Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Managing and developing cyber capabilities

Lecture 1: Frameworks Overview for Cybersecurity Management

Part-II

NIST Cybersecurity Framework (CSF)

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Outline: Lecture 1

- Lecture 1 is divided in three parts:
  - Part I: Introduction to Cybersecurity Management Frameworks
  - **Part II: NIST Cybersecurity Framework**
    - **Introduction**
    - **NIST CSF 1.1**
      - Overview
      - Core: *Identify, Protect, Detect, Response, Recover*
      - Tier
      - Profile
      - How to use Framework
    - **NIST CSF 2.0**
  - Part III: ISO/IEC-20071, CIS controls and others

NIST Cybersecurity Framework (CSF 1.1)

Introduction

Introduction

- This cybersecurity Framework was developed by National Institute of Standards and Technology (NIST) as part of Improving Critical Infrastructure Cybersecurity, in 2014.
- Framework provides voluntary recommendations to help organizations for cybersecurity risk management and mitigation, built on existing standards and best practices.
- It facilitates communication among internal and external entities on cybersecurity risks and management.
- This Framework is ***not a one-size-fits-all*** solution for managing cybersecurity risk, but it aims to shorten and enhance risk management for organizations
- The framework is designed for organizations of any and all domains or size.
- Organization may differ in customizing the guidelines of this framework.
- Organizations can identify crucial activities for their business goals and prioritize those to have broader impact and benefits.

A!

Source: https://www.nist.gov/cyberframework/background

NIST Cybersecurity Framework (CSF 1.1)

