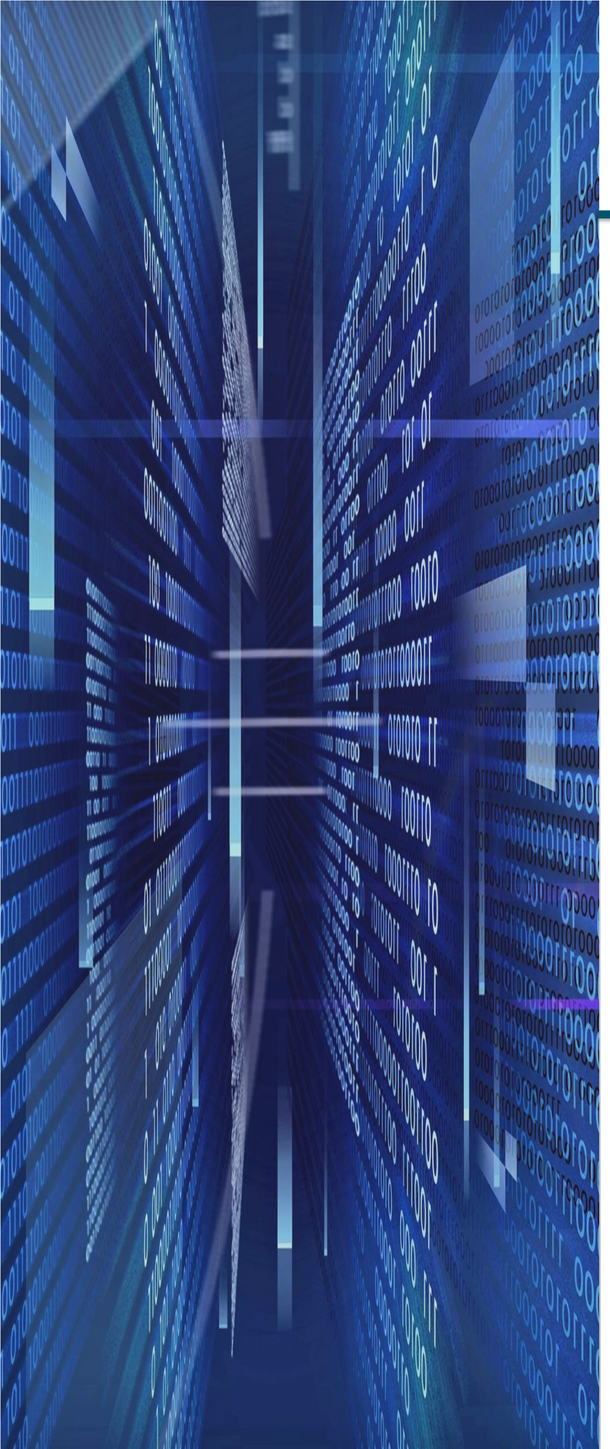


# The NIST Cyber Security Framework

Prof. Federica Paci

# Today’s lecture

- What is CSF?
- CSF structure
  - Functions, categories, subcategories
  - Tiers
  - Profiles
- How to apply the CSF

# The Cyber Security Framework (CSF)

- Developed by NIST
- Executive Order 13636, Improving Critical Infrastructure  Cyber Security, February 2013
- "…*directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure*" NIST, 2019

