SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M6.5 – Nist CSF Laboratory

Contents

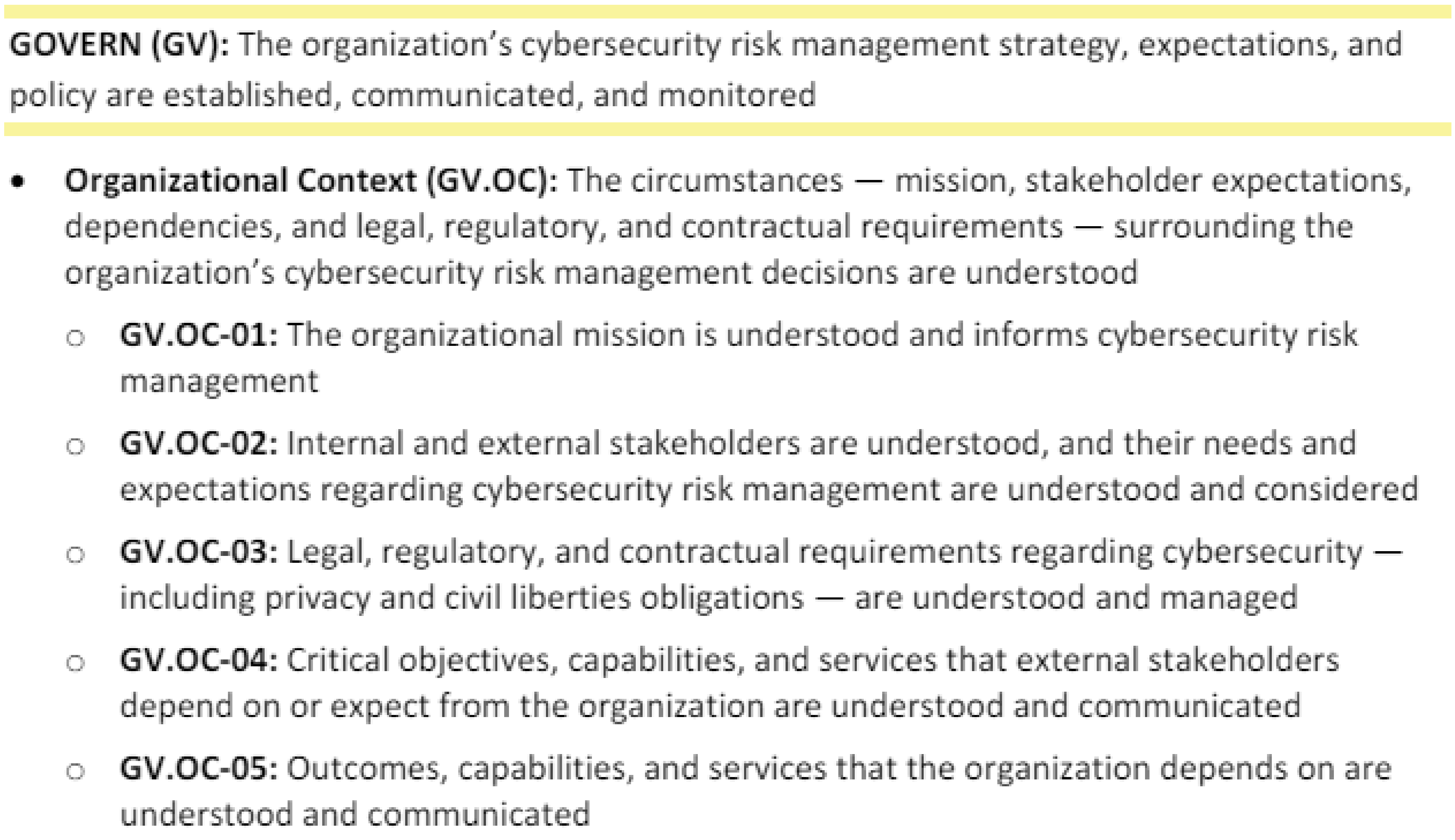
6.5. Nist CSF Assessment Report

- How to read the Nist CSF
- Organization, stakeholders, assets, risks and opportunities. Purposes of the assessment
- How to conduct the assessment (for the purposes of the laboratory and the exam)

How to read the Nist CSF

IMPORTANT ASPECTS

See M6.4



GOVERN (GV): The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

- **Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization’s cybersecurity risk management decisions are understood
    - **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management
    - **GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
    - **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
    - **GV.OC-04:** Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated
    - **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are understood and communicated

How to read the Nist CSF

IMPORTANT ASPECTS

This document is version 2.0 of the NIST Cybersecurity Framework (Framework or CSF). It includes the following components:

- CSF **Core**, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.

- CSF Organizational **Profiles**, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.

- CSF **Tiers**, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

(source: Nist CSF v. 2.0)

How to read the Nist CSF

IMPORTANT ASPECTS

the Framework provides a common **taxonomy** and mechanism for organizations to:

1) Describe their **current** cybersecurity posture;
2) Describe their **target** state for cybersecurity;
3) Identify and prioritize opportunities for **improvement** within the context of a continuous and repeatable process;
4) Assess **progress** toward the target state;
5) **Communicate** among internal and external stakeholders about cybersecurity risk.

(source: Nist CSF v. 1.1)

Organization, stakeholders, assets, risks and opportunities.

PURPOSES OF THE ASSESSMENT

The Cybersecurity Framework is designed to **reduce risk** by improving the management of cybersecurity risk to **organizational objectives**. Ideally, organizations using the Framework will be able to measure and assign values to their risk *along with* the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be.

