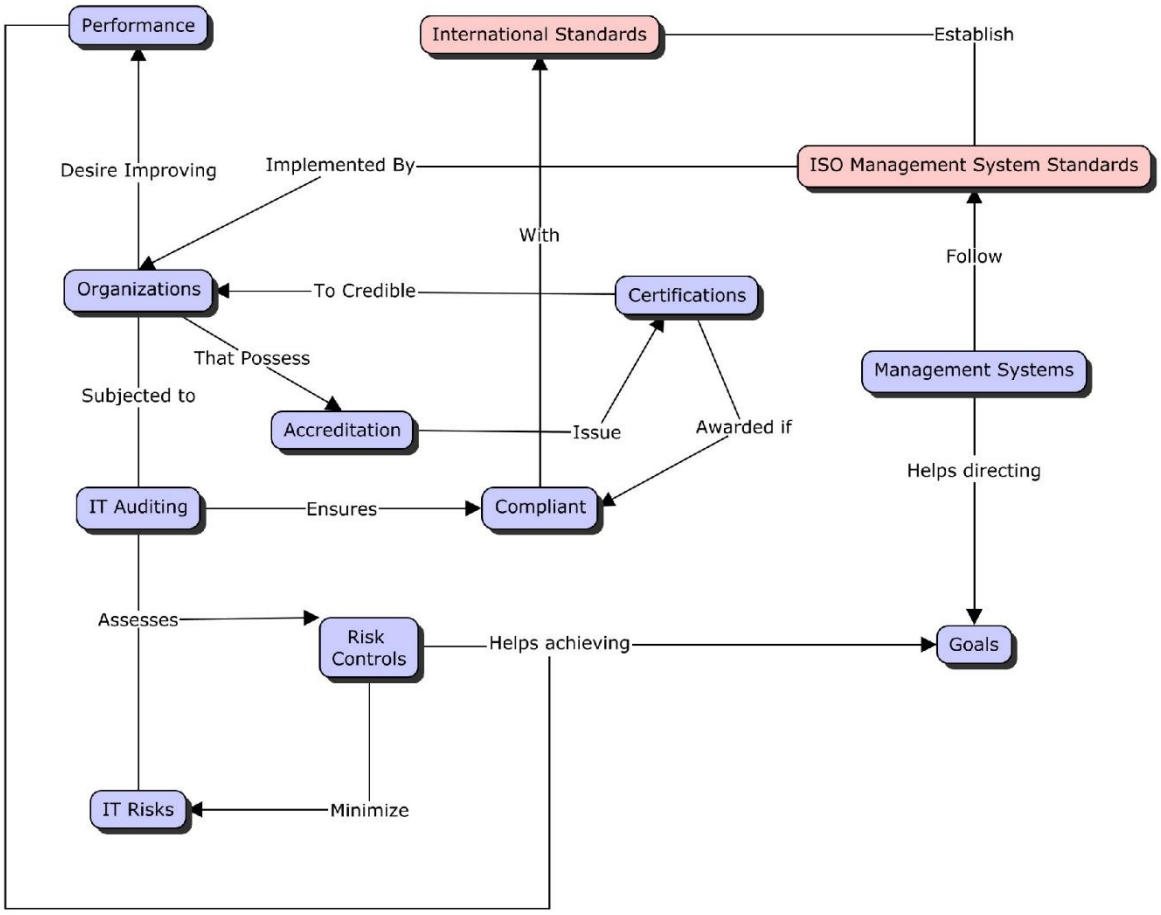
1 – Conceptual analysis



Concept	Definition
Accreditation	Certification of competence by an **independent body** that assures a company operates accordingly with **international standards** in some area of expertise.
Certification	Provision given to some company by an **independent body** when the **product**, **service** or **system** being offered to customers meets certain specific **requirements**.
Compliance	Goal that **organizations** aspire to achieve through efforts that ensure they **comply** with relevant **laws**, **policies**, and **regulations**.
Risk Controls	Methods that allow **organizations** to evaluate potential losses and act accordingly thus **reducing** the scope or even **eliminate** pertinent **threats**.
Goals	Objectives, targets, purposes, intentions and plans that someone set out to do.
International Standards	**Guidelines** followed by organizations in order to **increase their performance** in the context of their future goals.
ISO Management Standard	**Management system standards** implemented by **organizations** with the objective of achieving **better performance** and achieve their **goals** accordingly. These **standards** are agreed upon by experts and are followed **internationally**.
IT Audits	Examination of the **management controls** within an **Information Technology Infrastructure** and the **review** and **evaluation** of such **information systems**.
IT Risks	Any **risk** related to information, information processing or **information technology** and how a specific **threat** might **exploit** such **vulnerabilities**.
Management Systems	Set of **policies**, **processes** and **procedures** followed by organizations to coordinate all their **business components** in order to fulfil the **tasks required** to achieve their **goals**.
Organizations	**Social structure** unit compromised of **multiple people** working together to meet a need or to seek collective **goals** and **achievements.**
Performance	The offer of **services**, levels of service and **service quality** required to meet current and future **business requirements**

2 – Description of the analysis

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

- The interplay between **ISO Management Standards** and **IT Audits** since **accredited** bodies might issue **certifications** upon **evaluating** and **reviewing** how these standards are being applied by organizations and their management systems.
- Also, I intend to display that these **standards** are international and applied by organizations all over the world and that companies that **comply** with them display a rapid growth rate according to **ISO surveys**.
- In order to comply with **ISO standards** organizations, undergo (an optional) **certification** process conducted by independent certification bodies that can be **accredited**. Since ISO alone does not provide credibility, most **organizations** enrol in these **certification** processes because they search for **credibility** that their services meet **specific requirements**.
- The goal of **IT Audits** is that of examining an organization's systems and business processes and mitigate the risks by utilizing **risk control** methods. These processes are described in **ISO27001** guidelines with the objective of identifying and **minimizing** these **risks** to an acceptable level. **IT audits** are thus a vital part of the **management systems** approach as they enable the **organization** to conclude if they have managed to achieve their **goals** and are **complying** with the **standard** being applied.