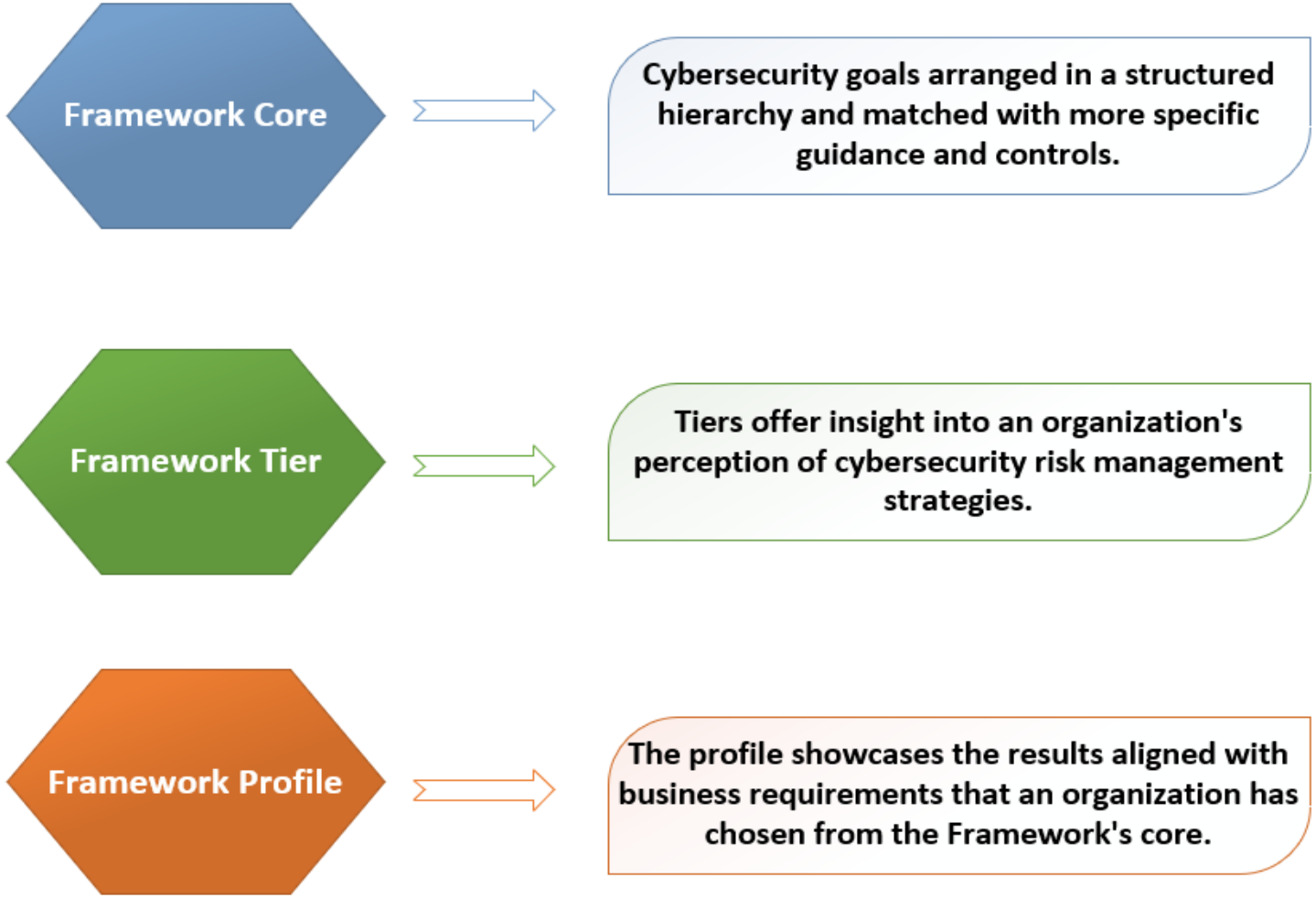
Overview

NIST Cybersecurity Framework (CSF 1.1): *Overview*

Three Primary Components of NIST Cybersecurity Framework

Core, Tier, Profile

Every aspect of the framework strengthens the correlation between business or mission objectives and the cybersecurity measures.