(source: Nist CSF v. 1.1)

How to use the Framework in the laboratory assessment

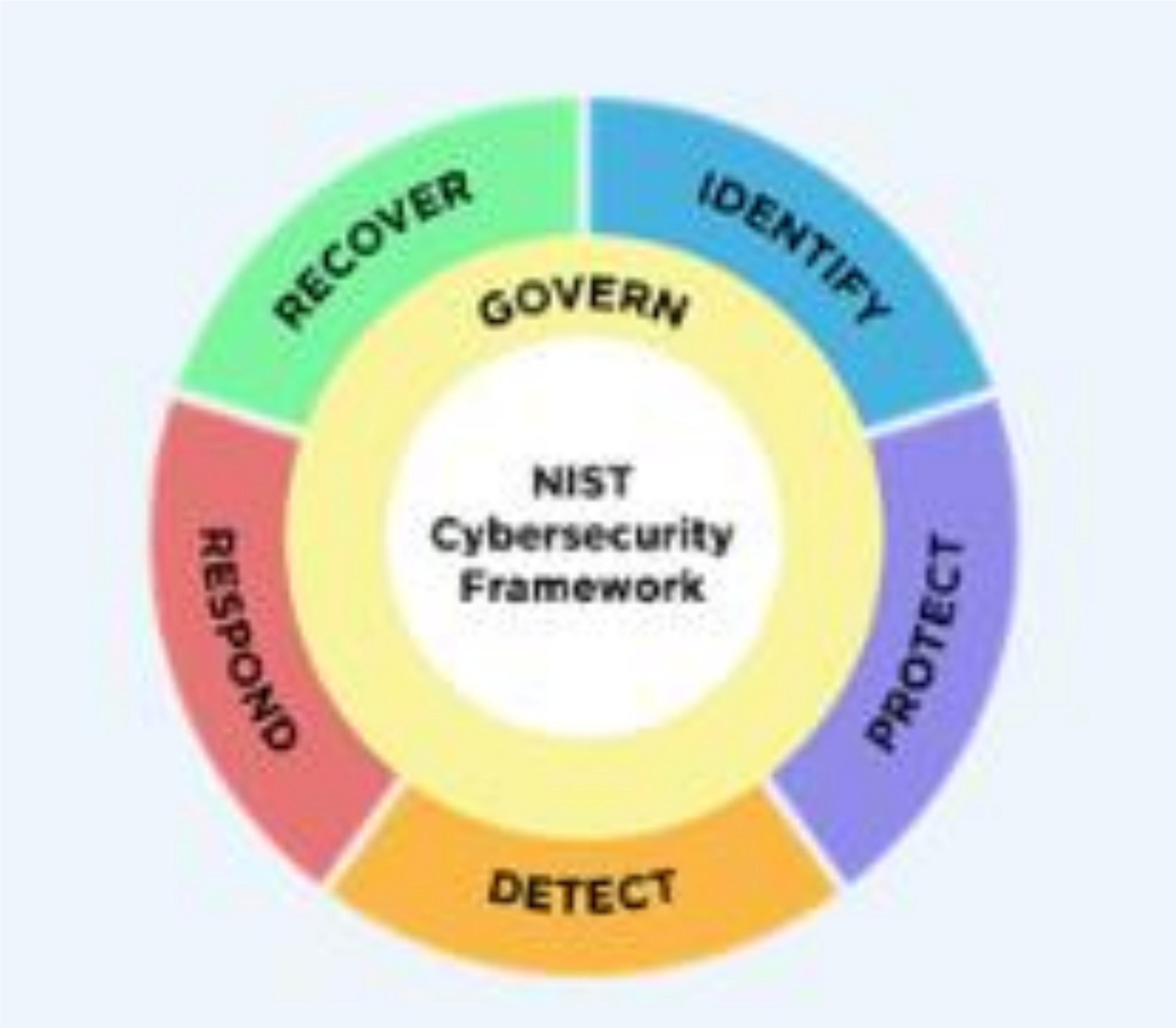
The **simulation** that we will do for the purposes of both the laboratory and the exam will not be able to consider all the real factors encountered in a real organization. Some activities, such as risk analysis, for example, involve carrying out **interviews** with top management capable of quantifying the impacts and the whole process of risk analysis itself, especially the *quantitative* kind, can even require *months* of work.

Nonetheless, the exercise is useful to understand, learn and familiarize yourself with daily used tools for cybersecurity workers within the organizations, developing, where appropriate, an approach to recognizing risks **at a glance**.

To better understand the security controls, you can use examples described in this Reference Tool offered by Nist for each subcategory