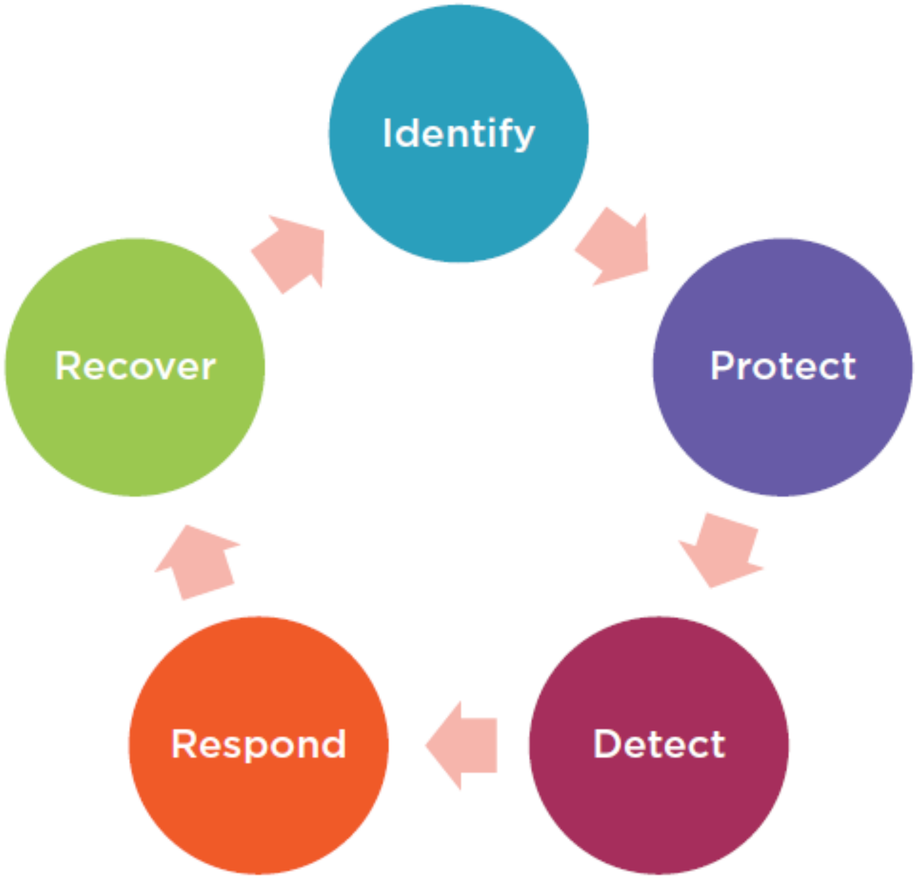
# The Cyber Security Framework (CSF)

cybersecurity framework


- Catalog of Cybersecurity Activities
- Outcome-based
- Current Version 1.1 (April 2018)

# CSF Structure Core

- 5 activities or functions broken down
  - 23 categories
    - 108 subcategories
  - 5 Informative References
    - CIS, COBIT 5, ISA, ISO/IEC 27001, NIST SP 800-53
- All of this is referred to as the **core**



# Functions, Categories and Subcategories

**Functions (5)**

Activities (WHAT)

**Categories (23)**

Activities breakdown (WHAT/HOW)

**Subcategories (108)**

Detailed statements on how to implement (HOW)

