Asset & Configuration Management Process

Document name	Process_Design_Document_ACM_V0.1.docx
Version	0.1
Status	☒ In progress ☐ Approved ☐ Validated
Update date	2025/05/02
Owner	
Level of confidentiality	☐Public ☒Internal ☐Limited ☐Confidential

Document Control

CHANGE HISTORY:

AUTHOR(s)	VERSION	DATE	CHANGES
David El Nawar	V0.1	2025/05/02	Document creation

APPROVAL

ROLE	NAME	DATE
Team Lead	Nicolas FRANCOIS	

Table of Contents

1. Introduction

1.1. Main definition

Asset & Configuration Management (ACM) is the practice that ensures accurate and reliable information about **assets and configuration items**, and the relationships between them, is maintained and available when and where it is needed. ACM supports decision making, enables effective change, incident and problem resolution, and protects the organisation from legal, security, and financial exposure.

An **IT asset** is any financially valuable component (hardware, software, license, or contractual entitlement) required to deliver or support an IT service.

A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT service. Information about each CI is recorded in the **configuration management database (CMDB)** along with attributes and relationships:

- **Attributes** are the descriptive data points that uniquely identify a CI or asset and tell you everything you need to know about it at any point in its life-cycle
- **Relationships** express how one CI or asset is connected to another, forming the service topology that underpins impact, root-cause and dependency analysis

1.2. Objectives, challenges & benefits

As part of its **carve-out from Solvay**, Syensqo is building an **independent IT backbone** and must establish a **Configuration Management Database (CMDB) it can trust**. A reliable CMDB will sit at the heart of every ITIL practice, underpinning service health, compliance, security and cost control, getting it right from day one is a strategic imperative.

To reach this goal, **Asset & Configuration Management must**:

- Maintain a single, authoritative source of truth for all assets and configuration items. Only a rigorously governed CMDB lets operations teams pinpoint what is running where, restoring services faster whenever incidents strike.

- Support change planning and risk assessment through trusted CI relationships. Accurate dependency maps enable Change and Release Managers to understand blast-radius, schedule work intelligently and avoid unnecessary downtime—ultimately lowering audit and compliance exposure.

- Optimise asset life-cycle cost and licence compliance. By tracking ownership, contract terms and utilisation from procurement to retirement, ACM empowers Syensqo to negotiate better with vendors, eliminate shelfware and balance on-prem, cloud and SaaS spending.

- Provide actionable data for capacity, security and financial management. Financial controllers, security analysts and capacity planners all rely on timely, complete CMDB data to make informed decisions across ITSM and ITOM functions.

Syensqo must ensure **data accuracy and completeness** in a highly dynamic environment, **reconcile multiple discovery feeds and manual updates**, **keep pace with rapidly changing cloud and SaaS footprints**, and ali**gn a diverse set of stakeholders on clear ownership and stewardship rules**.

Overcoming these challenges is the price of admission for a CMDB that the organisation can depend on: **quicker root-cause analysis**, **fewer audit findings**, **tighter cost control** and **better-informed decisions across the entire IT landscape**.

1.3. Actors

The main actors involved in the ACM process include:

- **Delivery Lead**

Owns the ACM vision, funding and overall governance:

  - Endorse the CMDB strategy, target KPIs and budget.
  - Approve major policy changes and tool investments.
  - Chair executive reviews; remove organisational blockers and escalate systemic risks.

- **Service Owner**

Guarantees data quality for the CIs that underpin their service:

  - Accountable for data accuracy of every CI and asset underpinning their service.
  - Signs off mandatory attributes and relationships.
  - Approves lifecycle transitions to *End-of-Life* and *Retired* and ensures audit findings are remediated on time.

ITIL role: Service Owner

- **Delivery Manager** (assumed by each Delivery Manager over their scope)

Governs the CMDB day-to-day and enforces global standards:

  - Defines the CMDB data model, relationship catalogue, policies and KPIs.
  - Approves mass imports, validates "CI created/updated" release gates and accepts discovery feeds into production.
  - Governs reconciliation rules, signs off audit results and oversees relationship integrity for all production CIs.

ITIL role: Configuration Manager

- **ITSM Team Member**

Creates and maintains CI data on the ground:

  - Creates and enriches CI/asset records, maps relationships, resolves reconciliation exceptions and duplicates.
  - Fixes or flags orphan / duplicate links.
  - Runs quarterly sample audits and documents corrective actions.

