alc

NIST CYBERSECURITY FRAMEWORK PRACTITIONER™

DURATION: 5 DAYS

CYBER SECURITY

ALC's 5-day NIST Cybersecurity Framework Practitioner™ (NFP) course is designed for information security professionals who wish to gain an understanding of the NIST Cybersecurity Framework and its application. The course immerses participants in all aspects of the theory behind the framework, but applies a regional flavour on how the framework can be applied to an Australian or New Zealand context through the use of a case study. Each section has been designed to introduce the NIST view, then expand on this with more detailed and practical information, before making use of a case study to practically apply the knowledge learnt.

WHO SHOULD ATTEND

This course is designed for individuals with at least one year's experience in any of the following:

- Information Technology, Information/Cyber Security
- Other professionals familiar with information security fundamentals

LEARNING OUTCOMES

The key objective is for each participant to complete the course and immediately be able to apply the NIST Cybersecurity Framework in their own work context:

- NIST Cybersecurity Framework Overview
- Identify, Protect, Detect, Respond, & Recover Functions

The course approach has been designed to blend the introduction of a topic via theory and practical exercises, Exercises include:

- Develop an asset register
- Identify threats, determine risks, and make recommendations
- Evaluate service provider models, contrasting risks and opportunities
- Discuss risks associated with storing data in the cloud
- Select security architecture design principles
- Create a data classification scheme and use this for managing risks with cloud solutions
- Define security zones and a security architecture model
- Identify and discuss the advantages and disadvantages of different encryption technologies
- List and prioritise business-critical operations for business continuity
- Evaluate the benefits of an in-house incident response capability versus using a managed service model

GET AHEAD OF THE GAME
GET CERTIFIED

1300 767 592
customerservice@alc-group.com
alctraining.com.au

ALC.Training
@alcgroup
alc-training

COURSE CONTENTS

1. NIST SYBERSECURITY FRAMEWORK OVERVIEW

- Framework Overview
- Informative References Overview
- Core Functions & Categories
- Implementation Tiers
- Framework Profile
- Establishing or improving a cybersecurity program
- Introduction to the Case Study

2. IDENTIFY FUNCTION

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management
  Case Study Exercise 1 – Apply the concepts learnt in the Identify Function

3. PROTECT FUNCTION

- Identity Management, Authentication and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology
  Case Study Exercise 2 – Apply the concepts learnt in the Protect Function

4. DETECT FUNCTION

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
  Case Study Exercise 3 – Apply the concepts learnt in the Detect Function

5. RESPOND FUNCTION

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements
  Case Study Exercise 4 – Apply the concepts learnt in the Respond Function

6. RECOVER FUNCTION

- Recovery Planning
- Improvements
- Communications
  Case Study Exercise 5 – Apply the concepts learnt in the Recover Function

7. CASE STUDY

- Practical Workshop
  - As a group, select an appropriate workshop
  - Systematically work through the steps in the framework
  - Select informative references from ISO27002, PCI DSS, ISM or other resources
- Last hour of the day
  - Each group to present their respective report
  - Issue mock exam for delegates to practice overnight