Security and Awareness Training Programs

Best Practices Webinar

September 22, 2022
11:00am – 12:00pm ET

#FISSEA | nist.gov/fissea
Basic is Easy. Amazing is Hard. Getting From Good to Great.
The OIG Perspective

Danny Urquijo
IT Audit Manager
Department of Homeland Security
Office of the Inspector General
What Does the OIG Look for in Security and Awareness Training?
People

• Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external).

• Not only are roles and responsibilities defined across the organization, but performance measures are in place.

• Any lessons learned are not only documented but followed.

• Security and awareness requirements followed.

• Industry best practices are used.

• Training is up to date, people are first line of defense.
Process

• Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.

• Policies and procedure need to be standardized and followed across the organization.

• Compliance must be measured and enforced.

• If there are lessons learned and best practices, apply them to your policies and procedures.

• Policies and procedures need to ensure the proper handling of incident notification and response.
Technology

- Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external).

- Measure and evaluate effectiveness.

- Adequacy of technology used and new threats.

- Effective internal controls.

- Security and protection of the organization’s technological resources and systems.
Reaching Capability Maturing Model Integration (CMMI) Level 5

- Reaching level 4 - Organizations reach a level of maturity where processes, projects, and measurability are clearly defined and controlled.

- Reaching level 5 - Organizations reach this level of maturity when processes, projects, and measurability are standardized and optimized throughout their entire enterprise.

- Challenges/Barriers
  - Lack of expertise
  - Limited talent pools
  - Restrictive budgets
  - Lack of management support
The OIG Perspective

Q&A
Agency Panel

Panelists:

Tomm Larson
Awareness Lead (Cybersecurity)
Idaho National Laboratory

Garth Chablal
IT Specialist
Social Security Administration

Ed Conley
IT Specialist (PSA)
Indian Health Service
Overview

Tell Us About Your Program
Making Training Engaging
Management Buy-In
Events Throughout the Year?
Advice for the Audience
Get Involved

Subscribe to the FISSEA Mailing List FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2022
Email fissea@list.nist.gov

#FISSEA
FISSEA Fall Forum
November 15, 2022
1:00pm – 4:00pm ET

REGISTER TODAY: nist.gov/fissea

#FISSEA
Complete FISSEA Survey

surveymonkey.com/r/FISSEABestPracticesEvent

#FISSEA
Thank You for Joining the Webinar!