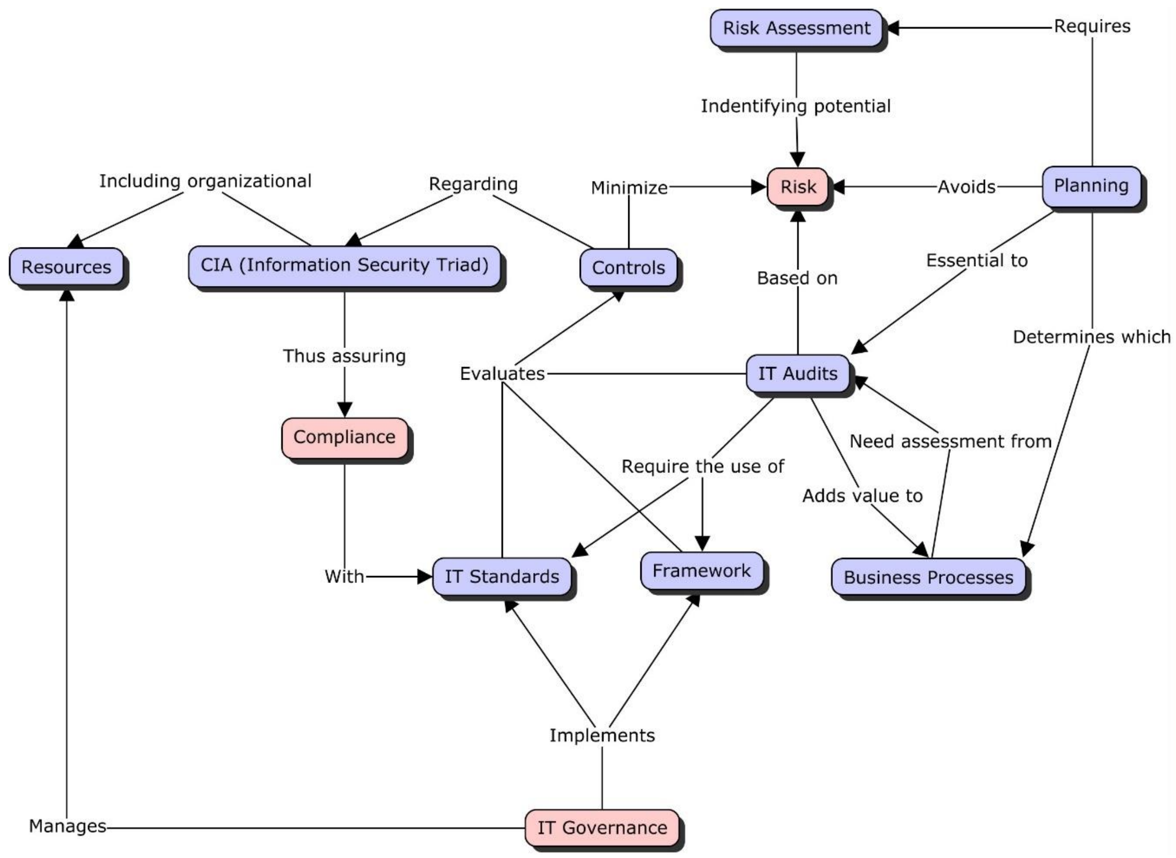
GSI (Case C) - Student number (5 digits) and name: 82069 – José Brás

1 – Conceptual analysis



Concept	Definition
Business Processes	Set of diverse **tasks** linked to one another in specific **sequence** thus producing a **service** or **product** that will be offered to the **customers**.
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 **laws**, **policies**, and **regulations**.
Controls	Procedures **assuring** that the **Information Technology** that an **organization** is using operates as **intended**.
Framework	Set of **definitions** providing information on how an **IT Audit** should be **planned** and **conducted**.
IT Audits	Examination of the **management controls** within an **Information Technology Infrastructure** and the **review** and **evaluation** of such information **systems**.
IT Governance	**Processes** that help an **organization** thrive in its **goals** through the assurance of an **effective** use of **Information Technology**.
IT Standards	**Information** required to meet the **compliance** pre-requisites of **Information Security audits**, but also providing **guidance** to improve **effectiveness** and **efficiency**.
Planning	Management **process** that involves the *à-priori* **decision** of what the **organization** is meant to do and how it should **proceed** in order to **achieve** its **goals**.
Resources	**Supplies** such as staff **money** or **stocks** required to **accomplish** planned **activities**.
Risk	Probability of a **negative event** occurring leading the **organization** to potential **danger**.
Risk Assessment	The **identification** and the **analysis** of potential **events** that may **negatively** impact the **organization**.

