

# **ITSM PROJECT - DISSERTATION DOCUMENT**

## **IT Service Management**

Gabriel Rovesti - 2103389

Michael Amista' - 2122865

Elena Marchioro - 2130393

*August/September 2024*

## Table of contents

<b>Table of contents</b> .....	<b>2</b>
<b>List of Figures</b> .....	<b>5</b>
<b>List of Tables</b> .....	<b>5</b>
<b>1. Introduction</b> .....	<b>6</b>
<b>2. Background and scenario analysis</b> .....	<b>7</b>
2.1. Bank overview and structure .....	7
2.1.1. Bank services .....	7
2.2. IT Services Portfolio .....	8
2.3. Strategy and challenges .....	9
2.4. Current connectivity services .....	9
2.4.1. Home Connectivity .....	9
2.4.2. USB Connectivity .....	9
2.5. Identified issues and inefficiencies .....	10
<b>3. Service management analysis and governance</b> .....	<b>11</b>
3.1. Existing ITSM Processes .....	11
3.1.1. Service Strategy .....	12
3.1.2. Service Design .....	12
3.1.3. Service Transition .....	13
3.1.4. Service Operation .....	13
3.1.5. Continual Service Improvement .....	14
3.2. Limitations of current framework and bottlenecks .....	14
3.3. Impact on overall IT service portfolio .....	14
3.4. Rationale for decommissioning plan .....	15
<b>4. ITIL 4 Framework</b> .....	<b>17</b>
4.1. Four Dimensions of Service Management .....	17
4.2. Service Value System (SVS) .....	18
4.2.1. Guiding Principles .....	18
4.2.2. Continual improvement .....	20
4.2.3. Service Value Chain (SVC) .....	23
4.2.4. Practices involved in the scenario .....	24
<b>5. Decommissioning plan</b> .....	<b>28</b>
5.1. Identify and inventory IT Assets .....	28
5.2. Costs assessment .....	31
5.3. Evaluate disposal and decommissioning options .....	31
5.4. Communication with stakeholders .....	32
5.5. Transition to new services .....	32
5.6. Monitor and verify IT asset disposal and decommissioning .....	33
5.7. Update and optimize IT asset lifecycle management .....	33
<b>6. Rollout plan</b> .....	<b>34</b>
6.1. Description of the approach .....	34
6.2. Implementation of the approach .....	35
6.2.1. Plan .....	35
6.2.1.1. Architecture Management .....	36
6.2.1.2. Risk Management .....	38
6.2.1.3. Service Financial Management .....	39

6.2.1.4. Strategy Management .....	40
6.2.2. Improve .....	41
6.2.2.1. Information Security Management .....	41
6.2.2.2. Supplier Management .....	43
6.2.2.3. Change Control .....	44
6.2.2.4. Service Level Management .....	46
6.2.3. Engage .....	48
6.2.3.1. Supplier Management .....	49
6.2.3.2. Infrastructure and Platform Management .....	50
6.2.3.3. Change Control .....	52
6.2.3.4. Service Level Management .....	53
6.2.3.5. Service Desk .....	54
6.2.4. Design & Transition .....	55
6.2.4.1. Architecture Management .....	56
6.2.4.2. Risk Management .....	56
6.2.4.3. Release Management .....	57
6.2.4.4. Service Validation and Testing .....	59
6.2.4.5. Service Design .....	59
6.2.4.6. Deployment Management .....	60
6.2.5. Obtain & Build .....	62
6.2.5.1. Supplier Management .....	62
6.2.5.2. IT Asset Management .....	64
6.2.5.3. Continual Improvement .....	66
6.2.5.4. Information Security Management .....	67
6.2.5.5. Service Configuration Management .....	69
6.2.5.6. Change Control .....	70
6.2.6. Deliver & Support .....	72
6.2.6.1. Service Desk .....	72
6.2.6.2. Incident Management .....	74
6.2.6.3. Infrastructure and Platform Management .....	76
6.2.6.4. Monitoring and Event Management .....	77
6.2.6.5. Service Level Management .....	79
6.2.6.6. Release Management .....	80
6.2.6.7. Service Configuration Management .....	82
<b>7. Metrics, performance and maturity .....</b>	<b>85</b>
7.1. Continual improvement .....	85
7.1.1. Critical Success Factors (CSFs) .....	85
7.1.2. Key Performance Indicators (KPIs) .....	87
7.1.3. KPI/CSF Mapping .....	91
7.2. Feedback mechanisms .....	92
7.3. Ongoing review and optimization process .....	94
<b>8. Timeline, milestones and baselines .....</b>	<b>96</b>
8.1. Overview .....	96
8.2. Project phases .....	96
8.3. Key milestones .....	98
8.4. Baselines of CSFs and KPIs .....	101
8.5. Gantt rollout chart .....	103

<b>9. Conclusions .....</b>	<b>104</b>
9.1. Summary of key recommendations .....	104
9.2. Expected benefits and outcomes .....	104
<b>10. Appendix A: References &amp; Sources .....</b>	<b>106</b>
10.1. General ones .....	106
10.2. Chapter 1 & Chapter 2 .....	106
10.3. Chapter 3 .....	106
10.4. Chapter 4 .....	106
10.5. Chapter 5 .....	107
10.6. Chapter 6 .....	107
10.7. Chapter 7 .....	107
10.8. Chapter 8 .....	108
10.9. Chapter 9 .....	108
<b>11. Appendix B: Acronyms .....</b>	<b>109</b>
11.1. A .....	109
11.2. C .....	109
11.3. D .....	109
11.4. H .....	109
11.5. I .....	109
11.6. O .....	109
11.7. K .....	109
11.8. U .....	109
11.9. V .....	110
11.10. W .....	110
11.11. R .....	110
11.12. S .....	110
11.13. V .....	110

## List of Figures

Figure 2: Organizational chart of the bank .....	7
Figure 3: Logic of governance to be implemented in the bank .....	11
Figure 4: ITSM processes currently employed by the Bank .....	12
Figure 5: ITIL 4 Four dimensions .....	18
Figure 6: ITIL 4 Service Value System .....	18
Figure 7: ITIL Continual Improvement Model .....	20
Figure 8: ITIL 4 Service Value Chain .....	23
Figure 9: Information security management framework .....	41
Figure 10: Change control best practices .....	45
Figure 11: Ideal IT Asset Management lifecycle .....	64
Figure 12: Service desk workflow and qualities .....	73
Figure 13: Monitoring and event management logical workflow .....	77
Figure 14: Release management in an Agile workflow .....	80
Figure 15: Gantt chart of the discussed planning .....	103

## List of Tables

Table 1: Home Connectivity Service Assets .....	30
Table 2: USB Connectivity Service Assets .....	30
Table 3: Mapping of CSFs to KPIs .....	92

## 1. Introduction

In the evolving landscape of digital banking, the ability to adapt and continually optimize IT services is crucial for maintaining competitive advantage and precision in the market. This project focuses on the strategic *decommissioning* of two connectivity services within our bank's IT service portfolio:

*Home Connectivity* and *USB Connectivity*.

The decision of *decommissioning* the services offers more central control while crafting the basis to continue expand internationally in embracing new themes and technologies, reducing complexity and optimizing redundancy and resources in an efficient way.

This high-level project plan outlines the approach we will take to decommission the described services while ensuring minimal disruption to our users and operations.

Throughout this document, we will explore the involvement of key IT Service Management (ITSM) processes according to ITIL 4, assess potential risks, and define success criteria. Our goal is to execute a good transition that aligns with our bank's strategic objectives and describes thoroughly the decommissioning plan, present and operated up to that point. The following plan has the aim to optimize the portfolio and different resources, reducing costs and paving the way for connected and unified solutions for the same bank. Using this document, the company can potentially improve its processes and operations, reviewing them and ensuring correct control, implementing as a result practices and processes closing with a *rollout* plan.

After the implementation of this rollout plan, some key metrics and measurements will be discussed so to implement correctly the principles of ITIL and discuss an overview of the changes to implement.

## 2. Background and scenario analysis

### 2.1. Bank overview and structure

Our bank, leader in banking services provision for individuals and companies, has recently expanded its operations into overseas countries through acquisitions and partnerships. This has led to challenges in managing its IT services portfolio, particularly in terms of connectivity solutions for its workforce.

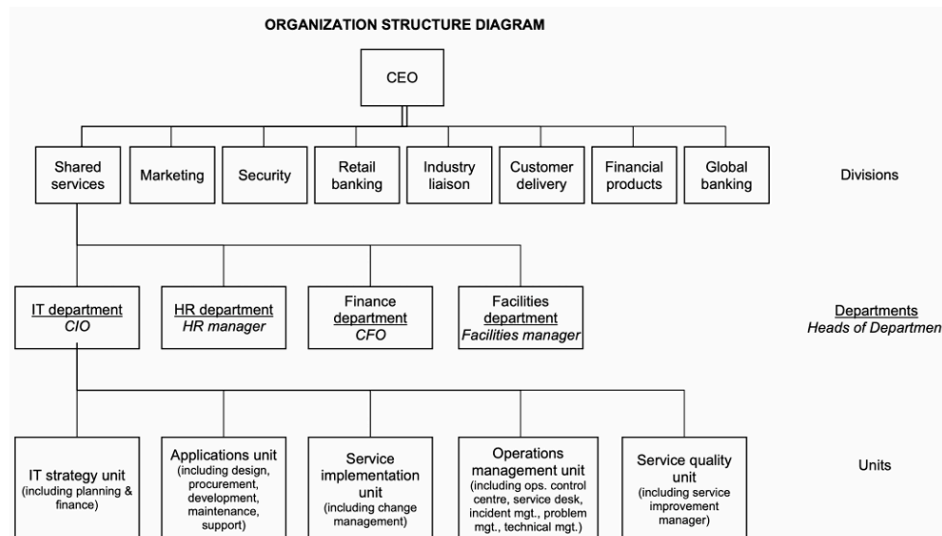


Figure 2: Organizational chart of the bank

Figure 2 shows the main bank divisions, each led by a divisional director reporting directly to the CEO. Each department is structured to support global operations while retaining local flexibility over bank single operations. These are mainly divided between banking (retail/customer/industry/finance) and non-banking (marketing/shared services/security) divisions.

The strategy focuses upon:

- Activities integrations and services sharing with recently acquired overseas banks
- Expanding customer base and service offerings internationally
- Leveraging partnerships with other financial institutions to broaden the range of services offered

#### 2.1.1. Bank services

The bank offers a range of services considered critical for its operations, both for individual/private and corporate customers:

- 24-hour automated teller machine (ATM) service
- 24-hour customer call centre for telephone banking and inquiries
- 24-hour internet banking
- 24-hour global payments service
- Branch services for in-person banking
- Third-party sales support service
- Regulatory service

In addition, the bank provides other services considered supplementary:

- Statement production
- Marketing and customer offers

Together with these ones, the core services form the foundation of the bank's operations, ensuring 24/7 accessibility and support for customers through various channels. The services are designed to meet the diverse needs of the bank's customer base, domestically and internationally.

## 2.2. IT Services Portfolio

Like with the company divisions, the department is made up of five units, each headed by a manager, where the focus is to implement IT strategy within all operations and ensuring the quality implementation of each change and service.

The *IT department structure* is as follows:

- IT strategy unit: IT strategy, planning, and finance
- Applications unit: Application design, procurement, development, maintenance, and support
- Operations management unit: Operations control center, service desk, incident and problem teams, technical management
- Service implementation unit: Change management process
- Service quality unit: Service improvement initiatives

These units work collaboratively to ensure quality implementation of each change and service, focusing on maintaining high availability and security across the IT infrastructure.

The *infrastructure* needs to be always available, so to provide high availability and provide a “virtual first” approach so to ensure continuous usage of each service with the appropriate level of security.

These are comprised by the following:

- Server and storage management
- Network management
- Database management
- Cybersecurity services

Apart from banking services and third-party software, the bank provides different other services.

First and foremost, the *connectivity* ones:

- Home connectivity: cabled internet connection using VPN access to the bank's network, composed of subscription, usage and support fees. This is also composed by CCA Home variant, existing with a telephone set complementary to the previous one.
- USB connectivity: log on to the company's network on-the-fly, using VPN when on the route. This consists of a USB token and subscription/usage fees. This is also composed by the IT Service Token variant, so to allow the same using Wi-Fi.

Other services to list include the *application* ones, so to include core banking support, CRM systems to interact with customers and analytics, complete with *support*, using IT service desk practices so to intervene against incidents and problems, while practicing change and release management.



## 2.3. Strategy and challenges

Thanks to these services, the corporate vision is focused firmly and foremost on expansion. The goal is integrating automation purely respecting the regulatory/financial/legal constraints present in operation.

The plan is based on joining the forces of forces of recently purchased foreign banks, making customer pool and service package international and using partnerships with other financial establishments to increase the quantity of services provided.

Plans have been made for the business over the coming period including, retail banking market share in its home country from seven percent to ten percent, boost income from internet banking with seventy percent; an increase in profits by fifty percent via international customers among others. On the other hand, a lot of problems are facing this ambitious plan because it is too hard. Some issues include communication barriers due to different time zones and cultures following its recent expansion into the global stage.

## 2.4. Current connectivity services

In the section we're going a bit more in detail of the connectivity services, on which to launch the decommissioning plan discussed in further detail in the fifth chapter about Decommissioning Plan (in Section 5).

### 2.4.1. Home Connectivity

*Home Connectivity* is a service offering implemented seven years ago to support the bank's Work from Home (WFH) policy. It consists of:

A cabled internet connection installed at the user's home location A desktop computer provided as part of the service VPN access to the bank's network

The service is provided by a third-party supplier with the following cost structure:

- Desktop hardware: \$800.45 (one-off)
- Desktop support: \$45.95 (monthly)
- Central DSL connection: \$12,604 (yearly)
- Internet subscription: \$46.15 (monthly)
- Installation fee: \$110 (one-off)
- Usage: First 100 MB free, thereafter \$0.20 per MB

Currently, approximately 3000 out of 25000 end users utilize this IT Service. A year after its launch, the service was expanded to include a VoIP option, specifically for Call Center Agents to perform their activities from home and maximize efficiency. This variant, called CCA Home Connectivity, serves 2500 users and includes an additional telephone set (\$100.83, one-off) component.

### 2.4.2. USB Connectivity

*USB Connectivity* was designed for employees with high mobility, such as sales agents. It allows users to log on to the company's network using VPN when they are en route. The service consists of:

- USB token (free)
- Internet subscription: \$28.39 (monthly)
- Usage: First 100 MB free, thereafter \$0.20 per MB

This IT Service is used by 7,000 employees, so to allow for easy and fast access from whenever possible, at all circumstances.

## 2.5. Identified issues and inefficiencies

This step in current IT services is crucial in effective IT Asset Management, as it aligns with the core message of ITIL 4's principle of "Focus on Value", better explained in Section 4. The preference to close services and the planning process are justified by the analysis such that the problems are solved, and the organization gains more value from the transition.

As the practice itself highlights, it's important to emphasize the importance of managing the full lifecycle of IT assets to "maximize value, control costs, manage risks, support decision-making about purchase, re-use, retirement, and disposal of assets, and meet regulatory and contractual requirements". In light of this, a careful examination should be conducted, revealing the following inefficiencies:

- *Cost inefficiency*: At the moment the services are quite expensive both in terms of hardware and monthly fees and this expenditure might not be necessary with the advent of new and cheaper methods. These things only help the institution in managing its expenditure well.
- *Limited flexibility*: Services like Home Connectivity are tied to a specific location, which may not align with increasing flexibility trend, specifically for working arrangements. This may potentially reduce the value delivered to users and shared within the organization.
- *Management complexity*: Managing multiple connectivity services, specifically when shared between internal users and external providers, might be difficult and might increase the complexity of IT operations and support, potentially leading to higher operational costs and increased risk of service disruptions.
- *Scalability concerns*: As the bank expands internationally, scaling between regions may prove challenging and costly, partly contrasting strategic growth objectives and company's vision.
- *Security risks*: The use of physical USB tokens for connectivity poses danger to the security of the bank's IT assets if these are lost or stolen.
- *Technological obsolescence*: Given the quick progress in connectivity technologies, it is possible that these services could now be considered old models; leading therefore to reduced productivity or unimproved user experience that in turn affects their business value. This obsolescence affects the value derived from these IT assets.
- *Inconsistency in maintenance and user experience*: Different user groups may use various connections as "routers" hence making it hard for them to access anything online like videos or music altogether without facing any hitches (thus lowering service quality).

### 3. Service management analysis and governance

This section provides an in-depth analysis of the bank's current IT Service Management (ITSM) situation, based on current IT Service Management processes examining the current ITSM framework processes and ITIL General Management Practices applied in this specific context. We'll examine each stage of the service lifecycle, identifying strengths, weaknesses, and areas for improvement. This analysis will form the foundation for our *application* of ITIL 4 and the *decommissioning* of the Home Connectivity and USB Connectivity services.

In order to make a good release and deployment management aiming to build and delivering the right capability to provide the services according to intended and specified objectives. This is important in order to make a good release of both services and products, both existing and future, so to deliver the correct amount of value to customers and stakeholders. Important considerations should also be made when considering the type of planning, deployment and execution.

As the bank situation is analyzed, it's crucial to understand the shift in logic that this ITIL 4 application represents. Figure 3 illustrates the new logic we aim to implement in this document:

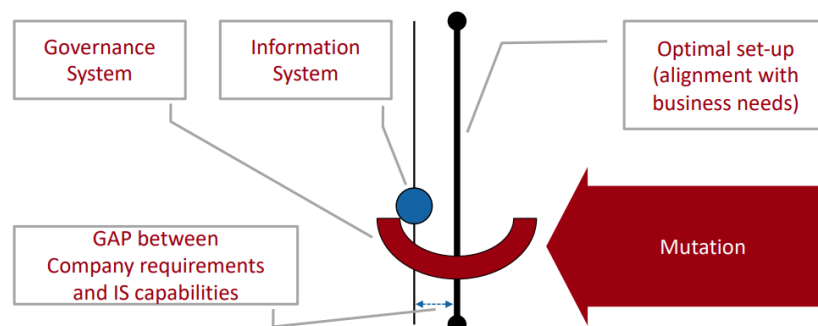


Figure 3: Logic of governance to be implemented in the bank

The focal point of this model is the identification and management of the gap between company needs and information systems capabilities, as it is not considered as a shortcoming but rather an inbuilt function that propels innovation and advancement.

The aim is not really to check out this gap altogether; it would be extremely difficult in a fast-paced business environment. Instead, the aim is to reduce it and utilize it as a catalyst for encouraging beneficial change. This new idea contradicts with the traditional ITSM methodology now being adopted by the bank.

