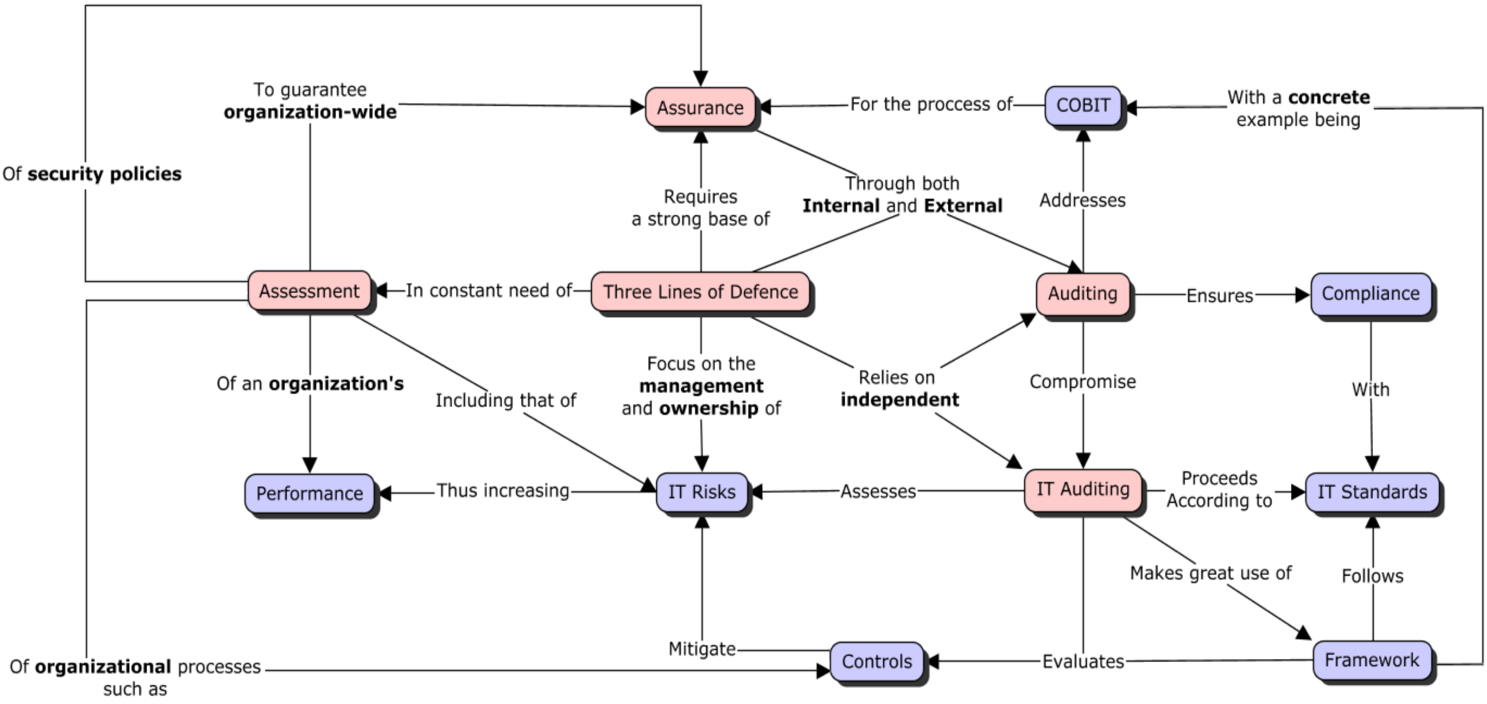
## 1 – Conceptual analysis



| Concept | Definition |
|---|---|
| Assessment | Process intended on **identifying** the **strengths** and **weaknesses** as well as **suggesting methods** to boost **efficiency**, **productivity**, and **profitability** of an **organization's processes** and **practices**. |
| Assurance | Practice of **assuring information** and **managing risks** related to the use of **information** and the **systems** and **processes** used for those **purposes**. This process also includes the **protection** of data **confidentiality**, **integrity** and **availability**. |
| Auditing | **Review** or **assessment** of **processes** defining an official **inspection** of **organizational accounts** that might also be done in the context of **Information Technologies**, also including **IT Audits**. |
| COBIT | **Framework** for **information technology management** and IT **governance** that provides a set of **controls** to be **implemented** over **information technology** organizing them around a **framework** of **IT-related processes**. |
| Controls | Procedures **assuring** that the **Information Technology** of an **organization** is using operates as **intended**. |
| Compliance | **Goal** that **organizations** aspire to achieve through efforts that ensure they **comply** with relevant Information Security **laws**, **policies**, and **regulations**. |
| Framework | Set of **definitions** providing information on how an **IT Audit** should be **planned** and **conducted**. |
| IT Auditing | Examination of the **management controls** within an **Information Technology Infrastructure** and the **review** and **evaluation** of such **information systems**. |
| IT Standards | **Guidelines** followed by organizations in order to **increase their performance** in the context of their future goals. |
| IT Risks | Any **risk** related to information, information processing or **information technology** and how a specific **threat** might **exploit** such **vulnerabilities**. |
| Performance | The offer of **services**, levels of service and **service quality** required to meet current and future **business** and **security requirements**. |
| Three Lines of Defence | **Activities** defined in **enterprise risk management** across the three different **lines** of **defense** and possessing **separate responsibilities** that **enable effective risk** and **management** against any kind **threat**. |

