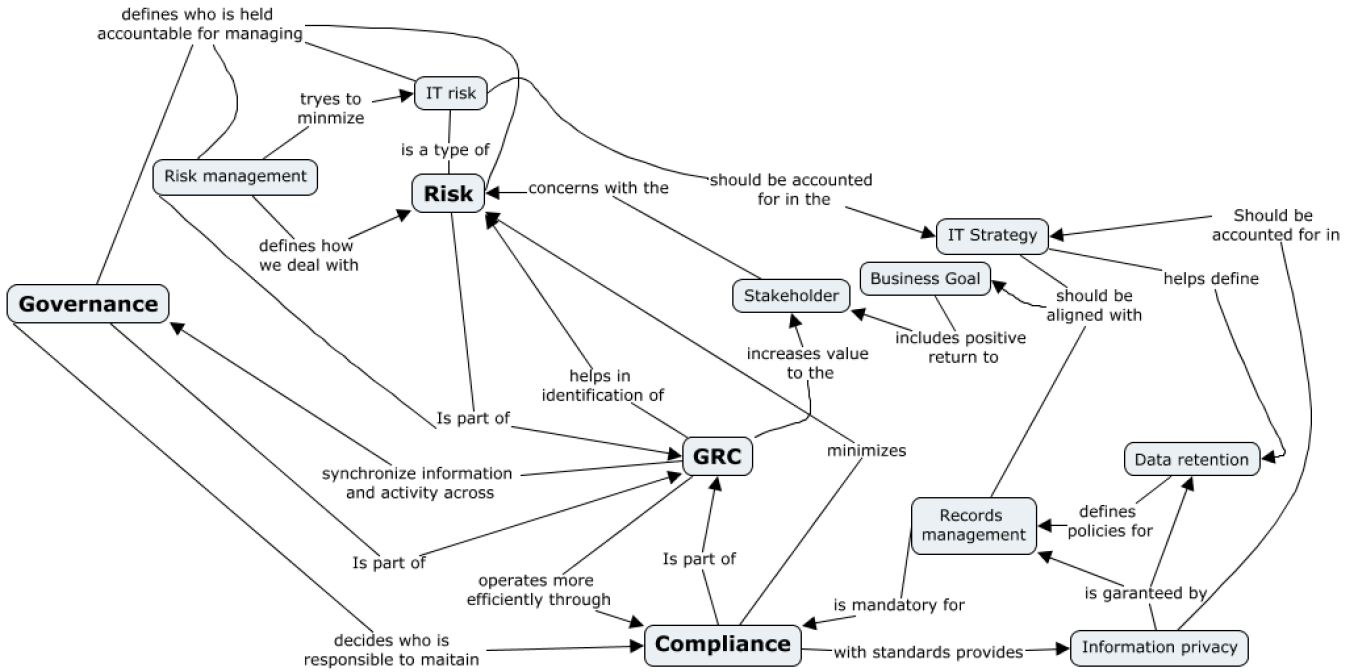
GSI (Case C) - Student number (5 digits) and name: 97155 – João Tiago Aparício

1 – Conceptual analysis



Concept	Definition (one sentence by concept)
Governance	“Defines the ownership and associated roles and responsibilities for oversight functions and business as usual (BAU) activities”
Risk	“The potential for uncontrolled loss of something of value. Or intentional interaction with uncertainty”
Compliance	“Adhering with the mandated boundaries (laws and regulations) and voluntary boundaries (company's policies, procedures, etc.).”
IT Strategy	“The overall plan which consists of objectives, principles and tactics relating to use of technologies within a particular organization.”
Risk management	“The set of processes through which management identifies, analyses, and, where necessary, responds appropriately to risks that might adversely affect realization of the organization's business objectives.”
Information privacy	“The relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them.”
Records management	“An organizational function devoted to the management of information in an organization throughout its life cycle, from the time of creation or inscription to its eventual disposition.”
Data retention	“The policies of persistent data and records management for meeting legal and business data archival requirements.”
IT risk	“risk related to information technology”
GRC	“Discipline that aims to synchronize information and activity across governance, and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps.”
Stakeholder	“An individual or group who can affect or be affected by the actions of a business.”
Business Goal	“describe what a company expects to accomplish over a specific period of time.”

2 – Description of the analysis

GRC, or Governance, risk management, and compliance is a set of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity. The different parts of that concept relate to each other in the following way:

Governance defines who is held accountable for managing risk and who is responsible to maintain compliance with standards. Compliance with set values through the use of standards minimizes risk.

The use of these three related facets in an integrated way increases the value to the stakeholders that concern with Risk but with the compliance with standards and governance as well.

In the perspective of the application of these concepts in IT, IT Risk is managed by the people defined in the governance framework. The IT risk should be accounted for in the IT Strategy that by itself must be aligned with the business goals. With the IT Strategy in mind, the data retention policies are defined in order to do the record management the proper way. These two are guaranteed by Information privacy standards. And Compliance with standards provides that information privacy.

GRC ensures that the organization operates more efficiently through compliance, helps identification of risk and synchronizes information and activity across Governance.

3 – Research

In the case described in "GDPR_Timelex.pdf", a Danish furniture company was proposed for a fine of DKK 1.5 million by the Danish supervisory authority. This fine was proposed because of errors in the reporting to the authority questionnaire, non-compliance with information retention periods as well as incorrect records management.

In terms of compliance with the GDPR, the mistakes were quite evident. But that may be related to a poor governance of IT, if the accountability framework is not clearly defined or no one is held responsible for checking the compliance within the defined legislation, that generates a higher the risk of an investigation by a supervisory authority. Moreover, the non-compliance with the defined standards and legislation generates other risks related to information security. As if for example an information breach were to happen, more confidential information would be compromised.

An effective and integrated GRC implementation, would have had a strong relationship between the governance risk management and compliance. As these have a relationship that creates synergy when used in an integrated way. Helping to identify risk, information synchronization and efficient operationality, of in this case Record management. The process of defining the record management may also be poorly defined within the enterprise because of Stakeholder interests, or even through IT strategy. This may be the product of ignoring Information privacy regulation while defining the IT Strategy. The non-compliance with the GDPR principles may be a sub product of not having an effective ERP system that seemed to be implemented during the investigation period.

4 – Topic for discussion

GRC is often done wrong, and so it is extremely important to understand what fails, what are the main practical issues that arise along with the implementation of GRC?