# NIST Cybersecurity Foundation Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What Can You Achieve with This Training?

- Build a foundational understanding of **NIST cybersecurity standards and frameworks** to support your organisation's security initiatives.
- Learn how to identify and assess **cybersecurity risks, threats, and vulnerabilities**.
- Understand the structure and purpose of the **NIST Cybersecurity Framework (CSF) 2.0** and the **NIST Risk Management Framework (RMF)**.
- Recognise how **administrative, technical, and physical security controls** help organisations manage cybersecurity risks.
- Develop essential knowledge of **security awareness, incident response, and organisational resilience**.
- Explore how to apply **NIST guidance to practical business scenarios**, supporting cybersecurity governance and continual improvement.

The **NIST Cybersecurity Foundation Training** is a **two-day introductory programme** designed to help participants understand the cybersecurity principles, standards, and guidance developed by the **National Institute of Standards and Technology (NIST)**.

The course provides a structured introduction to cybersecurity risk management and supports participants in contributing to organisational security programmes and informed decision-making.

Throughout the training, participants explore **fundamental cybersecurity concepts, NIST publications, risk management, security controls, security awareness, and incident management**.

The programme explains the relationship between information assets, threats, vulnerabilities, and risks, and how these concepts influence organisational cybersecurity decisions.

Participants are introduced to key NIST publications, including **NIST SP 800-12, NIST SP 800-53, NIST SP 800-37, and NIST SP 800-171**, alongside the **NIST Cybersecurity Framework (CSF) 2.0**.

The course also covers the **NIST Risk Management Framework (RMF)**, providing an overview of its seven lifecycle stages: **Prepare, Categorise, Select, Implement, Assess, Authorise, and Monitor**.

Additional modules address the protection of **Controlled Unclassified Information (CUI)**, the importance of employee security awareness, and the fundamentals of cybersecurity incident management.

Through **scenario-based learning**, participants explore how NIST publications can guide practical security activities, from identifying risks and selecting controls to monitoring, incident response, and continual improvement.

By the end of the course, learners will have a foundation for supporting **NIST-aligned cybersecurity activities, governance, and risk management** within their organisations.

BILGINC IT Academy

info@bilginc.com

bilginc.com


### Exams and Assessments

The course includes a **certification examination** covering fundamental cybersecurity principles and concepts, **risk management**, and **cybersecurity controls**.

## Prerequisites

There are **no prerequisites** for attending this training course.

The programme is suitable for individuals seeking an introduction to cybersecurity principles and NIST guidance.

## Who Should Attend

This course is intended for professionals who want to understand**NIST-based cybersecurity practices** and contribute to organisational information security activities.

It is particularly suitable for:

- **Managers, consultants, and team leaders** supporting cybersecurity initiatives within their organisations
- Employees involved in **cybersecurity or information security activities** who want to understand relevant frameworks and best practices
- Professionals seeking broader knowledge of **cybersecurity governance, risk management, and incident response**
- Individuals interested in **starting a cybersecurity career** or improving their understanding of NIST guidance
- **IT personnel and system administrators** supporting the implementation and maintenance of secure systems

# NIST Cybersecurity Foundation Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

## What You Will Learn

By the end of this course, participants will be able to:

- Explain fundamental **cybersecurity concepts**, including assets, threats, vulnerabilities, risks, and security controls.
- Describe the purpose of major **NIST cybersecurity standards, frameworks, and publications**.
- Recognise the core scope of **NIST SP 800-12, SP 800-53, SP 800-37, and SP 800-171**.
- Explain **NIST's risk-based approach to cybersecurity management**.
- Support basic risk assessments by identifying **assets, threats, and vulnerabilities**.
- Relate **likelihood, impact, and risk responses** to organisational security decisions.
- Describe the **seven stages of the NIST RMF** and their relationship with security controls.
- Recognise **NIST SP 800-53 control families** and the processes used to select, implement, assess, and monitor controls.
- Distinguish between **administrative, technical, and physical security controls**.
- Explain the **six Functions and overall structure of NIST CSF 2.0**.
- Understand the role of **Current and Target Profiles** and **Implementation Tiers** in cybersecurity improvement.
- Recognise the fundamental principles of protecting sensitive information under **NIST SP 800-171**.
- Understand how **security awareness and employee responsibilities** contribute to organisational cybersecurity.
- Explain the basic incident management stages of **preparation, detection, analysis, containment, response, and recovery**.
- Apply **NIST concepts to practical scenarios** to support foundational organisational cybersecurity activities.

## Training Outline

### 1. Cybersecurity Fundamentals

This module introduces the terminology and principles needed to understand cybersecurity and the NIST ecosystem.