# CSF Functions

**ID**

Identify

Attività che consentono a un organizzazione di capire gli assets da proteggere

**PR**

Protect

Misure di prevenzione che una società deve attuare

**DE**

Detect

Attività che una società deve attuare per riconoscere attacchi in corso

**RS**

Respond

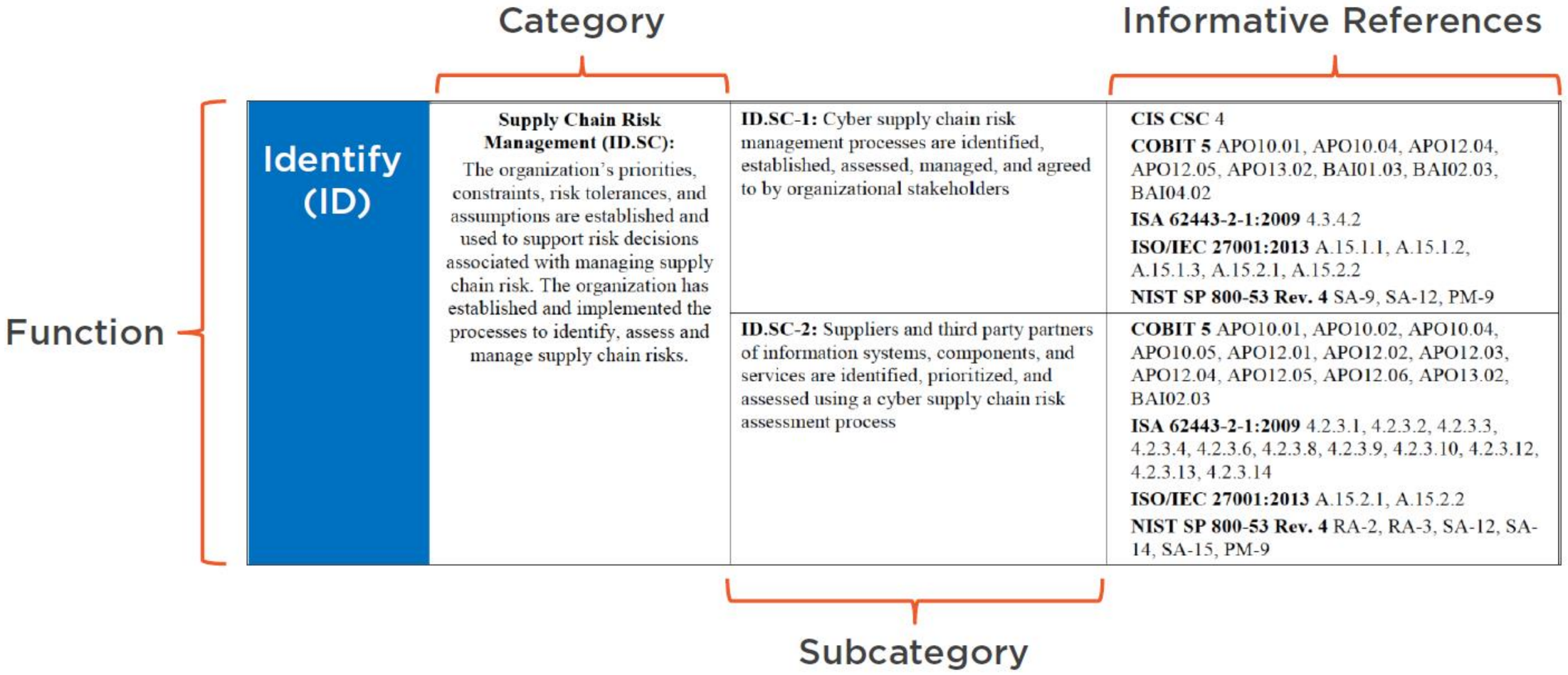
Azioni che una Società deve attuare per contenere un attacco

**RC**

Recover

Attività che consentono a una società di ristabilire gli assets compromessi

# Breakdown example



# Identify

- The organization must identify:
  - Systems and data
  - Critical business processes that depend on those systems and data
  - The weaknesses and strengths associated with those systems
  - All resources (people, technology, money, equipment, facilities)
  - Vulnerabilities, threats, likelihood, impact, and frequency and overall risk
  - Governance (Laws, regulations, etc.)

# Identify Categories

| Function | Categories |
| --- | --- |
| Identify (ID) | Asset Management (ID.AM) |
| | Business Environment (ID.BE) |
| | Governance (ID.GV) |
| | Risk Assessment (ID.RA) |
| | Risk Management Strategy (ID.RM) |
| | Supply Chain Risk Management (ID.SC) |

Contiene 6 categorie

comprende processi e politiche che governano l'azienda: viene creata una politica per affrontare cybersicurezza

# Protect

- The Protect function focuses on:
  - Ensuring strong authentication and access control
  - Protecting data
  - Secure maintenance of assets
  - Securing “people”
  - Sound policies and procedures
  - Ensuring the right administrative, technical, and physical controls are in place

# Protect Categories

| Function | Categories |
| --- | --- |
| Protect (PR) | Identity Management, Authentication, Access Control (PR.AC) |
| | Awareness and Training (PR.AT) |
| | Data Security (PR.DS) |
| | Information Protection Processes and Procedures (PR.IP) |
| | Maintenance (PR.MA) |
| | Protective Technology (PR.PT) |

