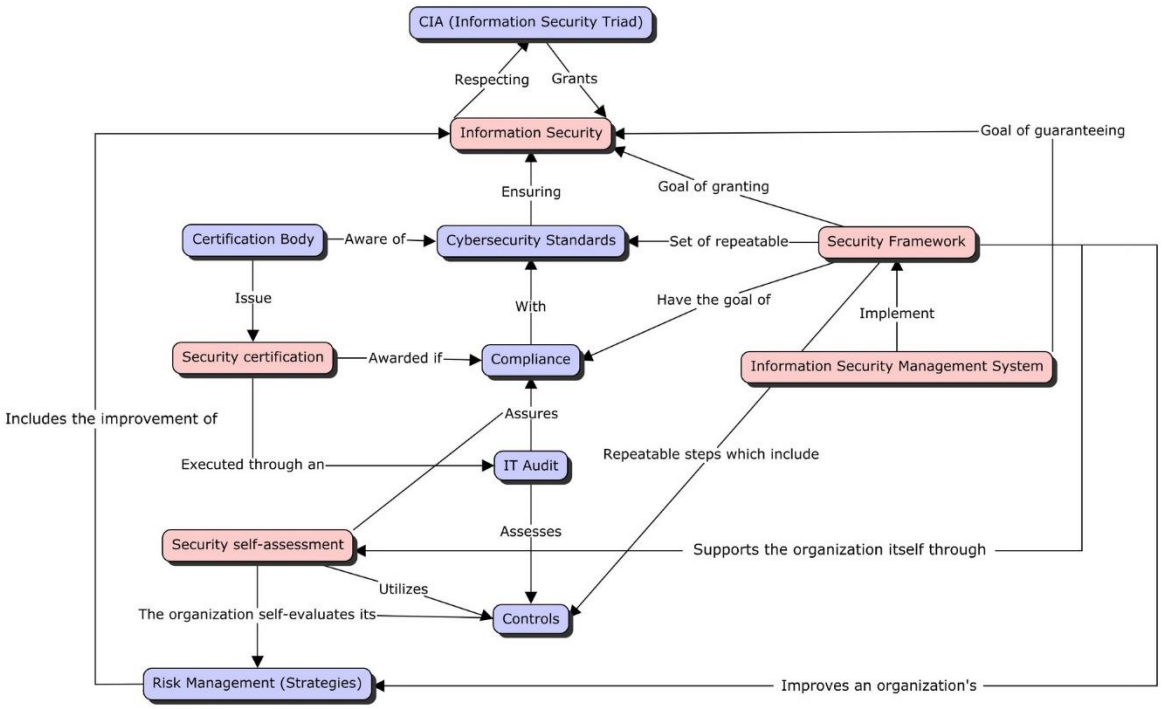
1 – Conceptual analysis



Concept	Definition (one sentence by concept)
Certification Body	Organization **accredited** by a recognized accreditation body for its competence to **audit** and to issue **certification** confirming that an **organization** meets the **requirements** of a **standard.**
CIA (Information Security Triad)	**Triad** that constitutes one of main pillars of knowledge about **Information Security**. The **three letters** stand for **confidentiality**, **integrity** and **availability**. **Management**-wise this is used as a **model** to **evaluate** the **information security** of an **organization**.
Compliance	**Goal** that **organizations** aspire to achieve through efforts that ensure they **comply** with relevant Information Security **laws**, **policies**, and **regulations**.
Controls	**Procedures** assuring that the **Information Security practices** that an **organization** is using operate as intended.
Information Security	Practice of preventing **unauthorized access**, use, **disclosure**, disruption, **modification**, inspection, **recording** or **destruction** of information.
Information Security Management System	Set of all the interrelated **information security** elements of an **organization**, as described in the **ISO/IEC 27001,** that ensures **policies**, **procedures**, and **objectives** can be created, implemented, communicated, and evaluated to **better guarantee** an organization's overall **information security**.
IT Audit	Examination of the **management controls** within an **Information Security Infrastructure** and the **review** and **evaluation** of such **information systems**.
Cybersecurity Standards	**Techniques** generally set forth in **published** materials that attempt to protect the **cyber environment** of a user or **organization**.
Risk Management	**Identification**, **evaluation**, and **prioritization** of risks followed by **coordinated** organizational **actions** to **minimize** and **control** the probability of **harmful** events **affecting** the **organization**.
Security Certification	Provision given to some company by an **independent body** when the **product**, **service** or **system** being offered meets certain specific **security requirements** and **standards**.
Security Framework	**Flexible** and **repeatable** set of performance-based procedures that including **information security** measures and **controls** that may be adopted by owners and operators of **critical infrastructure** to help them **identify**, **assess**, and **manage** cyber risks
Security Self-Assessment	**Evaluation** and **measurements** done by the **organization itself** regarding the cybersecurity **architecture**, **practices** and **risk management strategies** being currently **employed**.

