NIST Cybersecurity Framework Practitioner™

Duration: 5 days

The NIST Cybersecurity Framework was released in 2014 and is gaining widespread use by organisations across the globe. The continuous improvement lifecycle assists organisations to use a tiered, risk-based approach when safeguarding their most critical assets, before, during and after a potentially disruptive cybersecurity incident.

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. There are no pre-requisites to attend, however, to gain the most from the course, it is advisable that delegates have had at least one year in an information security or cyber security role.

Who Should Attend

This course is designed for:

- Information Technology
- Information Security
- 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 Function, Protect Function, Detect Function, Respond Function, Recover Function
- Informative References
- Practical Workshop
- Mock Exam
- Final Exam

The course approach has been designed to blend the introduction of a topic via theory and practical exercises, designed to maximise understanding and retention. Strong use is made of a case study throughout the week’s training. 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

Course Contents

1. NIST Cybersecurity Concepts

- Framework Overview
- Informative References Overview
- Core Functions & Categories
- Implementation Tiers
- Framework Profile
- Establishing or improving a cybersecurity program

2. Identify Function

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

3. Protect Function

- Identity Management, Authentication and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

4. Detect Function

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

5. Respond Function

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

6. Recover Function

- Recovery Planning
- Improvements
- Communications

7. Case Study

- Practical Workshop

8. Review & Exam