# Detect

- The Detect function:
  - Focuses on detection processes and technologies
  - Looks for anomalies and unusual events
  - Ensures continuous security and risk monitoring

# Detect Categories

| Function | Categories |
| --- | --- |
| Detect (DE) | Anomalies and Events (DE.AE) |
| | Security Continuous Monitoring (DE.CM) |
| | Detection Processes (DE.DP) |

# Respond

- Respond function is concerned with:
  - Planning for incident and contingency response
  - Ensuring the robustness of incident communications
  - Analyzing the root causes of incidents
  - Mitigating damage to systems, data, equipment, facilities, and people
  - Improving the overall contingency planning and response processes

# Respond Categories

| Function | Categories |
| --- | --- |
| Respond (RS) | Response Planning (RS.RP) → definire un piano di azione |
| | Communications (RS.CO) |
| | Analysis (RS.AN) |
| | Mitigation (RS.MI) |
| | Improvements (RS.IM) |

# Recover

- The Recover function focuses on:
  - Business continuity, incident recovery, and disaster recovery planning
  - Maintaining communications during the recovery process
  - Improving the recovery effort

# Recover Categories

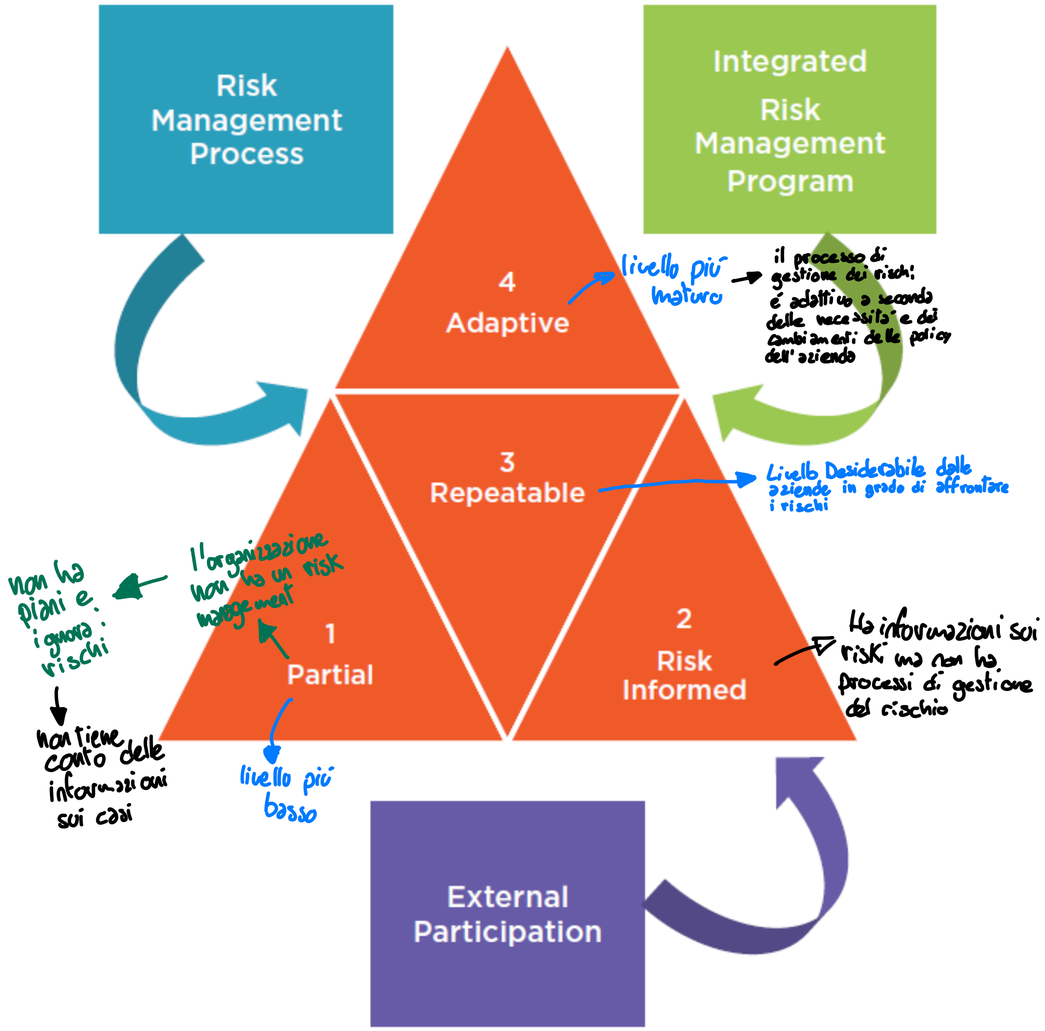
| Function | Categories |
| --- | --- |
| Recover (RC) | Recovery Planning (RC.RP) → definire un piano e le persone che lo devono attuare |
| | Improvements (RC.IM) |
| | Communications (RC.CO) |