- I conclude by relating the two major concepts and by saying that an **IT audit** is applied to **organizations** that implement **ISO MSS**, since audits are a fundamental point in that of the **management system** approach.

Finally, one can observe the point that links all these topics are both the **International Standards** provided by the **ISO MSS** and the **ISO Management Standards** themselves. Both these topics are a fundamental point to that of issuing **certificates** (that **validate compliance** with these **standards**) and as **guidelines** being used in the **auditing** process, hence connecting all the concepts being displayed in the concept map.

3 – Research

Being the **security** of IT systems one of the most relevant properties in **organizations** I have selected the **ISO/IEC 27001** as the most relevant **standard** for further **discussion**. This standard is the most important when we refer to **Information Security Management Systems** (**ISMS**) which are a set of systematic approaches for managing and securing sensitive data. When using this MSS I would propose **standard 54534** in particular since it takes concern with **maintaining** and **improving** information **security systems** in the context of **organizations**.

The reason for me selecting this **MSS** is because it defines how **organizations** should **manage** their **data** depending on their **infrastructure**, **business model** and **objectives**. Since **cybersecurity** is one of the most **important** areas organizations should focus nowadays, this course tackling that area as well, this **MSS** is of the **utmost importance** since it defines the **requirements** any **organization** shall follow to improve the **security** of their **information systems**.

Finally, having previously worked in the field of IT and dealt with the European Union-wide law of **General Data Protection Regulation** (**GDPR**) I recognize the **importance** of information systems' engineers being **aware** of the importance of **data protection**, this **MSS** being the one that has the potential to **comply** with such **laws**.

4 – Topic for discussion

Having read the documents for this weekly case I came to know a **wide range** of **ISO standards**. Thus, I would like to further discuss if these **standards** should be **mandatory** to **follow** by **organizations** independently of their size and scale. If this is the case, I would like to expand on the **importance** of undergoing **certification processes** to **verify compliance** with the said standards.

Also, with the advent of **large-scale cyber-attacks** I would like to discuss how the MSS proposed above would be applied in a modern large-scale company since these companies tend to hold the most sensitive data, including databases with customers personal data stored.

Finally, I would like to discuss how these standards relate and apply with companies that are employing the trendiest topics in computing such those of **machine-learning** and **blockchain** since the enterprise **adoption** of such **techniques** became such a **game changing factor** for IT's major players.