ITIL role: Configuration Analyst

- **Helpdesk**

First-line touchpoint that captures CI references and flags issues:

  - Captures CI references when logging incidents, requests and changes.
  - Flags missing or obviously incorrect data to the Configuration Manager for correction.

ITIL role: Service Desk Agent

- **Tool Administrator**

Keeps discovery, reconciliation and security tooling running:

  - Configures, maintains and tunes discovery probes, SaaS connectors and ETL jobs.
  - Owns reconciliation and normalisation engines.
  - Supplies evidence logs for audits and supports root-cause analysis of data-quality issues.
  - Manages CMDB role-based permissions and audits who can create, edit or bulk-import CIs.
  - Schedules regular CMDB exports and documents backup / restore procedures, including RTO & RPO targets.

ITIL role: Tool Administrator

2. Process description

2.1. Process triggers, inputs, outputs

1. **Triggers -** *What initiates the process ?*

The trigger of the A&C process is a data event or business action that requires the CMDB to be created, updated, reconciled or audited.

Examples of triggers:

- Automated discovery detects a new, changed or removed component.
- Change implementation adds, modifies or retires infrastructure.
- Purchase order / goods receipt registers a new asset.
- Service request or incident exposes missing or inaccurate CI data.
- Scheduled or ad-hoc audit flags a discrepancy.

2. **Input -** *What formally enters the process ?*

A **CI event record** (from discovery, change, procurement, ticketing or audit) containing the information needed to create or correct CMDB data.

Typical input elements:

- Discovery payload with technical attributes and identifiers.
- Closed RFC with affected CI list and change details.
- Procurement record (PO, invoice, serial numbers).
- Ticket or audit finding describing the data issue.
- Supporting documents: contracts, spec sheets, architecture diagrams.

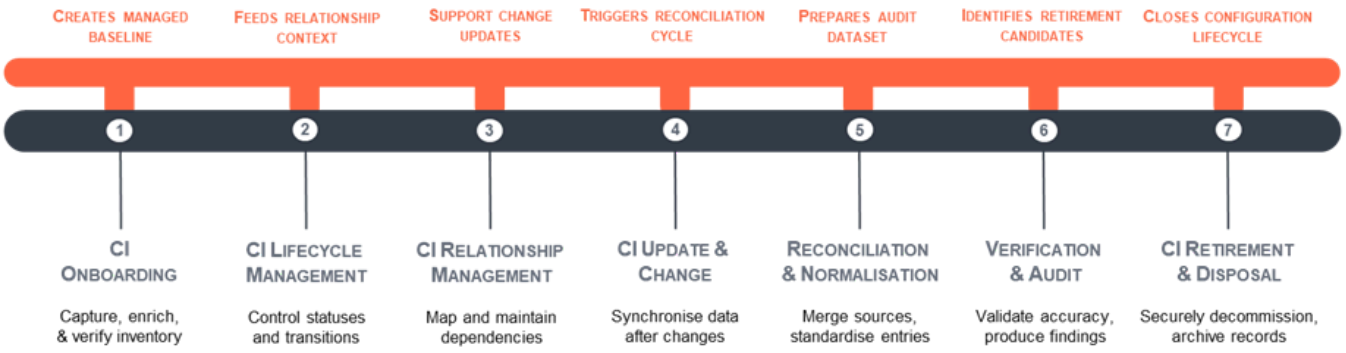
3. **Outputs -** *What does the process deliver ?*

Authoritative, traceable CMDB updates and evidence artefacts that enable downstream ITSM practices.

Examples of outputs:

- New or updated CI records promoted to **Active – Verified** status.
- Accurate relationships and lifecycle status changes logged.
- Reconciliation exceptions resolved or queued for action.
- Audit reports and KPI entries (accuracy, sync compliance).
- Notifications to stakeholders (Service Owner, Change Manager, Security).

2.2. Process activities



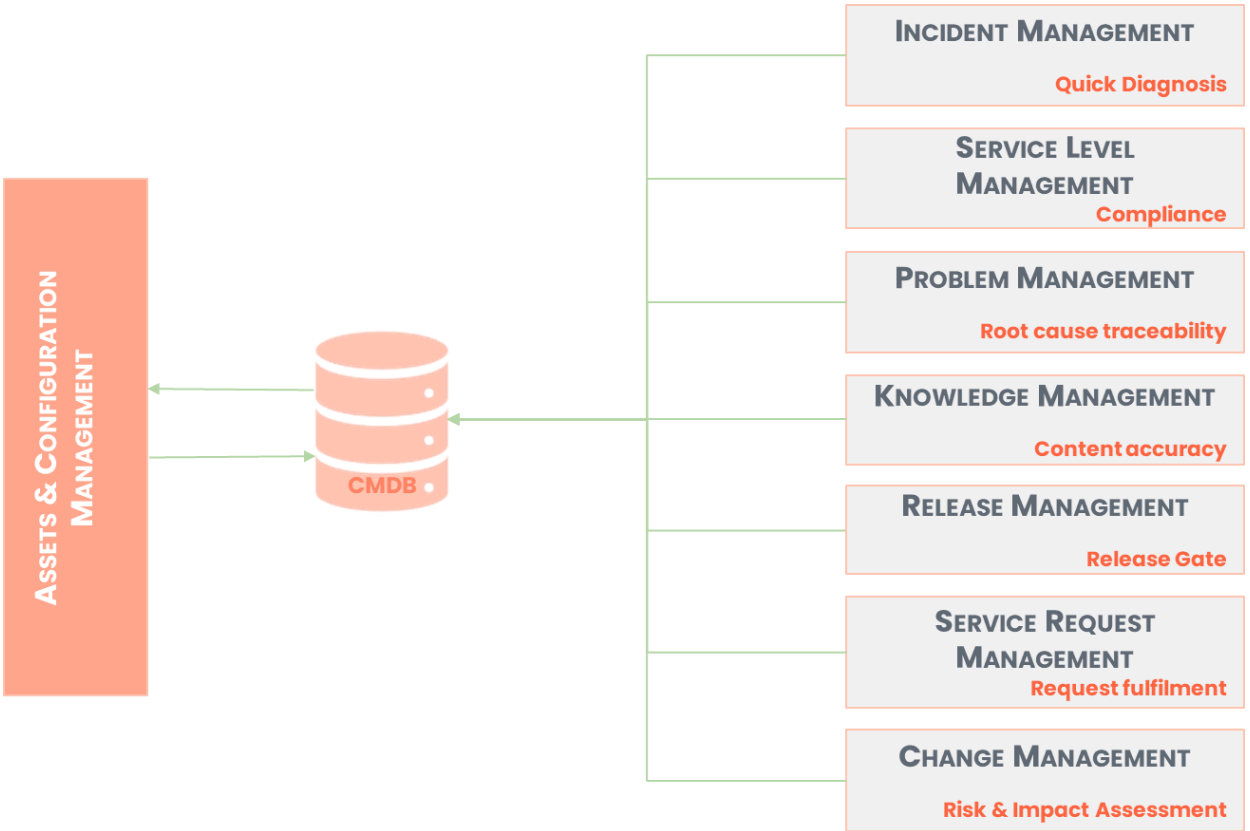
The ACM lifecycle is divided into seven stages:

- **CI Onboarding:** Identification & draft creation → Attribute enrichment → Relationship mapping → Validation & promotion
- **CI Lifecycle Management:** Status accounting across “In Stock, In Use, In Maintenance, Retired” plus entry/exit criteria per CI class

- **CI Relationship Management:** Catalogue definition→Creation & Validation→Continuous maintenance of dependencies
- **CI Update & Change:** 24-h post-RFC updates, nightly discovery deltas, manual corrections
- **Reconciliation & Normalisation:** Best-source merge, duplicate detection, vendor/product normalisation, exception handling.
- **Verification & Audit:** Monthly CMDB vs. discovery checks, quarterly hardware scans, semi-annual licence true-ups, annual independent audit.
- **CI Retirement & Disposal:** Service-owner authorisation, secure wipe, financial closure, record lock & retention

2.3. Link with other ITSM processes

The ACM relies on structured interactions with several other practices.



- **Change Management**

Every Request for Change (RFC) must reference at least one Configuration Item so the Change Manager can run a proper risk-and-impact assessment. Once the change is implemented and approved, an automated validation job checks that the CI's status and attributes have been updated to reflect the authorised state. The configuration manager co-owns this control with the Change Manager, ensuring the CMDB and the change record never drift apart.

- **Knowledge Management**

"How-to" articles and troubleshooting guides are only useful if they describe the environment as it really is. Service owners therefore monitor CI attribute updates, particularly version upgrades or platform moves, and trigger reviews of any linked knowledge-base articles. The Knowledge Manager works closely with the service owners to keep this feedback loop tight.