# CSF Tiers

rappresentano il livello di implementazione delle attività descritte

"…the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework." - NIST

# What are the CSF Tiers?




The Tiers range from Partial (Tier 1) to Adaptive (Tier 4)

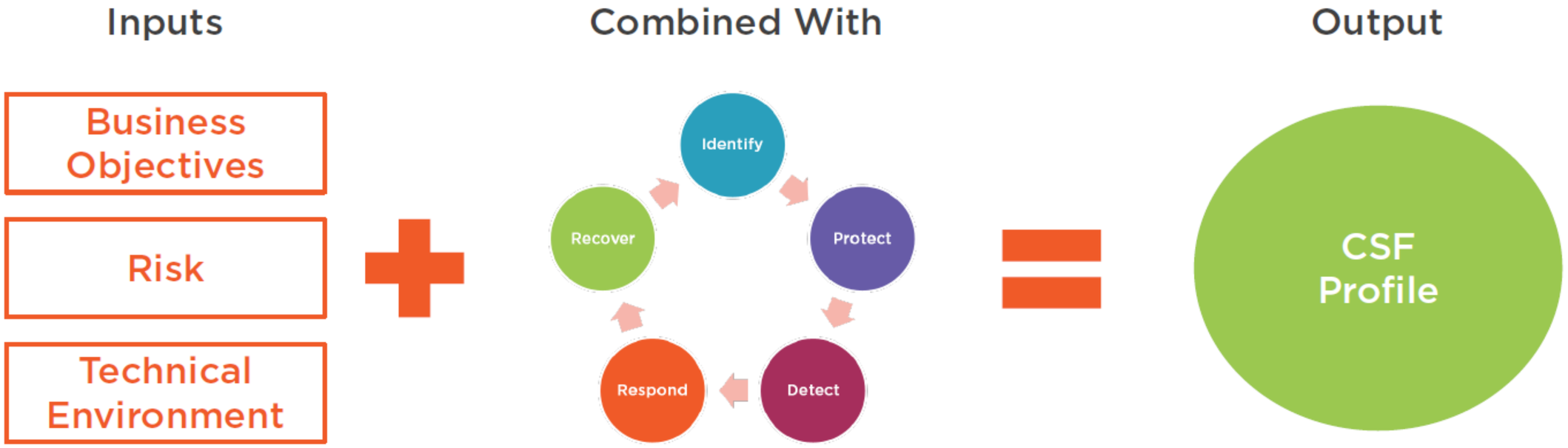
Describe

- an increasing degree of rigor
- how well integrated cybersecurity risk decisions are into broader risk decisions
- the degree to which the organization shares and receives cybersecurity info from external parties.

