INFIMA

Security Awareness Training - CMMC

(As of Jan 1, 2025)

Organizations seeking CMMC Level 2+ accreditation must provide Security Awareness Training to their employees, based on NIST 800-171.

To help meet clients' CMMC requirements, INFIMA's coursework is designed in tandem with security experts, law enforcement and attestation professionals. No provider (INFIMA included) can provide explicit compliance certification for organizations using their Security Awareness Training products. Due to this, we cannot be held liable for compliance-related liabilities.

INFIMA provides a 4 Course Core for all employees to address Sections 3.2.1 and 3.2.3 of NIST 800-171. Additionally, coursework is provided to address the "Role-Based" training requirements of Section 3.2.2 of NIST 800-171.

Core Curricula *(based on NIST 800-171, Sections 3.2.1 and 3.2.3)*

Today's Cyber Attacks: A.I., Phishing and Staying Secure*

-Learn how to avoid hackers' most popular attacks, including AI-driven advances

Social Engineering Attacks and A.I.*

-How Social Engineering risks are changing with the advent of A.I.

Online and Digital Safety*

-Understand how to avoid risky online behaviors to avoid its many dangers

Device and Data Security*

-Your computer holds tons of data that can be challenging to securely store and dispose

Role-Based Curricula Examples *(based on NIST 800-171, Section 3.2.2)*

IT and Security Professionals

Security Beyond the Office ● Ransomware and Other Malicious Software ● Preventing Insider Threats ● Protecting Sensitive Data ● Social Engineering: Attacks and Avoidance ● Avoiding Web-based Attacks

Executives

Preventing Wire Fraud ● Recognizing Insider Threats ● Protecting Sensitive Data ● Social Engineering: Attacks and Avoidance

Financial Controllers

Preventing Wire Fraud ● Recognizing Insider Threats ● Social Engineering Threats