## 2 – Description of the analysis

With this concept map I plan on delving deeper in the analysis of the following topics:

- Firstly, an organization to successfully implement the **Three Lines** of **Defence** as defined by **enterprise risk management** must possess solid **assurance practices** to **effectively** implement **controls** and deal with **risk-related** activities such as those of **management** and **ownership**. Furthermore, I intend on showing that these **lines** of **defence** also rely on **assessment** processes such **audits** to **evaluate** the **controls** implemented by the **organization** and successfully help **mitigate risks**. The goal of **implementing** these **practices** is that of **assuring** a successful **first line** of **defence** through the usage of **risk ownership** and **management** procedures.
- Likewise, I intend on showing that through a successful **implementation** of a **standards-following framework** such as **COBIT**, one can successfully **evaluate** the applied **controls** in effect to deal with **organizational risks** and effectively **formulate policies** to provide **assurance mechanisms** and **oversight** a company's **performance**. The practice of implementing a **risk framework** which **complies** with **international information technology standards** provides a strong **second line** of **defence** in assurance procedures.
- **Audits** are a process that is done by **independent bodies** to assess **risks** and **control** practices. These bodies might be **internal** or **external** and intend on ensuring **compliance** of **IT processes,** implemented by an **IT Framework,** with **International IT standards**. This **assessment procedure** carried through **audits** of organizational **processes** and **systems** defines the **third line** of **defence** regarding **assurance** and **risk management** for modern-day **companies**.
- Additionally, I proceed on showing that organizations that **implement** these **lines** of **defence** through **assessment** and **assurance** processes intend on **reducing** and **mitigating** risks thus increasing their **performance** and aiding with the **achievement** of company-wide **objectives** such as the meeting of **security** and **information technology quality requirements**.

Finally, one can observe the point that links all these topics are the **Three Lines of Defence.** We can observe that this concept is **deeply interlinked** with those of **assurance** and **assessment** thus contributing with **risk reduction** and **mitigation** procedures. These practices to **solidify** an **organization's defence lines** can ultimately **employ auditing** procedures, thus **assuring compliance** with the **IT standards** set by the **company** and **ensuring** a proper **reduction** and **mitigation** of risks**.**

## 3 – Research

An **auditing process** is an **assessment procedure** that should be carried by an **independent body** in order to **assess** the **business** and **information technology practices** being employed, thus properly **evaluating** the **controls** that ensure **proper risk management** strategies. Nonetheless, a **successful audit** of an **organization's IT systems** ultimately has the scope of helping the **company** by **assessing** its **practices** and thriving against its competitors.

As we have observed regarding **Enron**, one of the largest **energy companies** in the **United States**, and **Arthur Andersen**, Enron's **auditing** and **accounting** partners, and one of the **biggest auditing firms** in the country, the **failure** of such **audits**, eventually might lead to a **company's downfall**, as the **ineffective evaluation** of **risk-management procedures** being applied, not only contributed to the **company filing** for **bankruptcy**, but to one of **biggest auditing failures** in American **history**.

Through the **concealment** of **business process information** and through a **deceptive stance** Enron's Chief Financial Officer took regarding **high-risk accounting practices**, executives and **accounting personnel** were able to keep secret the usage of **accounting loopholes** and **poor financial reporting**, that had **hidden billions** of **dollars** in **debt** from failed deals and projects, to Enron's board of directors and to their **auditing** and **accounting** partners.

With this being stated, **auditors** need to be **meticulous** and include in their **evaluating scope** the **assessment** of every **IT system** and process that is **aligned** with and **automates** every **business applications** and **information security** procedure. With this prudent scope of analysis, one can **successfully evaluate** the implemented **controls mechanisms** and aid **risk management practices** thus increasing an **organization's performance**.

## 4 – Topic for discussion

I would like to inquire which **assessment** and **auditing procedures** suit modern-day **large-scale technology companies** that **employ** and **commercially succeed** with products that rely on trendy-computing topics such as those of **blockchain**, **big data analytics** and **cloud computing**.