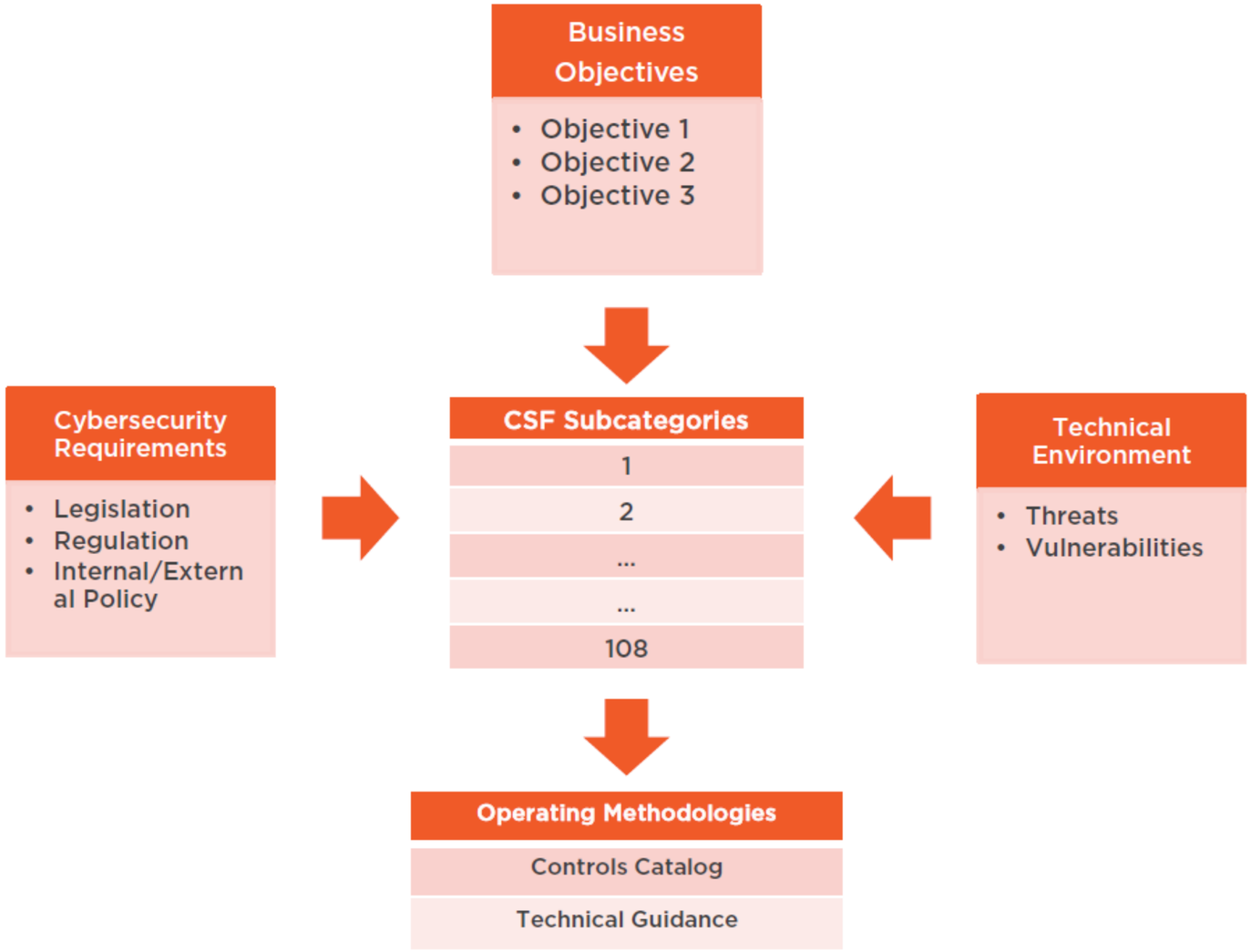
# An example of Tier - Adaptive

- Risk Management Process
  - The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators; actively adapts to changing technologies and threats
- Integrated Risk Management Program
  - Organization-wide approach to managing cybersecurity risk; risk informed policies, processes, and procedures to address potential cybersecurity events; cybersecurity risk is managed with other organizational risk
- External Participation
  - The organization receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve; communicates proactively with others and actively maintains strong supply chain relationships