It emphasizes flexibility, continual alignment, governing systems and other aspects of governance that include the information system aspects. While evaluating the current framework and suggesting enhancements, this fresh perspective will steer our analysis towards developing a more responsive and business-oriented ITSM. In the subsequent sections, we shall look into how every single aspect of the bank's current ITSM aligns or clashes with that model as well as highlighting possible areas where changes can be made in order to shift to a more dynamic and response-oriented system on this basis.

#### 3.1. Existing ITSM Processes

Changing is a standard of ITIL 4, and the framework provides a set of guidelines established by the ITIL foundation so to manage changes with minimal friction or risks. With many changes happening at a very rapid pace, IT organizations need a structured way to integrate and deploy change to minimize obstructions and do it coherently avoiding organization silos where possible.

The bank adopts what ITIL at its core provides: faster/safer change processes so to guarantee continual change implementation, according to a series of steps, starting from requests for change (RFC), review and updates whenever authorized and applied, coordinating the right implementation. In this section, we'll delve more into the detail of the present ITSM processes applied, so to guarantee clarity and a good understanding of processes to the reader, so to better explain the rollout and implementation operations.

Such processes can be seen in Figure 4:

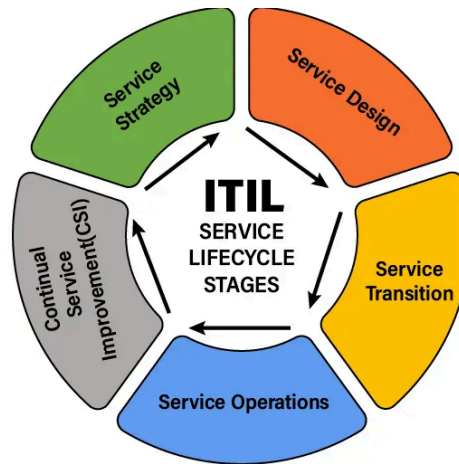


Figure 4: ITSM processes currently employed by the Bank

### 3.1.1. Service Strategy

The objective of this process is “decide on a strategy to serve customers and which types of services to offer them”. Beginning with an assessment of customer needs and the marketplace, the Service Strategy lifecycle stage identifies which services the IT organization should offer and the capabilities that need to be developed. Its ultimate goal is to ensure that the IT organization adopts a strategic mindset and approach.

In general, some positives might be found: close collaboration within units and managerial role is definitely a good thing, also having a well-maintained and accessible IT service catalogue. However, a significant gap exists in the informality of not keeping a service portfolio which can limit bank's ability to take informed choices as regards service investment as well as decommission.

Consequently, such a shortfall is a determinant of whether the Home Connectivity and USB Connectivity services should be closed down; given that nobody might have really known about their strategic value or lifecycle status. This also influences the limited detailed cost information available and insufficient data on service usage by customers, further reducing the value available and which can be given.

While customer relationships seem positive, there may be room to improve how the bank anticipates and influences service demand. The financial management of IT services happens at a high level, but more detailed cost information would be beneficial. Overall, the bank could benefit from a more structured approach to service strategy that better aligns IT capabilities with business needs.

### 3.1.2. Service Design

The goal of this process is to “design new services, as well as changes and improvements to existing ones”. In the context of the Bank, this stage plays a critical role in ensuring that IT services are aligned with business needs and are designed to be effective, efficient, and compliant with industry standards.

There are service level agreements (SLAs) in place, but negotiations were started during the design and extended into transition. This is a good practice but perhaps could have been developed with more thought, precision and processing. The bank is good at collaboration with third-party suppliers; it also has a back-up system for their continuity, but with the bank evolving into a global entity, the processes need further development, considering the vision of expansion.

Though there is no mentioning of capacity planning, and this is an area for which special attention needs to be paid. The bank does maintain a remote backup site for the critical services, which is good. It also has policies for service continuity and security, though probably these areas may need further emphasis due to international operations and the regulatory environment. The applications are either developed in-house or purchased and customized. This demonstrates some active management of suppliers. However, dependence on external suppliers and short-term staff can harm consistency and quality in the long term.

### **3.1.3. Service Transition**

The goal of this is to “build and deploy new or modified services”, ensuring changes are carried out in a coordinated way so to be prepared and exploit strengths and key points areas of improvement.

Six months ago, the bank released two updates to their standard desktop build within a very short time, which brought HQ staff to their knees. This may indicate some possible potential for process improvement in the area of release planning and coordination. Although the practice of software testing is mature, it is very focused on functionality. In the past, this has sometimes meant that new IT services have proven difficult to support following implementation. The bank deploys automated discovery tools for configuration management, but incident and problem teams reported this data as unhelpful for diagnosis, indicating that there may be a misalignment in data collection.

Knowledge management is very informal, though there is a formal plan on the books to communicate new policies. As the bank grows, more structured management of data and information will be increasingly important.

### **3.1.4. Service Operation**

It ensures that IT services are delivered effectively and efficiently. The bank’s current Service Operation practices show some strengths but also areas needing improvement.

The bank has a central operations control center in the HQ country, but some of the branch IT infrastructure is managed locally. There is a process supported by software for service request handling that is aligned to allow business users to order directly from the service catalogue. While the asset and risk management seem well-coordinated, the integration could still pose a challenge between teams and locations. The bank seems more focused on IT operations than in integrating the newly acquired companies—something that would call for some improvement.

There is no mention of any formal processes with regard to facilities management other than high-level control by units and branches. Units and departments apply management between them, having very close communication, but detailed information regarding management of the life cycle process is not available. Operations staff involved in traditional operations mostly concentrate on service operation activities. It is possible that such personnel could not be involved during the service design or transition stages and may thus lack the relevant perspective and effectiveness.

### **3.1.5. Continual Service Improvement**

This ensures usage of methods from quality management in order to learn from past successes and failures, aiming to continually improve effectiveness and efficiency of IT processes and services, adopting continual improvement line by ISO 20000 - Information Technology requirements.

A strong culture of improvement is present within the bank, and investment funding is available for a wide range of projects throughout the organization, including IT. Formal mechanisms for process evaluation and benchmarking are absent. A service improvement manager, reporting to a senior member of the service quality unit, oversees formal IT service improvement, but finds it difficult to get the staff to focus on service-level improvements.

There is nothing mentioned about periodic service reviews, which would work as a measure for consistency among the units in their operations. While the culture is supportive of improvement, more organized ways to determine, implement, and monitor the improvement initiatives can help in better placement for the bank to respond continuously by adapting and optimizing its IT services.

### **3.2. Limitations of current framework and bottlenecks**

The current framework, while providing a solid foundation for IT service management, definitely provides rigidity and not careful consideration on low-level processes, leading to silos between different stages, hindering the ability required in rapidly evolving environments. There is not a clear focus on value co-creation with customers, but rather a general vision of control between departments and units. The crucial vision should ensure more control for the bank's customer-centric strategy.

As the bank moves forward towards more dynamic and responsive, the current framework struggles to fully incorporate modern development technologies, to ensure a more reactive control, leading to recurring issues in service delivery. This is particularly evident by the missing formal, well-maintained service portfolio, effectively hindering strategic decision-making about service investments and retirements.

- Agile practices like Scrum or Kanban, which promote iterative development and continuous delivery, are not easily integrated into the more linear ITSM processes currently adopted.
- The framework doesn't adequately support the concepts of continuous integration and continuous delivery (CI/CD) that are central to DevOps practices and crucial for maintaining competitiveness in digital banking services.
- Processes here don't readily accommodate the "fail fast, learn quickly" approach advocated by Lean methodologies and while there is control between cross-functional/self-organizing teams, multifunctionality should be guaranteed in order to maintain values and competitiveness

The bank will appreciate the probable benefits that an ITIL 4 shift can bring to it by recognizing these limitations. Much of Agile is encapsulated while retaining the robust service management foundation of ITIL. This would mean that the bank will be able to move towards a more flexible and value-driven approach to the management of IT services, better equipped to handle the challenges brought forward by modern banking in a digital age.

### **3.3. Impact on overall IT service portfolio**

Limitations within the current framework of ITSM methodology have far-reaching effects on the IT service portfolio, thereby affecting delivery of value from the bank's information technology, the ability to innovate, and respond to changing market demands. In simple terms, this has bearing effects on the competitive position and operational efficiency of the bank, down to the smallest details of service management and delivery.

- First and foremost, a not properly managed service portfolio creates the big risk of misalignment of IT services against changing business needs, specifically when the methods are not properly formal. With the bank's geographical expansion, this has slowly become a problem. In the absence of a clear, up-to-date view of all services and their interdependencies, along with their strategic value, it is hard for the bank to make effective decisions related to investing in, maintaining, or retiring services. This may perpetuate obsolete or duplicative services, missing the opportunities to create new, value-added services that would really help drive competitiveness for the bank.
- Another critical issue is this lack of portfolio visibility, which can result in inefficient use of resources. Without an enterprise-wide view of services, the bank may be overinvesting in some areas and under-resourcing others. This sort of imbalance in the allocation of suboptimal performance across the portfolio implies that some services receive disproportionate attention and resources, while others, which are probably more strategically important, are relatively neglected. This can also mean that, with respect to the international expansion of the bank, the inconsistent quality of service across regions or business units impinges on the ability of the organization to put forward both a unified and high-quality service offering to its global customer base.
- The rigid lifecycle actually present significantly reduces the bank's ability in service management. The bank may find itself unable to quickly introduce new services or modify existing ones to meet emerging customer demands or capitalize on new technologies. The present siloed approach can result in inconsistent service quality across different areas of the portfolio, where each service may be managed according to slightly different standards or processes, leading to a more fragmented customer experience. Inconsistency can be particularly damaging to customer satisfaction and loyalty, specifically without a clear overview of services and their interdependencies. This can clearly increase complexity and identify opportunities, as well as be an obstacle to innovation and full leverage of technologies and methodologies.

Their cumulative effect will be a service portfolio that is, at best, stable but patently unfit to help drive the strategic objectives for which a bank will need to position itself vis-à-vis an increasingly digital and competitive landscape. The portfolio will be replete with antiquated and expensive services to maintain, have gaps in the ability to address the emerging needs of customers, and a general lack of agility in enabling the positioning of the bank as a leader in innovative banking services.

These impacts can only be addressed by deep change in how the bank approaches its IT service portfolio. This change can then be propelled toward a more flexible and value-driven framework, such as ITIL 4, encompassing Agile and DevOps practices to construct a more agile and responsive service portfolio for the bank. It would help the bank align IT services better with business strategy, innovate and deploy new services at much faster rates, and offer high-quality and customer-centric banking experiences with consistency across its global operations.

### **3.4. Rationale for decommissioning plan**

The link between what is present from the describe already applied ITSM processes and the following high-level descriptions and practices present in within the next chapter and subsections is given by the Service Transition. In this, building and decommissioning, may it be for test environments, infrastructures and facilities, is a documented procedure. When benefits are compelling, decommissioning might not be guaranteed: that's why a thorough process of "complete" decommissioning might further contribute to the success criteria of a project, including fine-grained control on project management practices and alike.

In ITIL 4, the IT Asset Management practice takes a more important role, emphasizing the entire lifecycle of assets from acquisition to disposal, since in order to be done effectively, this needs to revolve on the following steps:

- *Comprehensive inventory management*, so to accurately track all assets related to Home Connectivity and USB Connectivity services
- *Efficient resource allocation*, to allow for proper reallocation or disposal of assets freed by the decommissioning process, so to allow for good financial optimization and accurate valuation of assets, potentially being cost-saving and recovering from expenses during the decommissioning process
- *Compliance and risk management*, ensuring decommissioning adheres to regulatory requirements and minimizes risks associated with data security and asset disposal. This is also important on the front on environmental responsibility, so to allow for proper disposal and recycling of hardware in line with environmental regulations and corporate social responsibility social responsibility goals

The “complete” decommissioning process goes beyond merely turning off services, since a thorough assessment needs to be done on all associated assets, data and dependencies, so to ensure data integrity and security, continually meeting stakeholders expectations and facilitating smooth transitioning. Setting such detail and care in decommissioning means that the bank is not only assured of a smooth transition away from these services but also sets a very clear example of how, in the future, services reached the end of their life cycle in alignment with ITIL 4. It showcases the bank’s commitment to the continued improvement and strategic alignment of IT services with business goals.



## 4. ITIL 4 Framework

ITIL 4 is a framework for effective IT service management to help businesses adapt to the new digital era and create value through IT services. In transitioning from current IT service management practices, the Bank is adopting a more flexible and value-oriented approach, to incorporate:

- A shift from high-level processes to more fine-grained practices interacting with each other to ensure more flexibility and control
- Focusing on co-created value to emphasize such for all stakeholders, not just for service delivery
- Integration of Agile philosophy, to ensure and incorporate modern ways of working, possibly holistically to ensure a comprehensive view of service management

This transition aligns with our bank's need for greater agility and customer focus, particularly in the decommissioning of legacy services. By itself, the framework comprises two key elements: the four dimensions model and the Service Value System (SVS).

### 4.1. Four Dimensions of Service Management

The *four dimensions model* encompasses a *holistic* approach to service management. It includes the following dimensions:

1. *Organizations and people*: this dimension concerns the people involved in executing and managing the work, encompassing aspects such as culture, structure, skills, and adaptability to change. Organizations need to consider how people collaborate to create value within IT services.
  - This dimension is very important in the bank's case in managing the transition from the old connectivity services to the new Token Connectivity service by way of staff training, management of cultural changes, and the lining up of the IT and business units regarding the decommissioning process.
2. *Information and technology*: this dimension revolves around the technologies used in IT service management, including tools, knowledge, and the management of information generated, stored, and utilized by businesses about the IT services they offer. This dimension ensures that businesses effectively leverage information and technology to deliver valuable IT services.
  - Such dimension is particularly relevant since it transitions from hardware-based connectivity to a more flexible token-based system. This includes the management of the technological shift and how the old and new services are documented, with all relevant information available.
3. *Partners and suppliers*: concerns the relationships with other organizations involved in designing, developing, shipping, and improving services, including suppliers, business partners, external organizations, and other parties contributing to service provision.
  - For the bank, this dimension means managing relationships with existing service providers and potential new partners for the Token's connectivity service, which will play a vital role in the negotiation of contract terminations and a seamless transition.
4. *Value streams and processes*: the last dimension provides a comprehensive definition of all the activities, workflows, and processes necessary to improve business conditions. It also examines the various components of the business and their involvement in the value creation process.
  - The design of processes regarding this new connectivity service—a substitute for the old, which is eventually going to be phased out under this very same decommissioning project—ensures the new service seamlessly integrates into the bank's existing value streams.

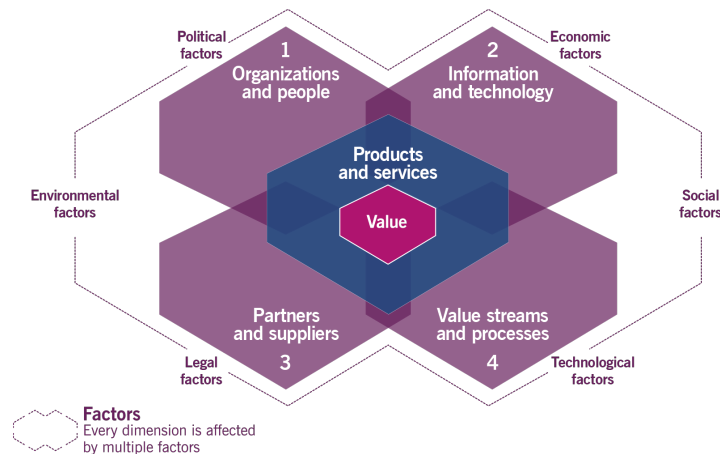


Figure 5: ITIL 4 Four dimensions

## 4.2. Service Value System (SVS)

The *Service Value System* includes everything needed to deliver value to customers by showing how all the components and activities of an organization work together to facilitate value creation. It consists of:

1. Guiding principles
2. Governance
3. Service value chain
4. Continual improvement
5. Practices

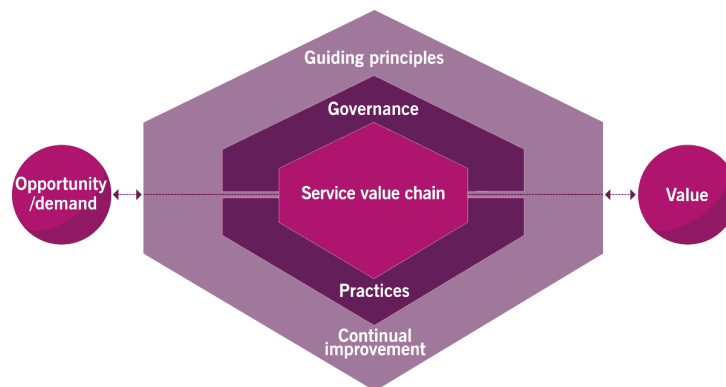


Figure 6: ITIL 4 Service Value System

Into the next sections, each will be explained with the right amount of detail, so to understand precisely how each will be applied for our use case.

### 4.2.1. Guiding Principles

The *guiding principles* in ITIL 4 are general recommendations that should guide an organization in all circumstances, regardless of changes to its goals, strategies, type of work, or management structure. They want to be universal and enduring, helping the organization to adopt and adapt ITIL guidance, supporting successful actions and good decisions at all levels.

Let's analyze one by one the relevance of each to the bank's decommissioning project are as follows:

1. *Focus on value*: All activities conducted by the bank should link back to value, emphasizing to what is delivered to customers and stakeholders. Every decision taken in the decommissioning process should be evaluated based on its contribution to overall value creation, ensuring the good transition when decommissioning from Home Connectivity and USB Connectivity, so to add value improving service quality, reducing costs or enhancing security.
2. *Start where you are*: Don't remove what was done in the past, but use it, encouraging good reuse of existing processes and assets as a foundation. This approach allows us to leverage existing knowledge and resources, making the transition more efficient, saving time and basing metrics on data already present, with the right amount of time and effort. For our decommissioning project, it's important to assess the current state of connectivity services, including their usage, costs and associated assets.
3. *Progress iteratively with feedback*: This principle suggests implementing changes incrementally and obtaining feedback at every step. We can apply this in our roadmap for decommissioning by simply phasing the cutovers. It's important to start from pilot group of users to be migrated to each connectivity service first, so to have a correct feedback loop at each stage to further tune our processes and iron out any issues before full-scale implementation.
4. *Collaborate and promote visibility*: Effective collaboration between different teams and stakeholders is crucial for the decommissioning project's success. It's important to ensure clear communication channels between IT, finance and user departments throughout all phases, accompanying them with regular updates and transparent reporting on the project's progress, helping maintaining stakeholder engagement and support. This helps in solving visibility problems, bottlenecks, uncover waste and ensuring better information is available for good decision making.
5. *Think and work holistically*: This principles reminds us to consider broader impact of the actions across the organization. While decommissioning these services, we must consider how it affects other IT services, user productivity and the bank's overall operations, retaining closer work between departments and ensuring smooth transition, aligning with the bank's holistic IT strategy. As a matter of fact, no service/practice/process stands alone, and outputs need to be coherent and integrated.
6. *Keep it simple and practical*: Simplicity is key in managing complex changes and it's important to use the minimum and necessary number of steps to accomplish an objective, producing solutions based on outcomes and stakeholders collaboration. Our program of decommissioning will be focused on those practical easy-to-implement and easy-to-understand steps. It's useful to avoid complications in the transition process, making the shift to different connectivity services as smooth as can be for IT staff and end-users alike.
7. *Optimize and automate*: Value of work carried out by human and technical resources means taking something and making it as effective as it can be while using technology consistently with frequent tasks so to make them faster. Finally, during the scope of this overall phase-out of Home Connectivity and USB Connectivity, we will also look to find some way of optimizing processes and automating these process flows. This could take the form of an automated inventory for retired assets, optimization of the user transition process, or having carried out monitoring for the new Token Connectivity Service to ensure its efficacy.

#### 4.2.2. Continual improvement

The ITIL continual improvement model allows to align an organization's practices and services with changing business needs, through assessment and improvement of every element involved in the management of products and services. It's useful to apply its series of principles applicable at every step, allowing guidance towards a successful decommissioning project.

It takes place in all areas of the organization and at all levels, from strategic to operational and to maximize the effectiveness of services, each person contributing to service provision should keep continual improvement in mind, increasing the likelihood of successful initiatives at all levels.



Figure 7: ITIL Continual Improvement Model

Let's analyze one by one the relevance of each to the bank's decommissioning project are as follows:

1. *What is the vision?* - The corporate vision is focused on expansion and to do this, targets were set in order to be achieved by the next financial year and measure step by step the advancements on operating. Decommissioning successfully decommission Home Connectivity and USB Connectivity services while transitioning users to Token Connectivity, improving overall service quality, reducing costs, and enhancing security is the key focus of the current.
  - The main goal is to successfully transition from legacy connectivity services to a more efficient, secure, and cost-effective solution that aligns with the bank's digital transformation strategy. This incorporates modernization of IT services, enhanced security posture, cost optimization and alignment with broader organization goals.
  - To achieve this, it's important to conduct stakeholder workshops to ensure alignment across departments, review the bank's strategic plans to ensure consistency and analyze current industry trends so to validate bank direction correctly. The vision will be clearly communicated to all levels within the organization, allowing each member to understand the intent and desired result of the decommissioning project.
2. *Where are we now?* -: Currently, there are 3000 users on Home Connectivity and 7000 users on USB connectivity. These services are costly to maintain and can pose some important security risks. In general, it's important to provide a thorough assessment of the current state, including asset inventory, user satisfaction levels and operational costs, with the help of precise metrics to reach such goals.

This entails a detailed assessment of our current state. This shall be done by gathering:

- Current pattern of usage of services provided by Home Connectivity and USB Connectivity
- Associated costs for supporting these services
- Security vulnerabilities inherent in these current systems
- User satisfaction with current services
- An inventory of all hardware and software assets related to these services
- All current contracts with service providers and their terms
- The current management and support processes of these services

This information will be gathered through the following tools and techniques:

- Audit of the asset management systems
- Analysis of the service costs by Financial Analysis
- Questionnaires or user surveys and interviews
- Security vulnerability assessments
- Process mapping exercises

This will give a benchmark with detail, providing the clear picture of our starting point, highlighting those areas of strength and bringing out the opportunities that are there to be made for improvement.

3. *Where do we want to be?* - The current goal is to have all users transitioned to Token Connectivity within 12 months, with monitored levels of user satisfaction, reduced operational costs, enhancing security measures in place between different position of the company.

From our vision and assessment of the current state, we will define specific, measurable objectives for our target future state. This can include the following:

- 100% decommissioning of Home Connectivity and USB Connectivity services within 18 months
- Migrate all users to the new Token Connectivity service
- Reduce connectivity-related IT costs by 25%
- Reduce security incidents related to remote connectivity by 50%
- Achieve 90% user satisfaction rate with the new connectivity solution
- Streamlined IT asset inventory with an accuracy rating of 99%
- Compliance with relevant data protection and financial regulations

We would view these objectives as *SMART* — *Specific, Measurable, Achievable, Relevant, and Time-bound* — to achieve the Bank's foreseen vision and organizational strategy.

4. *How do we get there?* - This step requires the development of a detailed roadmap for the decommissioning plan including steps like:
  - Asset inventory and disposal plan, conducting risk assessment and mitigation strategies
  - Resource allocation plan (human, financial, and technological) and prepared change management/communication plans

- Phased rollout of Token Connectivity, with detailed project timeline and key milestones to be reached so to achieve baselines
  - Supplier contract management and termination process
  - Procurement plan for any new hardware or software required
  - Security and compliance measures, including training programs for IT staff and end-users and contingency plans for potential issues
5. *Take action* - We will execute our plan in phases, starting with a pilot group and gradually expanding to all users. Each phase will include:
- Initiate decommissioning of Home Connectivity and USB Connectivity services
  - Deployment of a new Token Connectivity service—phase-wise implementation
  - User training programs
  - Change management and communication plans execution
  - Progress tracking against the project timeline and KPIs
  - Regular review with stakeholders and feedback sessions
  - Risk monitoring and mitigation on a continuous cycle
  - Plan adjustment as required based on real-time feedback and results

In that respect, a Project Management Office needs to be established to manage the Implementation phase. It will coordinate across all work-streams, guaranteeing that decisions are made on time.

6. *Did we get there?* - In this step, it's important to continuously monitor progress against defined KPIs and CSFs, including regular assessments:
- User satisfaction surveys
  - Cost reduction metrics
  - Security incident reports
  - Financial analysis to verify cost savings
  - Security audits to confirm improved risk posture
  - Asset disposal efficiency and review of asset inventory accuracy
  - Compliance checks against regulatory requirements

For this step, it's important to provide a comparison report between what we have achieved and what was set out in our original objectives, along with how far the Bank is in relation to them.

7. *How do we keep the momentum going?* - In this step, ongoing review processes are to be included, like:
- Monthly project team meetings
  - Quarterly stakeholder reviews
  - Annual comprehensive assessments
  - Regular review cycles for IT services and processes, establishing ongoing monitoring processes and created new knowledge base of lessons learned from the decommissioning project

- Setting up suggestion schemes for continuous improvement ideas from staff, developing roadmaps for future IT service improvements, ensuring continual improvements in IT service management processes

In this step, establish a Continual Improvement Register (CIR) to monitor and track various continual improvement initiatives across the IT department is fundamental.

These seven steps, when applied meticulously, set the foundation for a structured and all-rounded approach to our improvement initiative. This methodology is going to help us see our way through the decommissioning of services like Home Connectivity and USB Connectivity and provide a framework for continual improvement in our IT service management practices.

#### 4.2.3. Service Value Chain (SVC)

Among others, the *Service Value Chain* is an important component of the SVS that provides flexible operating models for the creation, delivery, and continual improvement of services. As shown in Figure 8, the SVC is composed of *six activities*:

1. Plan
2. Improve
3. Engage
4. Design and Transition
5. Obtain/Build
6. Deliver and Support

These activities transform inputs into outputs, allowing the organization to create value by following each step of the SVC.

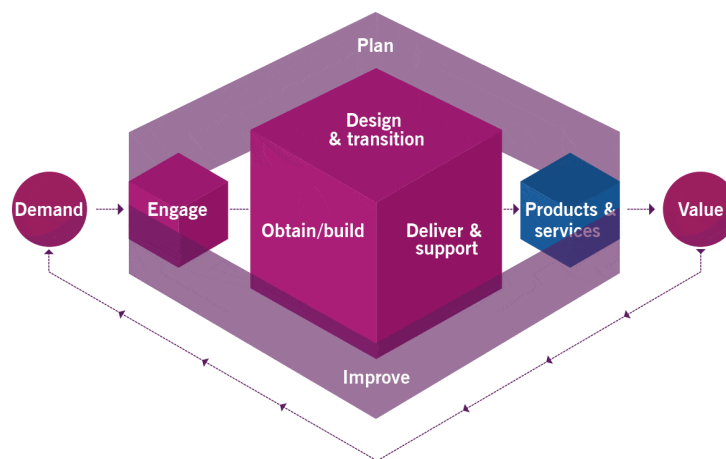


Figure 8: ITIL 4 Service Value Chain

Now, in the context of the bank's decommissioning project, SVC activities may apply as follows:

- *Plan*: This activity involves the development of a decommissioning plan that includes objectives, scope, timeline to follow, resources required, and key stakeholders involved in the decommissioning process. By going into more detail, the objectives and success criteria are established, along with all necessary steps to achieve the goal, after a thorough analysis of the assets to be decommissioned, the cybersecurity policies, requirements, and constraints of the organization

- *Improve*: Based on the information provided about the inefficiencies and issues, discussed in Section 2.5, associated with the *Home Connectivity* and the *USB Connectivity* services, as well as the opportunities for improvement that align with the bank's vision that is focused on expansion, this activity produces improvement initiatives as the decommissioning of the services listed above. The decommissioning proposal will then be passed on to the unit responsible for planning to be reviewed
- *Engage*: This activity is applied to communicate with internal stakeholders and third-party suppliers information regarding the decommissioning process and its potential impact on their timelines and contractual agreements. Keeping stakeholders involved during the decommissioning by providing updates and gathering their opinions ensures that the outcome of the decommissioning process is aligned with their expectations. Additionally, clear communication with third-party suppliers helps to maintain positive relationships for future collaborations and a smooth transition to the new services
- *Design and Transition*: This activity takes the outputs of the previous activities that outlined the decommissioning process, such as the timeline, policy compliance, and improvements to services, and transforms them into requirements and specifications including detailed procedures for decommissioning activities, like data migration, hardware removal, and software deactivation, and ensuring that contract and agreement requirements for the third-party providers are accurate to be then communicated
- *Obtain/Build*: This activity is employed to ensure that all the necessary components for the assets replaced during decommissioning are available and meet the agreed specifications. It also ensures that the required approvals and permissions are granted and through procurement and supplier management that all the necessary resources are available when needed
- *Deliver and Support*: The purpose of this activity is to ensure that services are delivered and supported according to agreed specifications and stakeholders' expectations. It involves following each step of the decommissioning plan and providing support during the transition by monitoring the process and handling any issues that may arise

#### 4.2.4. Practices involved in the scenario

ITIL 4 comprises 34 *management practices* aimed at *helping organizations deliver effective service across the value chain*. These practices are defined as “sets of organizational resources designed for performing work or accomplishing an objective”.

They will be applied into the relevant chapter of rollout implementation, each described in further detail. They are divided into three *categories* as follows:

- *General management* practices: these apply across the organization to ensure the success of the business and the services it offers
- *Service management* practices: these are specific to the development, deployment, delivery, and support of particular services
- *Technical management* practices: they are adapted from technology management domains for service management



Of the 34 practices included in ITIL 4 the ones we are going to use in our scenario are the following, considering all discussed categories:

1. *General management practices:*

- *Architecture Management:* the purpose of this practice is to provide an understanding of all the various components that form an organization and how these components are interconnected. This allows the organization to accomplish its current and future objectives. Architecture management practice provides the principles, standards, and tools that allow an organization to handle complex change in a structured and Agile way.
  - We use it in our scenario to review and update the IT architecture following decommissioning and ensure its alignment with future objectives.
- *Continual Improvement:* the aim of the continual improvement practice is ensuring that an organization's practices and services keep pace with the evolving business needs through the ongoing improvement of products, services, and practices, or any element involved in the management of products and services.
  - In the bank context, this practice recognizes the decommissioning process as a means of improvement employed to align with the current business needs.
- *Information Security Management:* the purpose of this practice is to protect all the information necessary for the organization to conduct its operations. This includes understanding and managing risks to the confidentiality, integrity, and accessibility of information, along with other elements of information security such as authentication and non-repudiation.
  - This practice in our case ensures the security of data, respecting proper data destruction protocols, and compliance with security policies throughout the asset decommissioning process.
- *Knowledge Management:* this practice aims to maintain and improve the effective, efficient, and convenient use of information and knowledge across the organization. Knowledge is one of the most valuable assets of an organization thus this practice provides a structured approach to defining, building, re-using, and sharing knowledge in various forms.
  - In our scenario, it is used to document and share the knowledge gained during the decommissioning to ensure that stakeholders get the right information, in the proper format, at the right level, and at the correct time, according to their access level and other relevant policies.
- *Risk Management:* this practice's aim is to ensure that the organization understands and effectively deals with risks. Managing risk is crucial to guarantee the ongoing sustainability of an organization and add value for its customers. Risk management is an essential part of all organizational activities and is therefore central to the organization's SVS.
  - We utilize it in our scenario because innovation is inherently risky but could provide major benefits in improving products and services, thus our aim is to make an accurate assessment of the risks associated with the decommissioning of assets, develop mitigation strategies and monitor the risk impact.
- *Service Financial Management:* this practice supports decision-making by the governing body and management of the organization regarding how to allocate financial resources effectively. It offers insight into budgeting, costing, and accounting activities related to the products and services.

- In our context, it is useful to analyze costs associated with decommissioning and manage budget allocations thus all the financial implications originated from the change.
- *Strategy Management*: The objectives of this practice are to formulate the goals of the organization and adopt the courses of action and allocation of resources necessary for achieving those goals. Strategy management establishes the organization's direction, focuses effort, defines or clarifies the organization's priorities, and provides consistency or guidance in response to the environment
  - In our context is used to define and plan the strategy for the decommissioning plan by directing the change to be aligned with the bank's focus.
- *Supplier Management*: the purpose of this practice is to ensure that the organization effectively manages its suppliers and their performance to facilitate the seamless delivery of high-quality products and services. This includes developing closer, more collaborative relationships with key suppliers to realize new value and reduce the risk of failure.
  - The application of this practice concerns the management of the relationships with the suppliers involved in providing the necessary services and ensuring contractual obligations are met during decommissioning.

2. *Service management practices*:

- *Change Control*: this practice aims to increase the number of successful service and product changes by thoroughly assessing risks, approving changes, and managing the change schedule. The scope of change control is defined by the organization. It includes all IT infrastructure, applications, documentation, processes, supplier relationships, and anything else that might directly or indirectly impact a product or service.
  - Change control is used in our case to oversee the decommissioning process, ensuring that it is planned, approved, and executed accurately.
- *IT Asset Management*: the aim of this practice is to plan and manage the entire lifecycle of all IT assets. This helps the organization maximize value, control its costs, manage risks, support all the decisions regarding asset purchase, re-use, retirement, and disposal, and comply with regulatory and contractual requirements.
  - In our scenario, it is used to track and manage the assets decommissioned by updating their records and ensuring their proper disposal
- *Monitoring and Event Management*: the goal of the monitoring and event management practice is to systematically observe services and service components, as well as recording and reporting selected changes of state identified as events. This practice helps to identify and prioritize infrastructure, services, business processes, and information security events, and to establish the proper response to those events.
  - We use it to monitor the decommissioning process in order to identify and address any issues in real time and ensure that any event or incident that may arise during the decommissioning process is managed correctly.
- *Problem Management*: this practice wants to reduce the occurrence and impact of incidents through the identification of their actual and potential causes and managing workarounds and known errors.
  - Problem management in our context is used to analyze and prevent the issues related to the decommissioning process.

- *Release Management*: release management practice aims to ensure that new and updated services and features are ready and available for use.
  - This practice is used in our scenario to manage the decommissioning of assets ensuring that the changes are correctly executed and validated.
- *Service Configuration Management*: the purpose of this practice is to ensure that accurate and reliable information about the configuration of services, and the supporting configuration items, is always available in case of need. It includes details about how CIs are set up and the connections between them
  - In the bank context this practice is used to guarantee that all the records about the configuration items being decommissioned are updated and accurate
- *Service Level Management*: the aim of the service level management practice is to establish business-based objectives for service levels and to ensure that service delivery is properly assessed, monitored, and managed in accordance with these objectives.
  - In our scenario, this practice is used to update the service level agreements, a document agreement between a service provider and a customer that specifies services required and expected level of service, or create new ones based on the decommissioning and then ensure that the service performance targets align with the new state.
- *Service Validation and Testing*: the purpose of the service validation and testing practice is to ensure that new or changed products and services meet defined requirements. The service validation focuses on establishing deployment and release management requirements which are then verified through testing.
  - In our case, this practice is used to verify and test through quality and performance indicators that all the changes related to the decommissioning meet the requirements defined.
- *Service Desk*: the purpose of this practice is to capture demand for incidents, resolving them and provide pronto assistance for service requests. This is to be intended as a clear path for users to report problems, classifying them and possibly automating contacts and resolution, as part of any service operation.
  - In the bank scenario, this is used to provide better focus and support for technical issues, everyday problems met by users and also employees, better responding to their own needs.

### 3. *Technical management practices*:

- *Deployment Management*: this practice aims to push new or changed hardware, software, documentation, processes, or any other component to live environments. It is also used when deploying components to other environments for testing or staging purposes.
  - In the bank scenario, it is used to move the hardware changed to live scenario once it has been tested.
- *Infrastructure and Platform Management*: infrastructure and platform management practice aim to manage infrastructure and platforms used by an organization, as well as to monitor the technology solutions available, including those provided by external service providers.
  - It is used in our case to ensure that the underlying infrastructure and platforms are properly managed during the decommissioning process.

## 5. Decommissioning plan

To effectively decommission Home Connectivity and USB Connectivity services an effective plan should be designed considering different factors such as the value of IT assets, ongoing agreements and obligations with third-party suppliers, security policies, impact assessment plans and all pertinent analysis before decommissioning the services.

ITIL 4 provides a practice, named “IT Asset Management”, that manages the lifecycle of all IT assets for an organization, so any financially valuable component that can contribute to the delivery of an IT product or service. A definition of this practice is reported here to highlight the key message of this practice:

- “The purpose of the IT asset management practice is to plan and manage the full lifecycle of all IT assets, to help the organization: maximize value; control costs; manage risks; support decision-making about purchase, re-use, retirement, and disposal of assets; meet regulatory and contractual requirements.”

Considering that the IT Asset Management practice is strictly related to the purpose of this document, the whole decommissioning plan should be based on the practice purposes and obviously considering all other relevant elements of ITIL 4 framework.