https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

How to use the Framework in the laboratory assessment



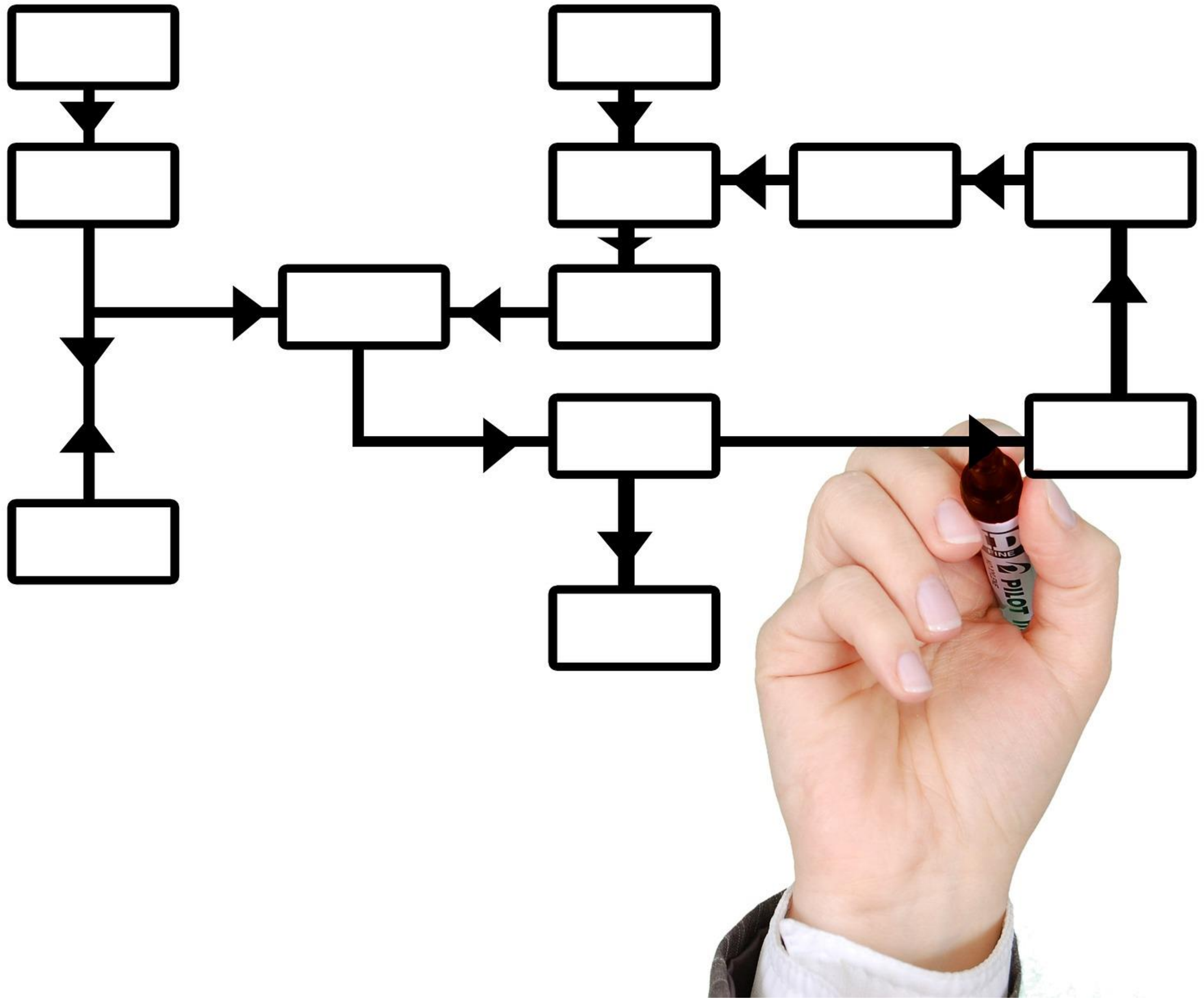
Step 0. Take a quick read at the categories and sub-categories of the Nist CSF 2.0

https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

Take a brief look at the Framework (.pdf) and in particular, chapters 3 and 4.0

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

How to use the Framework in the laboratory assessment



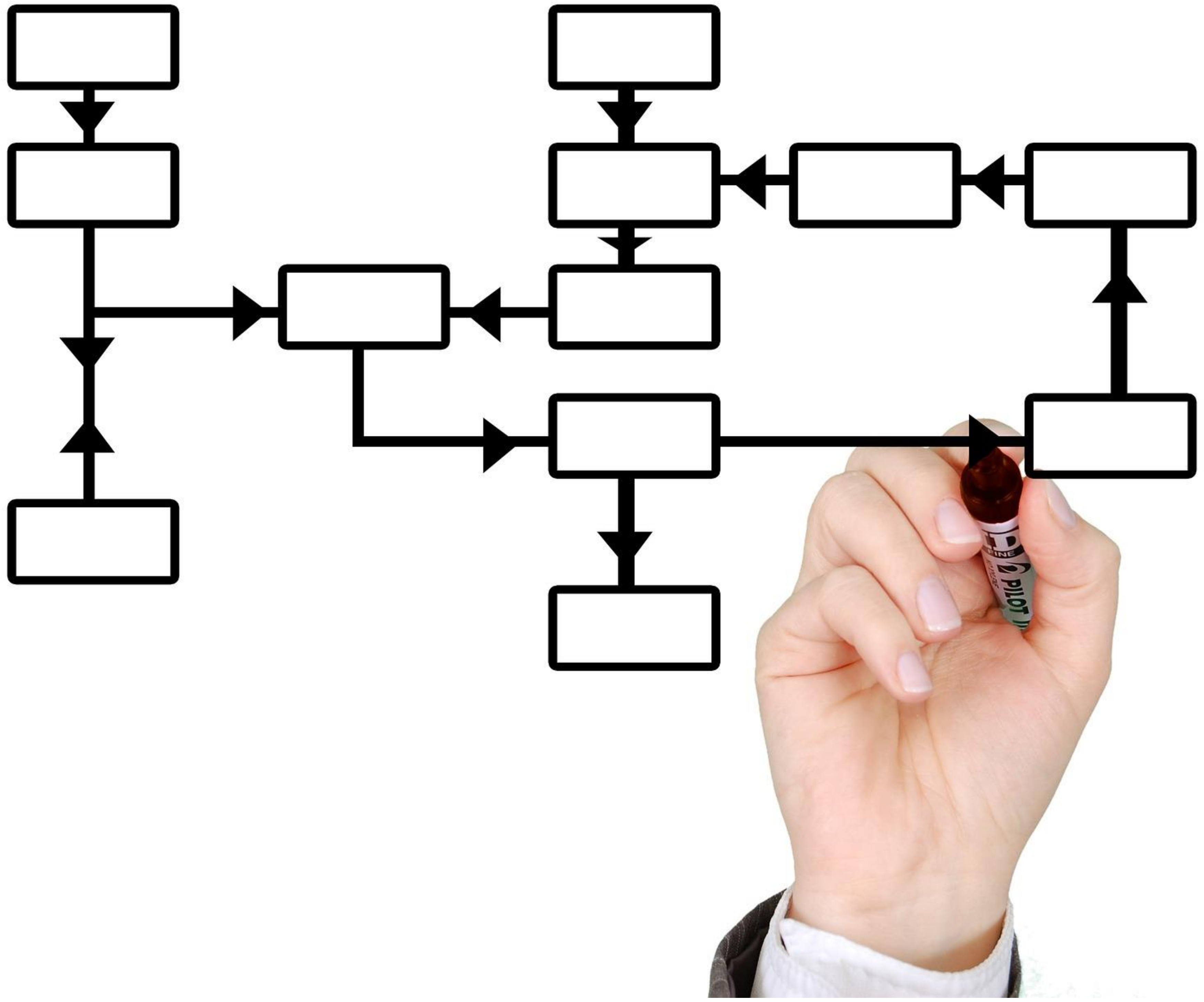
Step 1. Choose a **use case**. Assume an organization. Some examples of organizations are as follows:

- A hospital
- A bank or financial institute
- An energy supply company
- A public administration (of various kinds)
- A Telecomunication company

Start describing a drafted organization chart, stakeholders, assets, risks and opportunities (some examples follow)

Use generative AI to help create a realistic and unique organization chart and/or draw inspiration from the following

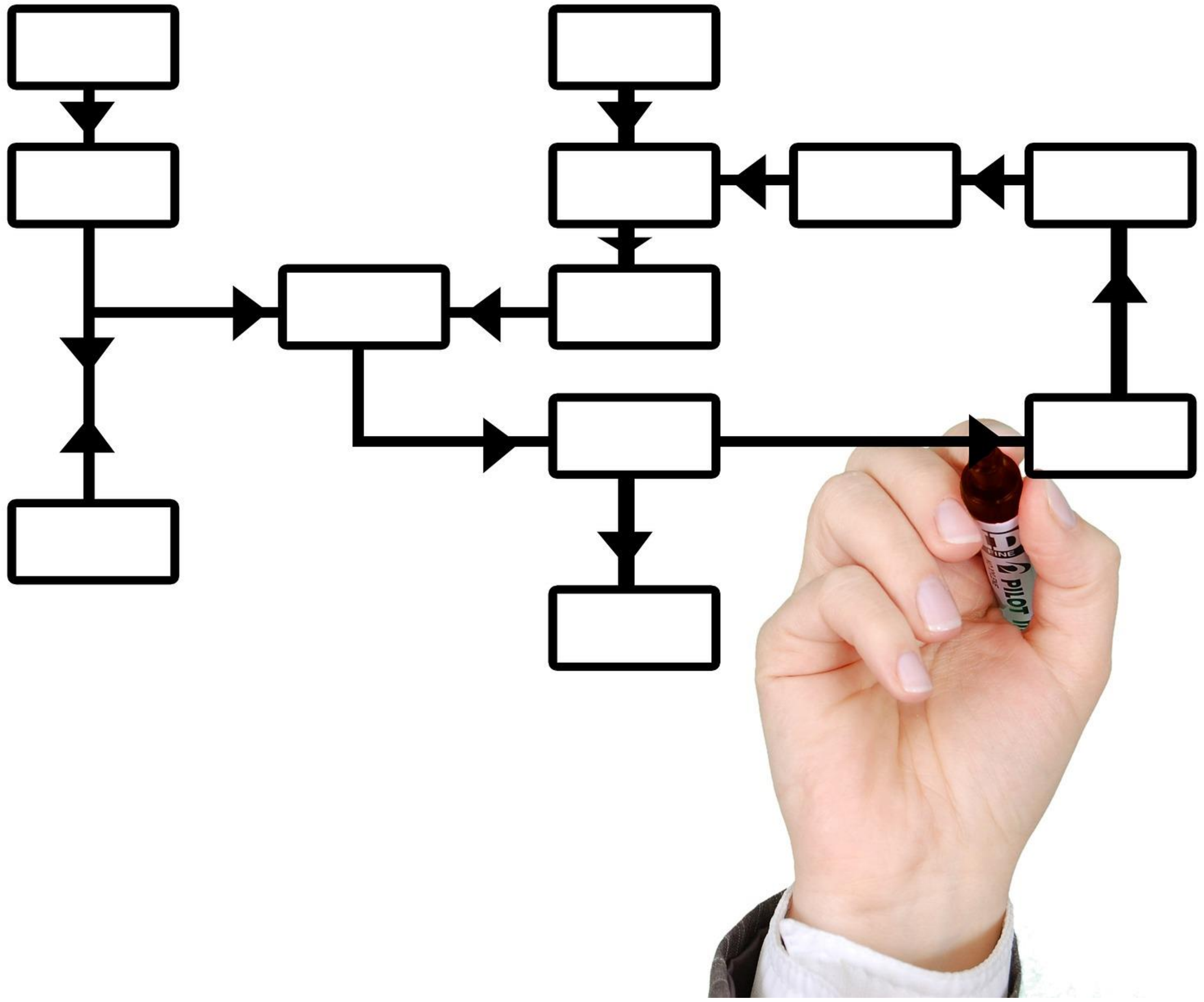
How to use the Framework in the laboratory assessment



Step 1. Drafted organization chart for a hospital:

a) CEO/President
b) Medical Director
c) Department Heads (Surgery, Medicine, Pediatrics, Radiology, etc.)
d) Nursing Director
e) Human Resources
f) Finance and Administration
g) Patient Services
h) Information Technology
i) Quality Control