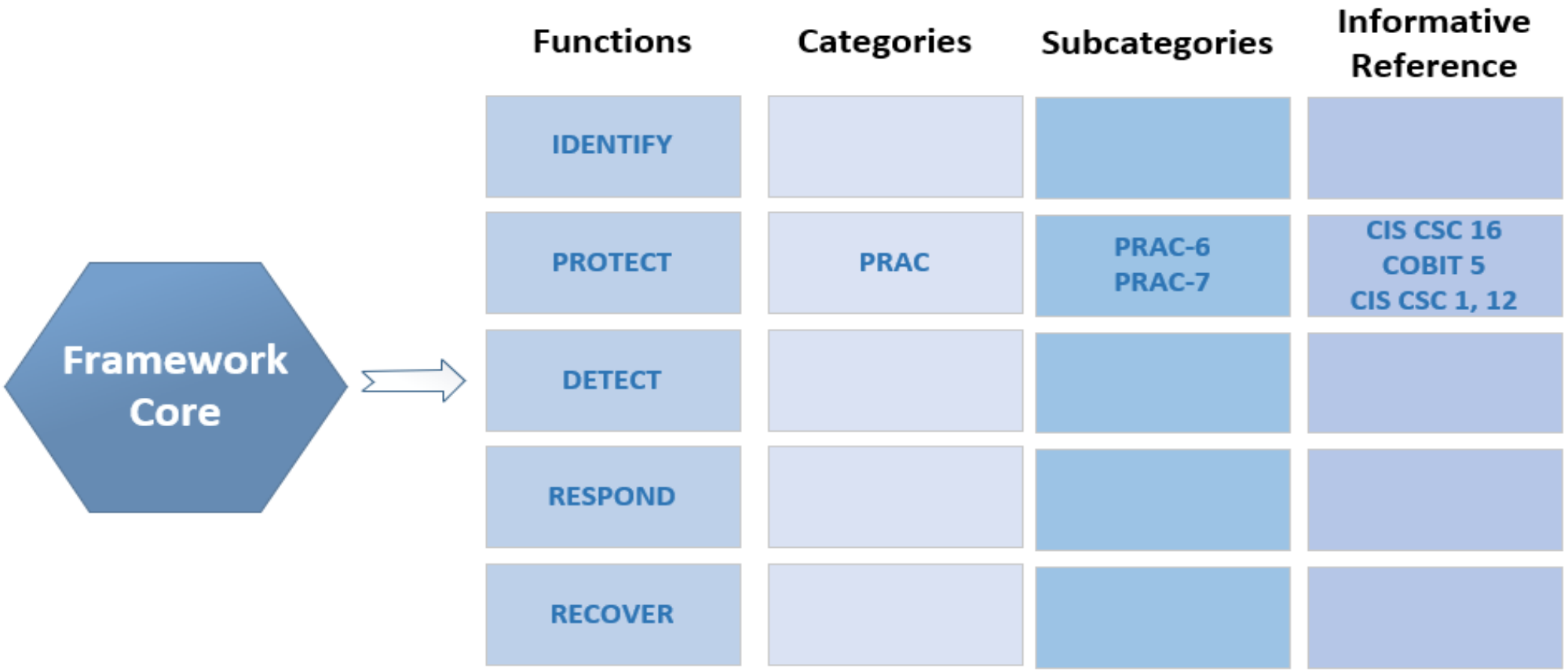


Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework (CSF 1.1)

Framework Core

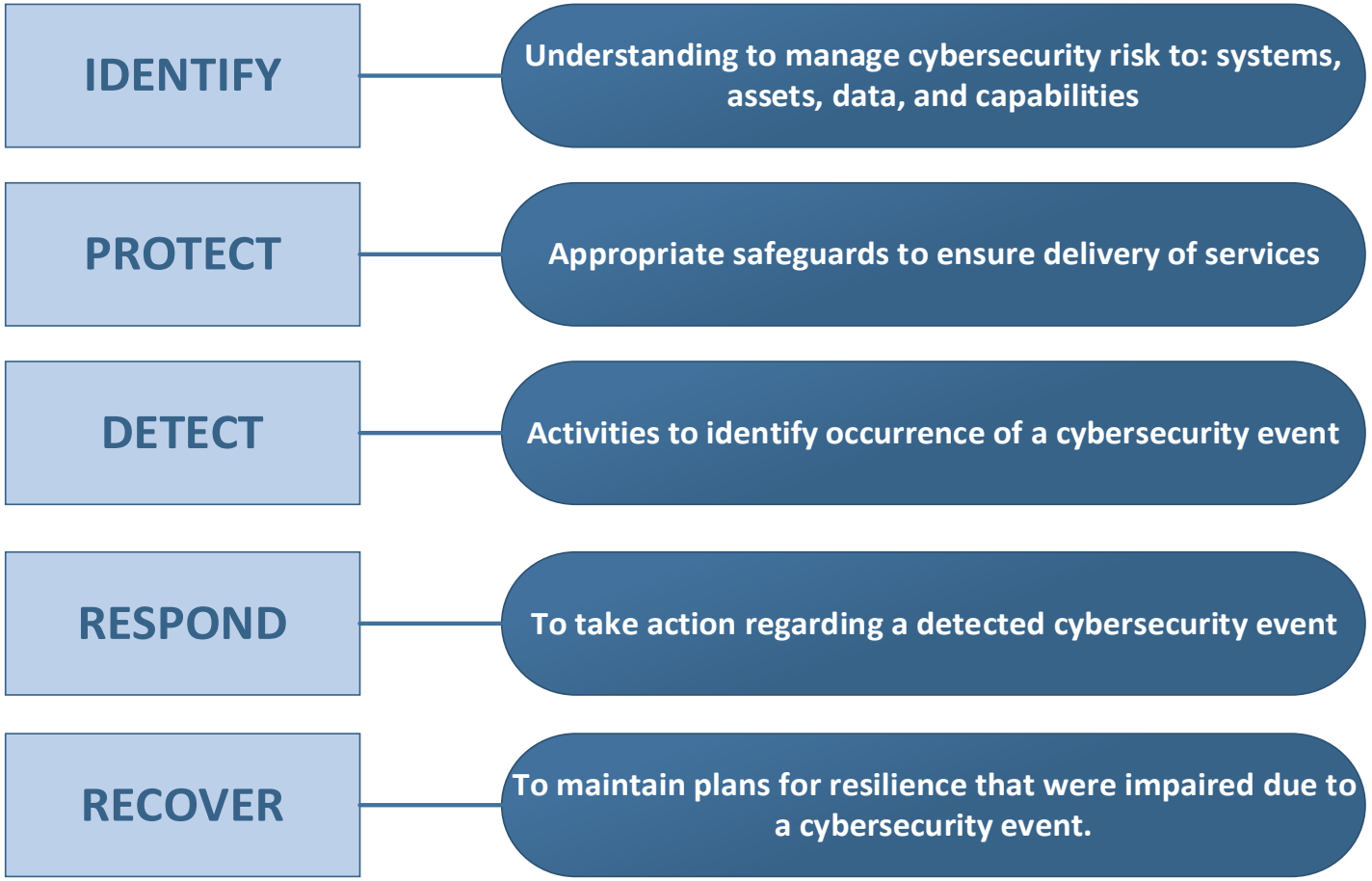
NIST Cybersecurity Framework (CSF 1.1): *Core*