The decommissioning plan should be assigned to the IT department which can follow the entire process, from the planning to service implementation and even the future improvements, in collaboration with the Finance Department to merge the strengths of both departments to identify a plan that minimizes the costs sustained by the bank.

According to what was discussed, the decommissioning plan can be characterized by the following high-level steps:

1. Identify and inventory IT Assets
2. Assess the current costs associated with maintaining these services and potential savings from decommissioning
3. Evaluate disposal and decommissioning options
4. Communication with stakeholders
5. Transition to new services
6. Monitor and verify IT asset disposal and decommissioning
7. Update and optimize IT asset lifecycle management

### 5.1. Identify and inventory IT Assets

Before analyzing any possible decommissioning plan, an inventory of all IT assets related to the services to be decommissioned should be formalized. In fact, IT asset management practice requires accurate inventory information, which it keeps in an asset register that can be a database or list of assets, capturing key attributes such as ownership and financial value.

This information can be gathered in an audit, but it is much better to capture it as part of the processes that change the status of assets, for example, when new hardware is delivered or decommissioned as in this scenario. The idea is to use the asset register to interact with other practices such as service configuration management, incident management, change control, and deployment management in a way that asset status information can be maintained with less effort.

As discussed before, the bank wants to decommission two services: Home Connectivity and USB Connectivity, so it is fundamental to provide an asset register for both services to identify all the

components that make those services valuable. It follows the asset register that describes both services where every asset is characterized by the following fields:

- *Asset ID*: a unique identifier for that asset
- *Asset Description*: a short description of the asset
- *Ownership*: the owner of the asset. Here the bank owns all of these assets, though they are provided and supported by third-party suppliers
- *Financial Value*: the cost associated with each asset, which is important for financial reconciliation post-decommissioning
- *Acquisition Date*: acquisition date of that asset. Note that acquisition dates vary as users may have joined the services at different times. Keeping track of these dates is important for understanding the lifecycle of the assets
- *Supplier*: the suppliers involved help manage the termination process and ensure compliance with contractual obligations
- *Contract End Date*: This helps in planning the decommissioning process in alignment with contract terms to avoid penalties
- *Notes*: Additional notes provide context and details for each asset, ensuring clarity during the reading process

As additional notes to the reader, explanation of acronyms pertinent to the context of the following tables:

- N/A = Not Applicable
- ISP = Internet Service Provider
- HC = Home Connectivity (followed by a progressive number)
- USB = USB Connectivity (followed by a progressive number)

Asset ID	Description	Ownership	Financial Value	Acquisition Date	Supplier	Contract End Date	Notes
HC001	Desktop Hardware	Bank	\$800.45 per unit	2023-01-15	Supplier A	N/A	200 units deployed to users
HC002	Desktop Support	Bank	\$45.95 per month	2023-01-15	Supplier A	End of notice period	Monthly support service
HC003	Central DSL Connection	Bank	\$12,604 yearly	2023-01-15	ISP B	End of notice period	Central connection for service
HC004	Internet Subscription	Bank	\$46.15 per user/month	Various (3000 users)	ISP B	End of notice period	Monthly subscription per user
HC005	Installation Fee	Bank	\$110 per installation	Various (3000 users)	ISP B	N/A	One-time installation fee
HC006	VoIP Telephone Set	Bank	\$100.83	2023-06-01	Supplier C	N/A	Deployed to CCA Home Connectivity users

Table 1: Home Connectivity Service Assets

Asset ID	Asset Description	Ownership	Financial Value	Acquisition Date	Supplier	Contract End Date	Notes
USB001	USB Token	Bank	\$0 (free)	2023-02-10	Supplier D	N/A	Provided free of charge
USB002	Internet Subscription	Bank	\$28.39 per user/month	Various (7000 users)	ISP E	End of notice period	Monthly subscription per user

Table 2: USB Connectivity Service Assets

As we can see in Table 1 and Table 2, the assets are categorized by connectivity type, to make easier the visualization and comprehension of assets and relevant information.

## 5.2. Costs assessment

Through the asset register, is possible to observe the current costs of the assets that shape Home Connectivity and USB Connectivity services. Before taking any decision, it is fundamental to assess the current costs associated with keeping these services and potential savings from decommissioning. Since the transition to the new IT Service Token Connectivity will lead the bank to spend zero leaving the internet subscription to the users, it is convenient to decommission all the IT assets that characterized the old services.

A careful focus needs to be done on the ongoing agreements with third-party suppliers who distribute and maintain the IT assets. It is important to consider any outstanding payments with suppliers, understanding the bank obligations and the actual expiration of the contracts. After doing that analysis the bank will have more information to effectively plan the dismissal of IT assets at the minimum possible cost, considering both hardware and contracts. This analysis should be conducted in collaboration with the Finance Department of the bank who can contribute positively to identify the most convenient plan for the bank.

## 5.3. Evaluate disposal and decommissioning options

The decommissioning of Home Connectivity and USB Connectivity services at the bank requires a *careful evaluation of the different options for disposing of and decommissioning IT assets*. This process must balance business needs, budget constraints, and organizational policies with considerations for security management, compliance, and environmental impact. By aligning with ITIL 4 framework principles, the bank can ensure a value-focused, collaborative, and compliant decommissioning process.

The bank has several options for disposing of and decommissioning IT assets:

1. *Selling Assets*: generating revenue from the sale of decommissioned hardware can offset some of the costs associated with the new services or recover some expenses sustained for the old services. Selling assets can be particularly advantageous if the equipment is still in good working condition and has market value. Anyway, the process requires identifying buyers, negotiating prices, and ensuring that the sale does not violate any contractual agreements with suppliers. So, a specific analysis should be performed before selling assets.
2. *Assets*: donating hardware to educational institutions or non-profit organizations supports social causes and enhances the bank's corporate social responsibility (CSR) profile.
3. *Destroying Assets*: physical destruction ensures that all data is irretrievably destroyed, providing the highest level of data security. This method is often used for obsolete or non-functional equipment.

Every strategy must ensure that all the data is destroyed to avoid possible data breaches. The bank must ensure that all data stored on decommissioned hardware is securely erased following the bank's data destruction policy and regulatory requirements. Using certified data destruction methods and documenting the process ensures compliance and mitigates the risk of data breaches. All access credentials and permissions associated with the decommissioned services must be revoked to prevent unauthorized access. This includes disabling user accounts, revoking VPN access, and ensuring that no residual access remains on any network or system.

In order to make the right decision, the bank should consider the recommendation of some of the guiding principles that ITIL 4 provides. In fact, first of all, it is fundamental to focus on value but not just considering the financial impact but the broader value that the decision can bring. For instance, deciding to donate the assets can improve the bank's CSR profile, promoting a positive brand image and helping the bank with its plan of expansions, helping so in reaching a wider

number of customers as planned by the bank. A good advice is also to start where you are. The bank should consider and eventually leverage existing processes and relationships with vendors and stakeholders to simplify the decommissioning of services, both in terms of costs and time analysis.

#### 5.4. Communication with stakeholders

One of the key principles of organization and people dimension is to ensure that *communication systems are well defined and support the organization overall strategy*. Communication takes a crucial role in effective decision making and change management as in this case.

To ensure a smooth transition during the decommissioning of the Home Connectivity and USB Connectivity services, effective communication with both internal stakeholders and third-party suppliers is paramount. For internal stakeholders, particularly the employees using these services, it's essential to clearly inform them about the decommissioning plan, timelines, and available alternatives such as Token Connectivity. Transparency in communication builds trust and reduces resistance, while engaging employees in the transition process fosters their participation and support.

For third-party suppliers, notifying them about the service termination as per contractual agreements and documenting all communications is vital. Adhering to notice periods and maintaining clear documentation ensures compliance with contractual obligations and avoids penalties.

Collaborating closely with suppliers facilitates a coordinated transition and ensures that alternative services are in place before fully decommissioning the current services. Professional and respectful communication helps maintain positive relationships with suppliers for future collaborations and supports effective change management in line with the ITIL 4 framework's principles of focusing on value, starting where you are, collaborating, and promoting visibility.

#### 5.5. Transition to new services

Before effectively decommissioning the old services, it is *fundamental to plan a smooth transition from the old services to the new ones*. If the old services are decommissioned before the new ones become available this can create a period of turbulence due to the lack of services and methods to conduct the bank daily work.

The transition from the Home Connectivity and USB Connectivity services to the new Token Connectivity service at the bank requires a strategic approach that emphasizes continuous involvement of internal customers, as guided by the ITIL 4 framework. Despite internal customers' willingness to participate in IT service design, their engagement often decreases once the specifications are set, leading to challenges in service implementation.

To address this, it is crucial to establish a collaborative and iterative transition process, where customers are consistently updated and involved through regular communication and feedback loops. This approach aligns with ITIL 4 principles of "progress iteratively with feedback" and "collaborate and promote visibility", ensuring that any issues are promptly addressed, and adjustments made as needed.

Additionally, incorporating comprehensive training and support sessions can ease the transition, fostering customer confidence and satisfaction. By maintaining transparency and fostering a culture of continuous engagement, the bank can ensure a smoother transition to the new service, delivering new value to its customers.

After completing the transition process listening to feedback and involving customers during its definition, the old services, both Home Connectivity and USB Connectivity, can be decommissioned and the new Token Connectivity service can be released and delivered.



## 5.6. Monitor and verify IT asset disposal and decommissioning

Once the IT assets belonging to old services are effectively decommissioned, it is important to *make sure that everything proceeds well along the way*.

To ensure the effective disposal and decommissioning of IT assets, specific processes of monitoring and verification should be implemented and used during the decommission of the services. This aligns with the monitoring and event management practice of the ITIL 4 framework, which provides a structured approach to oversee the status and movement of IT assets. Utilizing advanced tools such as GPS, RFID, or blockchain, the bank can track and document each asset's journey from decommissioning to final disposal. These tools offer real-time visibility and enhanced security, ensuring that the assets are handled according to predefined specifications and standards.

Receiving and reviewing detailed reports and certificates from vendors or partners is essential to confirm compliance. These documents should verify that the IT assets have been disposed of or decommissioned as per the bank's requirements. To maintain accuracy and quality, the bank must audit and inspect these reports and certificates regularly.

This process includes cross-referencing the documented data with actual asset movements and ensuring that all regulatory and policy standards are met. Any discrepancies or issues identified during audits should be promptly reported and addressed. This not only ensures compliance but also enhances the overall integrity of the decommissioning process. By integrating ITIL 4's monitoring and event management practice, the bank can create a robust system for asset tracking and verification. This approach not only mitigates risks associated with asset disposal but also provides a comprehensive audit trail, reinforcing accountability and transparency.

## 5.7. Update and optimize IT asset lifecycle management

The *final step* in the IT asset disposal and decommissioning process is to update and optimize IT asset lifecycle management. This involves a comprehensive update of the IT asset inventory and records to accurately reflect the changes and outcomes from the disposal and decommissioning activities. Each asset's status, from decommissioning to final disposal, should be meticulously documented, ensuring that the inventory remains up-to-date and precise. This not only provides a clear audit trail but also supports effective asset tracking and management.

In addition to updating records, it is crucial to analyze and evaluate the performance and results of the decommissioning process. This involves a thorough assessment of the entire procedure, identifying strengths, weaknesses, opportunities, and threats. Opportunities for improvement should be explored, leveraging insights gained during the decommissioning process. This might include adopting new technologies or methodologies that can enhance efficiency and security.

Feedback and insights gathered during the decommissioning process are invaluable for driving continuous improvement. Utilizing this feedback, the bank can refine and optimize its IT asset lifecycle management. This aligns with the ITIL 4 guiding principle of continual improvement, which advocates for the ongoing enhancement of processes, tools, and skills.

## 6. Rollout plan

The following chapter and sections present in greater detail the rollout plan and the implementation of each process designed in the previous phases and discussions, taking into consideration how processes will be introduced and how they will be achieved and activated. This is designed to be a comprehensive, phased approach aligning with ITIL 4 principles and the bank's strategic goals. The plan aims to minimize disruption to ongoing operations, while ensuring a smooth transition to the new service model.

To give more context over the actual solution, it's important to use multiple steps and investigations, so to further specialize the solution and make it general when decomposed in processes able to actually solve the decommissioning. This is to be done with the careful establishment of goals, coordinated by the administrative units and intents clearly respecting the overall vision statements and objectives established and assessed, which need to be respected using metrics like KPIs reported inside of SLAs, to be according to change schedules and timing/economic constraints.

### 6.1. Description of the approach

Central to this plan is the application of ITIL 4's Guiding Principles, informing every stage of the decommissioning process in a careful and guided way. Also, the SVC is used as an operating model to ensure the Bank maintains its focus on delivering value to customers, effectively managing its IT services.

The plan is divided into *several phases*, each addressing specific aspects of the decommissioning process. These include initial assessment and planning, stakeholder engagement and communication, service transition design, implementation and post-implementation review. Throughout these phases, a variety of ITIL practices are employed so to ensure clear establishment and control across processes. A critical component here is the establishment of clear governance structure and decision-making processes, with the help of structure able to construct and define clearly roles and responsibilities, setting up steering committees and establishing escalation procedures. These governance mechanisms will ensure that the decommissioning process remains aligned with the bank's overall strategy and that any issues or risks are promptly addressed.

Moreover, the plan incorporates robust approaches toward risk management in terms of identifying, assessing, and controlling possible risks associated with the decommissioning of these services. This involves the creation of contingency plans and ensuring that there are enough resources in place to handle any unforeseen challenges that may crop up along the way.

The success of the associated rollout plan will be substantiated upon the attainment of properly defined KPIs and CSFs: it will enable the periodic monitoring of realization and ensure changes can be implemented on time. The approach is based squarely on ITIL 4's principle of continual improvement, which underpins the fact that the process of decommissioning is on course towards objective realization.

In the next sections, the specifics of each of the phases of the rollout plan will be examined in more detail, outlining key activities, timelines, and resources required for successful implementation. It is with this comprehensive, structured approach that the bank can stand up to the complexities of decommissioning these services in a way that minimizes disruption and maximizes value for all stakeholders involved.

## 6.2. Implementation of the approach

The *implementation strategy* is designed to be both comprehensive and flexible, recognizing that decommissioning these services will impact various facets of our organization. That's why the approach is structured considering one by one the working in parallel around the different value chain activities to ensure a focus on value creation. Governance and risk management are key to this part: that's why, for each practice employed, we foresee the formation of steering committees to oversee and ensure a good governance structure crucial in navigating a highly regulated banking environment.

Moreover, our approach to the implementation embeds robust performance measurement using carefully defined KPIs and CSFs. Such metrics will aid tracking not only in its progress but also in making data-driven decisions and adjustments along this process of decommissioning.

In the following sections, we will outline in finer detail key activities, timelines, and resources required to undertake each phase of our proposed implementation. This level of detail will give all stakeholders a clear roadmap for the effective execution of our decommissioning strategy, articulating what is expected of them in this important transition. By adopting this disciplined, yet flexible, implementation methodology, we aim to ensure that the retirement of the Home Connectivity and USB Connectivity services is a success in terms of minimizing business disruption while maximizing value for the organization and its customers.

The order of application is *not linear*; each SVC activity is to be applied into the timeline section, establishing the correct order of action, ensuring coherence with the line described within the ITIL 4 chapter.

- Each key activity considered for each SVC activity and for each practice has relevant inputs and outputs not strictly related to the SVC activity considered but multiple ones at a time; whenever key activities are specified, they are written in a way to make it relatable to that specific SVC activity.
- For instance, for each practice there will be different key activities named as "Plan", in this case it is clear the key activity plan is an output of the plan SVC activity and not an activity performed strictly for that context.

Such specification makes sense in the ITIL context, so to create a value stream, based on the following:

- structure of the organization
- the team involved
- competences
- organizational culture

When creating a Value Stream within the SVC as base, recognizes the stakeholders involved and the activities and practices so to recognize needs and then generating value at each step.

### 6.2.1. Plan

The purpose of the *Plan* value chain activity is to ensure a shared understanding of the vision, current status, and improvement direction for all four dimensions and all products and services across the organization. Using the following ITIL4 practices and applying them to the plan activity, will ensure that the decommissioning process conveys the bank's vision, current status, and improvement direction for all four dimensions and all products and services across the organization.

The *inputs* necessary for the realization of this activity are the following:

- The policies, requirements, and constraints provided by the organization's governing body
- The consolidated demands and opportunities provided by "Engage"
- Performance information from the value chain, improvement status reports, and improvement initiatives from "Improve"
- Knowledge and information about new and changed products and services from "Design and Transition", and "Obtain/Build"
- Knowledge and information about third-party service components from "Engage"

These inputs will then be processed to produce the following *outputs*:

- Strategic, tactical, and operational plans
- Make portfolio decisions for "Design and Transition"
- Develop architectures and policies for "Design and Transition"
- Identify improvement opportunities for "Improve"
- Manage a product and service portfolio for "Engage"
- Address contract and agreement requirements for "Engage"

#### **6.2.1.1. Architecture Management**

In the decommissioning process, the *Architecture Management* practice is used as a basis for all the plan value chain activity. It is responsible for developing the new reference architecture for the IT Service Token Connectivity service they are going to implement and dismissing USB Connectivity and Home Connectivity service's architectures. More in depth it considers the *environmental architecture* that describes what influences impacted the organization and the change it implied after the merging with the U.S. based company as a consequence of the bank's focus on expansion and globalization.

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of current architecture*
  - All the components related to the USB Connectivity and Home Connectivity services have to be identified and recorded. A map has to be created with all the dependencies between the components and how they interact with the system. This activity is necessary to assess what part of the architecture is going to be involved in the changes from the decommissioning process.
  - The unit responsible for this activity is the *Operation Management Unit* which is responsible for the operation of IT infrastructure. This unit also includes the technical management team responsible for developing and supporting the IT infrastructure.
- *Define Target Architecture Model*
  - The organization's architecture should be optimized to achieve and support its strategy. This requires a new target architecture model that considers the environmental architecture, integrating the influences from the merging with the U.S. based company, and that aligns the organization's vision and strategic goals of expansion and globalization through the introduction of the new IT Service Token Connectivity service and the removal of USB and Home Connectivity services from the architecture.

- The *IT Strategy Unity* is responsible for the planning thus it will be in charge of this activity with the support where needed from the Application and Service Implementation Units. This activity will also involve the Global Banking Division and Security Division for compliance and ensuring the new model adheres to legislation. The CIO will then supervise this activity to ensure the target architecture model is aligned with the organization's goals.
- *Gap Analysis*
  - This activity consists of analyzing the differences between the current and target architectures to understand what changes are required to the technologies, information, people, and partners to cover the gap, assess their potential impact and define the starting point for the decommissioning.
  - The *IT Strategy Unit* will be assigned to this activity because it is responsible of developing and maintaining the IT strategy and planning. Thus this unit has the capacity to conduct a throughout gap analysis with the support if needed of Applications and Operational Management Units that may have a deeper knowledge and understanding of the applications, their dependencies, and operational gaps relative to the new architecture.
- *Documentation and Communication*
  - All the changes planned have to be reported to other divisions, thus it is necessary to maintain detailed and accurate documentation of the new target architecture highlighting all the major changes and the focus points. Then a communication plan is developed to inform all the relevant stakeholders and third-party providers about the changes, the implications and the expected outcomes.
  - The *IT Strategy Unit* is entrusted with this activity to manage the production of accurate and detailed documentation regarding the decommissioning plan. It also involves the *Marketing* and *Shared Services* divisions that respectively handle the communication with the stakeholders and the sharing of the documentation to the relevant teams through the HR and Facilities departments.
- *Compliance*
  - To proceed with the decommissioning it is necessary to ensure the compliance of the new target architecture with the relevant regulations, standards, and the organization's practices, so this activity is crucial to verify that the implementation of the new architecture adheres to the bank's vision while complying to their policies, requirements, and constraints.
  - The responsible for this activity is the *Security Division* with the help of *Operations Management* and *Service Implementation* Units. The Security division is assigned because it is responsible for the bank's security policy and adherence to legislation of the target architecture. The other units will support the Security Division with their knowledge of the services to identify where possible issues may be found.
- *Resource Allocation*
  - This activity is used to determine the resources required to implement the new target architecture, including the organization of the personnel and the technologies. Then a plan is produced containing how these resources are used throughout the decommissioning process.
  - Assigned to this activity is the *HR Department* to ensure the right human resources are determined and the *Finance Department* for the budget allocation. The *IT Strategy Unit* and *Applications Unit* may support the other departments with the understanding of the capabilities required and the financial planning.

### 6.2.1.2. Risk Management

In the decommissioning process, the *Risk Management* practice is used to gather inputs to build the decommissioning plan, focusing on risks that may create issues during the process. By considering the possible risks that may be involved during the decommissioning, the change can be driven to a safer road and can be used as an opportunity to create new value.

Possible risks may include:

- Legal and regulatory changes
- Possible competitors
- Dependencies on suppliers and partners
- Technological changes

As an output of this practice, we obtain a portfolio of risks that helps the planning in avoiding possible threats and creating opportunities to produce new value.

The following are to be considered the *key activities* to be applied for this practice:

- *Risk Identification*
  - In this activity potential risks related to the decommissioning and implementation processes are identified through the analysis of past projects involving decommissioning, changes, and implementation of services and marking common risks and issues. It is also important to engage stakeholders in brainstorming sessions and discussions to gain insight into other potential risks.
  - The *Security Division* is responsible for risk management, thus it is assigned to this activity to identify any possible risk regarding the decommissioning process and legal compliance. It will also receive the support of the IT Strategy Unit to review past projects and the HR management to gather more information regarding possible risks from stakeholders.
- *Risk Assessment*
  - After identifying the risks, it's crucial to analyze them using both qualitative and quantitative metrics. The qualitative analysis involves evaluating the likelihood of impact, while the quantitative analysis is conducted through Monte Carlo simulations to assess the potential impact of risks on project timelines and costs. Once all the risks have been evaluated to each of them is assigned a priority level based on its severity and potential impact on the decommissioning process.
  - The *Security Division* is responsible for risk management, thus it is their job to conduct the risks qualitative and quantitative analysis and prioritization. It may require the support of the IT Strategy Unit and Service Implementation Unit for the Monte Carlo simulations.
- *Risk Mitigation Planning*
  - This activity consists in developing mitigation strategies for high-priority risks including contingency plans, preventive measures, and response actions. For each risk mitigation strategy, a plan with how the technological, budget and human resources are assigned is developed and a supervisor is assigned to each plan to monitor and manage the risks and to ensure the mitigation plan is applied effectively in case the issues occur.
  - In formulating mitigation strategies, both the *IT Strategy Unit* and the *Security Division* are involved, and the Financial and HR Departments can assist with the allocation of resources.

- *Risk Register*

- The bank already has a well maintained and documented risk register so all the new risks and their mitigation plans are added to this register with all their information regarding the management activities, including risk identification, assessment, and mitigation plans ensuring that each of them is detailed and always up to date to be used in case of need.
- The management of the risk register is the responsibility of the *Security Division*, which is responsible for the Bank's global risk management policy, and thus is in charge of this activity.

### 6.2.1.3. Service Financial Management

In the decommissioning process, the *Service Financial Management* practice is used to plan in terms of financial information. It considers budgets, reports and forecasts to allocate the right amount of resources for the decommissioning and implementation.

Its functions fall into three categories:

- Budgeting/Costing: focuses on predicting and controlling the income and expense of money related to the services to be decommissioned and forecasts the difference in expenses with the implementation of the IT Service Token Connectivity considering the demand. This is then translated into anticipated operating and project costs, which are used to set budgets and rates to ensure adequate funding for decommissioning.
- Accounting: enables the organization to fully account for expenditure and compare forecast and actual costs and expenditure.
- Charging: the need to charge consumers for the service provided.

We observe that financial control within the IT department is comprehensive at a high level, but only limited information is known as the detailed cost of individual IT services and the usage by each customer.

The following are to be considered the *key activities* to be applied for this practice:

- *Financial Forecast*

- This activity consists of developing a detailed financial forecast for the decommissioning of the Home Connectivity and USB Connectivity services and the implementation of the IT Service Token Connectivity service.
- The IT Strategy Unit's *IT Finance Team* is assigned to this activity, with help from across the unit to make the forecast as detailed and accurate as possible.

- *Resource Allocation*

- This activity includes planning how to allocate the required financial resources based on the financial forecast, which is based on the anticipated costs and was produced in the previous activity.
- Based on the forecast, the *IT Finance Team* will allocate resources in the best way possible with the help of the Operational Management Unit to identify which part of the decommissioning process needs to be prioritized. The CFO will report the decisions made to the CEO through the Shared Services Director.

- *Monitoring Financial Performances*

- This activity involves scheduling periodic reviews to evaluate financial performance by detailing all expenditures related to the decommissioning and implementation processes and comparing forecasted costs to actual costs to identify variances and take corrective actions.
- The *IT Finance Team* is responsible for evaluating financial performance, with the CFO reporting periodically on the effectiveness of the planning and actual expenses for the decommissioning process to the CEO.

#### **6.2.1.4. Strategy Management**

*Strategy Management* plays a critical role in guiding the organization's decisions. The strategy establishes the criteria and mechanisms that help decide how best to prioritize resources, capabilities, and investments to achieve those results, while the practice ensures that the strategy is defined, agreed upon, and achieved. We want the strategy to be more fluid, focusing on establishing the essential purpose and principles of the organization to then guide the decommissioning.

The objectives of this practice in our context are:

- Analyze the organizational environment to identify beneficial opportunities.
- Decide and align the organization's perspective and direction with relevant stakeholders, including its vision, mission, and principles.
- Ensure that the strategy is translated into tactical and operational plans for each organizational unit expected to deliver on the strategy.
- Implement the strategy through the execution of strategic plans and coordination of efforts at the strategic, tactical, and operational levels.
- Manage changes to the strategies and related documents to ensure that strategies evolve in line with changes in internal and external environments.

The following is to be considered the *key activity* to be applied for this practice:

- *Development of Tactical and Operational Plans*

- To align the decommissioning process with the bank's strategic direction, a comprehensive plan should be developed that defines all the steps necessary to achieve the goal while maintaining the organization's focus. The strategic plan defines the overall direction of reducing costs and implementing a new service in place of the one to be decommissioned that, after careful analysis, is an improvement aligned with the bank's goals. From the strategic plan, an operational plan is developed with detailed information on what each unit does on a day-to-day basis. This ensures that the operational plan is aligned with the bank's main goal.
- The *IT Strategy Unit* is in charge of the strategy and planning thus is assigned to this activity to identify if the decommissioning aligns with the bank's strategy and ensuring the plan to complete it is also in line with the organization's goals. To support the operational planning the *Operations Management Unit* is involved to ensure the plan is accurate and detailed.



### 6.2.2. Improve

The purpose of the *Improve* value chain activity is to ensure continual improvement of products, services, and practices across all value chain activities and the four dimensions of service management. By involving these ITIL4 practices and focusing on the “improve” value chain activity, the decommissioning project can be managed effectively, ensuring continual improvement and alignment with organizational goals. Each practice contributes to the overall improvement of service management and enhances the value delivered to the organization.

This SVC activity has a corresponding series of *inputs*:

- Feedback from the stakeholders and third-party service components as part of “*Engage*”
- Information on new and changed products and services coming from “*Design and transition*” and “*Obtain/Build*”
- Performance information about products and services from “*Deliver and Support*”
- Performance information and possibility for improvement from all activities in the value chain.

It’s also important, for this SVC activity, to focus on its corresponding series of *outputs*:

- Improvement initiatives and status reports on improvements for all activities of the value chain
- Value chain performance information for “*Plan*”
- Contract and agreement requirements for “*Engage*”
- Service performance information for “*Design and transition*”

#### 6.2.2.1. Information Security Management

*Information Security Management* plays a crucial role in any decommissioning plan and, due to this, it is much important to continuously improve this practice by ensuring that sensitive data related to the decommissioned services is securely disposed of and that data security practices are continually improved to mitigate risks and enhance compliance.

A good information security management system framework is articulated in different phases, as visible from Figure 9:

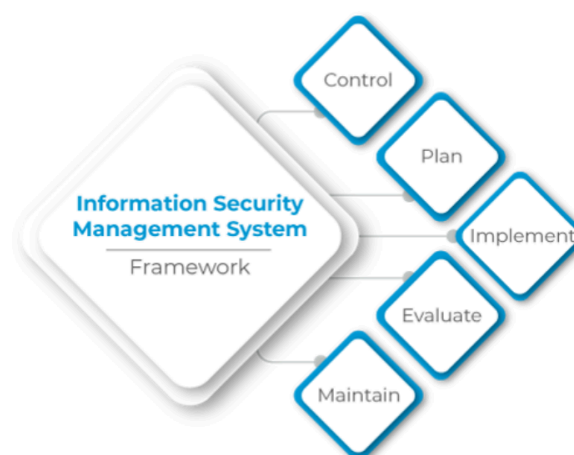


Figure 9: Information security management framework

In such cases, information needs to be managed and controlled carefully, planning how to collect information and ensuring good understanding of requirements, implementing appropriate practices when putting them into action, evaluating their correct setting up and then maintaining such on an ordinary basis.

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of Current Data Security Practices*
  - By conducting a thorough review of current data security policies and procedures, the decommissioning plan ensures a comprehensive understanding of the existing framework and its effectiveness in managing data disposal. This assessment is crucial for identifying any gaps and weaknesses in the current practices, allowing the organization to address vulnerabilities and implement improvements. Strengthening data security practices at this stage sets a solid foundation for the entire decommissioning process, ensuring that sensitive data is managed and disposed of securely.
  - This activity would primarily be led by the *Security division*, with support from the IT department, specifically the IT strategy unit and the *Service quality unit*. The CIO would oversee this process, ensuring alignment with overall IT strategy. The *Service quality unit*, which includes the service improvement manager, would be instrumental in evaluating the effectiveness of current practices and identifying areas for improvement.
- *Data Identification and Classification*
  - Cataloguing all data associated with Home Connectivity and USB Connectivity services is essential for identifying sensitive information that requires secure disposal. Enhancing data classification processes ensures that sensitive data is accurately identified and managed appropriately throughout the decommissioning process. This activity minimizes the risk of data breaches and ensures that all sensitive information is accounted for, thereby bolstering the overall security posture of the organization during the decommissioning phase.
  - This task would be a collaborative effort between the *Applications unit* and the *Operations management unit* within the IT department. The *Applications unit*, responsible for design, procurement, development, maintenance, and support, would have detailed knowledge of the systems involved. The Operations management unit, including the service desk and incident management teams, would provide insights into the operational aspects of data handling.
- *Develop a Secure Disposal Plan*
  - Developing a detailed plan for securely disposing of sensitive data involves outlining specific data destruction methods and establishing clear timelines for execution. This plan ensures that the decommissioning process is systematic and compliant with regulatory requirements and industry best practices. By aligning the disposal strategy with these standards, the organization demonstrates its commitment to data security and compliance, thereby mitigating potential legal and reputational risks associated with improper data disposal.
  - The *IT strategy unit*, under the guidance of the *CIO*, would take the lead in developing the secure disposal plan. They would work closely with the *Security division* to ensure compliance with security standards. The *Finance department*, led by the *CFO*, would be consulted to ensure the plan aligns with budgetary constraints and regulatory financial requirements.
- *Implement Secure Disposal Methods*
  - Utilizing secure methods such as shredding, degaussing, and data wiping to destroy data is critical for ensuring that sensitive information is erased. Regularly updating these data destruction methods to incorporate advancements in technology and security standards ensures that the organization stays ahead of emerging threats and vulnerabilities. This reactive approach enhances the effectiveness of data disposal practices and reinforces the overall security framework during the decommissioning process.

- The actual implementation would be carried out by the *Operations management unit*, specifically the technical management team. They would work under the direction of the *Service implementation unit*, which handles change management. The Applications unit would provide necessary support in terms of system access and data extraction.
- *Training and Awareness*
  - Providing training for employees on secure data disposal practices ensures that all staff members are aware of their roles and responsibilities in protecting sensitive information. Developing ongoing training programs keeps staff updated on the latest security protocols and emerging threats, fostering a culture of security awareness within the organization. This continuous education is vital for maintaining high standards of data security during the decommissioning process and beyond, reducing the risk of human error and enhancing overall compliance.
  - This would be a joint effort between the HR department and the IT department. The HR manager would oversee the overall training strategy, while the Service quality unit from the IT department would provide the technical content. The Security division would also be involved in developing the security awareness aspects of the training. The Customer delivery division might also contribute to ensure that any customer-facing employees are properly trained on data security practices during the decommissioning process.

#### 6.2.2.2. Supplier Management

The *Supplier Management* is paramount in the control of supplier relationships and contract termination. This involves not only navigating the complexities of ending existing contracts but also deriving valuable insights from these interactions to enhance future supplier engagements. The focus on improvement processes within the Supplier Management practice aims to learn from the current supplier interactions to refine and strengthen the organization's overall supplier management practices. The objective is to ensure a smooth and compliant decommissioning process while leveraging these experiences to optimize supplier selection, performance management, and contract negotiations in future engagements.

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of Current Supplier Relationships*
  - By reviewing existing supplier contracts, the organization gains a clear understanding of current supplier performance and contractual obligations. This assessment helps identify areas where suppliers have met or fallen short of expectations, providing valuable insights for managing contract terminations and future supplier engagements. It ensures that all contractual obligations are met during the decommissioning process, mitigating risks associated with non-compliance.
  - This activity would be primarily led by the *IT strategy unit* within the IT department, under the supervision of the *CIO*. The *IT strategy unit*, responsible for planning and finance, would review existing supplier contracts to gain a clear understanding of current supplier performance and contractual obligations. They would work closely with the Service implementation unit, which handles change management, to ensure all contractual obligations are met during the decommissioning process. The *Finance department*, led by the *CFO*, would be consulted to ensure financial aspects of supplier contracts are thoroughly reviewed.

- *Supplier Performance Evaluation*

- Evaluating supplier performance using KPIs and SLAs provides a data-driven basis for assessing how well suppliers have delivered services. This evaluation highlights areas where suppliers have excelled or underperformed, enabling the organization to make informed decisions about continuing or terminating relationships. It also provides a foundation for setting clearer expectations and performance standards in future contracts.
- This task would be a collaborative effort between the *Service quality unit* and the *Operations management unit* within the IT department. The *Service quality unit*, which includes the service improvement manager, would lead the evaluation of supplier performance using KPIs and SLAs. They would work closely with the Operations management unit, particularly the service desk and incident management teams, who have day-to-day interaction with supplier services. The *Applications unit* might also provide input, especially regarding the technical performance of supplier-provided systems. The CIO would oversee this process, ensuring it aligns with overall IT strategy and performance goals.

- *Document Lessons Learned*

- Documenting lessons learned from supplier management activities provides valuable insights that can be used to improve future practices. This documentation helps identify what worked well and what didn't, informing strategies for better supplier selection, performance management, and contract negotiation. By systematically capturing and analyzing these insights, the organization can continuously enhance its supplier management capabilities.
- The *Service quality unit*, under the guidance of the service improvement manager, would take the lead in documenting lessons learned from supplier management activities. They would collaborate with the IT strategy unit to ensure these insights inform future strategies for better supplier selection, performance management, and contract negotiation. The HR department might be involved in capturing any lessons related to supplier relationship management skills and training needs. The CIO would ensure that these lessons learned are shared appropriately across the IT department and with other relevant divisions like Industry liaison and Customer delivery, to improve overall organizational supplier management practices.

### **6.2.2.3. Change Control**

The *Change Control* practice focuses on managing the change process efficiently while continuously seeking opportunities for improvement. By learning from each change initiative, the organization can enhance its change management processes, making them more efficient and less disruptive. The objective is to manage changes associated with decommissioning Home Connectivity and USB Connectivity services in a structured manner while leveraging these experiences to refine and improve future change control practices.

A normal change control implementation, also described below, follows a logical implementation like Figure 10 shows:

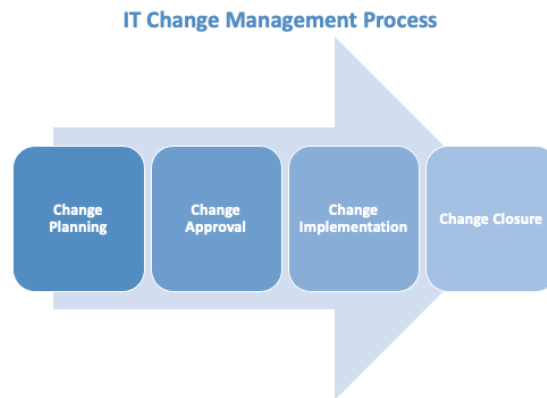


Figure 10: Change control best practices

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of Current Change Management Practices*
  - By reviewing existing change control procedures, the organization can gain a comprehensive understanding of the current framework's effectiveness. Identifying strengths and weaknesses in the current processes allows for targeted improvements, ensuring that changes are managed more efficiently and effectively during the decommissioning process and in future initiatives.
  - This activity would be primarily led by the *Service implementation unit* within the IT department, which includes change management responsibilities. They would work closely with the *Service quality unit*, particularly the service improvement manager, to review existing change control procedures. The Operations management unit, including the service desk and incident management teams, would provide valuable input on how changes have historically impacted day-to-day operations. The CIO would oversee this assessment, ensuring it aligns with broader organizational goals.
- *Risk Assessment and Impact Analysis*
  - Conducting a thorough risk assessment and impact analysis helps anticipate and address potential issues before they occur. By identifying risks and developing mitigation strategies, the organization can minimize disruptions and ensure a smoother transition during the decommissioning process. This reactive approach enhances the overall effectiveness of change management.
  - This task would be a collaborative effort between the *Service implementation unit* and the *IT strategy unit*. The *Service implementation unit*, with its change management expertise, would lead the risk assessment process. The IT strategy unit would contribute by aligning the risk assessment with overall IT and business strategies. The *Security division* would also be consulted to ensure all security-related risks are considered. The CIO would review and approve the final risk assessment and mitigation strategies.
- *Develop a Change Management Plan*
  - A detailed change management plan provides a roadmap for managing changes systematically and efficiently. By outlining clear timelines, responsibilities, and communication protocols, the organization ensures that all stakeholders are informed and prepared for the changes. This structured approach reduces the likelihood of miscommunication and operational disruptions.

- The *Service implementation unit* would take the lead in developing the change management plan, working closely with the *IT strategy unit* to ensure alignment with overall IT objectives. The HR department would be involved in planning any necessary training or staff communications. A detailed change management plan provides a roadmap for managing changes systematically and efficiently. This structured approach, overseen by the *CIO*, reduces the likelihood of miscommunication and operational disruptions.
- *Implement Change Management Strategies*
  - Implementing change management strategies according to the plan ensures that changes are carried out systematically and with minimal disruption. Continuous monitoring and adjustment during implementation allow the organization to address any issues promptly and refine processes in real time, enhancing overall change management efficiency.
  - The *Service implementation unit* would be responsible for implementing change management strategies according to the plan. They would work closely with the Operations management unit, particularly the service desk and technical management teams, to ensure changes are carried out systematically and with minimal disruption. The *Applications unit* would provide necessary technical support during implementation. Continuous monitoring and adjustment during implementation would be overseen by the Service quality unit, allowing the organization to address any issues promptly and refine processes in real time, enhancing overall change management efficiency.
- *Post-Implementation Review*
  - Conducting post-implementation reviews provides valuable insights into the effectiveness of the change initiatives. Gathering feedback from stakeholders helps identify what worked well and what could be improved. This feedback loop is essential for refining change management processes and ensuring continuous improvement in future initiatives.
  - The *Service quality unit*, led by the service improvement manager, would take primary responsibility for conducting post-implementation reviews. They would gather feedback from all relevant stakeholders, including the Operations management unit, Applications unit, and end-users from various divisions like Retail banking and Customer delivery. Conducting post-implementation reviews provides valuable insights into the effectiveness of the change initiatives.
  - This feedback loop is essential for refining change management processes and ensuring continuous improvement in future initiatives. The IT strategy unit would use these insights to inform future IT strategies and change management approaches. The CIO would review the findings and ensure that lessons learned are incorporated into future change management practices across the IT department and shared with other relevant divisions.

#### **6.2.2.4. Service Level Management**

In the context of decommissioning Home Connectivity and USB Connectivity services, the Service Level Management practice ensures that clear business-based targets for service levels are set, and that the delivery of services is properly assessed, monitored, and managed against these targets. Focusing on improvement within the Service Level Management practice guarantees that service delivery meets or exceeds business expectations. The objective is to monitor service levels and user satisfaction continuously, using insights gained from the decommissioning process to enhance future service delivery and management practices.

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of Current Service Level Agreements (SLAs)*
  - By reviewing existing SLAs, the bank can determine whether the service levels met business expectations and where improvements can be made. This assessment ensures that future SLAs are more aligned with business needs, enhancing overall service delivery.
  - This activity would be primarily led by the *Service quality unit* within the IT department, which includes the service improvement manager. The *Operations management unit*, particularly the service desk and incident management teams, would provide valuable input on how well current SLAs have been met in practice. This assessment ensures that future SLAs are more aligned with business needs, enhancing overall service delivery. The *CIO* would oversee this process, ensuring it aligns with broader organizational goals and customer satisfaction metrics.
- *Define New Service Level Targets*
  - Defining new service level targets ensures that the bank sets realistic and achievable goals for future services. These targets, grounded in business needs and historical performance, guide service delivery improvements.
  - The *IT strategy unit* would take the lead in defining new service level targets, working in close collaboration with the Service quality unit. The Operations management unit would provide input on what's realistically achievable based on historical performance data. The *CIO* would review and approve the final service level targets, ensuring they align with overall IT strategy and business objectives.
- *Service Monitoring and Reporting*
  - Continuous monitoring of service levels allows the bank to promptly identify and address any issues, ensuring that service delivery meets or exceeds expectations. Real-time data and analytics provide insights that drive reactive improvements.
  - The *Operations management unit*, particularly the service desk and technical management teams, would be primarily responsible for continuous monitoring of service levels. They would work closely with the Service quality unit to establish effective monitoring processes and tools. The *Applications unit* would provide necessary technical support for monitoring systems. These reports would be reviewed by the *CIO* and shared with relevant business divisions to ensure transparency and drive continuous improvement.
- *User Feedback and Satisfaction Surveys*
  - Regularly gathering user feedback ensures that the bank understands user experiences and expectations. This feedback is critical for identifying service delivery improvements and enhancing user satisfaction.
  - This would be a collaborative effort between the *Customer delivery division* and the IT department's *Service quality unit*. The *Customer delivery division* would lead the effort in gathering feedback from external customers, while the *Service quality unit* would focus on internal users across various divisions. The HR department might be involved in designing and administering internal satisfaction surveys. This feedback is critical for identifying service delivery improvements and enhancing user satisfaction. The *CIO* would review the feedback results and ensure that insights are incorporated into service improvement initiatives.

- *Training and Awareness*

- Training teams on best practices and lessons learned ensures they are equipped with the necessary knowledge and skills for effective service level management. Ongoing training programs help maintain high standards of service delivery.
- This would be a joint effort between the *HR department* and the *IT department*. The HR manager would oversee the overall training strategy, while the Service quality unit from the IT department would provide the technical content related to service level management. Training teams on best practices and lessons learned ensures they are equipped with the necessary knowledge and skills for effective service level management. The *CIO* would ensure that training initiatives align with overall IT strategy and service improvement goals.

### 6.2.3. Engage

The *Engage* activity is a critical component, serving as primary interface between organization and stakeholders, focusing on fostering relationships, understanding needs and expectations, while ensuring ongoing communication throughout the service lifecycle. In this case, it involves translating stakeholder requirements into actionable insight for other SVC activities. As an input-gathering and output-distributing activity, Engage facilitates information flow along the entire value chain. Drawing on effective management of stakeholder interactions, Engage empowers the Bank in such a way that alignment of its services is made best to meet customer needs and enables co-creation of value through continuous improvement.

Looking more closely at the Engage activity, it is necessary to keep in mind both the inputs—information and resources coming from other activities and from external sources—and outputs in terms of deliverables and insights into what this activity provides towards the other SVC activities. This puts the function of Engage as a central hub within the process of management in perspective.

This SVC activity has a corresponding series of *inputs*:

- High-level demand data
- Product and service portfolio from “*Plan*”
- Requirements for services and products from customers
- Contract and agreement requirements
- New and changed products and services information from “*Design and transition*” and “*Obtain/Build*”
- Supporting tasks and performance information from “*Deliver and support*”
- Third-party service component information from suppliers and partners (as part of supply chain management)
- Improvement initiatives

It’s also important, for this SVC activity, to focus on its corresponding series of *outputs*:

- Demand and opportunity for “*Plan*”
- Requirements for “*Design and transition*”
- Supporting tasks for “*Deliver and support*”
- Change or project request for “*Obtain/Build*”



- Contracts/agreements with internal /external suppliers for the processes “*Design and transition*” and “*Obtain/Build*”
- Information about third-party service components
- Improvement opportunities
- Service performance reports to customers

#### **6.2.3.1. Supplier Management**

In the context of the engage value chain activity, the *Supplier Management practice* focuses on maintaining strong relationships and clear communication with suppliers. This ensures that suppliers understand the bank’s needs and can effectively support the decommissioning of Home Connectivity and USB Connectivity services. The objective is to provide a good understanding of stakeholder needs, transparency, and continual engagement with all suppliers.

The following are to be considered the *key activities* to be applied for this practice:

- *Supplier Relationship Management*
  - Maintaining open lines of communication with suppliers ensures that they are well-informed about the bank’s current needs and expectations. This engagement helps address any issues promptly and fosters a collaborative environment. Regular engagement with suppliers leads to a better understanding of mutual needs and expectations, enhancing service quality and ensuring suppliers are aligned with the bank’s strategic goals.
  - This activity would be primarily led by the *Industry liaison* division, working closely with the IT department’s IT strategy unit. The Industry liaison division would be responsible for maintaining open lines of communication with suppliers, ensuring they are well-informed about the bank’s current needs and expectations. The IT strategy unit would provide input on technology-related supplier relationships. The *CIO* would oversee this process for IT-related suppliers, while other division heads (e.g., Retail banking, Global banking) would be involved for suppliers specific to their areas. The CEO would be kept informed of significant supplier relationships that impact overall business strategy.
- *Contract Management*
  - Effective contract management involves regularly reviewing contract terms, performance metrics, and compliance requirements. This ensures that suppliers meet their obligations and that contracts remain aligned with the bank’s changing needs. Reactive contract management ensures that supplier agreements remain relevant and beneficial, supporting smooth service delivery and compliance with business objectives.
  - The *Finance department*, led by the *CFO*, would take primary responsibility for contract management. The IT strategy unit would be involved in reviewing and managing IT-specific contracts. The Service quality unit within the IT department would provide input on performance-related aspects of IT supplier contracts. This ensures that suppliers meet their obligations and that contracts remain aligned with the bank’s changing needs. The *Industry liaison* division would be consulted to ensure contract terms align with industry standards and practices. The *CIO* and other relevant division heads would review and approve significant contract changes.

- *Supplier Performance Monitoring*
  - Establishing key performance indicators (KPIs) and service level agreements (SLAs) allows the bank to measure supplier performance objectively. Regular performance reviews and audits help identify areas where suppliers excel or need improvement. Continuous performance monitoring ensures that suppliers consistently meet their commitments, enabling timely identification and resolution of performance issues.
  - The *Service quality* unit within the IT department would lead this activity for IT suppliers, working closely with the Operations management unit. They would be responsible for establishing key performance indicators (KPIs) and service level agreements (SLAs) to measure supplier performance objectively. For non-IT suppliers, the relevant business divisions (e.g., Retail banking, Financial products) would be responsible for performance monitoring, with support from the *Shared services division*. The CIO and other division heads would review performance reports for their respective areas.
- *Supplier Risk Management*
  - Engaging with suppliers to identify potential risks and developing strategies to mitigate these risks is crucial for maintaining service continuity. Effective supplier risk management enhances the bank's ability to manage disruptions, ensuring service continuity and reducing potential impacts on business operations.
  - This would be a collaborative effort between the *Security division*, the IT strategy unit, and the *Finance department*. The Security division would lead in identifying potential security risks associated with suppliers. The IT strategy unit would assess technology-related risks, while the Finance department would evaluate financial risks. The CIO and CFO would oversee this process, with significant risks being reported to the CEO.
- *Collaborative Improvement Initiatives*
  - Engaging suppliers in collaborative improvement projects helps identify and implement enhancements in service delivery processes. Collaborative improvement initiatives strengthen supplier relationships and drive innovation, leading to enhanced service delivery and operational efficiency.
  - The *Service implementation unit* within the IT department would lead collaborative improvement projects with IT suppliers, working closely with the Applications unit and the Service quality unit. For non-IT suppliers, the relevant business divisions would lead improvement initiatives, supported by the Shared services division. Engaging suppliers in collaborative improvement projects helps identify and implement enhancements in service delivery processes. The *IT strategy unit* would ensure that these initiatives align with overall IT strategy. The CIO and other division heads would sponsor significant improvement projects, with updates provided to the CEO on major initiatives that impact overall business performance.

#### **6.2.3.2. Infrastructure and Platform Management**

The *Infrastructure and Platform Management* practice focuses on managing the infrastructure and platforms used by the bank, including monitoring the technology solutions provided by external service providers. This practice ensures that the bank's technological foundation is robust, reliable, and capable of supporting business needs while maintaining strong engagement and transparency with stakeholders. The objective is to provide a good understanding of stakeholder needs, maintain transparency, and ensure continual engagement with all stakeholders involved in the management of infrastructure and platforms.

The following are to be considered the *key activities* to be applied for this practice:

- *Stakeholder Requirement Analysis*
  - Understanding stakeholder needs ensures that the infrastructure and platform solutions are tailored to meet specific business requirements, enhancing overall efficiency and effectiveness. This engagement helps in building solutions that are not only technically robust but also aligned with business strategies, leading to improved satisfaction and trust among stakeholders.
  - This activity would be primarily led by the *IT strategy unit* within the IT department, working closely with various business divisions such as Retail banking, Global banking, and Financial products. The IT strategy unit would be responsible for gathering and analyzing stakeholder needs to ensure that infrastructure and platform solutions are tailored to meet specific business requirements. The Applications unit would provide technical insights on feasibility and implementation aspects. The *CIO* would oversee this process, ensuring alignment with overall IT strategy and business objectives. The *CEO* would be briefed on significant infrastructure and platform decisions that impact overall business strategy.
- *Monitoring and Performance Management*
  - Continuous monitoring enables the bank to maintain high performance and availability of infrastructure and platforms, ensuring that any potential issues are identified and resolved swiftly. This reactive approach minimizes downtime and service disruptions, thereby maintaining trust and confidence among stakeholders.
  - The *Operations management unit* within the IT department, particularly the technical management team, would take the lead in continuous monitoring of infrastructure and platforms. They would work closely with the Service quality unit to establish effective monitoring processes and tools. The *CIO* would receive regular performance reports and be alerted to any significant issues affecting business operations.
- *Capacity Planning and Scaling*
  - Effective capacity planning ensures that the bank's infrastructure and platforms can scale efficiently to meet growing business demands without compromising performance. This reactive planning avoids potential bottlenecks and service degradation, supporting sustained business growth and enhancing stakeholder confidence in the bank's technological capabilities.
  - The IT strategy unit would lead capacity planning efforts, working in collaboration with the *Applications unit* and the *Operations management unit*. They would analyze current usage patterns, forecast future needs, and develop scaling strategies. Effective capacity planning ensures that the bank's infrastructure and platforms can scale efficiently to meet growing business demands without compromising performance. The *CIO* would review and approve significant capacity planning decisions, with updates provided to the *CEO* for major infrastructure investments.
- *Integration and Coordination with External Service Providers*
  - Effective coordination with external service providers ensures that their solutions complement the bank's infrastructure and platforms, leading to a cohesive and reliable technology environment. This collaboration enhances service delivery, reduces integration issues, and fosters a strong partnership with service providers, benefiting overall business operations.
  - The *Service implementation unit* within the IT department would take the lead in coordinating with external service providers, working closely with the Applications unit for technical integration aspects. The *IT strategy unit* would ensure that external services align with the

bank's overall technology strategy. The *Security division* would be involved in assessing and managing security aspects of integrations with external providers. The *CIO* would oversee significant integration projects, with updates provided to the CEO on major partnerships or integrations that impact overall business capabilities.

#### 6.2.3.3. Change Control

The *Change Control practice* is crucial for ensuring that all changes to services, products, and the underlying infrastructure are effectively managed. This practice focuses on thoroughly assessing risks, approving changes, and managing the change schedule. The goal is to increase the number of successful changes while minimizing disruptions and ensuring transparency and continuous engagement with stakeholders. Effective change control is vital for maintaining operational stability and meeting stakeholder expectations.

The following are to be considered the *key activities* to be applied for this practice:

- *Risk Assessment and Impact Analysis*
  - Comprehensive risk assessment and impact analysis ensure that all potential risks are identified and mitigated before implementing changes. This reactive approach minimizes the likelihood of unexpected issues and disruptions, maintaining operational stability and stakeholder confidence in the change process.
  - This activity would be primarily led by the *Service implementation unit* within the IT department, which is responsible for change management. They would work closely with the *IT strategy unit* to ensure alignment with overall IT objectives and risk tolerance. The Security division would be heavily involved in assessing security-related risks associated with proposed changes. The *Applications unit* would provide technical insights on potential impacts to systems and applications. The CIO would review and approve risk assessments for significant changes, with high-impact risks being escalated to the CEO.
- *Stakeholder Communication and Approval*
  - Transparent communication and stakeholder engagement ensure that everyone is aware of and agrees with the proposed changes. This fosters a sense of ownership and collaboration, reducing resistance and ensuring a smoother implementation process. It also helps build trust and transparency, as stakeholders are kept informed throughout the change lifecycle.
  - The *Service implementation unit* would take the lead in stakeholder communication, working closely with the HR department for internal communications and the Customer delivery division for external stakeholder engagement. The *IT strategy unit* would be involved in communicating how changes align with overall IT strategy.
    - For changes affecting specific business areas, the relevant division heads (e.g., Retail banking, Global banking, Financial products) would be responsible for communicating with their stakeholders and obtaining necessary approvals. The CIO would be responsible for obtaining executive-level approvals, with the CEO being involved in decisions on major changes that significantly impact the organization. It also helps build trust and transparency, as stakeholders are kept informed throughout the change lifecycle.

- *Change Scheduling and Coordination*
  - Effective change scheduling and coordination minimize the impact of changes on business operations. By carefully planning change windows and considering dependencies, the bank can ensure that changes are implemented smoothly and efficiently, reducing the risk of conflicts and service interruptions.
  - The *Service implementation unit* would lead the change scheduling and coordination efforts, working closely with the *Operations management unit* to identify optimal change windows. The CIO would oversee the overall change schedule, ensuring it aligns with business needs and IT strategy.
- *Change Documentation and Reporting*
  - Detailed documentation and reporting provide a clear audit trail for all changes, ensuring accountability and transparency. This helps stakeholders understand the change process and outcomes, facilitates compliance with regulatory requirements, and supports continuous improvement by providing a historical record of changes.
  - The *Service implementation unit* would be primarily responsible for maintaining detailed change documentation, with support from the Service quality unit for quality assurance. The *Operations management unit* would contribute to documentation by recording operational impacts and lessons learned. The IT strategy unit would use change reports to inform future IT strategies and improvement initiatives. The CIO would review regular change reports, with significant changes or trends being reported to the CEO.

#### **6.2.3.4. Service Level Management**

The *Service Level Management practice* focuses on setting clear business-based objectives for service levels and ensuring that service delivery meets these objectives. This practice is essential for maintaining transparency, continual engagement, and good relationships with all stakeholders. Effective service level management helps align IT services with business needs, ensuring that stakeholders' expectations are met, and that service performance is continually monitored and improved.

The following are to be considered the *key activities* to be applied for this practice:

- *Establishing Service Level Agreements (SLAs)*
  - Well-defined SLAs ensure that there is a common understanding of service expectations between IT and business stakeholders. This clarity helps in setting realistic performance targets and fosters accountability. By aligning SLAs with business objectives, the bank can ensure that IT services support and drive business success, enhancing stakeholder satisfaction and trust.
  - This activity would be primarily led by the *Service quality unit* within the IT department, working closely with the IT strategy unit to ensure alignment with overall IT objectives. The Service quality unit would be responsible for drafting and negotiating SLAs with various business stakeholders. The CIO would oversee the SLA establishment process, ensuring that IT services align with broader business strategies. The heads of various business divisions (e.g., Retail banking, Global banking, Financial products) would be involved in reviewing and approving SLAs relevant to their areas.

- *Performance Review and Feedback*

- Regular performance reviews and feedback sessions help in maintaining alignment between service delivery and stakeholder expectations. This engagement fosters a culture of continuous improvement and ensures that the bank remains responsive to stakeholder needs. By actively seeking and incorporating feedback, the bank can enhance service quality and stakeholder satisfaction.
- The *Service quality unit* would take the lead in conducting regular performance reviews, working closely with the Operations management unit to gather and analyze performance data. The *IT strategy unit* would use these reviews to inform future IT strategies and service improvements. The *CIO* would review overall service performance reports, with significant issues or trends being reported to the CEO. The *Customer delivery division* might be involved in gathering and analyzing customer feedback for external-facing services.

- *Communication and Collaboration*

- Ongoing communication and collaboration between IT and business stakeholders ensure that everyone is aligned and working towards common goals. This collaborative approach enhances mutual understanding and cooperation, leading to more effective and efficient service delivery. By fostering a strong partnership, the bank can ensure that IT services are well-integrated into business operations, driving overall success.
- The *Service quality unit* would play a central role in facilitating ongoing communication and collaboration between IT and business stakeholders. They would work closely with the HR department to establish effective communication channels and processes. Regular meetings between the *CIO* and business division heads would be held to discuss service performance and address any concerns. The *CEO* might participate in high-level service review meetings to ensure alignment with overall business objectives.

#### 6.2.3.5. Service Desk

The *Service Desk practice* serves as a crucial touchpoint between the service provider and its users. It is designed to capture demand for incident resolution and service requests while acting as the single point of contact for users. The Service Desk practice is essential for maintaining good relationships, transparency, and continual engagement with stakeholders by ensuring efficient and effective handling of user issues and requests.

The following are to be considered the *key activities* to be applied for this practice:

- *Service Request Fulfillment*

- Effective service request fulfillment ensures that user needs are met promptly, contributing to higher levels of user satisfaction and productivity. By efficiently managing requests, the service desk not only maintains smooth operations but also actively supports users in achieving their goals. This responsiveness demonstrates a commitment to user needs and fosters a collaborative relationship. The resulting enhanced user experience strengthens the overall relationship between users and the service provider, reinforcing trust and encouraging continuous engagement.
- This activity would be primarily led by the *Operations management unit* within the IT department, specifically the service desk team. They would be responsible for receiving, triaging, and fulfilling service requests. For requests affecting specific business areas, the relevant teams within divisions like Retail banking, Global banking, or Financial products might be involved in

providing specialized support. The *CIO* would oversee the overall performance of the service desk, ensuring it aligns with IT strategy and business needs.

- *User Communication and Updates*

- Regular communication and updates keep users informed and engaged, reducing uncertainty and frustration. This transparency builds trust and confidence in the service desk's capabilities and ensures that users feel supported throughout the resolution process. Effective communication also helps manage user expectations and reduces the likelihood of repeat inquiries.
- The service desk team within the *Operations management unit* would be at the forefront of user communication, providing regular updates on request status and resolution progress. The *CIO* would be briefed on significant communication issues or trends, with potential escalation to the CEO for matters affecting overall business operations or reputation.

- *Stakeholder Engagement and Collaboration*

- Ongoing engagement and collaboration with stakeholders ensure that the service desk remains attuned to the needs and priorities of the organization. This alignment helps the service desk provide more relevant and effective support, contributing to overall business success. Strong stakeholder relationships also enhance the service desk's ability to advocate for resources and improvements that benefit users.
- The *Service quality unit* would take the lead in ongoing stakeholder engagement and collaboration, working closely with the service desk team to gather insights and feedback. They would organize regular meetings with representatives from various business divisions to discuss service desk performance and improvement opportunities. The *CIO* would oversee these engagement efforts, ensuring that the service desk remains responsive to evolving business requirements. For major initiatives or changes to service desk operations, the *CEO* might be involved in high-level discussions to ensure alignment with overall business objectives.

#### **6.2.4. Design & Transition**

The *Design and Transition* value chain activity is a critical component in the process of delivering products and services. Its importance lies in ensuring that the delivered offerings meet the required quality standards, are cost-effective, and are brought to the market within the stipulated time frame. This is achieved through meticulous planning and adaptation of services and products, ensuring they are continually designed to meet the expectations of stakeholders.

This SVC activity has a corresponding series of *inputs*:

- “*Plan*” provides portfolio decisions and architectures, as well as policies.
- “*Engage*” provides product and service requirements
- “*Improve*” provides improvement initiatives and status reports
- “*Deliver and Support*”, along with “*Improve*”, provides service performance information
- “*Obtain/Build*” offers service components and knowledge and information about new and changed products and services
- “*Engage*” provides knowledge and information about third-party service components
- “*Engage*” provides contracts and agreements with external and internal suppliers and partners

It's also important, for this SVC activity, to focus on its corresponding series of *outputs*:

- “*Obtain/Build*” receives requirements and specifications.
- “*Engage*” acquires contract and agreement requirements
- “*Deliver and Support*” receives new and changed products and services
- Valuable knowledge and information about new and changed products and services are shared with all value chain activities
- Performance information and improvement opportunities for “*Improve*”

#### 6.2.4.1. Architecture Management

In this activity of the decommissioning process, the *Architecture Management* practice is used to evaluate whether the services to be decommissioned and implemented meet the investment objectives once they have been approved in the previous activities. It is responsible for the service architecture, which describes the structure (how the service components fit together) and the dynamics (activities, flow of resources, and interactions) of the service. The target architecture produced by *Plan* can be used as a template or blueprint for multiple services and is essential to the design and transition activity.

The following are to be considered the *key activities* to be applied for this practice:

- *Refine and Update Service Architecture*
  - With the support of the new target architecture model and gap analyses, outputs of the *Plan* activity, the architecture is revised and updated following the documents previously shared by the Shared Services Division ensuring that the implementation is aligned with the target model. In the end, all architectural changes and updates are thoroughly documented, including the rationale behind each change and its expected impact on the organization.
  - The teams responsible for this activity are those assigned by the *HR Department* during the resource allocation *Plan* key activity, including, among others, the *IT Strategy, Applications and Service Implementation Units*.
- *Evaluate Architectural Performance*
  - This activity includes evaluating the performance of the new architecture after decommissioning and implementing the services as scheduled in the *Plan* activity. It also involves analyzing service performance data to assess the current architecture's efficiency and identify opportunities for improvement.
  - The responsible for this activity is the *IT Strategy Unit* with the support of the following units *Operations Management Unit* and *Service Quality Unit* which have the necessary knowledge about the services, technologies and how to evaluate their performances.

#### 6.2.4.2. Risk Management

In the *Design and Transition* activity the *Risk Management* practice is used to design the services to be decommissioned and implemented to address prioritized risks as already identified and assessed during the *Plan* activity. If approved, the risks should then be managed as part of the decommissioning.



The following are to be considered the *key activities* to be applied for this practice:

- *Integration of Risk Controls*
  - This activity consists of incorporating the mitigation strategies outlined in the *Plan* activity for each registered risk that may affect the transition to the new architecture. It involves integrating risk controls into the design of the services to be implemented and decommissioned. This includes ensuring that the design addresses all identified risks and incorporates suitable protective measures within the architecture and service design.
  - Responsible for this activity is the *Applications Unit*, which includes teams for application design, procurement, and development as well as the *Technical Management Team* from the Operations Management Unit, responsible for developing and supporting the IT infrastructure.
- *Risk Monitoring*
  - Throughout the decommissioning process, identified risks must be continuously monitored and mitigation strategies reviewed and adjusted as necessary to address new risks or changes in existing risks.
  - The *Security Division* is responsible for this activity because it covers risks and it will have the support of the *Operations Management Unit* and *Application Unit* which are directly assigned to the changes of the services to be decommissioned and implemented.

#### **6.2.4.3. Release Management**

In the context of decommissioning Home Connectivity and USB Connectivity services, the *Release Management* practice ensures that new and changed services and features are made available for use efficiently and effectively. Focusing on improvement processes within this practice guarantees that releases are managed smoothly, minimizing disruptions and enhancing future release initiatives. The objective is to facilitate the deployment of new services or upgrades while leveraging the experiences from the decommissioning process to refine and improve future release management practices. Since the bank has already faced up problems with new software releases, as the two desktop major updates, this practice is fundamental for the bank ecosystem improvement to minimize the problems after new features releases.

The following are to be considered the *key activities* to be applied for this practice:

- *Assessment of Current Release Management Practices*
  - By reviewing existing release management procedures, the bank can understand the effectiveness of the current framework and identify past issues. This review allows for targeted improvements, ensuring that releases are managed more efficiently and effectively, thus preventing the recurrence of previous problems experienced during major updates.
  - This activity would be primarily led by the Service implementation unit within the IT department, which is responsible for change management. They would collaborate closely with the Applications unit, which handles design, procurement, development, maintenance, and support. The Service quality unit, particularly the service improvement manager, would be involved in reviewing the effectiveness of current practices. By reviewing existing release management procedures, these teams can understand the effectiveness of the current framework and identify past issues. The CIO would oversee this assessment, ensuring it aligns with broader IT strategy and organizational goals.

- *Risk Assessment and Mitigation*

- Conducting a thorough risk assessment helps anticipate and address potential issues before they occur. By identifying risks and developing mitigation strategies, the bank can minimize disruptions and ensure a smoother transition during the decommissioning process, thus addressing problems that arose in past software releases.
- This task would be a collaborative effort between the *Service implementation unit*, the *Applications unit*, and the *Security division*. The *Service implementation unit*, with its change management expertise, would lead the risk assessment process. The *Applications unit* would provide technical insights on potential risks and impacts on systems. The *Security division* would ensure all security-related risks are considered. The CIO would review and approve the final risk assessment and mitigation strategies.

- *Release Planning and Scheduling*

- A detailed release plan provides a roadmap for managing releases systematically and efficiently. By outlining clear timelines, responsibilities, and communication protocols, the bank ensures that all stakeholders are informed and prepared, reducing miscommunication and operational disruptions that previously caused issues during major updates.
- The *Service implementation unit* would take the lead in developing the release plan. It would collaborate with the IT strategy unit to ensure alignment with overall IT objectives and business needs. The *HR department* might be involved in planning any necessary training or staff communications related to new releases. By outlining clear timelines, responsibilities, and communication protocols, these teams ensure that all stakeholders are informed and prepared, reducing miscommunication and operational disruptions that previously caused issues during major updates. The CIO would review and approve the final release plan.

- *Implementation and Monitoring*

- Implementing release initiatives according to the plan ensures that releases are carried out systematically and with minimal disruption. Continuous monitoring and adjustment during implementation allow the bank to address any issues promptly and refine processes in real time, preventing the recurrence of problems experienced during past major updates.
- The *Service implementation unit* would be responsible for overseeing the implementation of releases. The *Operations management unit*, particularly the service desk and technical management teams, would be involved in monitoring the release and its immediate impacts. The *Service quality unit* would be responsible for continuous monitoring and adjustment during implementation, allowing the bank to address any issues promptly.

- *Training and Awareness*

- Training teams on best practices and lessons learned from the decommissioning process ensures they are equipped with the necessary knowledge and skills for effective release management. Ongoing training programs help maintain a high level of competency and readiness for future release initiatives, reducing the risk of problems similar to those encountered during previous major updates.
- This would be a joint effort between the HR department and the IT department. The HR manager would oversee the overall training strategy, while the *Service implementation unit* from the IT department would provide the technical content related to release management. The *Service quality unit* would contribute insights from post-release reviews to inform training content. Ongoing training programs help maintain a high level of competency and readiness for

future release initiatives, reducing the risk of problems similar to those encountered during previous major updates.

#### 6.2.4.4. Service Validation and Testing

The purpose of the *Service Validation and Testing* practice is to ensure that decommissioned services and the implementation of the Token Connectivity service meet the requirements defined previously. The requirements are used to establish measurable quality and performance indicators. Service design, deployment management, and release management of this activity are all tightly integrated with the service validation and testing practice.

The *key activities* for this practice are:

- *Requirements Verification and Test Planning*
  - This activity consists of verifying that all functional and non-functional requirements for the decommissioned services and the new Token Connectivity service are clearly defined and documented. Then develop test plans by identifying the test cases and scenarios to be executed. For each test case, outline the inputs and corresponding outputs and check that they meet the defined objectives.
  - Responsible for this activity is the *Application Unit* that is in charge of IT service design activities and the development of all applications used and not from third parties.
- *Test Case Setup and Execution*
  - Once the test cases and scenarios have been identified, it's necessary to set up and configure the test environment to closely replicate the production environment in which the Token Connectivity Service will operate. This includes setting up the necessary infrastructure, tools and data. Detailed test cases and scripts covering all aspects of service functionality, performance, security and compliance must then be created and executed in the test environment.
  - This activity is performed by the Operations Control Unit's *Technical Management Team*, which has the necessary knowledge in development, is able to replicate the production environment, configure the necessary infrastructure, and run detailed test scripts, with the help of the Application Unit's Development Team, to validate service functionality, performance, security, and compliance.
- *Validation and Reporting of Decommissioning*
  - This activity consists of ensuring that all tests are passed and that the decommissioned services are validated against a checklist of criteria to confirm that they have been properly decommissioned with no remaining dependencies or risks. All test results are then documented, including successful outcomes and any problems encountered, highlighting any risks or areas of concern that require further attention.
  - The *Service Quality Unit* is responsible for measuring how the organization delivers its services compared to customer expectations. With the help of the Application Management and Operations Management units, they ensure that all tests are passed and that the services provided meet the required criteria.

#### 6.2.4.5. Service Design

The purpose of the practice of *Service Design* is to design products and services that are fit for purpose, fit for use and can be delivered by the organization and its ecosystem. This includes the planning and organization of people, partners and suppliers, information, communication,

technology and practices for the services to be changed, and the interaction between the organization and its customers.

It is important to take a holistic, result-oriented approach to all aspects of service design, and to consider all other aspects when changing or modifying any of the individual elements of a service design. The design and development of the changed services should not be done in isolation but should consider the impact on:

- All relevant stakeholders, including customers and suppliers
- The existing architectures
- The technology required
- The required measurements and metrics

This practice should be applied to the decommissioning process because, if not carefully planned, the decommissioning of Home Connectivity and USB Connectivity services could cause unexpected negative effects on customers or the organization that otherwise could have been avoided.

The *key activities* for this practice include other activities already described. Here are some that have not yet been described:

- *Service Interface and Integration Design*
  - This activity consists of understanding how the services to be decommissioned are integrated into the architecture and ensuring that their retirement doesn't cause any problems. Then it's a matter of integrating the Token Connectivity, ensuring it's robust and scalable, and that it interacts smoothly with existing systems and external entities. One of the focus areas of the design is the security of the Token Connectivity, which is critical given that we are in a banking environment.
  - The Application Unit's *Design Teams* with the help of *Technical Management Team* from the Operations Management Unit are tasked with this activity to ensure that the decommissioning of existing services and the integration of the Token Connectivity service are designed to avoid any problem with the provided services.
- *Design Validation and Review*
  - This key activity focuses on ensuring that the designs for both the decommissioning of the Home Connectivity and USB Connectivity services and the introduction of the Token Connectivity service meet the required standards and are consistent with the overall objectives of the organization. This activity involves critically assessing the designs to identify potential issues, ensure compliance with best practices and confirm that the designs meet stakeholder requirements before implementation.
  - The *Service Quality Unit* ensures that all designs are aligned with the bank's strategic objectives and compliance requirements. They review and validate designs for the changed services to meet organizational standards and stakeholder expectations.

#### **6.2.4.6. Deployment Management**

The purpose of the *Deployment Management* practice is to move the changed hardware and documentation into live environments. It is also involved in the deployment of components to the test environment. A *continuous delivery* approach is used for the decommissioning and implementation of the Token Connectivity service. The changed components are integrated, tested, and deployed when they are needed, providing frequent opportunities for customer feedback loops. It is also used a *phased deployment* approach to help the organization gradually decommission the

Home Connectivity and USB Connectivity services while incrementally introducing the Token Connectivity service. This reduces risk and enables continuous monitoring and validation of each phase of deployment. In our case, the infrastructure is delivered as a service, then the deployment of changed components is managed by the organization by automating the deployment as much as possible. Deployment is also under the control of the Token Connectivity provider, so the IT organization needs to ensure that they know which deployments are planned and which have taken place to maintain a controlled environment.

