**Reflection**

The SCM Process is all about ensuring accurate and reliable information about service configuration and the Configuration Items that support them is available when and where it’s needed, while also including information on CIs’ configuration and their relationships between them within an organization.

Activities in SCM involve Planning, Identification of Configuration(s) and CI, Configuration Control, Status Accounting, Verification and Audit, and Reporting (PICSAR).

Planning: Consists of planning and managing CIs to be inside the CMS for monitoring and maintenance. This includes CIs from Secure Libraries, DMLs, and even Definitive Spares.

Configuration Identification: Defining and documenting selected CIs and their components. They’re then uniquely identified, and this is the step where attributes and relationships are identified to the CI.

Configuration Control: Ensuring adequate control over CIs while keeping record of changes to status, approvals, location, and owner. The step where License and Version Control is checked for software legality and being up to date with the latest patches.

Status Accounting: Involves recording and reporting a CI’s change in state. E.g., A registered PC.

Verification and Audit: Ensures conformity between documented baselines to actual business environment. This also verifies CIs are where they are to be.

Reporting: Reports on CIs and their configured baselines, change history, revision status, and status reports of changes to the CI (E.g. Delivered, Serviced). This also handles reporting of unauthorized use of hardware and software.

*Benefits:*

One of the benefits to an organization with this process is having a better understanding of the assets and CIs that they use to deliver value, and how they interact with other services. This allows for improved resource utilization on the relationships between CIs which can then be allocated optimally to improve efficiency and reduces the need to acquire new resources when existing ones can be used effectively.

Another benefit is improved Incident Management. As configuration information is accurate and up to date, faulty CIs are identified faster and these speeds up the restoration of services, which is also a KPI of the Practice.

The next is improved Change Management. With a better understanding of an organization’s CIs, especially from the Configuration Control step, failed changes can be reduced from poor impact assessment, incorrect data in the CMS or poor version control. It therefore minimizes service disruptions from either unauthorized or failed changes.

*Pitfalls:*

One of the pitfalls is the risk of data inaccuracies between the different parts involved in SCM. Should the CMDB and/or CMS contain inaccurate or out of date information, it can lead sub-optimal decision making, and inefficient resource allocation.

Another being the complexity of the practice which, due to a lack of understanding, could lead to problems like the Danish Clock. Knowing that multiple CMDBs are part of a single CMS, which is then part of a single SKMS, staff who are unfamiliar with the nature of the practice may break it down into two, or multiple CMS to keep things in smaller containers. However, with two repositories of truth, certainty and accuracy cannot be achieved.

The last pitfall is the need to continuously maintain the CMDBs and CMS to have the most up to date information. This can be a time-consuming process and be demanding on an organization, and if its not properly managed negatively impact it some more.