2 – Description of the analysis

With this concept map I plan on expanding upon the following points:

- **Information Security Management Systems (ISMS)** intend on implementing **cybersecurity frameworks** in order for **organizations** to comply with **international security standards** that ultimately contribute to the **security** of **organizational information**, more specifically, these procedures intend on respecting the **triad of information security** in order to attain **information confidentiality**, **integrity** and **availability**.
- The importance of proper **risk management** being applied by **organizations** to provide strong **information security measures** such as the **consistency** of **encryption policies** and **information privacy** to provide proper **compliance** with **international security standards** such as the **ISO/IEC 27001** family.
- The connection between **Security Standards** and **IT Audits** since accredited bodies might issue **certifications** upon **evaluating** and reviewing how these **standards** are applied in **management systems**.
- We would like to display that both **Security Self-Assessment** and **Security Certification** are concepts which intend to provide **compliance** with **security standards**. Nonetheless, even though both concepts possess similar **goals**, the **main difference** is that **Security Self-Assessment** is performed by the **organization** itself utilizing **Controls** implemented by its **Security Framework**, whilst **Security Certification**, in the other hand, is a process conducted by a **Certification Body** and awarded if the **organization** displayed **Compliance** with the S**ecurity Standards** throughout specific **security-based IT audits**.

To conclude, one can observe that the concept interlinking the remainder is that of **Information Security**. **Organizations**, thus intend on **complying** with the **security standards** described in the security framework implemented by **Information Security Management Systems**, either through an **internal** security **self-assessment** or an external **security certification** process provided in conjunction between an **IT audit** and **certification bodies** with the ultimate **goal** of granting organizational **information security**.

3 – Research

The **Cybersecurity Framework**, developed by **NIST**, a federal agency in the United States, provides a common **language** and **systematic methodology** for managing **cybersecurity risk** and fostering **information security**. It consists of **standards**, guidelines to promote **information security**.

Vulnerability disclosure is a fundamental principle regarding the **information security** procedures of a **Cybersecurity Framework** since it provides **information** about **discovered vulnerabilities** on **systems** to parties that were unaware of its **disclosure previously**. As depicted in ISO 29147, the coordinated practice of **coordinated vulnerability disclosure (CVD)** describes a set of **activities** which include **identifying** and **disclosing vulnerabilities**.

These same set of **practices** is treated by the **Dutch National Cyber Security Centre** as a focused and coordinated effort, that contributes to the **security** of **IT systems** through the sharing of **knowledge** about **vulnerabilities**. Furthermore, these set of **guidelines** specify how **companies** might implement their own **CVD policy** with the goal residing on creating a **coordinated process** between a **reporting party** and the **organization itself**. The roles of both these entities are described below:

- A **reporting party** is an entity outside the **organization**, with the function of **discovering vulnerabilities** through **passive** observation or **active testing** of an organizational **IT system**. Furthermore, this entity has the **responsibility** of sharing this **knowledge** with the **organization** upon the **disclosure** of **vulnerabilities**.
- An **organization** has the responsibility of managing the **information security** of **IT systems** and **following** up on a **vulnerability report** by choosing to draw its **own CVD policy** up.

Finally, one of the main advantages of the **CVD practice**, is sharing **reported vulnerabilities** in order to help other **companies** that possess the same **IT systems** thus **creating** a **safer environment** and increasing the **security** of **organizational** and **customer information** in modern day enterprises.

4 – Topic for discussion

Nowadays **Information Security** and **Privacy** has gained traction among concerned citizens with **governments** enforcing strict **information privacy laws** such as **the General Data Protection Regulation (GDPR)**, that conflicted with **cybersecurity practices** of both public and private companies such as Facebook, contributing to a decline in the number of active users in Europe, causing a great **loss** of **revenue**.

We would like to discuss the fine **nuances** regarding the **ethics** about the usage of **sensitive user information** by **governments** to protect its **citizens** from **harmful acts** such as terrorism and organized crime.