Applying the NIST Risk Management Framework

Course Summary

Description

In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary risk-based cybersecurity framework (CSF) that is “prioritized, flexible, repeatable, performance-based, and cost-effective.” The CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation’s critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST).

In this session we will discover how the framework works, how to implement it, and what the proposed changes are as framework moves to version 1.1. This session will be an overview of what the frame work is, who needs to follow it, why your company may decide this framework is a good solution for your company to use. We also demo a free tool to help you understand where you current weaknesses are and how you can improve your compliance to the framework.

Topics

- Introduction
- Cybersecurity Policy Regulations and Framework
- RMF Roles and Responsibilities
- Risk Analysis Process
- Step 1: Categorize
- Step 2: Select
- Step 3: Implement
- Step 4: Assess
- Step 5: Authorize
- Step 6: Monitor

Audience

This course is designed for those wanting to learn how the risk management framework works, how to implement it, and what the proposed changes are as the framework moves to version 1.1

Prerequisites

There are no prerequisites for this course.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Applying the NIST Risk Management Framework

Course Outline

I. **Introduction**
   A. Key concepts including assurance, assessment, authorization
   B. Reasons for change to the Risk Management Framework (RMF)
   C. Key characteristics of security
   D. Security controls

II. **Cybersecurity Policy Regulations and Framework**
   A. Evolution and interaction of security laws, policy, and regulations in cybersecurity
   B. Accessing the correct documents for cyber security guidance
   C. Assessment and Authorization transformation goals

III. **RMF Roles and Responsibilities**
   A. Tasks and responsibilities for RMF roles

IV. **Risk Analysis Process**
   A. Four-step risk management process
   B. Impact level
   C. Level of risk
   D. Effective risk management options

V. **Step 1: Categorize**
   A. Key documents in RMF process
   B. Security Categorization
   C. Information System Description
   D. Information System Registration
   Lab: Categorize a fictitious DoD agency information system

VI. **Step 2: Select**
   A. Common Control Identification
   B. Security Control Selection
   C. Tailor security controls
   D. Monitoring Strategy
   E. Security Plan Approval
   Lab: Select security controls for a fictitious DoD agency information system

VII. **Step 3: Implement**
   A. Security Control Implementation
   B. Security Control Documentation
   Lab: Discuss and review decisions related to implementation of security controls

VIII. **Step 4: Assess**
   A. Assessment Preparation
   B. Security Control Assessment
   C. Security Assessment Report
   D. Remediation Actions
   Lab: Consult NIST SP 800-53A to determine appropriate assessment techniques for a fictitious DoD agency.

IX. **Step 5: Authorize**
   A. Plan of Action and Milestones
   B. Security Authorization Package
   C. Risk Determination
   D. Risk Acceptance
   Lab: Practice compiling the documents that make up the Security Authorization Package

X. **Step 6: Monitor**
   A. Information System and Environment Changes
   B. Patches
   C. Ongoing Security Control Assessments
   D. Ongoing Remediation Actions
   E. Key Updates
   F. Security Status Reporting
   G. Ongoing Risk Determination and Acceptance
   H. Information System Removal and Decommissioning
   Lab: Identify vulnerabilities and deficiencies in the information system of a fictitious DoD agency and propose steps to remediate them.

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically