HALO

JANUARY 2024

Service Automation Framework

How to achieve efficient Service Delivery through enterprise CMDB architecture and a comprehensive Service Design process

usehalo.com

INTRODUCTION

Service Automation Framework

The Halo Service Automation Framework (SAF) establishes a standardised and shared collection of service-related definitions throughout the Halo platform, facilitating genuine automation of service levels across IT service management processes. SAF is an integral component of Halo, particularly for clients seeking an enterprise-class Configuration Management Database (CMDB) to provide the foundation that will deliver automation and efficiencies within ITSM.

SAF is a dynamic compilation of best practices that will continuously evolve. Importantly, where, and how to adopt SAF is contingent upon the customer's maturity level, as detailed later in this document.

The Importance of SAF

How frequently do ITSM products get deployed, only to later question the minimal value gained from the platform in terms of genuine process automation and a clear understanding of ownership and accountability during unforeseen issues?

Boasting an expensive ticketing system is not a source of pride, yet it's estimated that around 70% of organisations find themselves in this exact situation. The solution is surprisingly straightforward. Prioritise upfront efforts, coupled with sustained investment in defining and maintaining IT and business services, alongside their broader ecosystems in the CMDB. This includes establishing ownership and accountability for supporting and delivering these services, which is crucial.

At Halo, we comprehend the significance of such an investment. We've streamlined the process to make it as effortless as possible, facilitating this crucial step and thereby optimising opportunities and investments in the Halo platform.

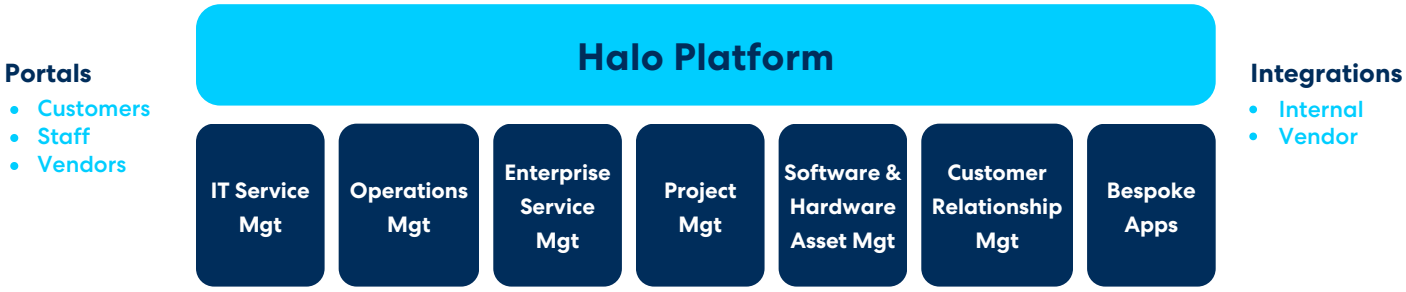
THE STRUCTURE OF SAF

Strong, scalable, flexible foundations

SAF forms the foundations of the Halo platform driving automation across all our product offerings. Like all foundations, they need to be strong, scalable and flexible providing real and sustained value.

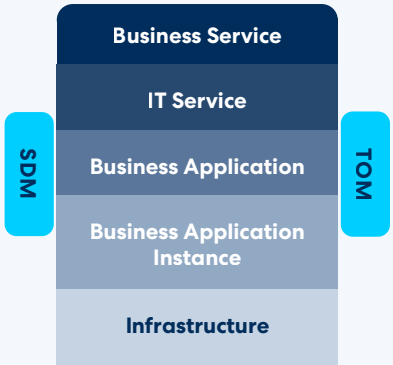
Key components of SAF include:

- A predefined, top-tier CMDB Service Data Model (SDM) centred around the definition of services.
- A Target Operating Model (TOM) outlining ownership and accountability for the support and delivery of each service.
- A series of procedures leveraging SDM and TOM to automate ITSM processes such as assignment, escalation, notification, communication, approval, and review.
- A data certification process allowing service owners to validate the coverage and quality of their data ecosystem.



Service Data Model (SDM)

- Best practice CMDB class model based on real-world practical usage.
- Focuses on services that own and consume business applications which in turn are deployed and connected to infrastructure.
- Interconnected foundation data in CMDB is intrinsic to all ITSM processes.



Target Operating Model (TOM)

- RACI model for ownership, support and delivery of services from an individual and team perspective.
- Facilitates improved quality and coverage of CMDB data through federated governance.
- Drives automation in all ITSM processes such as assignment, escalation, approval/review and notifications.

RACI (responsible, accountable, consulted and informed)

ADOPTING SAF

Principles built to evolve

Halo products are unifying their utilisation of data sourced from the Configuration Management Database (CMDB). The standardisation is embodied in the Service Automation Framework (SAF), which delineates the placement of service and application-related data within the CMDB. It also specifies the responsible entity from a configuration management standpoint and outlines the automation facilitated by this standard.

SAF has been developed on foundational principles that have and will continue to evolve over time. These principles serve to meet the following key objectives:

- Automate all key processes. Examples include:
  - Automated assignment of Incidents to Level 1 teams with one-click escalation to Level 2 or Level 3 teams.
  - Automated ownership, management, approval and review for Change Control.

- Facilitate federated ownership and management of CMDB data by establishing clear ownership and accountability for configuration managers, who possessing knowledge and comprehension of a specific service, are tasked with the responsibility and accountability for its data representation within the CMDB.

- A certified governance framework ensures the optimal quality and coverage of CMDB and Target Operating Model (TOM), promoting transparency.

- Empower consistent reporting and analytics throughout the IT estate by implementing a unified operating model.

The service at the centre of IT

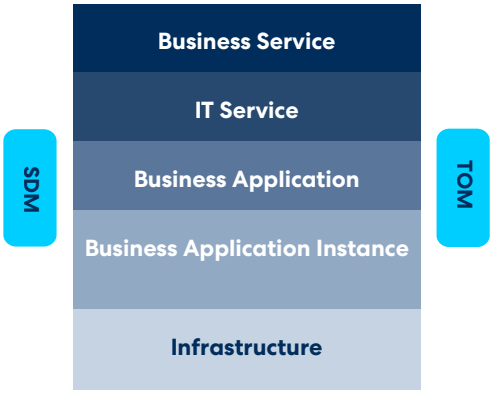
As depicted in the image below, services occupy a central position in IT. By delineating services within this STM and enhancing them with essential data, a unified and normalised perspective of the IT environment can be attained.

Specifically, the effectiveness of ITSM processes is greatly enhanced by ensuring that all fundamental data, from the CMDB to process reference data, is harmonised with services.

Process Automation from SDM and TOM	
TOM	Clear understanding of roles across support and delivery
Configuration	Federated maintenance by people that understand the construct of the service
Incident	Drives categorisation, assignment, escalation, notification, resolution codes, cause codes, impact and SLM.
Major Incident	Drives categorisation, subscription, communication, mobilisation, resolution codes, cause codes, impact analysis, health and SLM.
Problem	Drives categorisation, ownership, escalation, notification, resolution codes, cause codes, impact and SLM.
Change	Categorisation, risk analysis, ownership, impact, approval/review, closure codes, break glass, conflict & collision, freezes and blackouts.
Request	Entitlement, catalogue, assignment, approval.
Knowledge	Federated maintenance by people that understand the construct of the service
Reporting	Key operating metric aligned to services such as performance, availability, capacity data.

SDM taxonomy

Below is a summarised view of the SDM components. All the components (classes) within the SDM are related together with the appropriate verbiage to describe the relationship.



Benefits

- Establishes a standardised and consistent set of terms and definitions across all Halo products.
- Enables service reporting, cost transparency, and offers prescriptive guidelines for service modelling within the CMDB.
- Provides a blueprint to map various types of IT services to the business applications and infrastructure they are connected to and running on.
- Adopting the SDM framework ensures the full benefits of the platform while future-proofing it.
- Focuses on elements that bring immediate business value while also outlining a roadmap for future maturity.

Definitions

Business Service: Tailored for business clientele, this service supports customer interactions or internal business processes. It aligns with recognised business capabilities comprehended by both business and IT departments, and users can conveniently request it through the catalogue. Business services consume IT services.

IT Service: A technological facility or process supporting one or more business services, playing a vital role in service-oriented processes. It comprises multiple technology layers, such as networks, operating systems, hardware, databases, applications, and products. Examples include application-aligned, infrastructure, cloud, end-user, facilities, HR, and management services.

Business Application: Comprising one or more components, business applications form end-user software designed to facilitate specific business capabilities. A collection of these often form an application-aligned IT service.

Business Application Instance: Physical deployments of business applications, encompassing their environment (e.g., DEV, UAT, PROD, DR), their geography and/or business line.

Infrastructure: Physical and logical assets serving as the foundation for business application instances. These assets include data centre-based servers, clusters, databases, network devices, firewalls and storage as well as end-user devices such as desktops, laptops, mobiles, tablets and printers. A collection of these are managed by an infrastructure, cloud or end-user IT service.

All above can be owned by internal or external parties but importantly are stored, managed and governed within the Halo CMDB.

SDM CLASSES

The building blocks

• Business Application

This is the best starting point, as all organisations understand these. A business application encompasses all configured software to deliver specific business capabilities. These business applications serve as the logical representation of instances to execute business functions accurately and are typically software employed by business users and may include products.

• Business Application Instance

These are physical deployments of logical business applications, and can extend across multiple environments (e.g. production, disaster recovery, testing and development), be deployed based on geographical considerations (e.g. NAM, LATAM, EMEA, APAC) or be deployed based on business line.

IT Service

Expanding beyond business applications and their instances, the utilisation of IT services allows for the monitoring and management of the technology delivered to the business. An IT service is typically falls into one of the following types:

- An application aligned IT service consumes (and may own) one or more business applications and their respective instances. Typically a group of business applications that deliver a common business outcome, and are owned and delivered by a common set of teams and individuals, can be grouped together into an IT service.
- An infrastructure aligned IT service manages (and may own) infrastructure CIs of a common type. An example is a Linux hosting IT service which manages all Linux Servers (cloud or on premise). An infrastructure IT service may also have applications that it owns and consumes.
- A management or facilities aligned IT service such as the change management process or security operations respectively.

• Business Service

Tailored for business clientele, a business service supports customer interactions or internal business processes. It aligns with recognised business capabilities comprehended by both business and IT departments, and users can conveniently request it through the catalogue. Business services consume IT services.

• Infrastructure CIs

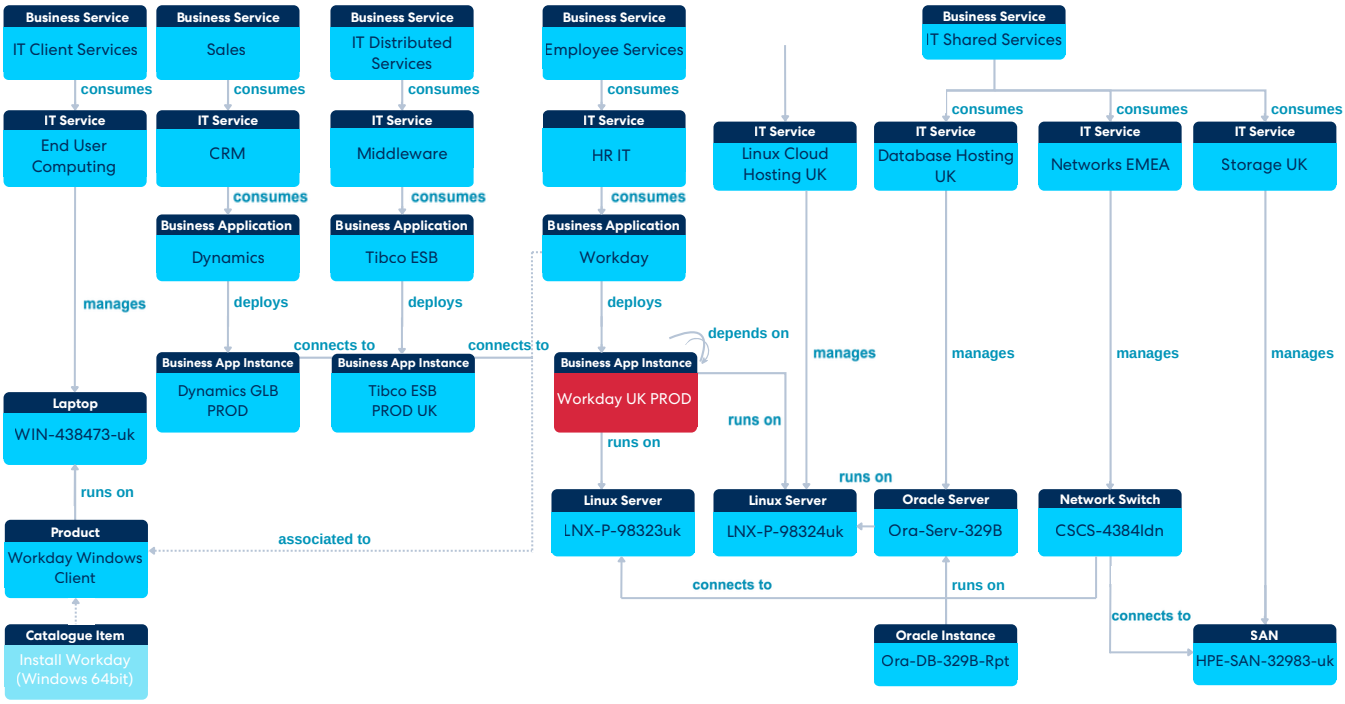
These include both tangible and abstract components within the IT estate, subject to configuration and change management. This spectrum spans conventional elements like servers, databases, storage, and switches to more complex entities such as appliances, web servers, clusters, firewalls, routers, circuits, and more.

A prudent approach must be taken to avoid overloading the CMDB with excessive asset classes, either through manual input or discovery methods. Instead, the focus should be on selectively incorporating those elements that directly contribute to tangible business outcomes.

WORKING EXAMPLE

An SDM blueprint for Workday

The following provides an example of a SDM blueprint for Workday[1], where Workday is hosted on cloud infrastructure, with an Oracle database and provides a data feed to Microsoft Dynamics[2] via the enterprise service bus.



Crucially, the Workday business application comprises various instances, with one notable example being Workday UK PROD, representing a specific regional deployment of the software. The "HR IT" application-aligned IT service oversees ownership and utilisation of several business applications, including Workday.

Workday is deployed on cloud-based Linux servers hosted by AWS, managed by the "Linux Cloud Hosting UK" infrastructure-aligned IT service. Different infrastructure configuration Items (CIs) are managed by their respective infrastructure IT services.

Employee data from Workday UK PROD is transmitted through the Tibco ESB to Microsoft Dynamics. Finally, the comprehensive overview includes the end user device, where a Workday client package is installed via the catalogue item which requests and deploys it.

[1]Workday, Inc., is a cloud-based financial management, human capital management, and student information system software vendor.
[2]Microsoft Dynamics is CRM software-as-a-service product.

SDM Evolution

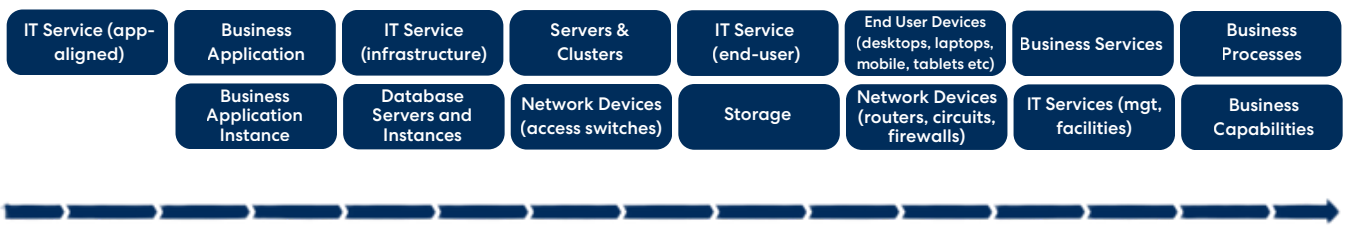
The extent of CMDB scope coverage based on the SDM is determined by the customer's maturity level. For those in the early stages of their journey, the emphasis should be on simplicity and value.

During the enable phase, the focus shifts towards onboarding, based on business criticality, the business applications and grouping them and their respective instances into IT services that own and consume them.

As the CMDB matures, there is a need to incorporate more business applications and infrastructure CIs along with the IT services that manage them. Simultaneously, attention should be maintained on enhancing data quality and coverage.

Enable	Enrich *	Enhance *	Mature *
Since all organisations understand their **business applications**, model these and their related **business application instances** by business criticality in the CMDB. Create (application-aligned) **IT Services** by grouping together business applications that are owned by the same teams and define a common function to the organisation. Relate them together in the CMDB to define the owning and consuming IT Services of a business application. Introduce Halo **TOM** for these IT Services (see later).	Import from your discovery sources, key infrastructure CIs. These include **servers, clusters, database servers, database instances** and (access layer) **network switches** . Create the relationships between them and relate business application instances to the clusters, servers and database instances that they depend on. For each infrastructure CI in the CMDB relate a (infrastructure or cloud) **IT Service** that represents and manages the infrastructure type (e.g. Linux Hosting, Windows Hosting, MySQL Hosting, Networks etc). Continue to onboard more business applications, and their associated IT services and business application instances. Connect the latter to the infrastructure CIs.	Import end user devices and assign to their users. Create and relate these to an (end-user) IT Service that manages these. Introduce additional infrastructure CI classes and relate to an associated (infrastructure) IT Service that owns and manages them (e.g. storage, web, and other network devices). Relate to associated (infrastructure) IT services.	Prioritise the introduction of business services that own and consume the IT services. Introduce or join business processes and business capabilities; to model the business architecture of the organisation and how it connects with IT. Introduce additional IT Service types such as management (for process ownership) and facilities. Examples include “Change Mg”, “Major Incident Mgt”, “Security” and “Building Mgt”.

* Continue to improve data quality and coverage in SDM and TOM activity from previous stage.



Cumulative on-boarding of CI class types and relationships between them.

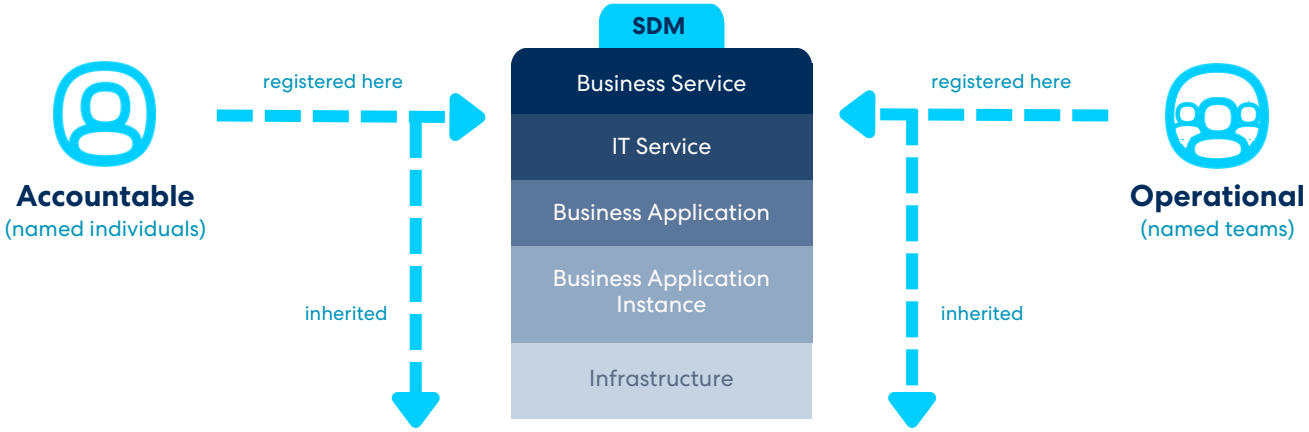
Ownership, federated

Recognising the critical role of configuration management, it is essential to federate the management and governance of this process. The key contributors to understanding service domains are the individuals responsible for the day-to-day support and delivery of services. Empowering and holding these individuals accountable for their data becomes crucial in this evolving process.

Taxonomy

Below is a summarised view of the TOM and the benefits it provides, that work hand in glove with the SDM to define all the key teams and individuals that play a role in the ownership, support and delivery of a given IT service.

The construct and benefits of this is described in the picture below.



Construct

RACI (responsible, accountable, consulted and informed) model for ownership, support, and delivery of IT services

Designed to be scalable and flexible, works in conjunction with Halo SDM and serves as a comprehensive repository for critical support and delivery information.

Repository is continuously updated through strong federated and dedicated configuration management roles, ensuring alignment with the services they are responsible for.

Define both internal and external teams, including vendors to facilitate a unified view of IT inventory and clarity of roles and responsibilities of different stakeholders.

Serving as an aggregation point for reporting and analytics.

Benefits

Alongside SDM, TOM serves as a central repository for crucial tasks, providing valuable insights such as:

- Understanding the interconnectedness of IT inventory.
- Identifying ownership, support, delivery, and approval responsibilities.
- Knowing who is currently on call during issue occurrences.
- Tracking open tickets (incidents, problems, changes, releases) in Halo related to specific items.
- TOM fosters accountability and responsibility for maintaining data cleanliness, thereby enhancing the efficiency of ITSM processes.
- Streamlines workflows and improves the overall management of IT services by taking the manual decision make out by automating assignment, escalation, notification, approval and review of Incident, Major Incidents, Problems, Changes and Requests.

TOM ROLES

TOM is categorised into two role types established for a given IT service:

01

Operational roles

These teams are responsible for specific functions within a designated process. Within Halo, these teams actively facilitate the automation of assignment, escalation, notification, approval, and review processes.

02

Accountable roles

Named individuals assigned to a specific role for a given service. These roles primarily serve for awareness across the organisation and as points of contact for service-related work activity.

Once TOM roles are defined for an IT service, they are automatically inherited down to the business applications and instances owned by the IT service. However, at these lower levels, the TOM data can be modified as needed.

Important note: TOM data is only referenced on infrastructure CIs and can be interrogated to drive process automation. Best practices recommend avoiding the storage of TOM data at these lower levels due to the challenges of maintaining data across numerous infrastructure CIs, as it becomes too burdensome and impractical.

Operational roles

These represent a set of process roles within the TOM, designed to be scalable and adaptable, and associated with specific IT services. The below table shows some examples which can be adapted and extended as needed.

Overview		
Process	**Operational role**	**Responsibilities within the Team**
Configuration	Maintenance	• Managing their service specific data within the CMDB and TOM. • Certification of their data footprint in the CMDB. • SPOC for all CMDB data governance for a given service
Change	Owner	• SPOC with responsibility for end-2-end lifecycle of the Change created for the given service.
Change	Approval	• Responsible for assessing the overall Change for a given service and providing formal approval. This scope includes schedule, scope, downtime, impact, risk, accuracy, conflicts, collisions, tasks, implementation plan and rollback plan.
Change	Review	• Responsible for reviewing (FYI only) the overall Change for a given service. This scope includes schedule, scope, downtime, impact, risk, accuracy, conflicts, collisions, tasks, implementation plan and rollback plan.
Change	eCR sponsor	• Responsible for approving an emergency Change for a given service. This scope includes schedule, scope, downtime, impact, risk, accuracy, conflicts, collisions, tasks, implementation plan and rollback plan.
Incident	L1 support	• When a new Incident for a given service is created, this team is automatically assigned to resolve the issue.
Incident	L2 support	• When an existing Incident for a given service, is escalated this team is automatically assigned to resolve the issue.
Incident	L3 support	• The final level of escalation for an Incident for a given service.
Problem	Owner	• SPOC with responsibility for end-2-end lifecycle of the Problem created for the given service.
Request	Approval	• Responsible for assessing the overall Request for a given service and providing formal approval. This scope includes schedule, scope, costs and accuracy.
Knowledge	Approval	• Responsible for assessing the relevance, quality and coverage of knowledge article for a given service and providing formal approval.
Knowledge	Owner	• SPOC with responsibility for end-2-end lifecycle of the knowledge article created for the given service.
Catalogue	Owner	• SPOC with responsibility for end-2-end lifecycle of a catalogue item for the given service.

Accountable roles

These signify a collection of awareness roles within the TOM, crafted for scalability and adaptability, and linked to specific IT services. The table below illustrates some examples that can be adjusted and expanded as required.

Overview	
Operational role	Responsibilities within the Team
CIO	• Regional and business aligned CIO with overall responsibility for the service
COO	• Regional and business aligned CIO with operations responsibility across the business line
Service owner	• The service owner; highest level of ownership from a day to day perspective
Service owner deputy	• The service owner 2nd in command
Operations manager	• The lead from a BAU perspective for the service
Operations supervisor	• The deputy lead from a BAU perspective for the service; more hands on
Engineering manager	• The lead from an engineering perspective for the service
Engineering supervisor	• The deputy lead from a n engineering perspective for the service; more hands on
Risk officer	• Responsible for operational risk and compliance for the service
Architect	• Responsible for the technology stack

TOM WORKING EXAMPLE

Inheritance in practice

Working example - Application

The following illustrates an instance of a TOM blueprint established for the application aligned IT service named "HR IT," cascading down to the business application instance labelled "Workday UK PROD." Roles at this lower level can be overridden to align with the operational structure specific to the business application instance.

IT service

Field	Value	Upstream CIs	Downstream CIs	Process	Operational role	Team name	Accountable role	Individual name
Name	HR IT	Workday (Business Application) SAP (Business Application)	Employee Services (Business Service)	Configuration	Maintenance	HR IT Support	Service owner	Shirley Sweeny
Lifecycle state	Operational			Change	Owner	HR IT Support	Service owner deputy	Sunil Gupta
Health state	Degraded			Change	Approval	HR IT Mgt, HR Business	Enterprise architect	Joseph Abrahams
Criticality	High			Change	eCR sponsor	Donald Morse	Risk & compliance mgr	Imran Khan
Owning entity	ACME Corporation			Incident	L1 support	HR IT Support	Operations mgr	Cathy Longcroft
Type	Application-aligned			Incident	L2 support	HR IT Engineering	Operations supervisor	Donald Morse
Location	London, UK			Problem	Owner	HR IT Support	Engineering mgr	Kathy Lee
Description				Request	Approval	HR IT Mgt	Engineering supervisor	John Jacobs

Business Application Instance

Field	Value	Upstream CIs	Downstream CIs	Process	Operational role	Team name	Accountable role	Individual name
Name	Workday UK PROD	LNX-P-98323uk (Linux Server) LNX-P-98324uk (Linux Server)	Workday (Business Application) Tibco ESB PROD UK (Business App Instance)	Configuration	Maintenance	HR IT Support	Service owner	Shirley Sweeny
Lifecycle state	Operational			Change	Owner	**Workday Support***	Service owner deputy	Sunil Gupta
Health state	Outage			Change	Approval	HR IT Mgt, HR Business	Enterprise architect	Joseph Abrahams
Criticality	High			Change	eCR sponsor	Donald Morse	Risk and compliance mgr	Imran Khan
Owning entity	ACME Corporation			Incident	L1 support	**Workday Support***	Operations mgr	**Roger Redhat***
Type	Vendor			Incident	L2 support	**Workday Engineer***	Operations supervisor	**Jill Sanders***
Location	London, UK			Problem	Owner	HR IT Support	Engineering mgr	Kathy Lee
Description				Request	Approval	HR IT Mgt	Engineering supervisor	John Jacobs (anomaly)
Owning Srvc	**HR IT**							

** overridden to make ownership more granular at the business app instance level*

TOM WORKING EXAMPLE

Working example - Infrastructure

The following illustrates an instance of a TOM blueprint established for the infrastructure aligned IT service named "Linux Cloud Hosting UK". Note that the infrastructure CIs that this service manages are cross referenced, but the TOM data does not need to be inherited downwards for the reasons explained above.

IT service

Field	Value	Upstream CIs	Downstream CIs	Process	Operational role	Team name	Accountable role	Individual name
Name	Linux Cloud Hosting UK	Monitoring (Business Application)	IT Shared Services (Business Service)	Configuration	Maintenance	HR IT Support	Service owner	Fred Baker
Lifecycle state	Operational			Change	Owner	HR IT Support	Service owner deputy	Silka Gupta
Health state	Online			Change	Approval	HR IT Mgt, HR Business	Enterprise architect	Moses David
Criticality	High			Change	eCR sponsor	Donald Morse	Risk & compliance mgr	Mohammed Rizwan
Owning entity	ACME Corporation			Incident	L1 support	HR IT Support	Operations manager	Cathy Lu
Type	Application-aligned			Incident	L2 support	HR IT Engineering	Operations supervisor	Will Gill
Location	London, UK			Problem	Owner	HR IT Support	Engineering manager	Amanda Aldridge
Description				Request	Approval	HR IT Mgt	Engineering supervisor	Alfred McGee

Linux Server

Field	Value	Upstream CIs	Downstream CIs	Process	Operational role	Team name	Accountable role	Individual name
Name	LNX-P-98324uk	Ora-Serv-329B (Oracle Server)	Workday PROD UK (Biz App Instance)	*Inherited from owning service "Linux Cloud Hosting"*				
Lifecycle state	Operational							
Health state	Outage							
Criticality	High							
Owning entity	ACME Corporation							
Type	Vendor							
Vendor	Amazon AWS							
Location	London, UK							
Owning Srvc	**Linux Cloud Hosting UK**							

DATA GOVERNANCE

Quality is the foundation

Like all service management tools, Halo's effectiveness across an organisation is determined by the quality of foundational data in the platform. Emphasising data quality and coverage necessitates ongoing investment and managing SAF data (both SDM to TOM), is most effectively handled through a federated ownership model, where each service owner designates a team of configuration managers responsible for ensuring the accuracy, coverage, and quality of the data footprint.

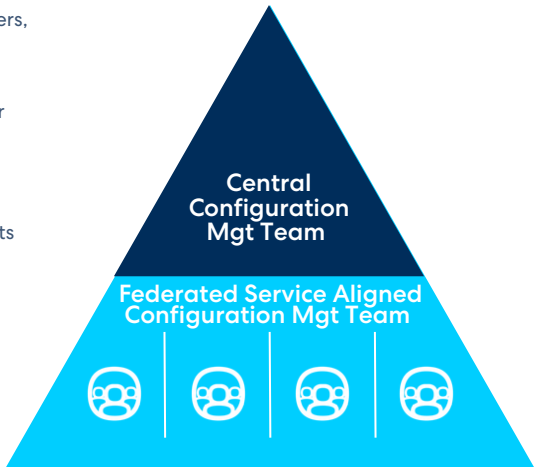
At regular intervals, usually every 6 months, configuration managers validate the accuracy and coverage of data in SAF. This encompasses all CMDB classes within scope, along with their attributes, upstream and downstream relationships, TOM operational and accountable roles, and any process reference data linked to their services.

Best practices also recommend the establishment of a centralised configuration management function tasked with guiding, asserting, educating, and enforcing the quality of data in the CMDB and publishing regular scorecards and health cards.

This ensures that the Federated service-aligned configuration management teams are effectively performing their responsibilities.

SDM and TOM

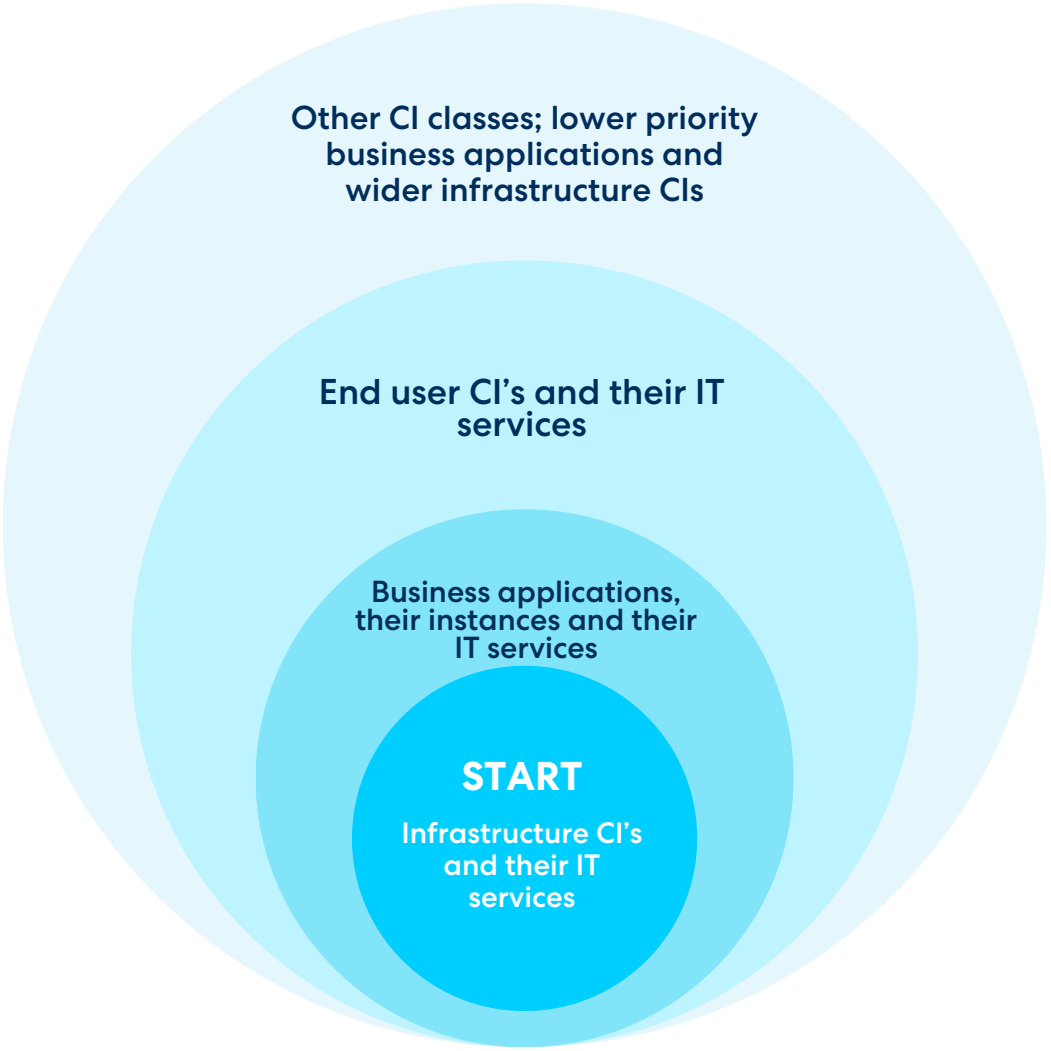
- Critical activity commences immediately and remains ongoing throughout normal business operations (BAU); an investment that never ceases.
- Encompasses the following elements: CMDB classes and relationships, operational and accountable responsibilities within the TOM, teams, members, roles, and users. Additionally, it includes process-aligned reference data owned by process owners.
- Prioritises a people-oriented approach, emphasising the importance of clear roles and responsibilities based on a federated configuration management framework; establishes service-aligned teams that take ownership and accountability for their respective areas.
- To ensure the accuracy and reliability of the data, all the relevant data points within this scope undergo periodic certification.
- A centralised configuration team oversees the entire process, providing guidance and resolving bottlenecks as needed.
- The Suspect CI process plays a vital role in identifying, validating, and remediating issues present in the CMDB.
- Furthermore, this initiative is part of the CIO dashboard suite, providing insights into service health based on data completion.
- To drive improvements in data quality and coverage, the approach leverages various tools, reports, and dashboards. These tools aid in identifying areas for enhancement and provide valuable feedback on data integrity.
- SAF is underpinned by a formal and periodic data recertification process where configuration managers are responsible for validating their service footprint data in the CMDB and wider process aligned reference data and formally attest the quality and coverage of this.



SAF MATURITY JOURNEY

A two-year roadmap

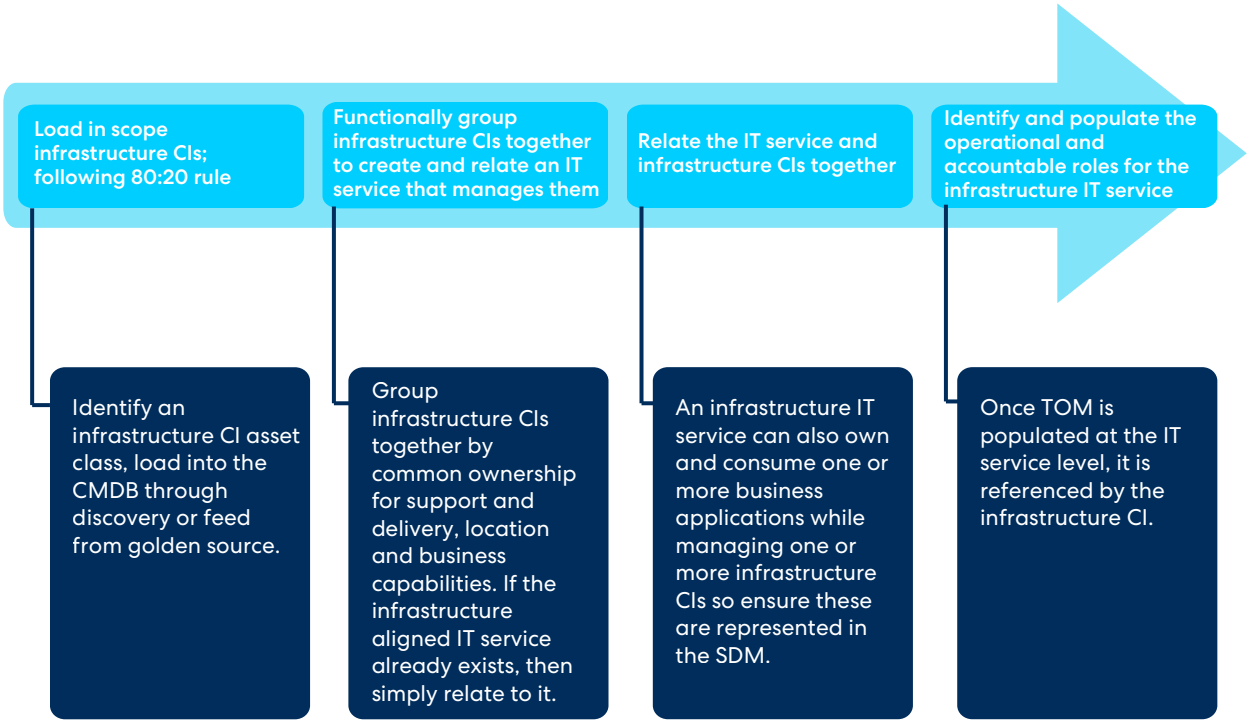
Based on your current maturity level defining your 2 year roadmap for your CMDB is essential. The picture below describe the typical maturity road map organisations starting their CMDB journey.



STAGE 1

Stage 1 - Infrastructure

Start with your core infrastructure CIs and associated infrastructure IT services and their associated TOM information.



The following is a set of typical infrastructure IT services that can be used as a starting point as they are common across many sectors and clients. The core business IT services are industry aligned and often very specific to customers.

STAGE 1

The following is a set of typical infrastructure IT services that can be used as a starting point as they are common across many sectors and clients. The core business IT services are industry aligned and often very specific to customers.

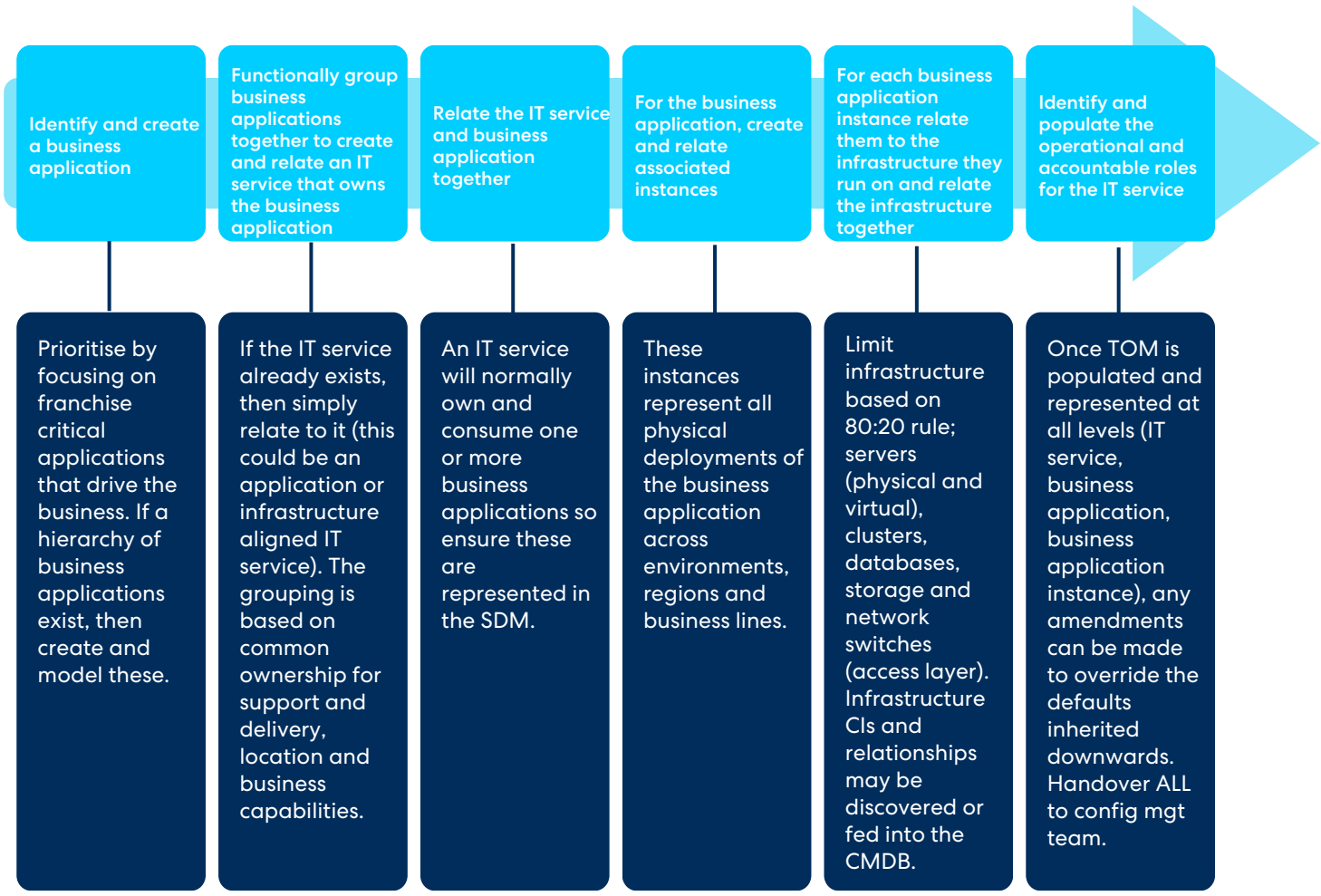
Service Type									
Delivery	Strategy & Planning	Development	Operations	Security & Compliance					
End User	End User Computing	Comms & Collaboration	Connectivity	Mobile					
Shared	Finance	HR	Procurement	Facilities	Audit, Risk & Coompliance	Legal	Property	Corporate Comms	Health, Safety, Security & Environment
Core Business	Industry sector specific service 1	Industry sector specific service 2	Industry sector specific service 3	Industry sector specific service 4					
Infrastructure									

Cluster	High Availability	Load Balancer					
OS Server	Windows	Linux	Unix	Mainframe	ESX	Web	UNIX
DB Server & Instance	Oracle	SQL Server	MySQL	Informix	DB2	MangoDB	
Web Server	IIS	Apache	Nginx	GWS			
Other Server	File	Directory	Mail	Print	Distribution	Storage	
Network Device	Switch	Router	Hub	Circuit	Firewall	Patch Panel	
Computer	Workstation	Laptop	Tablet	Mobile	Handheld Scanner		
Peripheral	MRP, Printer, Scanner	Appliance	PDU	UPS	Rack		
Storage	SAN	NAS	DAS				

STAGE 2

Stage 2 - Application

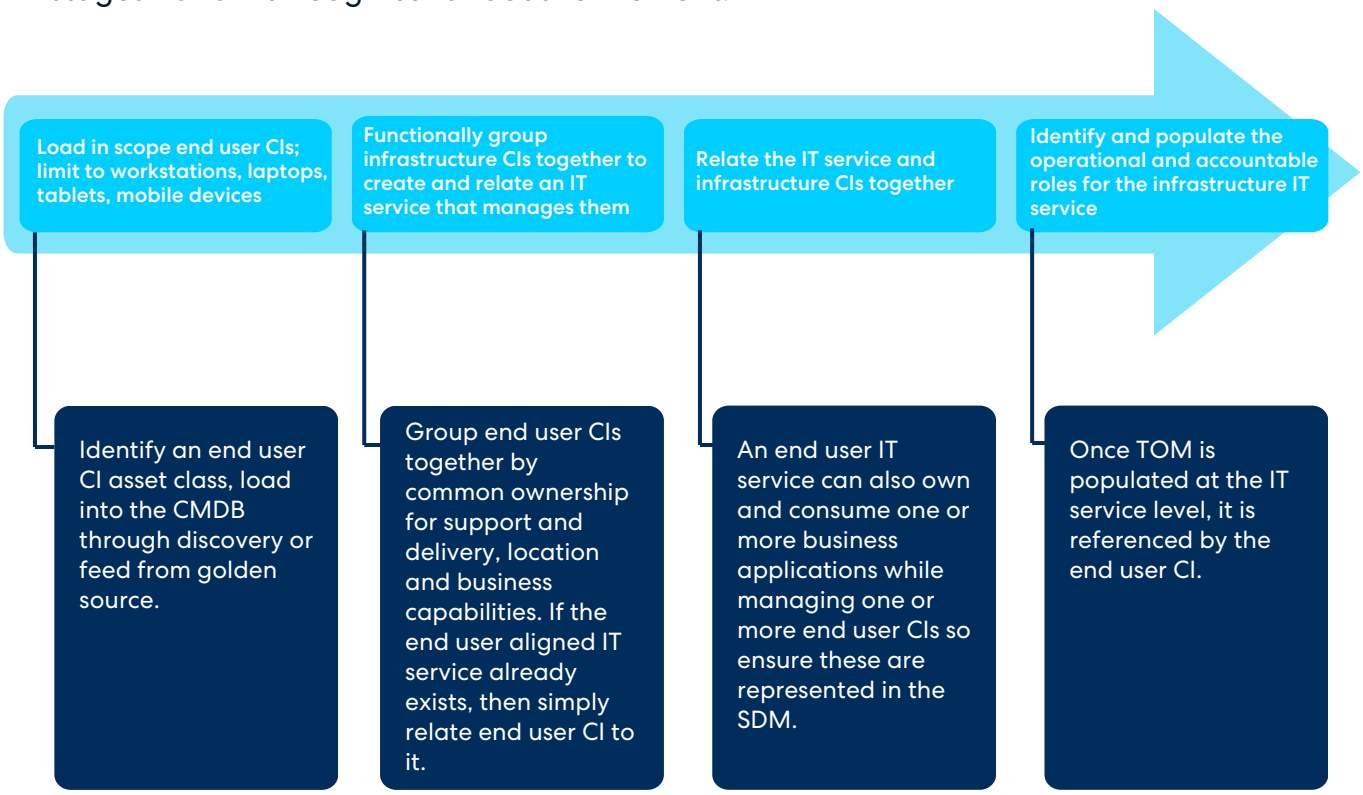
Onboard your business applications along with their corresponding application aligned IT services, deployed instances, and relevant TOM information. Simultaneously enhance data in stages 1 and 2 through continuous refinement.



STAGE 3

Stage 3 - End User

Onboard your end-user devices along with their corresponding end user aligned IT services, along with the relevant TOM information. Simultaneously enhance data in stages 1 and 2 through continuous refinement.

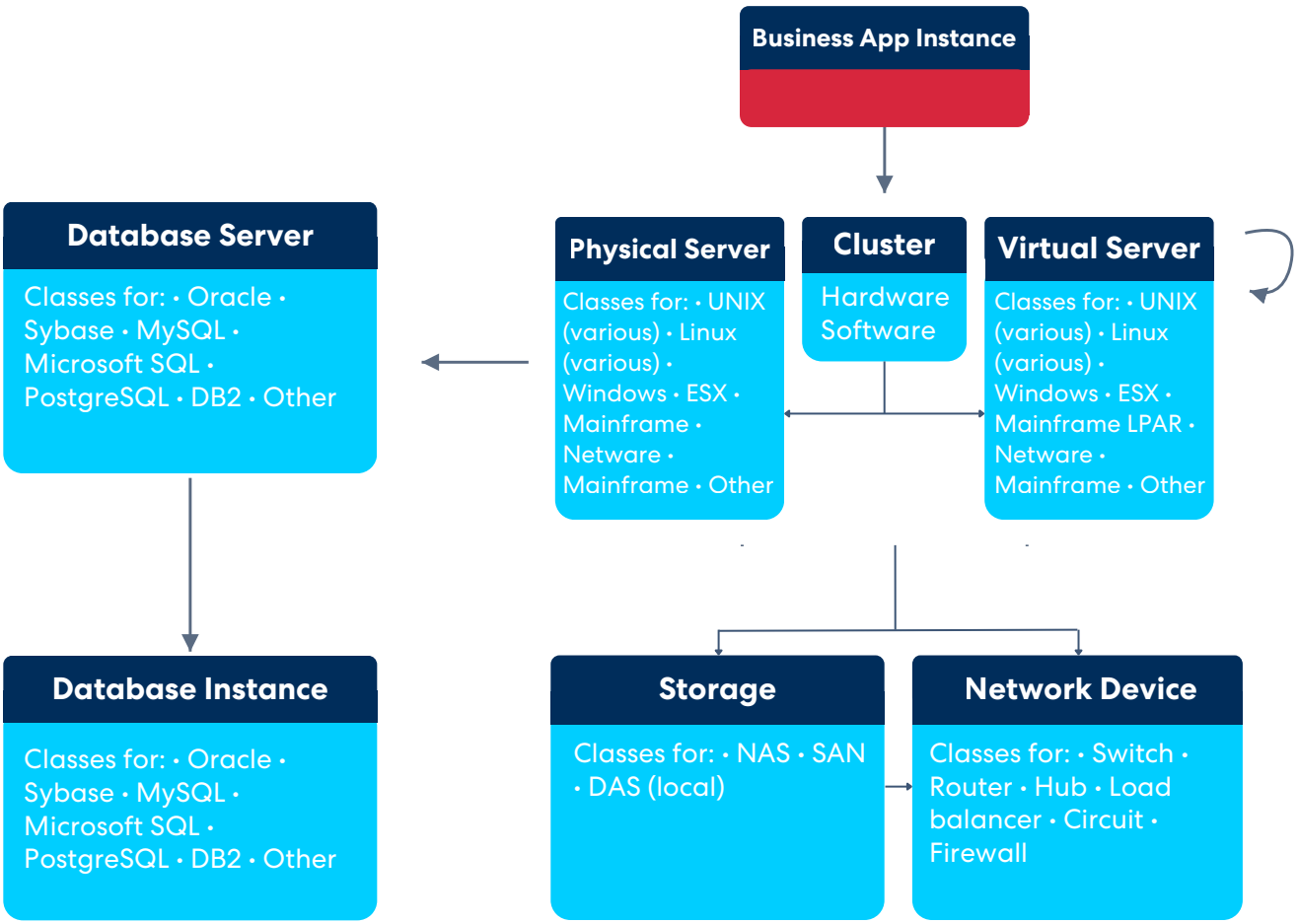


If gaining control over end-user devices is crucial for business operations, such as a software asset management initiative, expedite the progress of this stage.

STAGE 4

Stage 4 - Mature

Persist in enhancing the current quality and coverage of data within the SDM and TOM by implementing a federated, structured, and focused program of work for configuration managers and the central configuration team.



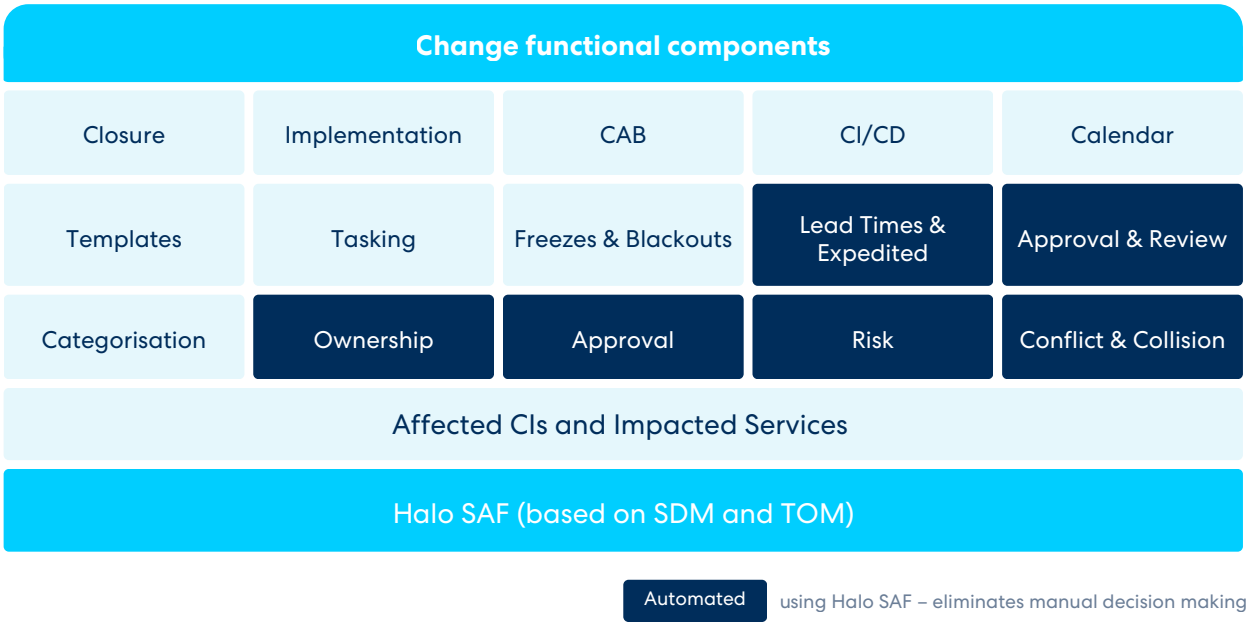
Advance the maturity of existing SDM and TOM data, and introduce new classes as necessary, substantiating their inclusion with a clear business justification.

Where SAF drives automation

The main processes which benefit from SAF in terms of automation tend to be Change, Incident and Major Incident. That's not to say that other do not, because they do, but the benefits in terms of efficiencies, risk mitigation and wider impact (financially, regulatory, or reputationally) tends to be more limited.

Change Management

The SAF drives the following automations in a normal Change:



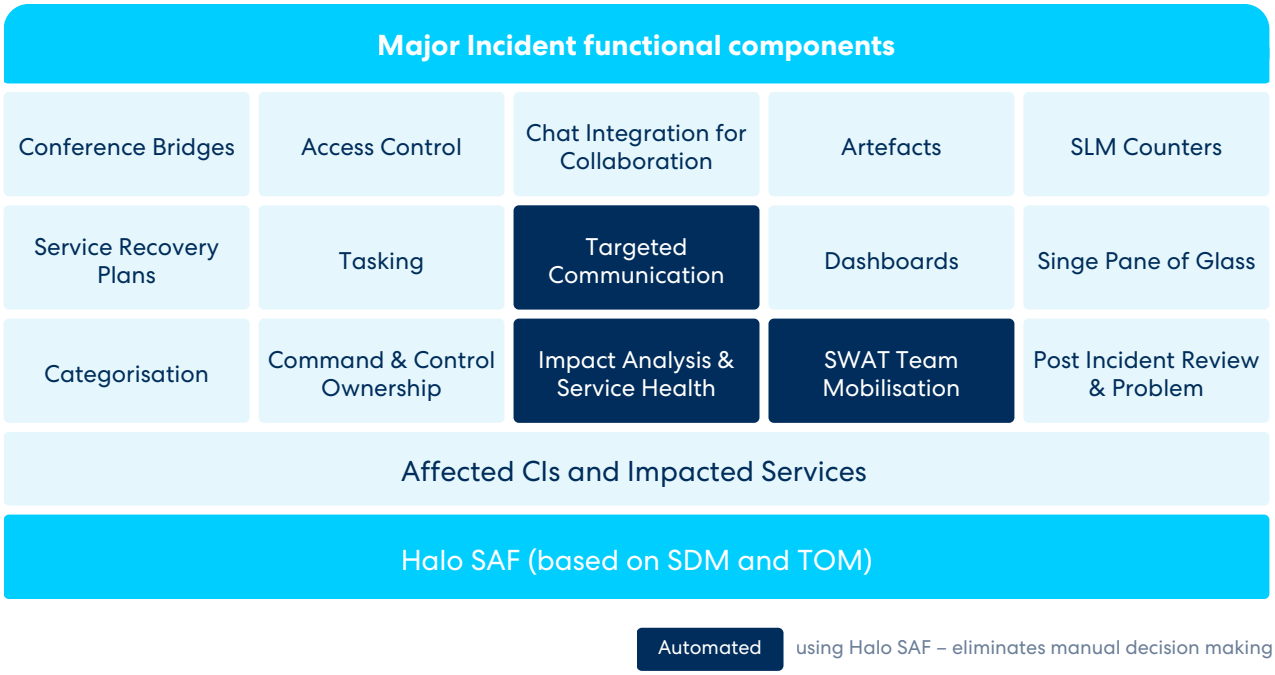
- Based on the primary CIs affected (which are typically infrastructure CIs or business application instances) by the Change, traverse the CMDB relationships in

SAF to understand the business application instances and IT services potentially impacted by the Change.

- Based on the primary CI affected, determine the owning/managing IT services and from its TOM automatically set the ownership of the Change.
- By assessing the type of change being performed and the prior history of success and failure of such Changes, assess the risk. The higher the risk, the more authorisations potentially required.
- Based on the impacted IT services and business application instances run collision and conflict checks with other Changes within the time window indicated.
- Based on the impacted IT services and business application instances, use their TOM data to determine the authorisation teams need to approve. Like wise use this data to determine which teams need to review the Change.

Major Incident Management

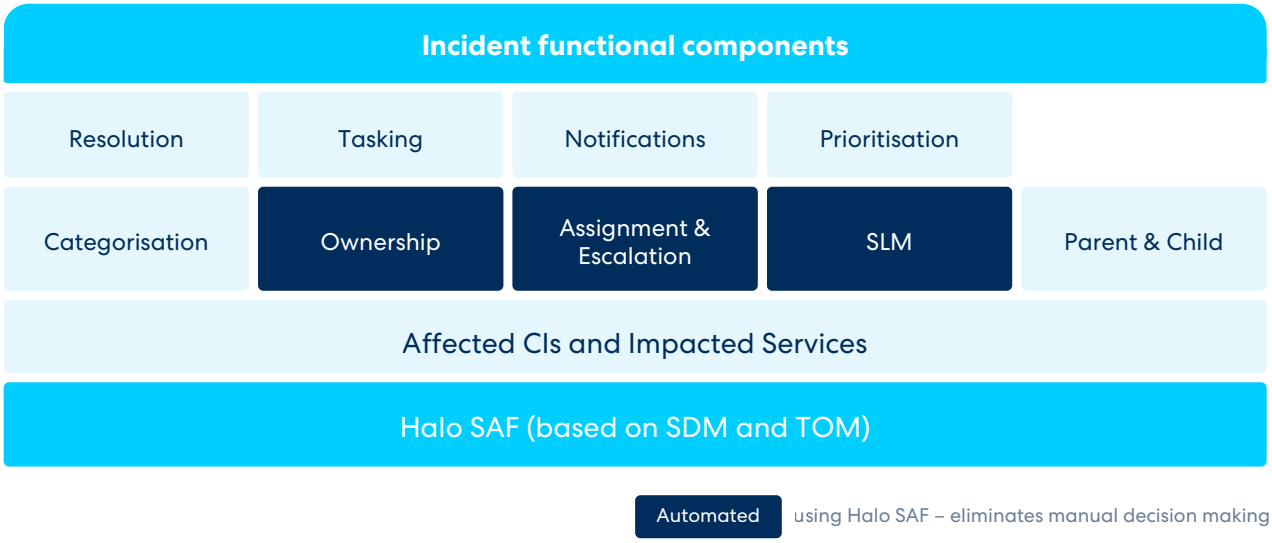
The SAF drives the following automations in Major Incident:



- Based on the primary CIs affected (which are typically business application instances) by the major incident, traverse the CMDB relationships in SAF to understand other business application instances and IT services potentially impacted by the incident.
- Based on the impacted IT services and business application instances run checks to understand recent Incidents and Changes which may have caused this major incident.
- Based on the primary affected business application instance, use its TOM data to determine the SWAT (rapid response teams) to interrogate to determine on call team members. Mobilise these individuals quickly and efficiently by utilising the appropriate mobilisation tools (e.g. PagerDuty, Everbridge, Microsoft Teams etc).
- Based on the impacted IT services and business application instances, use their TOM data to determine the operational and engineering leads to assign assessment tasks to better understand impact, risk, mitigation actions, trigger service record plans and so forth.
- Based on the impacted IT services and business application instances, use their TOM subscription data to determine who to send targeted communications to.

Incident Management

The SAF drives the following automations in Incident:



- Based on the primary CIs affected (which are typically business application instances) by the incident, traverse the CMDB relationships in SAF to understand other business application instances and IT services potentially impacted by the incident
- Based on the impacted IT services and business application instances run checks to understand recent Incidents and Changes which may have caused this incident.
- Based on the primary affected CI, from its associated IT service interrogate the TOM data to determine the default (level 1) assignment team. Also determine the and start to measure against default response and resolution OLA's and overall SLA.
- Where escalation is required, manual or automated, use TOM to determine the next team in the escalation chain.

DASHBOARDS

A holistic, real-time view

Data from Halo SAF in combination with Halo processes empowers senior management and operations teams with intuitive analytical reports and dashboards (illustrated examples below).

This allows them to gain a holistic view of the IT landscape, comprehending the status of specific services from multiple perspectives. The normalised view, with comparative elements, fosters healthy competition among business verticals and service owners, driving towards elevated service quality.

In real-time, any organisational member can swiftly access a concise overview of the aspects they support, maintain, construct, or utilise.

CONCLUSION

Operate IT as a business

Utilise the Service Automation Framework (SAF) as a guide to map your IT services onto the Halo platform. Moreover, leverage SDM to promote standardisation and normalisation of the foundations of your environment. With SDM and TOM, the Halo SAF delivers significant benefits for enterprises aiming to operate IT as a business and helps established a rapid and scalable framework for automated and integrated service management.

Through targeted investment you can achieve significant business value through improved quality and transparency of data, enhanced data insights, process level automation, cost savings and cost transparency.