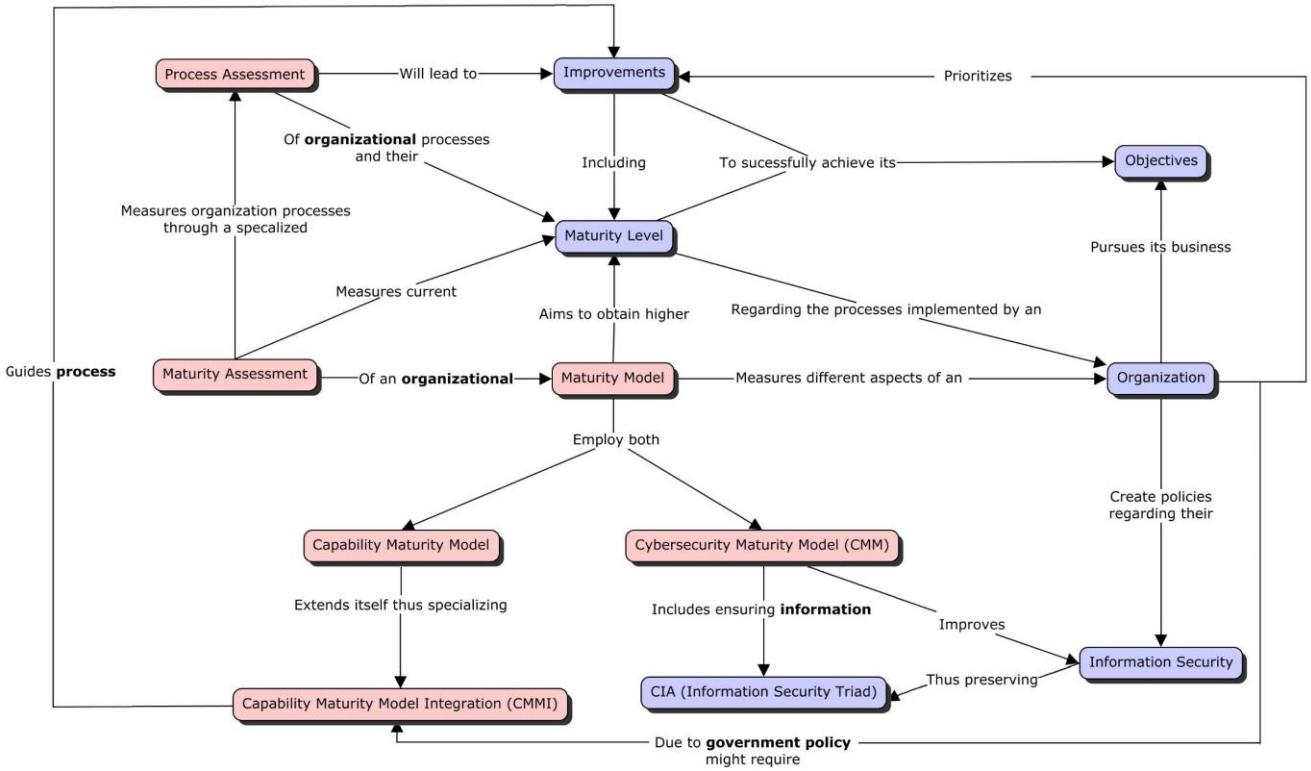
1 – Conceptual analysis



Concept	Definition
Capability Maturity Model	**Methodology** used to develop, refine and **improve software development** processes. This **development model** may also be applied to other **organizational processes**.
Capability Maturity Model Integration	**Program** focused in the area of **process level improvement training** and **appraisal** that can be used to **guide process improvement** across a **project**, division, or an entire **organization and** required by many U.S. **Government contracts** in area of **software development**.
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**.
Cybersecurity Maturity Model	**Model** providing a **framework** for the **measurement** of the **maturity** of the **information security processes** employed thus providing **guidance** to the next **maturity level.**
Improvements	Process of an **issue** moving from **one state** to a state that is **better** usually through some **action** or **intervention** intended to bring about that **change** and **improvement**.
Information Security	Practice of preventing **unauthorized access**, use, **disclosure**, disruption, **modification**, inspection, **recording** or **destruction** of information.
Maturity Assessment	Process used to **measure** the current **maturity level** of a certain **aspect** of an **organization** allowing to **prioritize** the **improvements** necessary to reach **higher maturity levels**.
Maturity Model	**Technique** that has been proved to be **valuable** in **measuring** different aspects of a **process** or an **organization**, specifically the ability for continuous **improvement** and providing a **framework** and **guidance** on how to reach the next **maturity level**.
Maturity Level	Integral part of **Maturity Models** defining their current **optimization** and **state** regarding **business** and **organizational** processes. The **higher** the **level**, the **higher** the **chances** that that **incidents** or **errors** will lead to **improvements** in these **processes**.
Objectives	**Goals**, targets, purposes, intentions and **plans** that an **organization** sets out to do.
Organization	Social **unit** of **people** that is **structured** and **managed** to pursue **collective objectives**.
Process Assessment	**Analysis** of organizational **processes** against a set of **criteria** to determine the capability of those **processes** to **achieve** the **scheduled organizational objectives**.