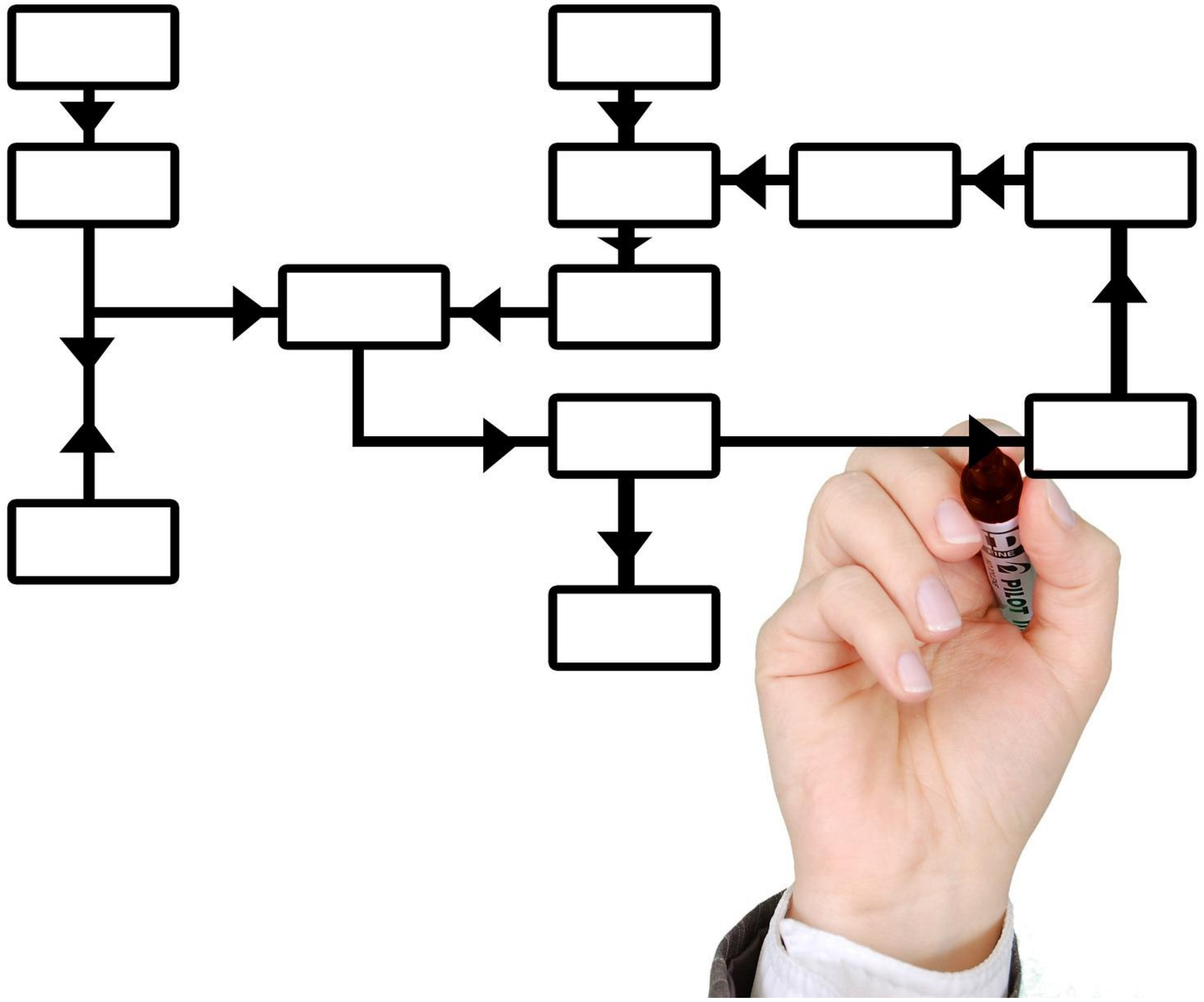
How to use the Framework in the laboratory assessment



Step 1. Drafted organization chart for a Bank or Financial Institute:

a) CEO/President
b) Board of Directors
c) Chief Financial Officer
d) Chief Operating Officer
e) Marketing and Sales Department
f) Human Resources
g) Risk Management
h) Compliance
i) Information Technology
j) Customer Service