- **Service Level Management (SLM)**

Service Level targets are meaningful only when the underlying service map is trustworthy. The CMDB supplies that map by linking each CI to its parent business service and by storing ownership and criticality flags. SLM dashboards draw directly on these links, and a dedicated KPI tracks the "percentage of CIs correctly tied to a service." The Service Level Manager and Configuration Manager jointly police data quality to guarantee credible SLA reporting.

- **Incident Management**

When an incident hits, speed matters. The incident form therefore auto-populates with CI details and shows the date of the last approved change, guiding the analyst toward likely causes and the right resolver group. Incidents raised without a CI are quarantined for correction. The Incident Manager drives this workflow, partnering with the Service Desk and the Configuration Manager to eliminate "orphan" incidents.

- **Release Management**

A release is not allowed into production unless every new or changed component is already present in the CMDB. The release checklist includes a gate called "CI created/updated" and the release automation pipeline pushes the final build attributes to the CMDB API. The Release Manager owns this gate, while the Configuration Manager validates that records are complete before the go-live milestone.

- **Service Request Management (SRM)**

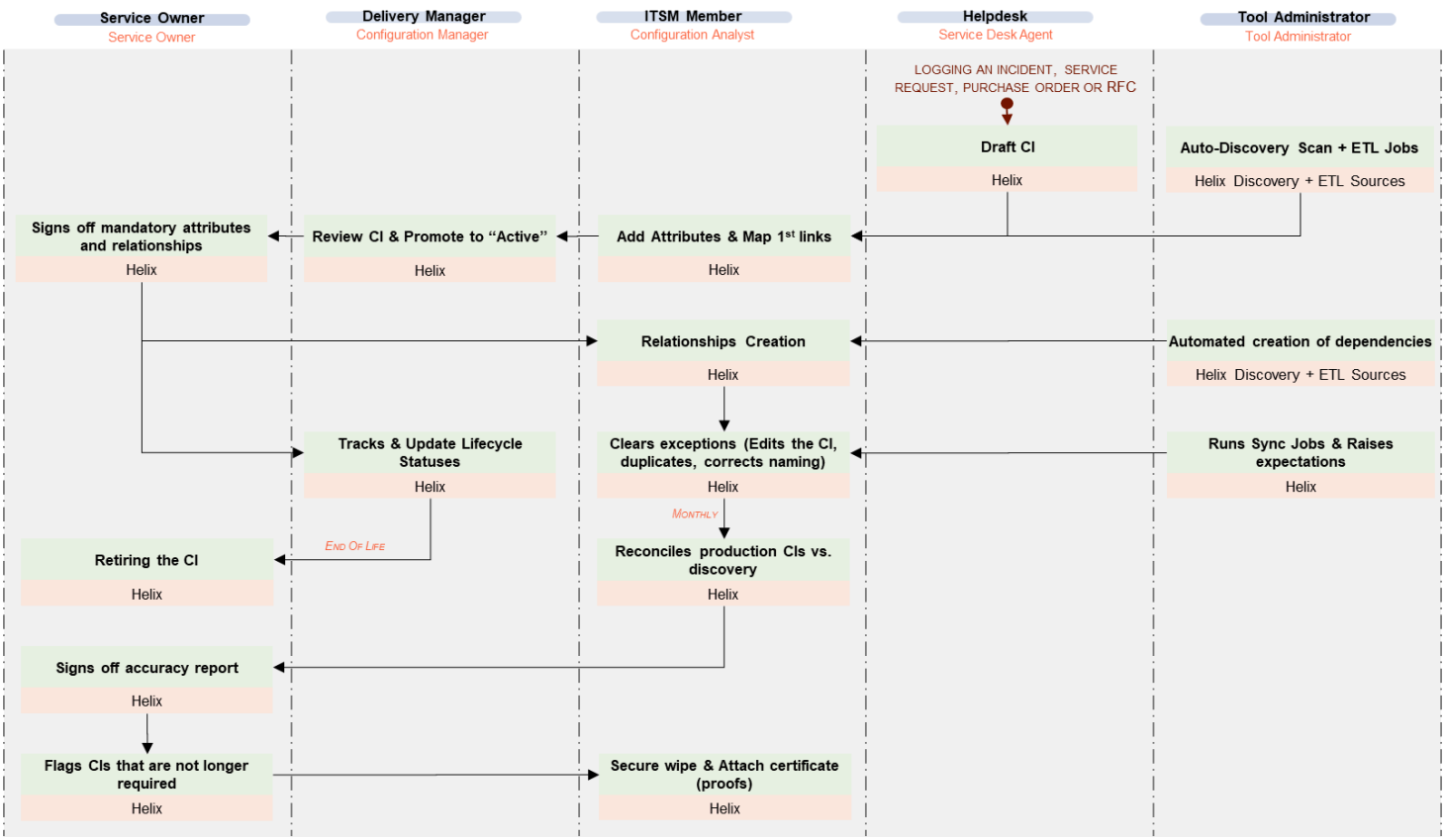
Many standard requests—new laptop, extra CPU, database clone—result in the creation or modification of assets and CIs. Request models therefore spawn work orders that update the CMDB, and a performance metric measures the "percentage of service requests with a timely CI update." The Service Request Manager governs the models, while service owners verify that the resulting CMDB entries meet quality standards.

