itSM Solutions®
IT Experience. Practical Solutions.

NIST Cybersecurity Framework Awareness Training

Overview

This training program is targeted at IT, Cybersecurity and Business professionals looking to understand the basic concepts associated with Digital Transformation, the NIST Cybersecurity Framework and Cybersecurity Risk Management.

Course Introduction

This course is based on the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1. It was published by the National Institute of Standards & Technology in April of 2018.

The **NIST Cybersecurity Framework** (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." Version 1.1 was published by the US National Institute of Standards and Technology in 2018, originally aimed at operators of critical infrastructure. Is being used by a wide range of businesses and organizations, and helps shift organizations to be proactive about risk management.

Course Organization:

The course is organized as follows:

Course Introduction – provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom and online self-paced. The introduction also covers the nature and scope of the examination.

Introduction to Digital Transformation – discusses the current state of cybersecurity in the context of today's threat landscape and what organizations must do in order to ask and answer the question, “Are we secure?”

The NIST Cybersecurity Framework Fundamentals – The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

Cybersecurity Risk Management – Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

Exam FAQ's

There is no exam associated with this course

Credits Earned

- **1** PDU Credit