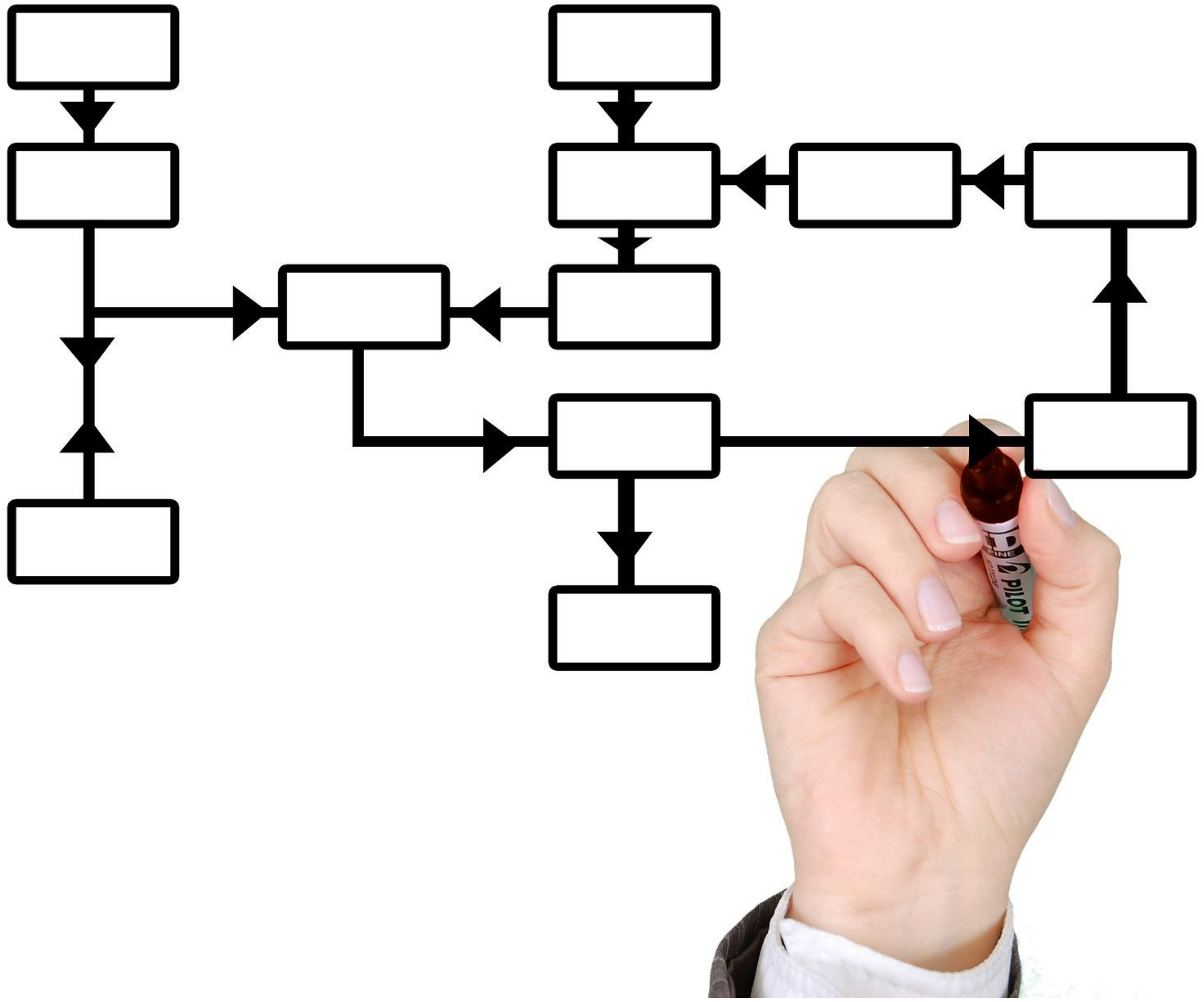
How to use the Framework in the laboratory assessment



Step 1. Drafted organization chart for an Energy Supply Company:

a) CEO/President
b) Operations Manager
c) Engineering and Design
d) Project Management
e) Finance and Accounting
f) Human Resources
g) Environmental and Regulatory Compliance
h) Information Technology
i) Customer Service

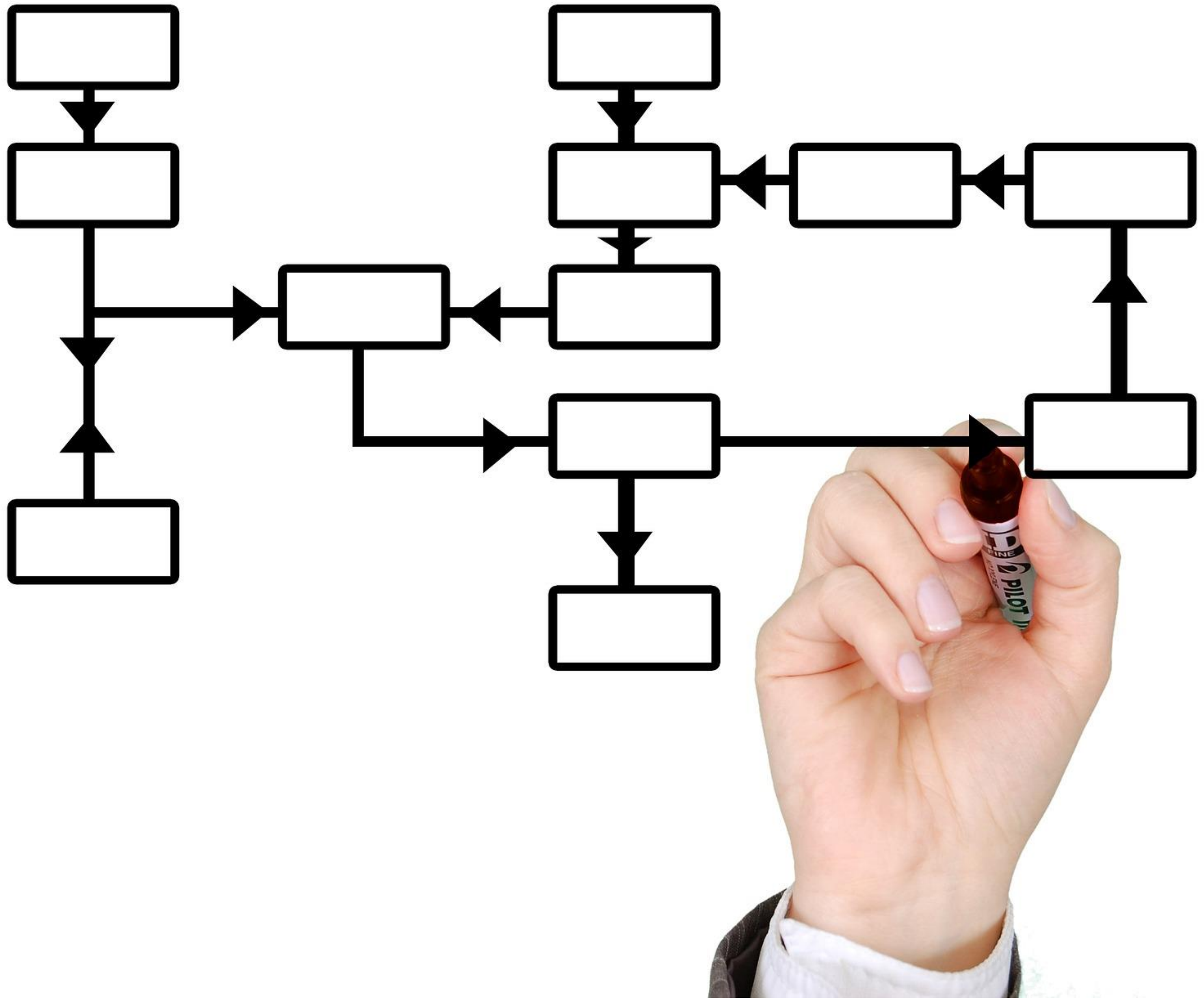
How to use the Framework in the laboratory assessment



