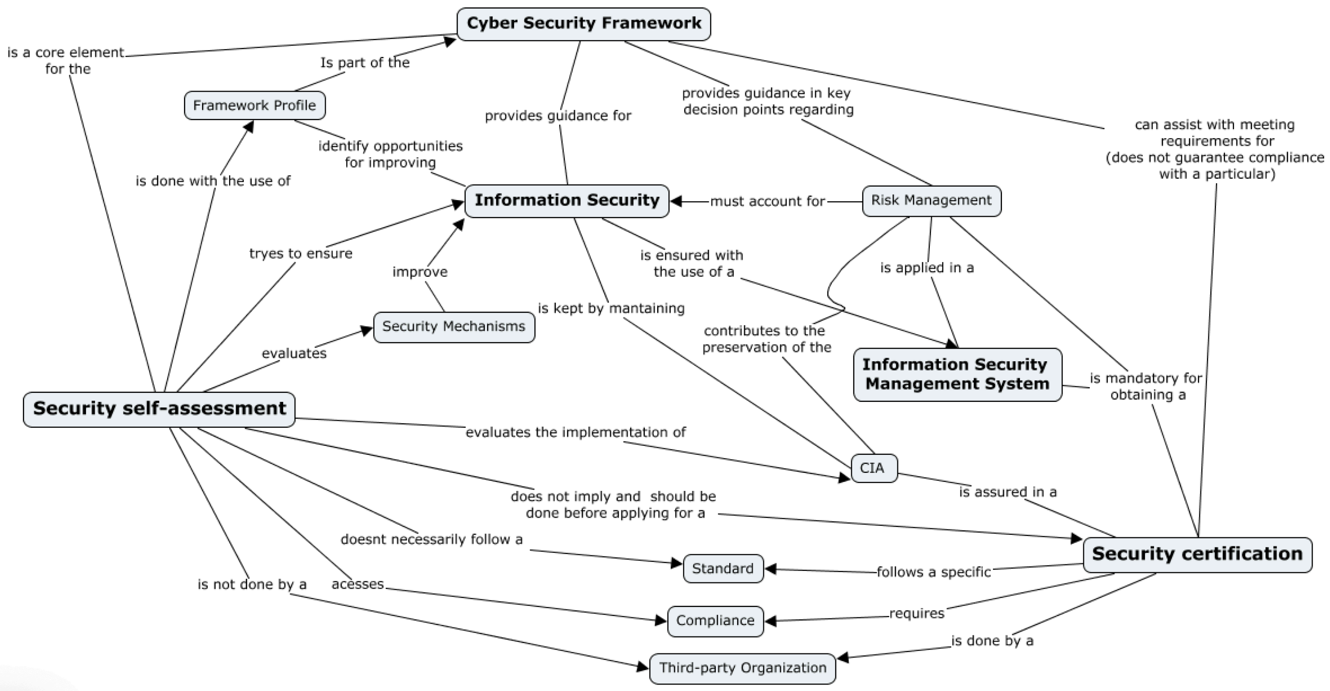
1 – Conceptual analysis


Cyber Security Framework
is a core element for the
Is part of the
Framework Profile
provides guidance for
provides guidance in key decision points regarding
can assist with meeting requirements for (does not guarantee compliance with a particular)
identify opportunities for improving
is done with the use of
Information Security
must account for
Risk Management
tryes to ensure
improve
is ensured with the use of a
is applied in a
Security Mechanisms
is kept by mantaining
contributes to the preservation of the
evaluates
Information Security Management System
is mandatory for obtaining a
Security self-assessment
evaluates the implementation of
CIA
is assured in a
does not imply and should be done before applying for a
doesnt necessarily follow a
Security certification
Standard
follows a specific
is not done by a
acesses
Compliance
requires
is done by a
Third-party Organization

Concept	Definition (one sentence by concept)
Cyber Security Framework	Voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk
Security Certification	Certification from a competent authority regarding an organization's practices concerning cyber security
Security Self-Assessment	The self-assessment by the organization of its own cyber security risks, allowing to measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk to acceptable levels
Information Security Management System	Systematic approach to managing sensitive company information so that it remains secure, it includes people, processes and IT systems by applying a risk management process
Risk Management	Application of risk management methods to information technology in order to manage IT risk
Security Mechanisms	Technical tools and techniques that are used to implement security services
Information Security	The practice of protecting information by mitigating information risks
Compliance	Adhering with the mandated boundaries (laws and regulations) and voluntary boundaries (company's policies, procedures, etc.).
CIA	The CIA triad meaning Confidentiality, Integrity and Availability respectively define the three goals regarding IT and information security
Standard	Something established by authority, custom, or general consent as a model or example
Framework Profile	Is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.
Third-party association	A third party is typically a company that provides an auxiliary product not supplied by the primary manufacturer to the end user (the two principals).

2 – Description of the analysis

With the concept map showcased in question 1, we intend to demonstrate the relationship between the concepts of Cyber Security Framework, Information Security Management System, Information Security, Security Certification and Security self-assessment.

Security self-assessment and Security certification are similar in the way that they both contribute to ensure Information security and complementary.

In one hand, a Security self-assessment does not imply and should be done before applying for a Security certification. A Security self-assessment doesn't necessarily follow a Standard, accesses a Compliance with regulation, is not done by a Third-party Organization.

On the other hand A security certification follows a specific standard, requires compliance with regulation and is done by a Third-party Organization.

An Information Security Management System, is a systematic approach to managing sensitive company information so that it remains secure, which applies risk management processes in order to preserve/enhance the three main information security goals which are:

- Confidentiality (Prevention of unauthorized disclosure or use of information assets);
- Integrity (Prevention of unauthorized modification of information assets);
- Availability (Ensuring of authorized access of information assets when required);

An Information Security Management System is a mandatory for obtaining a Security certificate, and its used to ensure Information security.

A Security certification assures the following of these goals (CIA). And a Security self-assessment evaluates the implementation of these goals (CIA).

In order to perform a Security self-assessment a Framework profile must be chosen; this is a part of a cyber security framework. Which is a core element for the security self-evaluation. The cyber security framework provides guidance for maintaining information security and the framework profile identifies opportunities to improve it. The security self-assessment evaluates security mechanisms to improve information security.

Last but not least, a cyber security framework can assist with meeting requirements for a Security certification but it does not guarantee compliance with a particular certification.

3 – Research

The concept of vulnerability is defined as weakness of software, hardware or online service that can be exploited or, more broadly, functional behaviour of a product or service that violates an implicit or explicit security policy

And the coordinated vulnerability disclosure is a method of vulnerability disclosure of the several that exist (such as Full Disclosure, Non-Disclosure, etc.) but still haven't defined what vulnerability disclosure is.

According to the ISO/IEC 29147:2014, "vulnerability disclosure is the act of initially providing vulnerability information to a party that was not believed to be previously aware. The overall disclosure process typically includes multiple disclosure events.".

This process of vulnerability disclosure has been included in NIST's revision of its cybersecurity framework as part of the framework's core and this inclusion ensures that processes are established to receive, analyse and respond to vulnerabilities reported to organizations from internal and external sources. With this revision, organizations will have the necessary aid to apply enough resources to the disclosed vulnerabilities accordingly.

4 – Topic for discussion

Nowadays some entities disclose vulnerabilities publicly in order to warn the general public about the risks they face when using a service. Should this approach be punishable since it attracts the attention of attackers?