI, and Continuous Improvement

- Defining and collecting key Performance Indicators.
- Calculating and presenting Measurable ROI.
- Establishing a Continuous Feedback Loop and using metrics for content iteration.
- Developing a Program Maturity Model for long-term strategic growth.
- Case Study: A bank tracks the drop in its phishing click rate from 20% to 3% over two years, directly correlating this behavioral change to a reduction in high-severity incidents.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com