Step 1. Drafted organization chart for a Public Administration:

a) Mayor/Chief Executive Officer
b) Department Heads (Public Works, Parks and Recreation, Finance, Health, etc.)
c) Attorney/Legal Affairs/Regulation office
d) Human Resources
e) Planning and Development
f) Public Relations (external communication. E.g. press interaction)
g) Information Technology
h) Economic Development
i) Community Services

How to use the Framework in the laboratory assessment



Step 1. Drafted organization chart for a Telecommunication Company:

a) CEO/President
b) Chief Technology Officer
c) Sales and Marketing Department
d) Human Resources
e) Information Technology
f) Network Operations
g) Customer Service
h) Finance and Accounting
i) Engineering and Design

How to use the Framework in the laboratory assessment

Step 2. AI driven **Risk** analysis. Use generative AI to perform an assessment for the chosen Organization.

Utilize prompts that reference the NIST CSF 2.0. The assessment should evaluate the **current** security posture and risk, including examples from at least five to no more than ten specific **sub-categories**.

The AI should consider the sub-categories among the most significant for the audited Organization (where usually related risk in higher)*, and the relative gaps that it is possible to find. It can be helpful to refer to multiple controls within the same category, for ease of presentation and consistency, but try choosing multiple categories for greater completeness and cross-disciplinary exercise.

***

“The non-implementation of the control (sub-category) arises a risk. Which one?”

*N.B. Risk is usually **higher** in the areas that are closer to the core business or to the main activities carried out by the specific organization, or represent the prerequisite for their achievement.

How to use the Framework in the laboratory assessment

Step 3. Human **Risk** analysis and assessment. Using the concepts and examples seen in the course, following a risk assessment procedure for the chosen use cases, which are **the most risky areas** and **activities** from the point of view of information security and cybersecurity? Did the AI address them correctly? What can be added or integrated? Are there any specific, additional, or different examples you would provide? Write them as a comment.

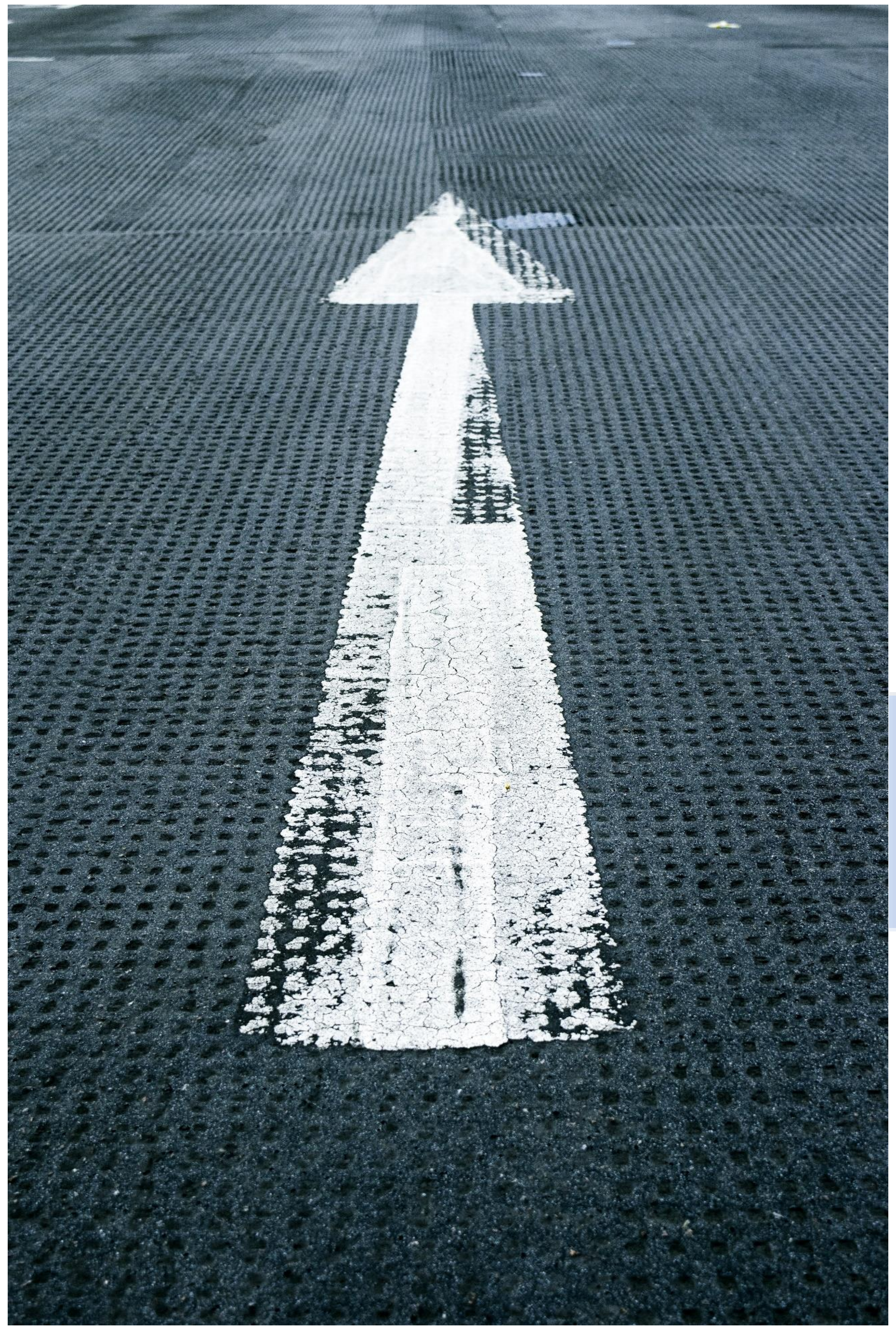
Think about the type of data processed, the purposes, the type of services provided and the consequences of an interruption (due to any event or threat) of the service or the loss of confidentiality, integrity or availability of information for all the stakeholders.