- **Problem Management**

Root-cause analysis relies on accurate historical data: what changed, when, and on which CI. Known-error records therefore link back to the affected CIs, and the CMDB in turn keeps a pointer to the associated problem ticket for audit traceability. The Problem Manager and the Configuration Manager share responsibility for maintaining these bidirectional links so that future incidents can be resolved (or prevented) more quickly.

3. Process Workflow

Detailed subactivities to be completed after workshops : Target mid june



3.1. CI Onboarding:

1. **Identification & draft creation:** As soon as the Service Desk logs a purchase order, RFC or incident—or the Tool Administrator's discovery probes detect an untracked component—a CI record is opened in Draft status.
2. **Attribute enrichment:** A Configuration Analyst (working in the Delivery Manager's team) populates mandatory fields from spec sheets, contracts and vendor portals.
3. **Relationship mapping:** The same Configuration Analyst links the CI to the applications, services or physical hosts it depends on, using architecture diagrams and discovery data maintained by the Tool Administrator.
4. **Validation & promotion**: The Configuration Manager reviews completeness and accuracy; once approved, the CI moves to Active – Verified and becomes authoritative for all ITSM processes.

3.2. CI Lifecycle Management

Lifecycle Management is the process of overseeing a Configuration Item (CI) throughout all stages of its existence — from initial planning and deployment, through operation and maintenance, to eventual retirement — ensuring accuracy, control, and alignment with IT and business objectives.

For each CI type, a list of statuses is defined as well as the entry and exit criteria for each status:

- Hardware & Computer System
- Software & Software Server
- Business Service
- Network Devices
- People & Organisation
- Documents & Contracts

The statuses are grouped into 4 lifecycle stages:

1. In Stock
2. In use
3. In Maintenance
4. Retired

Lifecycle stage	Who drives it	Key checkpoints
In Stock	Configuration Manager	PO matched, asset tag applied.
In Use	Configuration Manager	CI verified; relationships mapped; owner signed off.
In Maintenance	Configuration Manager + Service Owner	RFC approved; post-maintenance re-verification complete.
Retired	Service Owner (approval) + Configuration Manager (financial)	Data wipe certified; financial write-off booked; record frozen for audit.

3.3. CI Relationship Management

Effective CI relationships configuration ensures that every dependency between configuration items is captured, validated, maintained and retired in a way that supports impact analysis, risk assessment and cost allocation. This process includes:

1. **Catalogue definition:** The Configuration Manager publishes the authorised list of relationship types, mandatory link attributes and validation rules; the Tool Administrator embeds these rules in the CMDB.
2. **Creation & validation:** Auto-discovered links flow in via the integration hub managed by the Tool Administrator; human-verified links are bulk-loaded by the Configuration Analyst. Duplicates or illegal combos are resolved before the CI reaches Active status.
3. **Continuous maintenance:** Post-change scripts and nightly reconciliation keep dependencies accurate; any mismatch lands in the exception queue for the Configuration Analyst to fix, with escalation to the Configuration Manager if the backlog exceeds 5%.

3.4. CI update & change

Keeping the CMDB in sync with reality relies on three complementary triggers:

1. **Post-change window:** When an RFC closes, the Configuration Analyst has a strict (e.g., 24-hour) window to update affected CIs; the Configuration Manager monitors compliance.
2. **Discovery deltas:** Nightly reconciliation jobs (owned by the Tool Administrator) push mismatches into an exception queue; the Configuration Analyst must keep the queue below 5 % of daily deltas.
3. **Manual corrections:** Support teams raise ad-hoc anomalies to the Service Desk, which routes them to the Configuration Analyst for resolution within the agreed SLA.

3.5. Reconciliation & Normalisation

A four-step pipeline guarantees clean, standardised data:

1. **Best-source merge:** Information from procurement, change records, cloud APIs and discovery tools is merged, attribute by attribute, selecting the most authoritative value.
2. **Duplicate detection:** Matching rules collapse records that refer to the same physical or logical item.
3. **Vendor/product normalisation:** Names are aligned to the approved catalogue, ensuring consistent reporting.
4. **Exception management:** Any record still failing a validation rule is routed to the exception queue for Configuration Manager review.

3.6. Verification & Audit

CMDB accuracy is monitored on a rolling calendar:

Frequency	Activity	Primary actor	Supporting roles
Monthly	Reconcile Prod CIs vs. discovery	Service Configuration Manager	Tool Administrator, Configuration Analyst
Quarterly	Physical QR-code scan of hardware	Configuration Manager	Service Desk
Semi-annual	Licence true-up	Configuration Manager	Configuration Analyst, Finance
Annual	Independent audit (10 % sample)	CISO Office	Service Configuration Manager, BRM

3.7. CI Retirement & Disposal

When a component reaches end-of-life:

1. **Authorisation:** The Service Owner approves retirement; CI moves to Pending Disposal.
2. **Data sanitisation:** Secure wipe is executed; certificate uploaded by the

Configuration Analyst.

3. **Financial closure:** The Configuration Manager records depreciation or resale and updates cost records.
4. **Status change:** The Configuration Manager marks the CI Retired; the record is locked for the mandated retention period (e.g., seven years) to satisfy audit and legal requirements.

4. Roles & responsibilities to be validated during workshops :

Target end of june

ACM Activity	Service Owner	Configuration Manager	Configuration Analyst	Service Desk	Tool Administrator
CI On-boarding	***C***	***A***	***R***	***R***	***R***
CI Lifecycle Management	***A*** (for retire approval)	***A/R*** (for "In Use" & "In Maintenance")	***R***	***C***	***C***
CI Relationship Management	***C***	***A***	***R***	***C***	***R***
CI Update & Change	***R***	***A***	***R***	***C***	***R***
Reconciliation & Normalisation	***I***	***A***	***R***	***I***	***R***
Verification & Audit	***C***	***A***	***R***	***C***	***C***
CI Retirement & Disposal	***A***	***A***	***R***	***C***	***C***

*Responsible (**R**), Accountable (**A**), Consulted (**C**), Informed (**I**)*

- **CI On-boarding** – The **Configuration Manager** owns the policy and approves each new record; the **Configuration Analyst** performs the hands-on data entry. A draft CI is created either by the **Service Desk Agent** (via ticket) or automatically by the **Tool**

Administrator through discovery feeds.

- **Lifecycle control** – The **Configuration Manager** maintains lifecycle accuracy and cost data from *In Stock* to *Retired*. The **Service Owner** approves the final retirement of any CI and confirms that audit actions are closed.

- **Relationship upkeep** – Relationship catalogue rules are defined by the **Configuration Manager**; day-to-day creation, correction and duplicate cleanup are handled by the **Configuration Analyst**, with technical discovery support from the **Tool Administrator**.

- **Change synchronisation & reconciliation** – Automated change-sync and nightly reconciliation jobs are run by the **Tool Administrator**. Any resulting exceptions are resolved by the **Configuration Analyst** under the supervision of the **Configuration Manager**.

- **Verification & audits** – The **Configuration Manager** is accountable for overall data-accuracy metrics. The **Configuration Analyst** executes physical inventory scans, licence true-ups and evidence collection, while the **Service Desk Agent** assists with tag verification on site. The **Delivery Lead** reviews the KPI scorecard at executive level.

- **Retirement & disposal** – Business approval is given by the **Service Owner**; the **Configuration Analyst** performs secure-wipe steps and attaches evidence. The **Configuration Manager** locks the CI record, records the financial write-off and ensures retention requirements are met, with logistic support from the **Service Desk Agent**.