2 – Description of the analysis

The idea behind this concept map is making explicit the following points:

- The importance of **maturity models** in **organizations** in the establishment of **methodologies** both focused on the **improvement** of the **maturity levels**, regarding both **information security policies** through the usage of proper **cybersecurity frameworks** and **maturity models**, and the **software development** practices being currently employed by the **organization** to meet its **business needs** and **goals**.
- Furthermore, we display how **assessment protocols** being employed by the **organization** contribute to the development of the **maturity model** regarding its current **maturity level**, and how the enterprise's **maturity level** contributes not only to how an enterprise might **improve** its **processes** and **practices** following incidents such as **errors** and **failed business outcomes** regarding the **quality** of its **products** and **outputs** or in the **discipline** regarding the usage of **organizational resources**, but also how this **improvement** contributes to the achievement of its **business objectives** and how this process of **self-recovery** might help to the **stability** of the **company** in the long road **thriving** against its **direct competitors**.
- How **successfully implementing** a **cybersecurity maturity model** aligns itself with the **implementation** of **maturity models** by the organization's since it allows for a **better execution** of **information security practices** and policies thus contributing to the **improvement** of **organizational** and **customer information confidentiality**, **integrity** and **availability** and the **increasement** of **maturity levels** regarding **cybersecurity processes**.
- The relation **between** both **process assessment** and **maturity assessment techniques** to evaluate the **processes** being **employed** by the **current maturity model** with **objective** of further **improving** both the **maturity** of **processes** and the **maturity model itself**.
- The urge by **companies** to possess **programs** such as **Capability Maturity Model Integration (CMMI)** since it might be a requirement by **governments** for **companies** to win **public projects** and **contracts** in the **software development** area. Nonetheless, we intend on showing how this **program** attains the **improvement** of **processes** across **organizations**.

Finally, one can observe that the point **interlinking** all **topics** is that of the **maturity model concept**. It is important on denoting that **maturity models** are fundamental for **organizations** to **improve** the **maturity levels** of their **processes** and **practices** thus aiding at the **achievement** of the **objectives** set by **governance personnel** and aiding at the **recovery** from **failed organizational outcomes**.

3 – Research

Regarding the Capability Maturity Model Integration (**CMMI**) maturity levels, most specifically, the ***Defined*** **maturity level (level 3)**, we can observe that it **identifies proactive organizations** whose processes are **characterized**, **defined**, **documented** and **organized**. These properly **documented** and **organized processes** aid its users at becoming **proficient regarding** their use with **process characteristics** allowing them to be validated by **proper assessment programs** and easily **help** with the **improvement** of the **organizational practices** being employed. Furthermore, **organizations** with this **level** of **maturity** have **defined goals** and **strategies**, and **suitable technology** to achieve their **scheduled objectives**.

Furthermore, the **third CMMI level**, although possessing issues such as the **standardization** and **implementation** of **processes**, at its core is still applied to **organizations** that are still in a **developmental stage** – a **good stage** for **growth**, but one where there is **still plenty** of **improvement** to be **had**. At this **maturity level**, **organizations** present **medium quality**, but also **medium risk levels** when compared to organizations at **other stages** of this **model**. One such **organization**, currently at the **third level** of the **CMMI-DEV**, is ***Babel*** as we can **observe** in the CMMI Institute directory and the Babel website itself. As referenced by **Babel** in their **webpage**, **their certification** regarding this model was created to **optimize efficiency**, by **reducing costs**, thus making **monitoring processes** and the **minimization of errors** more **effective** whilst **reducing excessive corporate costs**.

4 – Topic for discussion

In the current climate of **severe**—and potentially **long-lasting**—**societal disruption** caused by *COVID-19*, could an **organization's** ability to achieve a **high level** of maturity in **business continuity** quickly become a **crucial factor** of **differentiation** from the **competition**?