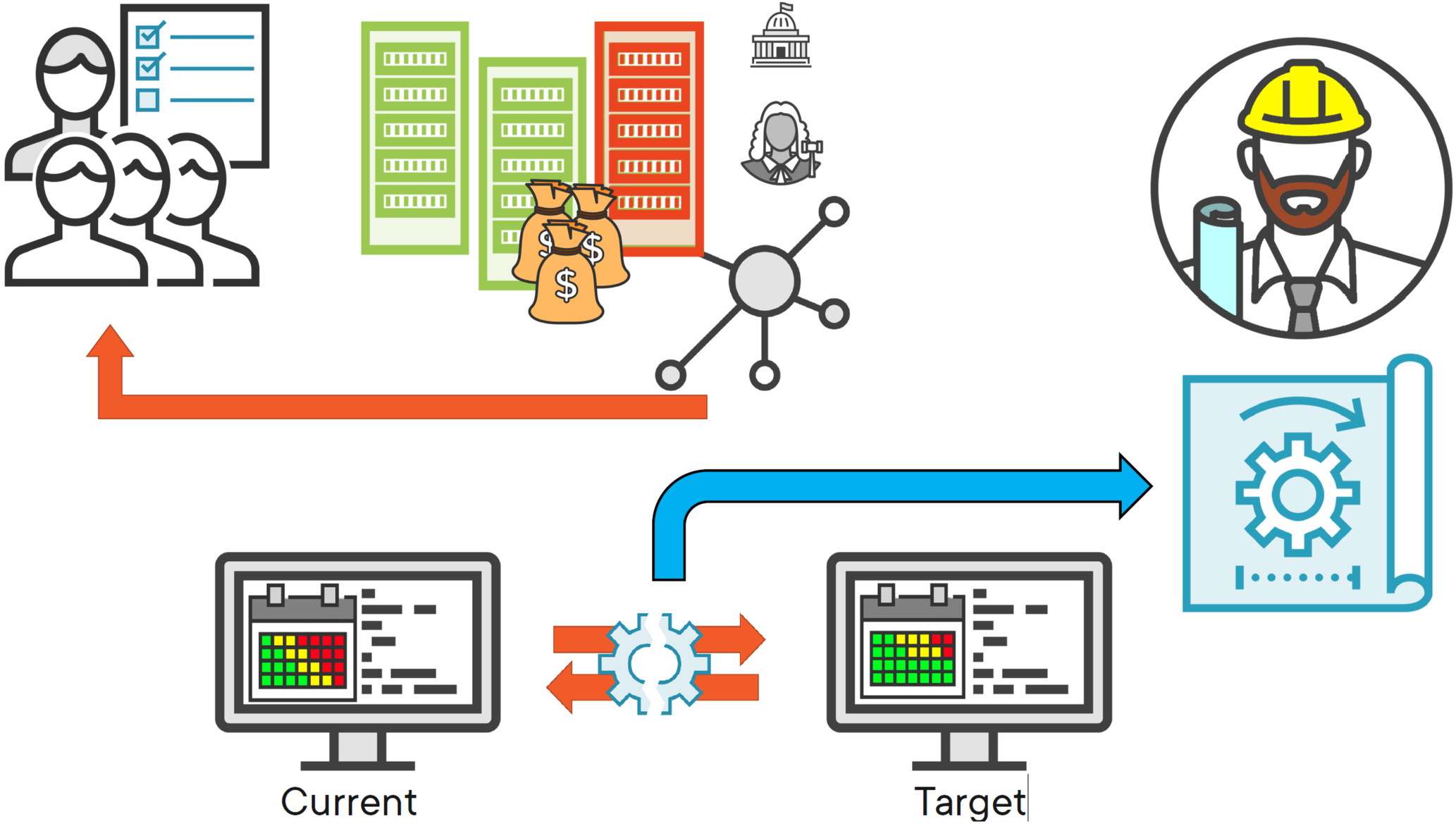
# What are CSF Profiles?



# Creating a Profile



# How to apply the CSF



# Summary

- The framework consists of standards, guidelines, and practices to reduce the cyber risk to critical infrastructures
- It consists of
  - Core  provides a set of desired cybersecurity activities and outcomes
  - Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program
  - Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

# Resources

https://www.nist.gov/cyberframework/online-learning/components-framework