2 – Description of the analysis

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

- Firstly, **risk** and **resource management** are activities both assessed by **IT Governance** integrating the best practices thus **ensuring** that an **organization's** IT is aligned with the **efficient management** of IT-related **risks** and **resources**.
- Also, I plan on demonstrating that IT audits are a **risk**-**based** approach that not only contribute to **risk assessment** but also to the **evaluation** of **controls** that ultimately help serving the purpose of **risk minimization** including that of information with respect to its **confidentiality**, **integrity** and **availability** (the **CIA triad** of **information security**). Since these properties are key factors when it comes to **IT auditing**, I included a link relating them with **organizational resources** since they might be used during **IT audits** to obtain the results an **organization** expected.
- Furthermore, I show that these **information security** requirements mentioned above (**CIA Triad**) when properly **assessed** during **IT audits** not only do reduce risks but assure compliance with the IT standards of put in place by **IT Governance**.
- I also display the importance of **IT Governance** integrating the best **standards** and frameworks to ensure the **IT** not only aligns with the **goals** of the organization thus offering **value**, but also **managing** the **risk** and **resources** associated with **IT efficiently**. By following **frameworks** like **COBIT** and through **IT auditing** following a set of **controls** we make sure an **organization** fully **complies** with the **IT standards** implemented by the **IT Governance**.

Finally, one can observe the point that links all these topics are both **Risk** and **Compliance** provided by the concepts implemented by **IT Governance** and evaluated through **IT Audits**. We can observe that both these concepts when properly synchronized through the use **Frameworks** and **Standards** will help by reduce potential **risks** thus assuring **information** is properly **secured** thus **complying** with the **IT standards** set by the **company**.

3 – Research

Data is at the center of **Information Systems**. An **Information System** can be characterized by its composition of **people** and/or **computers** that **process** or interpret **information**.

Nowadays **data is** the main way an **organization** will learn what to do and **improve** or put in **practice** what will **lead** to its **success** and the **achievement** of its **goal**. With this being stated, the **possession** of large amounts of data on its **customers** is not a positive sign. Having such **data** can be problematic since there has been lots of discussions about the abuse of **personal privacy** by **companies** making the general population **distrust** large **companies**.

In the present-day **organizations**, especially their **governance** structure, must be **keen** and **assure compliance** with **GDPR** and **risk management** techniques because the game is no longer about how **data** can help a **company** achieve its **goals** but how **legitimate** is the use of such data by the **companies**. The lack of **compliance** with **GDPR** has thus become a violation of **customer privacy** and the **information** that **companies** maintain of their **customers** shall be **subjected** to great **scrutiny** by the responsible **Data Protection Officers** (DPO). Alarming cases, such as the one mentioned in the *Timelex* document about the furniture manufacturer in Denmark that was subjected to a 200.000€ fine for **mishandling customer data** in their **IT systems**, are great examples of a **governance policy** that failed to **comply** with proper **resource management** and **information preservation** regulations.

Finally, one can observe that the **governance** of a **company** as to be aware of the **risks** of poor **records management** and improper **information retention** and subject itself to processes such as **IT audits** that make sure the **companies**' **data policy** and **framework** successfully **comply** with **standards** and **regulations** such as the **GDPR** in order for the company to **achieve** its goals and **avoid** diminishing **credibility** and dealing with the resultant **public exposure**.

4 – Topic for discussion

The question I intend on discussing next lecture is related with the fact that with the advent of **large**-**scale cyber**-**security attacks risk reduction** and **threat exposure** are each day becoming hotter topics in modern-day **enterprises**. Thus, I would like to understand how **compliance** with **ISO standards** reduces **risk** and **protects** international companies with large-scale distributed **databases** and **sensitive information** from attackers that might exploit **vulnerabilities** that **corporate management** did not know existed. Following this question, I would like to understand how enterprises should behave if data **exposure** happens.