5. Metrics & KPIs

5.1. Practice Success Factors and their KPIs

The following critical success factors define the core objectives of the Asset & Configuration Management process and are each supported by dedicated KPIs to measure performance, ensure operational control, and drive continuous improvement:

- **CMDB Accuracy –** Reflect real-time, verified infrastructure state.
- **Change Synchronisation** – Update CIs within 24 hours post-change..
- **Asset Visibility** – Ensure owner and location are always recorded.
- **Duplicate Management** – Eliminate redundant or conflicting CI records.
- **Relationship Completeness** – Link all CIs to service dependencies.
- **Exception Resolution** – Clear reconciliation issues within SLA.
- **Timely CI Retirement** – Retire obsolete CIs with full traceability.

Targets and thresholds will be fixed after KPI-design workshops (target date : end-June).

#	KPI	Description	Calculation mode	Owner
DQ-1	CMDB accuracy	% of CIs that pass nightly reconciliation against discovery and authoritative feeds.	(CIs passing reconciliation ÷ Total CIs) × 100	Configuration Manager
PI-1	Change synchronisation compliance	% of closed RFCs for which affected CIs were updated within 24 h.	(RFCs with CI updated ≤ 24 h ÷ Closed RFCs) × 100	Configuration Manager
VIS-1	Asset visibility	% of assets with both an owner and location recorded.	(Assets with owner & location ÷ Total assets) × 100	Configuration Analyst
DQ-2	Duplicate CI rate	% of CIs flagged as potential duplicates after normalisation.	(Duplicate-candidate CIs ÷ Total CIs) × 100	Configuration Analyst

DQ-3	**Relationship completeness**	% of production CIs that have at least one valid dependency link.	(Prod CIs with ≥ 1 relationship ÷ Prod CIs) × 100	Configuration Analyst
PF-1	**Exception backlog ageing**	Average number of days reconciliation exceptions remain open.	Σ age of open exceptions ÷ # open exceptions	Configuration Manager
LC-1	**Timely CI retirement**	% of CIs moved to Retired within 10 days of Service-Owner approval.	(CIs retired ≤ 10 days ÷ CIs approved for retirement) × 100	Service Owner

Categories *– DQ = Data Quality, PI = Process Integrity, CF = Compliance & Financial, VIS = Visibility, PF = Process Flow, LC = Lifecycle Control*

5.2. Risks indicators

Alongside these KPIs, the team monitors four risk indicators that act as early-warning beacons:

Indicator code	Metric	Threshold (alert)	Primary response
RI-1	Unauthorised discovered CIs	> 50 per month	Joint Security + Configuration Mgr review; clean-up plan
RI-2	Duplicate CI rate	> 2 %	Root-cause analysis of discovery patterns & reconciliation rules
RI-3	Orphaned hardware	Any occurrence	Immediate escalation to Service Owner
RI-4	Exception backlog ageing	> 5 days average	Extra steward capacity allocated; raise to CMDB Operational Board

6. Governance responsibilities participants & frequencies to be validated during workshops : Target mid july

6.1. Governance objectives

Syensqo operates a dedicated governance framework to ensure that **Asset & Configuration Management** is introduced, maintained and continually improved in a consistent, business-relevant way. Its objectives are to :

- Provide a clear, collaborative framework for managing the CMDB across IT, Finance, Security and external suppliers.
- Guarantee end-to-end traceability for the creation, enrichment, verification and retirement of every asset and configuration item.
- Support both the initial "green-field" build-out of the CMDB and the recurring verification and audit cycles that follow.
- Align CMDB data quality with operational reality and the organisation's risk appetite, enabling fact-based decisions.
- Drive data-driven decision-making through regular KPI dashboards, reconciliation results and audit findings.
- Identify and track corrective and preventive actions whenever accuracy, completeness or compliance falls below thresholds.
- Promote transparent communication between all stakeholders that provide or consume CMDB data.
- Manage the structured onboarding of new services, cloud platforms and discovery sources as Syensqo's IT landscape expands.
- Foster a culture of continuous improvement in Configuration Analystship, automation and process integration

6.2. Practice Comitology

Asset & Configuration governance relies on two committee types: operational and continuous improvement. Each has a specific scope, rhythm, and ownership. The following tables outline their purpose, cadence, key participants, and designated animators to ensure clear

accountability and structured decision-making.