- Exploring essential **cybersecurity terminology and principles**
- Understanding **information systems**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Identifying **assets** that require protection
- Recognising **threats and vulnerabilities**
- Introducing the concept of **risk**
- Understanding the purpose of **security controls**
- Establishing the **common vocabulary required to navigate NIST guidance**

### 2. The NIST Cybersecurity Ecosystem

This module provides an overview of NIST standards, frameworks, and publications and explains how they support different cybersecurity activities.

- Introducing **NIST standards, frameworks, and Special Publications**
- Distinguishing between **organisational cyber risk management guidance** and publications covering the **selection, implementation, and assessment of security controls**
- Reviewing key NIST publications:
  - **NIST SP 800-12**
  - **NIST SP 800-53**
  - **NIST SP 800-37**
  - **NIST SP 800-171**
  - **NIST Cybersecurity Framework (CSF 2.0)**

### 3. Cybersecurity Risk Management

This module introduces NIST's risk-based approach to cybersecurity and the fundamentals of risk identification and assessment.

- Understanding **risk concepts** and NIST's **risk-based cybersecurity approach**
- Identifying **assets, threats, and vulnerabilities**
- Understanding **likelihood and impact**
- Determining **risk levels**
- Selecting appropriate **risk responses**
- Maintaining ongoing **risk awareness**

### 4. NIST Risk Management Framework (RMF)

This module introduces the **RMF lifecycle** and explains its relationship with security controls.

BILGINC IT Academy

info@bilginc.com

bilginc.com


**The seven RMF stages:**

1. **Prepare:** Establishing the foundations for risk management activities
2. **Categorise:** Categorising information and systems
3. **Select:** Choosing appropriate security controls
4. **Implement:** Putting selected controls into operation
5. **Assess:** Evaluating security controls
6. **Authorise:** Addressing risk-based authorisation decisions
7. **Monitor:** Continuously monitoring security controls and system security

## 5. NIST Security Controls

This module examines the purpose and structure of**NIST SP 800-53** and the role of security controls in managing cyber risk.

- Understanding the **purpose and structure of NIST SP 800-53**
- Introducing **security control families**
- **Selecting** security controls
- **Implementing** selected controls
- **Assessing** control effectiveness
- **Monitoring** security controls
- Distinguishing between **administrative, technical, and physical controls**
- Understanding how controls contribute to **risk treatment**

## 6. NIST Cybersecurity Framework (CSF) 2.0

This module introduces the structure of**NIST CSF 2.0** and its application to organisational cybersecurity management.

**The six CSF 2.0 Functions:**

- **Govern:** Establishing cybersecurity governance and accountability
- **Identify:** Understanding assets, risks, and relevant organisational factors
- **Protect:** Implementing protective safeguards
- **Detect:** Identifying potential cybersecurity events and anomalies
- **Respond:** Taking action when cybersecurity incidents occur

BILGINC IT Academy

info@bilginc.com

bilginc.com


- **Recover:** Supporting recovery following cybersecurity incidents

**Additional framework components:**

- **Functions**
- **Categories**
- **Subcategories**
- **Organisational Profiles**
- **Current Profiles**
- **Target Profiles**
- **Implementation Tiers**

The module also explores how the CSF supports **cybersecurity improvement** and **communication among organisational stakeholders**.

## 7. Protecting Sensitive Information – NIST SP 800-171

This module introduces the protection of sensitive information in non-federal environments.

- Understanding **Controlled Unclassified Information (CUI)**
- Exploring the protection of **CUI in non-federal systems and organisations**
- Recognising the importance of **NIST SP 800-171** for **defence and government supply chains**
- Examining the relationship between **information requirements, security controls, and supplier assurance**

## 8. Cybersecurity Awareness and Training

This module examines the role of people and organisational awareness in NIST-aligned cybersecurity programmes.

- Understanding the **human element in cybersecurity**
- Developing **security awareness**
- Defining **employee security responsibilities**
- Promoting **acceptable security behaviour**
- Building **organisational cybersecurity capability**

## 9. Incident Management

This module introduces the fundamental stages of cybersecurity incident management.

BILGINC IT Academy

info@bilginc.com

bilginc.com


- **Preparation** for security incidents
- **Detection** of potential incidents
- **Analysis** of incident information
- **Containment** of incidents
- **Response** activities
- **Recovery** following incidents
- Connecting incident response with **risk management, security controls, monitoring, and organisational resilience**

### 10. Applying NIST in Practice

This module explores the practical application of NIST guidance through scenario-based activities.

- Applying **NIST publications to practical scenarios**
- Identifying **key cybersecurity risks**
- Selecting relevant **CSF Functions**
- Determining appropriate **security control areas**
- Evaluating **incident response approaches**
- Reinforcing the relationship between:

**Risk → Framework → Controls → Implementation → Monitoring → Response → Improvement**