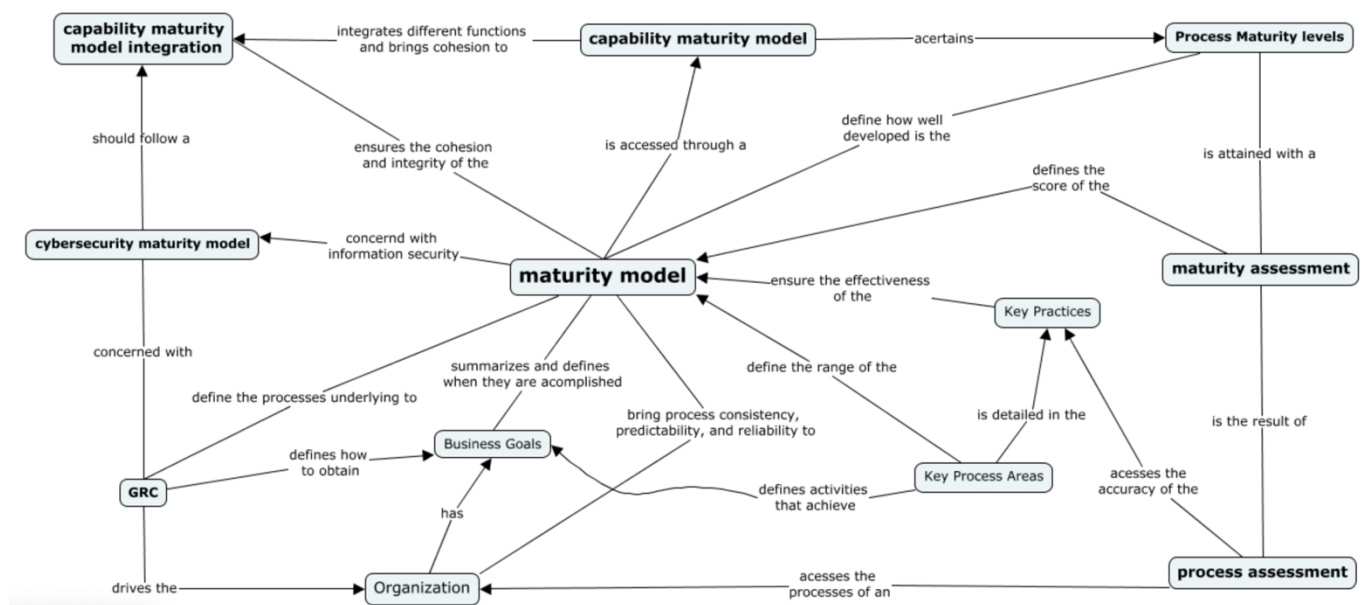


## 1 – Conceptual analysis



Concept	Definition (one sentence by concept)
<b>Maturity Model</b>	Set of structured <b>levels</b> that describe <b>how</b> well the <b>behaviours, practices</b> and <b>processes</b> of an organization can <b>reliably</b> and <b>sustainably produce required outcomes</b> .
<b>Capability Maturity Model</b>	Development model that works as a <b>tool</b> to <b>assess objectively</b> the <b>capability</b> of an organization to <b>implement</b> a certain project. It also works as an <b>optimization</b> process.
<b>Capability Maturity Model Integration</b>	Process <b>level improvement training</b> and <b>improvement</b> and appraisal program and it can be used to <b>guide process improvement</b> across a <b>project, division</b> , or an entire <b>organization</b> .
<b>Maturity Assessment</b>	<b>Scoring</b> the organization against defined criteria and a ranking scheme, generally organized in <b>ascending steps</b> with <b>strategies</b> on how to <b>move up</b> the <b>maturity scale</b> .
<b>Process Assessment</b>	<b>Examination</b> of <b>processes</b> by an organization against a set of criteria to <b>determine capability</b> of those processes to <b>perform</b> within <b>quality, cost</b> and <b>schedule goals</b> .
<b>Cybersecurity Maturity Model</b>	Helps organization <b>assess</b> and <b>improve</b> their <b>cybersecurity</b> efforts and helps <b>communicate</b> with <b>upper management</b> .
<b>Organization</b>	<b>Entity</b> composed by multiple people, such as an institution or an association.
<b>Process Maturity Levels</b>	<b>5-level process</b> maturity continuum - where the uppermost (5th) level is a notional ideal state where <b>processes</b> would be <b>systematically managed</b> by a <b>combination</b> of <b>process optimization</b> and <b>continuous process improvement</b> .
<b>GRC</b>	<b>Governance, Risk and Compliance</b> are a collection of <b>capabilities</b> that <b>enable</b> an organization reliably <b>achieve objectives, address uncertainty</b> and <b>act with integrity</b> .
<b>Key Practices</b>	The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.
<b>Key Process Areas</b>	Identifies a <b>cluster</b> of related <b>activities</b> that, when performed together, <b>achieve</b> a set of <b>goals</b> considered important.
<b>Business Goals</b>	<b>Objectives</b> and <b>action plans</b> that help you <b>move your business forward</b> .

## 2 – Description of the analysis

**Maturity Models** describe how well the behaviours, practices and processes applied by the organization can reliably and sustainably produce required outcomes that will help achieve the organization's **Business Goals** (set of objectives and plans that help the organization move forward). These goals are defined by **GRC** and along with **Key Process Areas** (set of activities that achieve a certain goal) allow the organization to summarize and define when they should the goals will be achieved which then translate into the definition of the maturity model.