1. Operational Committee

Committee	Objective	Frequency	Animator	Participants	Input (←) / Output (→)
CMDB Operational Board	-Monitor data-quality KPIs, change-sync breaches, exception backlog. -Approve onboarding of new services and discovery feeds.	Every 2 weeks	Configuration Manager	- Delivery Lead -Configuration Analysts, -Tool Administrator, -Service Owners	← KPI dashboard, exception list → Action log, onboarding approvals

2. Steering Committee

Committee	Objective	Frequency	Animator	Participants	Input (←) / Output (→)
CMDB Steering Committee	-Endorse policy changes and automation roadmap. -Accept or remediate residual data-quality risks. - Approve funding for improvements.	Quarterly	CIO & CISO	- Delivery Lead - Configuration Manager, - Service Owner, - Security, - Finance	← Quarterly scorecard, risk register → Policy updates, funded initiatives

7. Tooling & Deliverables

7.1. Tools

Typology	Tool / Module	Description of use in the process
CMDB Core	**BMC Helix CMDB**	Master repository for all assets / CIs, lifecycle states, attributes, relationships and audit history.
Discovery & Integration	**BMC Helix Discovery**	Auto-discovers on-prem servers, network devices and cloud resources; feeds raw data to CMDB.
Normalisation & Reconciliation	**Helix Reconciliation / Normalisation Engines**	Merge best-source data, detect duplicates, align vendor / product names, queue exceptions.
Collaboration & Governance	**Google Calendar**	Scheduling CMDB Operational Board, Steering Committee.
	Gmail	Distribution of meeting minutes, audit findings and exception-backlog alerts.
	Google Space "CMDB Community"	Central hub for publishing onboarding playbooks, service-owner notifications, data-quality bulletins.
	Google Sheets / Slides	KPI decks, migration trackers, action-item logs for board reviews.

7.2. Deliverables

Process step	Delivrable	Description
CI On-boarding	**Draft CI Record**	Initial entry in Helix CMDB capturing unique ID, type, discovery source.
	Enriched CI Record	Mandatory attributes completed; classification and ownership validated by Service Owner.

	Relationship Map	Dependency links established; visual topology available in CMDB UI.
CI Lifecycle Management	**Status Change Log**	Automated log of each transition with timestamp and approver.
CI Update & Change	**Change-Sync Compliance Report**	Automated report listing RFCs and corresponding CI updates, used in Operational Board.
Reconciliation & Normalisation	**Exception Queue**	List of records failing reconciliation or validation rules, prioritised by criticality.
	Reconciliation Summary	Nightly digest of totals, duplicates collapsed, conflicts resolved.
Verification & Audit	**Monthly Accuracy Dashboard**	KPI view of CMDB vs. discovery match rate, duplicate %, orphan count.
	Annual Audit Findings	Independent audit checklist, deviations and agreed remediation actions.
CI Retirement & Disposal	**Data-Wipe Certificate**	Proof of sanitisation attached to CI before status change.
Reporting & Improvement	**CMDB Health Dashboard**	Consolidated KPI set (accuracy, change integrity, licence compliance, visibility, duplicates, backlog age).

8. Glossary

Term	Definition
SYRA	ITSM platform. Central system of record for the change process
Asset	Any hardware, software, licence or contractual entitlement that has financial value for Syensqo and must be managed through its life-cycle.
Configuration Item (CI)	A component that needs to be controlled to deliver an IT service; each CI record resides in the CMDB with attributes and relationships.
Configuration Management Database (CMDB)	The authoritative repository that stores CI and asset records, their attributes, relationships, status history and audit trail.
Attribute	A descriptive data field that uniquely identifies a CI or asset (e.g. serial number, owner, environment, warranty end-date).
Relationship	A recorded dependency between two CIs or assets (e.g. *runs on, depends on, contains*), used for impact and risk analysis.
Service Map	The graph of CIs and relationships that underpin a business service, enabling SLA calculation and incident routing.
Discovery	Automated scan or API feed that detects infrastructure or SaaS resources and feeds raw data to the CMDB.
Reconciliation	The nightly process that merges data from multiple sources, selects the best value per attribute and flags conflicts.
Normalisation	Standardising vendor and product names to the approved catalogue to prevent reporting discrepancies.
Exception Queue	List of CI records that fail reconciliation or validation rules and require Configuration Analyst action.
Duplicate CI	Two or more CI records that refer to the same physical or logical component and must be merged.
Unauthorised CI	A discovered component with no corresponding authorised record in the CMDB.
RFC (CRQ)	Formal request to perform a change, submitted via the ITSM tool (SYRA).

Class-A Asset / CI	High-criticality item whose failure would significantly impact business operations; subject to stricter audit controls.
Orphaned Hardware	Physical equipment recorded in the CMDB with no service owner or business application linkage.