NIST Cybersecurity Framework (CSF 1.1): *Core*

The Framework core is organized by **five** key Functions.

Identify, Protect, Detect, Respond, Recover.



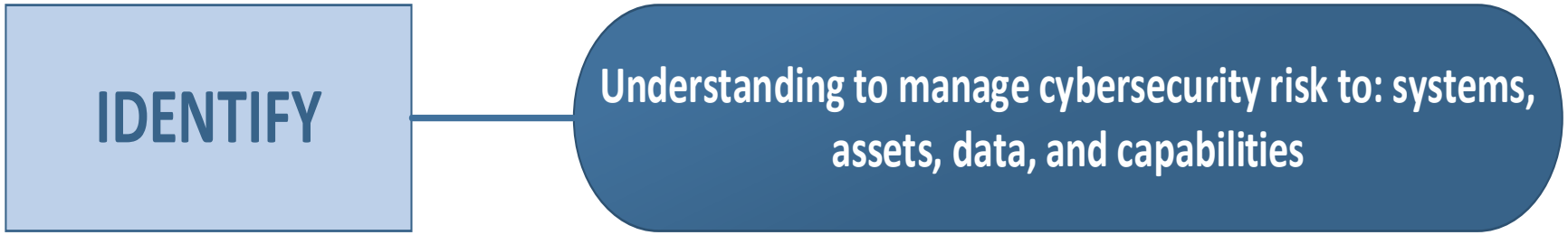
Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework (CSF 1.1): *Case Study*

Example Case Study: *Retail Industry*

Let's consider a retail company, XYZ company, and how five cybersecurity pillars can be applied to it.

NIST Cybersecurity Framework (CSF 1.1): Core: *Identify*

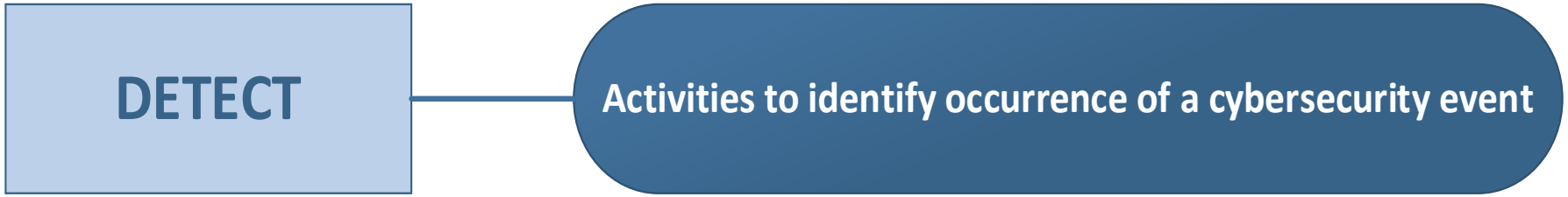


- Retail company XYZ is required to determine key critical assets e.g., customer information, payment systems, inventory management system
- By doing comprehensive assessment, retailers can prioritize their protection measures and utilize resources efficiently.
- Let's assume, according to their assessment, ***phishing attack*** is one of the major threats for the company.

NIST Cybersecurity Framework (CSF 1.1): Core: *Protect*

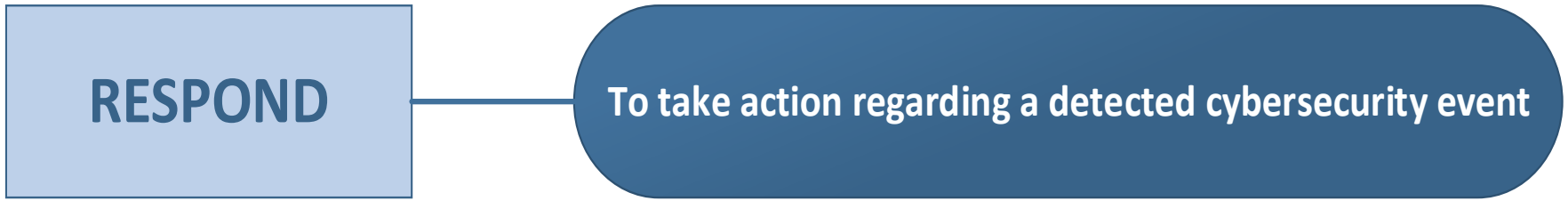
- XYZ company is required to take the necessary security measures to ensure the protection of customer data, payment and inventory systems.
- In the case risk of ***phishing attacks***, the company should deploy strong email authentication, email filtering, access control mechanism, multi-factor authentication.
- Additionally, the company XYZ provides training to their employees to identify various types of phishing attacks and how to report it.

NIST Cybersecurity Framework (CSF 1.1): Core: *Detect*



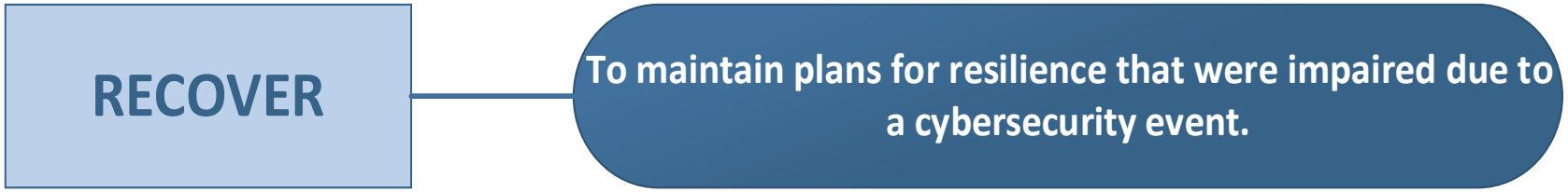
- Using various threat detection approaches and security monitoring tools, one can regularly keep track of any suspicious activities or unusual behaviors such as payment frauds, malware.
- For ***phishing attack***, the company XYZ detects various suspicious phishing emails through email filtering and analytics tools.

NIST Cybersecurity Framework (CSF 1.1): Core: *Respond*



- In case of a ***phishing attack***, cyber incident team of XYZ company need to execute the incident response measures to limit its impact.
- Team will take the necessary actions, e.g., isolating the affected systems informing the customers, suggest to reset their credentials,
- Efficient communication is crucial both with the employees and stakeholders to address the incident.
- The team will also coordinate with government authorities and law enforcement agencies to get root cause of the incident and further strengthen the security measures, i.e., block the phishing websites.

NIST Cybersecurity Framework (CSF 1.1): Core: *Recover*



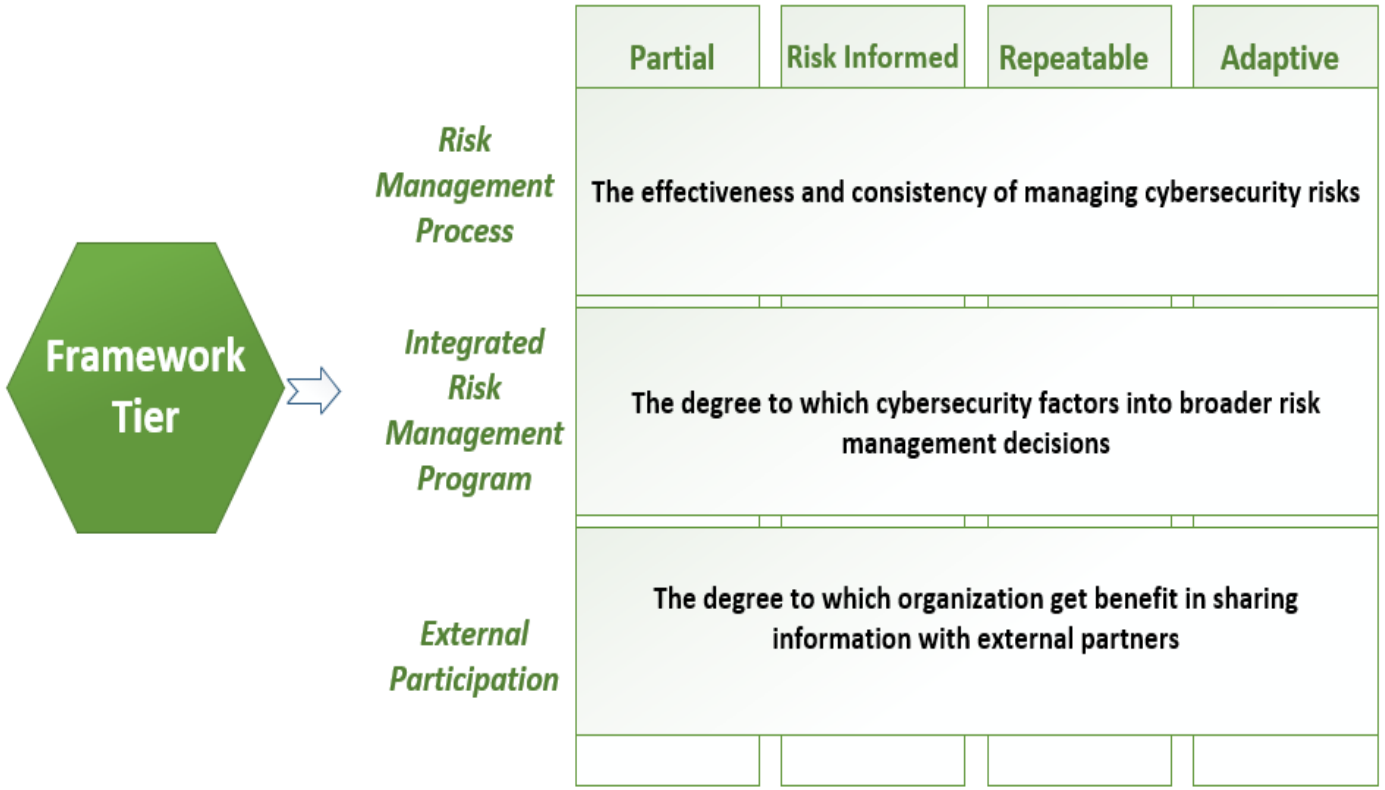
- In case of *a phishing attack*, XYZ company must initiate rapid recovery efforts.
- This involves restoring affected systems, assessing any damage or loss, and help customers in recovering loss (if any) during this phishing scam.
- Moreover, the XYZ retail company updates the security measures according to recent phishing attacks, to prevent similar incidents in the future.

NIST Cybersecurity Framework (CSF 1.1)

Framework Tier

NIST Cybersecurity Framework (CSF 1.1): *Tier*

- Provides insight into an organization's perspective on cybersecurity risk and measures to address that risk.
- **Four Tiers**: an increasing level of rigor and sophistication in the measures of managing cybersecurity risk.
- Tiers are not maturity levels but assist organizations in making decisions for risk management and prioritizing areas requiring more focus/resources.



Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework (CSF 1.1)

Framework Profile

NIST Cybersecurity Framework (CSF 1.1): *Profile*

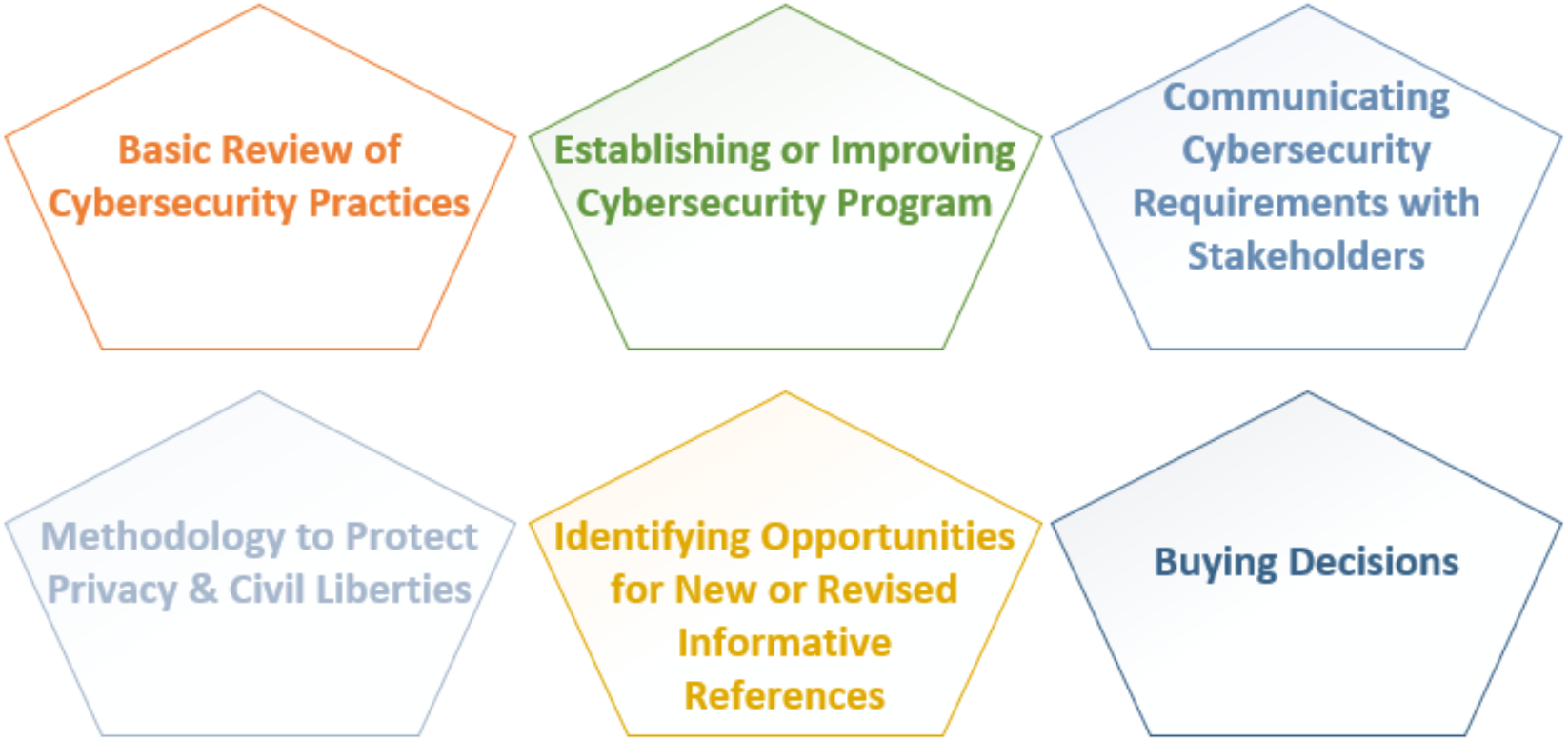
- Aligns the elements of framework core with the organization's business needs, risk tolerance, and available resources.
- Allows organizations to align their cybersecurity risk reduction plan with business objectives, legal requirements, industry best practices, and risk management priorities.
- Framework Profiles can be further elaborated by current profile and target profile.
  - ***Current Profile:*** on-going cybersecurity outcomes being achieved
  - ***Target Profile:*** desired cybersecurity outcomes to achieve
- Profiles assist in meeting business or mission requirements and facilitate the communication of risk within and across organizations.
- Contrasting both Profiles can expose disparities needing attention to fulfill cybersecurity risk management goals.

Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework (CSF 1.1)

How to use Framework

NIST Cybersecurity Framework: *How to use Framework*



Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

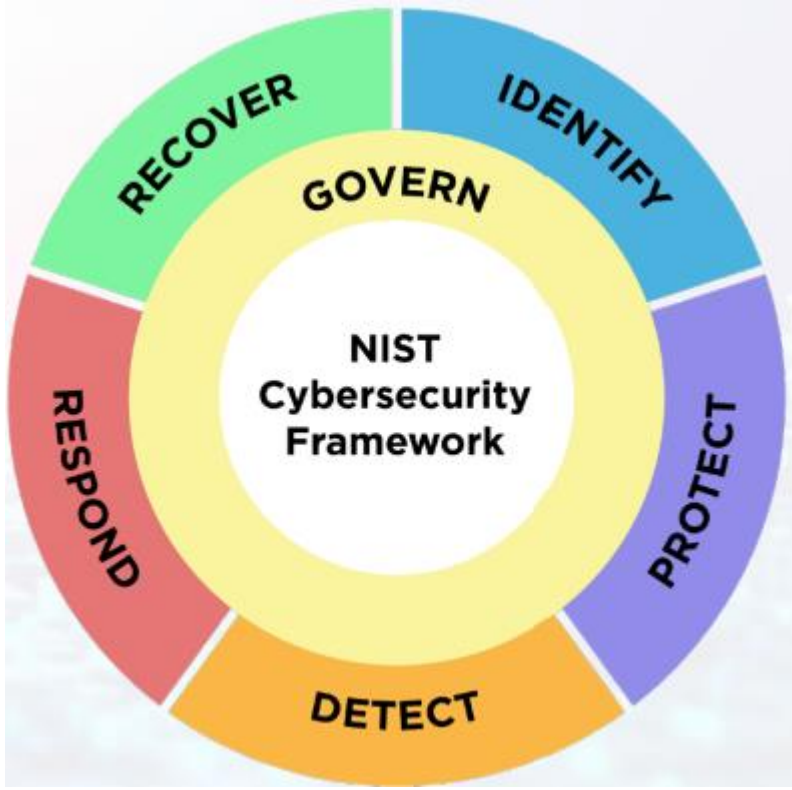
NIST Cybersecurity Framework (CSF 2.0)

Overview

Cybersecurity Framework (NIST): *CSF 2.0*

Mainly designed in the context of small-to-medium sized businesses (SMB), particularly those who have modest or no cybersecurity plans in place.

- ***Govern: O***rganization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- ***Identify:*** determine current cybersecurity risk to business.
- ***Protect:*** safeguards to prevent or reduce cybersecurity risks.
- ***Detect:*** provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.
- ***Respond:*** supports your ability to take action regarding a detected cybersecurity incident.
- ***Recover:*** activities to restore assets and operations that were impacted by a cybersecurity incident.



A!

Source: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Kiitos
aalto.fi