These models are evaluated using **Process Maturity Levels**. The maturity levels are defined by a **Capability Maturity Model (CMM)** which act as set of functions to assess, optimize organization's processes. To ensure the cohesion between several Maturity models a **Capability Maturity Model Integration (CMMI)** can be used, which consists on process level improvement training, and guide process improvement across projects, divisions. The **CMMI** then helps to ensure and cohesion integrity of the maturity model.

The evaluation is performed by doing **Maturity Assessment**, which assess the quality of the organization's maturity model and by also doing **Process assessment** that evaluates the accuracy of **Key Practices** (related activities that achieve a goal) which will ensure the effectiveness of the maturity model itself.

One of the examples of using a maturity mode is the area of information security, where we can apply a **Cybersecurity Maturity Model** that concerns the processes inherent to **GRC** of information security.

## 3 – Research

To determine the goal level of maturity an organization should aim for, it is necessary to weigh not only the benefits but the costs as well. The implementation of higher maturity levels requires higher costs. So, it is necessary to first understand the goals and inherent costs of implementing each certified CMMI level:

- Level 1: Performed
  - Pro: "Reliance on individuals and their embedded knowledge"
  - Con: Cost of extra giving training to collaborators
- Level 2: Managed
  - Pro: "Processes are repeatable (at project level) but not necessarily in the most effective way"
  - Con: Cost of designing the processes in a sustainable way with well-defined goals
- Level 3: Defined
  - Pro: "Best practices are shared across the organization; objective insight into process performance"
  - Con: Cost of ensuring employees use the implemented practices on a daily basis in an efficient way.
- Level 4: Quantitatively Managed
  - Pro: "The organization and programs objectively understand performance and improve repeatability / decrease variability"
  - Con: Cost of building and maintaining an infrastructure that helps improve predictability in a data driven approach.
- Level 5: Optimizing
  - Pro: "Organization process repeatability and variability is controlled; process performance goals and set and achieved"
  - Con: Cost of building and maintaining a constant improvement in the practices designed, that are efficiency driven while maintaining predictability

In the costs we also should consider the costs of not implementing the levels, that leads to higher risk.

## 4 – Topic for discussion

Considering the importance of assessment to establish the quality and level of the maturity model, how should the process assessment periodicity be estimated?