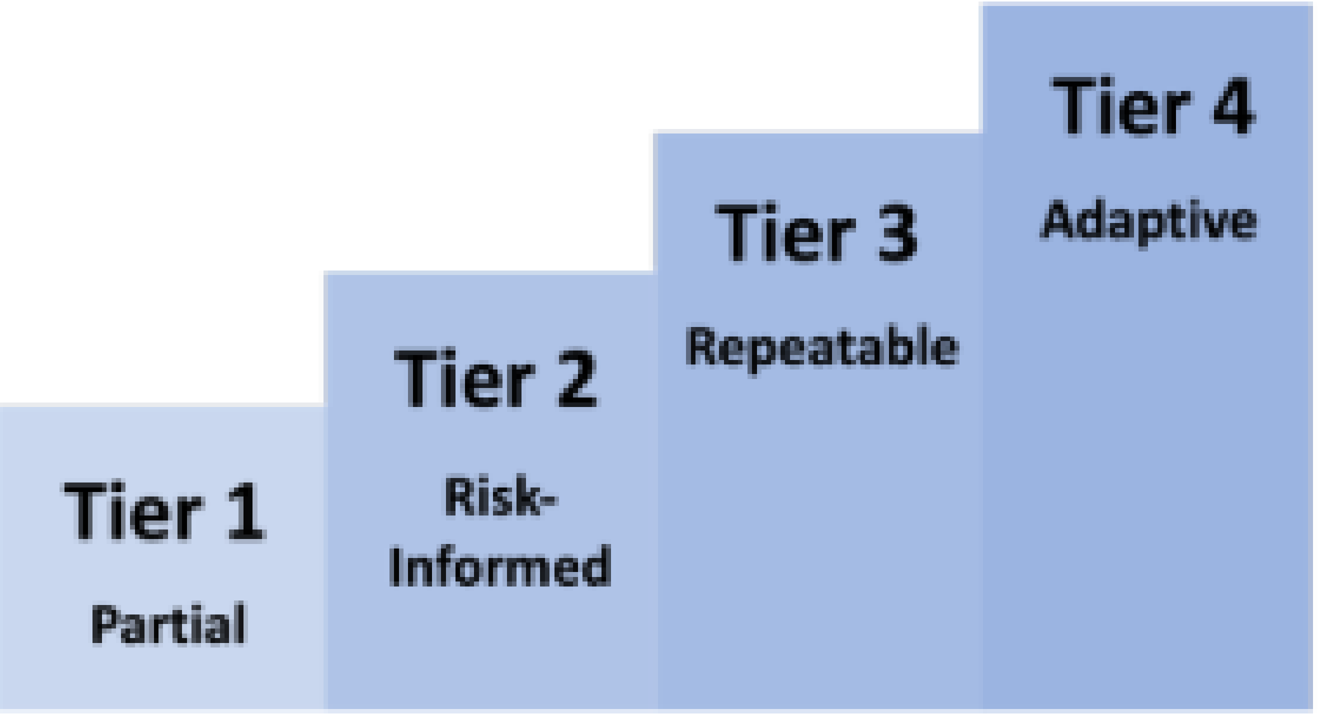
*What could go wrong for the **specific** organization?*

To manage cybersecurity risks, a clear understanding of the organization's business **drivers** and security **considerations** specific to its use of technology is required. Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary.

(Source: Nist CSF v. 1.1)

How to use the Framework in the laboratory assessment





(Source: Nist CSF v. 2.0)

Step 4. Having determined the current implementation status, decide the minimum level to reach (in terms of Tiers from 1 to 4, according to the scale offered by Nist CSF 2.0, on pages 8-11). You now have a gap between your **current** state and your **desired** level.

Choose the desired levels of implementation for each area considered (5 to 10 areas, according to Step 2). Now you have drafted a **profile** for the controls for the specific organization.

Explore why the current state isn't secure, what risks the organization is exposed to, and why it's good to implement certain controls, *prioritizing* each based on the risk highlighted, utilizing both the AI written report and your comment.

Report assessment for an organization, for the purposes of the laboratory, could be around 500 words.

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
✉ antonio.belli@unipd.it
simone.soderi@unipd.it

M6.5 – Nist CSF Laboratory

Thanks for your attention!