Maslak Mahallesi, Maslak Meydan Sk. No:5. Spring Giz Plaza. Maslak/İstanbul
+90 212 282 7700 - info@bilginc.com

NIST Security Framework Foundation

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **2 Days**

Overview

This theory based course provides a foundation awareness of the five functional pillars (Identify, Protect, Detect, Response and Recover) of the National Institute of Standards and Technology (NIST) security framework.

Prerequisites

There are no prerequisites for this course, however, participants are expected to have a basic understanding of computers and the internet.

What You Will Learn

The NIST Security Framework Foundation will focus on the following topics;

1. Identify

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

2. Protect

- Access Control
- Awareness & Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

3. Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

4. Response

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

5. Recover

- Recovery Planning
- Improvements
- Communications

Outline

Module 1 - Asset Management

The data personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organisation's risk strategy.

Module 2 - Business Environment

The organisation's mission, objectives, stakeholders, and activities are understood and prioritised; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Module 3 – Governance

The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Module 4 – Risk Assessment

The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals.

Module 5 - Risk Management Strategy

The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Module 6 – Access Control

Access to assets and associated facilities is limited to authorised users, processes, or devices, and to authorised activities and transactions.

Module 7 – Awareness and Training

The organisation's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Module 8 - Data Security

Information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.

Module 9 - Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Module 10 - Maintenance

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Module 11 - Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Module 12 - Anomalies and Events

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Module 13 - Security Continuous Monitoring

The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Module 14 - Detection Processes

Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Module 15 - Response Planning

Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Module 16 - Communications

Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Module 17 - Analysis

Analysis is conducted to ensure adequate response and support recovery activities.

Module 18 – Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Module 19 – Improvements

Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Module 20 – Recovery Planning

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Module 21 – Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Module 22 – Communications

Restoration activities are coordinated with internal and external parties, such as coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.