# *IT Security (420-F30-HR)*

# *Lab 04 – CyberSecurity Frameworks*

Date assigned: Friday, Feb 14

Date Due: Friday, Feb 14, 10h00 (end of class)

**Objectives:**

Learn:

1. Understand the purpose/role of a cybersecurity framework
2. Understand the different elements of the NIST Cybersecurity framework

**References:** S0401\_Foundations\_Frameworks, NIST Starter Guide

# Foundation and Frameworks – (Overview)

## Foundations - NIST

**Objectives:** Understand the NIST CyberSecurity Framework . Watch this [video](https://www.youtube.com/watch?v=Ula3TG8QS7g). It’s pretty dense, but much of the terms mentioned will be explored further later on in the course.

Reference:

NIST Starter Guides (Reference in MS Teams)

[Wiki article](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework)

**To Do:**

## Answer the following without cutting and pasting in your answers

What are the 6 Core functions of the NIST cybersecurity framework?

Identify, protect, detect, respond, recover.

## What is the purpose of the NIST Cybersecurity Framework?

They are a collection of guidelines designed to manage and mitigate cyber risks

## What is NIST (explain the acronym and the purpose of the organization and part of which government department?)

National institute of standards and technology (department of commerce). The org aims to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

## Complete the table below:

|  |  |
| --- | --- |
| **Task** | **Identify one of the key Functions**  **{Identify, Protect, Detect, Respond, Recover}** |
| Maintain and monitor logs | Detect |
| Train users to follow best practices for IT Security | Protect |
| Test and Update detection processes | Detect |
| Determine critical assets | Identify |
| Update Response Plan | Respond |
| Update/manage public relation or any public messaging | Recover |
| Create and maintain software and hardware inventory | Identify |
| Test Response Plan | Respond |
| Control access to assets and information | Protect |

# Foundation and Frameworks – (Detail)

**Objectives:** Understand planning with the NIST CSF

**To Do:** read [this](https://resources.infosecinstitute.com/topic/nist-csf-the-seven-step-cybersecurity-framework-process/) article and [this](https://www.linkedin.com/pulse/mapping-software-nist-csf-defense-depth-exercise-david) article

## What are the 7 steps recommended on how to establish or improve cybersecurity programs?

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze and Prioritize Gaps
7. Implement Action Plan

## Complete the table below:

|  |  |
| --- | --- |
| **Task** | **Identify one of the seven steps** |
| Identify vulnerabilities and threats to prioritized assets | Conduct a Risk Assessment |
| Execute the highest priority plan to fill the gap between current profile and target profile. | Implement Action Plan |
| Identify important systems and assets that need to be protected | Prioritize and Scope |
| Indicate which of the category and subcategory of the CSF are desired | Create a Target Profile |
| Examine the gaps between the current profile and the target profile. Determine which gaps should be addressed first. Plan on what’s needed to fill those gaps | Determine, Analyze and Prioritize Gaps |
| Indicate which of the category and subcategory of the CSF are presently achieved | Create a Current Profile |
| Determine risk on the organizational assets | Conduct a Risk Assessment |
| Determine which assets are more important to protect | Prioritize and Scope |

## Explain: In general business speak, what is a “gap analysis”?

When talking about gap analysis, we are talking about how you can analyse where you are and where you want to be and what the space in between represents and how you can get to where you want to be.

**Marking Scheme**

|  |  |  |
| --- | --- | --- |
|  | **Mark** | **Out of** |
|  |  |  |
| **Part A: Foundation (Overview)** |  |  |
| 6 core functions |  | 6 |
| Purpose |  | 2 |
| NIST |  | 2 |
| Table |  | 9 |
|  |  |  |
| **Part B: Foundation (Detail)** |  |  |
| 7 steps |  | 7 |
| Table |  | 8 |
|  |  |  |
|  |  |  |
| Handed in properly |  | 4 |
| **Total** |  | **38** |