The following are to be considered the *key activities* to be applied for this practice:

- *Planning and Scheduling Deployments*
  - This activity consists of developing a detailed deployment plan that defines the timeline, sequence, and methods for deploying the changes. The plan includes the definition of a deployment window and the customers that will be interested, as per the phased deployment approach to mitigate potential risks and incrementally roll out the change.
  - The *Planning Team* of the IT Strategy Unit is responsible for developing and overseeing the execution of detailed deployment plans.
- *Automate Deployment Execution*
  - Using automation in the deployment process ensures that the new Token Connectivity service is deployed efficiently and consistently, reducing the likelihood of errors and ensuring a smooth rollout of the service across the organization. Therefore, this activity consists of developing and testing scripts to automate the movement of customers to the new service when it's ready and detecting any problem it may occur during the decommissioning process.
  - The Application Unit's *Development Team* is responsible for this activity, developing and testing scripts that automate the deployment process. Their role is to ensure that the new Token Connectivity service is deployed efficiently and consistently with minimal manual intervention, thereby reducing the likelihood of errors during rollout.
- *Deployment Monitoring*
  - This activity involves continuously monitoring the deployment process to ensure it is following the plan and validating that each deployment phase meets the required quality standards. This activity is aided by coordination with the Token Connectivity provider and by automating deployments in this way the organization can maintain control over the deployment process and ensure that all changes are carefully managed and tracked.
  - The *Technical Management Team* from the Operations Control Unit is responsible for monitoring the deployment process and support the infrastructure.
- *Post-Deployment Review and Optimization*
  - This activity includes analyzing the data from the deployment to identify inefficiencies and optimize subsequent deployments. When the deployment is complete, ensure that documentation is updated to reflect changes made during the deployment and that stakeholders are informed of the success of the decommissioning.
  - The *Service Quality Unit* which includes the Service Improvement Manager, is responsible for analyzing deployment data to identify inefficiencies and opportunities for improvement.

### 6.2.5. Obtain & Build

The *Obtain & Build* activity is critical, since it focuses on ensuring all necessary components, including new services, technologies and service relationships are properly acquired, developed, integrated and supportive into the bank's IT evolving landscape. In the context of the user case, this encompassed the procurement of new connectivity solution, but also the termination of existing service contracts and establishment of new partnerships and collaborations, so to support bank's future needs. This may also involve the careful management of IT assets into the transition and effective completion process, ensuring resources are effectively handled, allocated and optimized according to the new service model.

This SVC activity has a corresponding series of *inputs*:

- Architectures and policies from “*Plan*”
- Change or project initiation requests from “*Engage*” and “*Deliver and support*”
- Third-party service component information, contracts, and agreements with external and internal suppliers from “*Engage*” (part of supply chain management)
- Requirements and specifications from “*Design and transition*”
- Improvement initiatives and improvement status reports from “*Improve*”
- Information about new and changed products and services from “*Design and transition*”

It's also important, for this SVC activity, to focus on its corresponding series of *outputs*:

- Contract and agreement requirements for “*Engage*”
- Service Components for “*Design and Transition*”
- Service components of “*Deliver and support*”
- Performance information and improvement opportunities for “*Improve*”
- New and changed information on service components to all value chain activities

#### 6.2.5.1. Supplier Management

In the context of decommissioning the connectivity services, the *supplier management practice* plays a pivotal role in ensuring a smooth transition, while maintaining cost efficiency and cost effectiveness. This practice is relevant since it is crucial for managing relationships with existing service providers and partners, aligning with current bank strategic objectives.

The following are to be considered the *key activities* to be applied for this practice:

- *Contract Review and Termination*
  - All contracts related to Home Connectivity and USB Connectivity Services will be reviewed by the IT Strategy Unit in collaboration with the Finance Department and Security Division. Identifying the termination clauses, notice periods, and penalties, if any, that could be incurred, and developing a phased termination approach that assures minimum financial and operational impact.
  - They will pay particular attention to termination clauses and potential penalties, developing a phased approach minimizing operational and financial impacts. In this way, the careful review will inform the timeline for decommissioning and then identify and contractual obligations which might affect the new connectivity services.

- *Supplier Performance Evaluation*

- The Service Quality Unit will thus be responsible for leading the assessment of current suppliers' performance against the established SLAs. It will therefore liaise with the Operations Management Unit in reporting and dealing with any outstanding issues or disputes. Finally, it shall provide a comprehensive performance report to the CIO and the CFO.
- By identifying strengths and weaknesses in current supplier relationships, the bank can refine requirements for current and future partnerships, ensuring better service quality for the new solution and the other ones.

- *New Supplier Identification and Negotiation*

- The IT Strategy Unit will conduct market research on the availability of suitable Token Connectivity service suppliers. The Service Implementation Unit will prepare RFPs, while the Finance Department, together with the CFO, will participate in the evaluation of proposals and the negotiation of terms with the selected suppliers.
- The focus will be on finding partners capable of meeting the bank's new connectivity needs, adding new features when discussed within the network of improved performance metrics. These revised needs will be used by the Service Implementation Unit to develop detailed RFPs. The price negotiation without trading off service quality will be led by Finance.

- *Transition Planning*

- The detailed transition plan will be developed by the *Service Implementation Unit* in collaboration with the *Operations Management Unit*, *Customer Delivery Division*, and *Retail Banking Division* to ensure minimum disruption of services. Input on international implications will come from the *Global Banking Division*. The plan will detail timelines with respect to the phasing-out of old services, implementation of new solutions, and management of any overlapping period to ensure continuous connectivity in all bank operations.

- *Risk Management*

- As a result of the fact that services pertaining to connectivity are mission-critical to banking operations, a solid process of risk management should underpin this activity. The Security Division and the IT Strategy Unit will make joint efforts to identify potential risks that could be brought into being by changing suppliers and transiting services.
- These will include cybersecurity risks, challenges with data migration, and possible service interruptions. Thereafter, mitigation strategies and contingency plans would be developed to suit these risks, making sure the Bank is prepared for a wide array of transition scenarios.

- *Establish a Supplier Transition Team*

- The CIO shall establish a cross-functional team led by the IT Strategy Unit Manager, with representatives drawn from all relevant departments and divisions. This would be an important team in terms of coordination through such a complex process of decommissioning Home Connectivity and USB Connectivity services while transitioning to Token Connectivity.
- Among the members will be representatives from IT, Finance, Security, Customer Delivery, and Global Banking, to ensure everything is covered in this transition. Team meetings will be held on a weekly basis to track progress, deal with problems, and make fundamental decisions for the decommissioning process.

- *Develop a Comprehensive Supplier Transition Plan*
  - The Service Implementation Unit shall develop the detailed plan outlining every step involved in transitioning from current connectivity services to Token Connectivity. It shall include timelines for contract terminations, supplier evaluations, on-boarding of new suppliers, and service migration activities.
  - It will also include addressing potential risks and mitigation strategies for those risks. This will then be reviewed by the CIO to align the plan with the IT strategy and finally approved by the CFO. This detailed plan would act as a roadmap for the whole decommissioning process, ensuring that all stakeholders are aligned on objectives, timelines, and responsibilities.
- *Implementation of Supplier Performance Monitoring System*
  - The Service Quality Unit shall establish and maintain an effective real-time supplier performance tracking system. It will track KPIs on the availability of service, response time, and customer satisfaction ratings for both existing and new suppliers.
  - These reports shall be regularly generated and provided to the CIO and division heads so that performance issues, which may further hinder the decommissioning process or cause defects in the new Token Connectivity service, can be quickly identified and solved.

#### 6.2.5.2. IT Asset Management

The practice of *IT Asset Management (ITAM)* involves the tracking and usage of all organization's assets, involving cataloguing, deploying and maintaining all assets lifecycle, also responsibly disposing them when necessary. It is essential to track, manage, and dispose of the IT assets associated with Home Connectivity and USB Connectivity services, including the preparation phase in implementing Token Connectivity.

An excellent ITAM seamlessly integrates processes throughout all stages, is conforming to the organizational strategy, easing risks, managing costs, and gives a single point of reference for budgeting and decision-making—its relevance across departments now, cutting its reach across diverse assets from technologic to tangible. A good lifecycle about this practice can be documented by Figure 11:



Figure 11: Ideal IT Asset Management lifecycle



The following are to be considered the *key activities* to be applied for this practice:

- *Comprehensive Asset Inventory*
  - This is a task to schedule a detailed inventory of all hardware, software, and licenses related to the Home Connectivity and USB Connectivity services. The primary objective of this task is to provide a proper record of detailed information for all IT assets that would have been affected by the decommissioning process, including asset location, current status, and ownership. Different pros are present, such as an improvement in the visibility of assets, better decision-making for disposal or reallocation, and reduced risk of overlooking critical assets during the transition.
  - This activity would be led by the IT Asset Manager within the IT department, with support from the Operations Management Unit for operational data about asset utilization, and the Applications Unit for information about software dependencies and licensing.
- *Asset Valuation and Depreciation Analysis*
  - The activity looks at all assets related to the decommissioned services for their current value and depreciation status. This would be done in order to inform any decisions about disposal or reallocation of the assets, and also to make sure that any financial reporting is undertaken correctly.
  - Benefits will include the optimum financial planning of the decommissioning process, making decisions related to asset disposal strategies, and compliance with financial reporting requirements. This would be an activity jointly run by the *IT Asset Manager* and the Finance Department, under the leadership of the CFO. The *CFO* would check and approve the methodology for valuation to ensure its coherence with the bank's financial policies.
- *Disposal and Decommissioning Planning*
  - Based on inventory and valuation data, this involves detailing a plan of disposition or reallocation. The objective here is to establish structured and compliant handling when decommissioning the assets.
  - Among the most important benefits there are waste reduction, strategic cost recovery through disposal, and reduced risk of data breaches through proper retirement of the asset. This activity would be led by the IT Asset Manager, with critical input from the Security Division Head in ensuring that all procedures for data sanitization and secure disposal have been complied with, particularly for assets with sensitive information.
- *Asset Reallocation Strategy*
  - This would involve an activity of strategizing how to reallocate any existing usable assets to other departments or services that need them within the bank, to maximize resources and cut down on unnecessary costs for procurement.
  - It will achieve this by reusing assets to save on costs, allocating resources better across the bank, and reducing the environment's burden by use during an extended lifecycle. This activity would be led by the *IT Strategy Unit Manager* in conjunction with the *IT Asset Manager*, in consultation with the *Operations Management Unit Manager* and the relevant divisional business heads, for example, Retail Banking and Customer Delivery, in the identification of prospective re-use opportunities for the assets being decommissioned.

- *Integration with New Token Connectivity Assets*
  - This activity involves the planning of integration of new assets to be acquired for the Token Connectivity service into the existing asset management framework. This is aimed at ensuring a smooth transition into, and management of, new assets.
  - This will deliver a number of benefits with enhanced identification and control of new assets, consistency of approach in the asset management process, and increased control over exposures across the entire IT assets estate when transition is complete. This activity would be driven by the IT Asset Manager, working closely with the manager of the Service Implementation Unit. The CIO would provide all necessary oversight and follow-up to ensure it complied with the overall IT strategy.
- *Compliance and Audit Preparation*
  - This activity ensures that all asset-related activities during the decommissioning process comply with regulatory requirements and internal policies. It also involves preparing comprehensive documentation of asset disposals and reallocations to support future audits.
  - Benefits include reduced compliance risks, improved audit readiness, and enhanced transparency in asset management practices. This activity would be a collaborative effort led by the IT Asset Manager, working closely with the Security Division Head and the Legal team (under Shared Services). The CFO would provide oversight to ensure financial compliance aspects are adequately addressed.

#### **6.2.5.3. Continual Improvement**

The practice of *Continual Improvement* aligns the organization's practices and services with changing business needs through continuous improvement of products, services, and practices. It entails the development of methods and techniques concerning improvement and the promotion of a culture of continual improvement throughout the organization in keeping with overall strategy.

The commitment and practice of improvement must be engrained into every piece of the organization, including securing resources, measuring accurately based on updated plans and similar. This has to be applied at all levels of the organization, may it be internally or externally, so to avoid wasting time when encountering difficulties.

The following are to be considered the *key activities* to be applied for this practice:

- *Encouraging continual improvement across the organization*
  - The establishment of an improvement culture where all employees are motivated and provoked towards the identification of and contribution to improvement opportunities. This shall comprise of creation of awareness, training, and recognition for efforts on improvements. Another major element concerns time and budget allocation for improvement initiatives so that they do not get submerged with the routines of daily work or other large projects.
  - The initiative to promote improvement is led by the *CIO* and the *Service Quality Unit*, while training initiatives are supported by *HR*. Department heads are responsible for fostering and promoting continuous improvement in teams and championing resources. Budgeting is the responsibility of the *CFO*, together with the *CIO* and the *IT Financial Manager*.

- *Securing time and budget for continual improvement*
  - The activity is crucial in ensuring continual improvement efforts are not overshadowed by daily operations or major changes. This involves making the correct business cases involving the right amount of resources, while integrating improvement activities into regular work schedules and project plans.
  - Roles like the *CFO*, in collaboration with the *CIO* and *IT Financial Manager*, is responsible for budgeting. Time constraints are to be allocated and precisely managed by the organization itself and its internal roles.
- *Identifying and logging improvement opportunities*
  - The process is involved with the identification and recording of opportunities for improvement from various sources across the organization. A Continual Improvement Register will be maintained, and these ideas are to be evaluated against criteria such as potential value, cost, risk, and alignment with organizational goals.
  - Different parts are involved here: The CIR is the responsibility of the *Service Quality Unit*, which also leads the evaluation process. All staff are responsible for recognizing and making proposals for improvements. The *Service Desk* is often involved in capturing user improvement suggestions. The *IT Strategy Unit* assures that it aligns with the general IT strategy. High impact decisions may involve the *CIO*.
- *Assessing and prioritizing improvement opportunities*
  - Improvement efforts must be made in order to have initiatives deliver the most value. Reviewing and analyzing improvement ideas captured within operations is fundamental, both for seeing and focusing over potential value opportunities, optimize estimated costs and being compliant to current regulations, while correctly categorizing how to make improvements and ranking opportunities.
  - *Service Quality Unit* defines the metrics and makes the evaluations here. The *IT Strategy Unit* analyzes the results for strategic impact. Department heads respond to how improvements have gone in their areas.
- *Measuring and evaluating improvement results*
  - This includes the development of improvement plans, including timelines, resource allocation, and execution of approved improvements. It further includes tracking improvement initiatives and their outcomes, assessing effectiveness, and identifying further actions necessary.
  - The planning and execution of most initiatives are normally led by the *Service Implementation Unit*, in close coordination with the departments affected by the improvement. The *Project Management Office* can be called upon for larger initiatives.

#### **6.2.5.4. Information Security Management**

The *information security management* practice has the goal to ensure service components are available as needed and meet agreed specifications, ensuring security risks are properly managed and security measures into new services from the outset. In this case, it's fundamental to ensure at all steps prevention, detection and correction, while keeping confidentiality at core. Most organizations will have an information security team responsible for the risk assessment process and who will define the policies, procedures, and controls. In high-velocity environments, like a Bank, information security has to be integrated into the day-to-day work of development and operations to

the extent possible, thereby shifting reliance from control of process to verification of preconditions such as expertise and integrity.

The following are to be considered the *key activities* to be applied for this practice:

- *Security Requirements Analysis*
  - This will involve running an in-depth analysis of security requirements for the new Token Connectivity service, considering multiple parameters like the applicability of regulations, data protection needs, and perceived threats. The goal is to identify the measures of security required and embed them in the very design of the new service.
  - It reduces the possibility of security breaches, ensures conformance to regulations, and enhances stakeholders' trust, thus crafting the firm foundation for secure development and implementation of the new service. The leader is the *Security Division Head*, but he works closely with the *IT Strategy Unit Manager* and the *Service Implementation Unit Manager*. The *CIO* provides oversight to ensure alignment with overall IT security strategy.
- *Service Architecture Design*
  - Developing a comprehensive security architecture for the Token Connectivity service, encompassing network security, access controls, encryption methods, and monitoring systems. Creates a robust security framework that protects the new service and associated data from potential threats.
  - It facilitates a structured approach to security, enabling easier management and updates of security measures, while enhancing overall system resilience. In general, it ensures security is built into the service from the ground up, rather than being added as an afterthought, so ensure continuous application in every process and subprocess. Spearheaded by the *IT Strategy Unit*, in collaboration with the *Security Division* and the *Applications Unit*. The *CIO* reviews and approves the final security architecture.
- *Security Controls Implementation*
  - This is held inside of the building phase of the Token Connectivity Service, including firewalls, intrusion detection systems and secure authentication mechanisms. It helps making operative the security measures identified in the planning and design phases, so to ensure theoretical security plans are effectively translated into practical protections, minimizing the risk of security vulnerabilities in the implemented services.
  - These are implemented by the *Operations Management Unit*, in particular by the technical management team, with the direction of the *Security Division*. The *Service Implementation Unit* is responsible for integrating such controls within the overall service implementation.
- *Security Testing and Validation*
  - Implementing this revolves performing complete security testing of the new service for token connectivity, including vulnerability assessments, penetration tests, and security audits to assure that all the applied security measures are effective and that potential vulnerabilities are preempted upon service launch. Important part is the early identification and addressing weaknesses in security mitigation to be performed during the early stages, which further reduces the possibility of any security incident after implementation, caring about security issues of the new service and make them considered.

- It is to be intended as a joint effort involving the *Security Division* and the *Service Quality Unit*. Independent testing may be engaged with external security consultants. The *CIO* and *Security Division Head* review results and approve necessary remediation actions.
- *Security Documentation and Training*
  - Security documentation for the new service and related training of relevant staff in security procedures and best practices. That all staff involved in running and supporting the new service understand security measures and what is expected from them.
  - It enhances the human element of security, reducing the likelihood of breaches through human error or non-awareness. A security-conscious culture instills this at an organizational level. The *Security Division* leads in documentation development, while the *HR Department* acts to coordinate training sessions. The *Unit for Service Quality* is saddled with training effectiveness and staff absorption of requisite information.

#### 6.2.5.5. Service Configuration Management

*Service configuration management* practice ensures accurate and reliable information is able to support CIs and make it available when needed, so to include information between them and their relationships. In order to maximize the retained value, a configuration management system is held to be accountable of containing and recording information, so to make CIs work together.

It is in this way that Service Configuration Management empowers decision-makers with real-time insight, powers efficient change processes, and acts as an important facilitator for many other ITIL practices. This ensures every component—from the smallest network switch to the most complex application—has a place accounted for and understood within the greater ecosystem. This will help in the smooth transition of digital infrastructure to the bank, reduce associated risks, and lay a foundation for future innovations.

The following are to be considered the *key activities* to be applied for this practice:

- *Configuration Item Identification and Registration*
  - This means the identification and registration of all CIs related to the services being turned off while making the transition to the Token Connectivity service. This shall capture the essential attributes: CI type, owner, status, relationship with other CIs.
  - It provides a clear picture of all the assets involved in the decommissioning and implementation of a new service, and hence one can control and manage those assets better during the transition process. This should be headed by the *IT Asset Manager* and collaborated with the *Operations Management Unit* and *Applications Unit* in support of the identification and registering of all relevant CIs.
- *Configuration Management Database Update*
  - The changes within the IT infrastructure from the decommissioning of old services to the implementation of the new Token Connectivity service drove the updates in the CMDB. This will involve the recording of new CIs, updating of existing ones, and removal of items that are now obsolete.
  - The goal of this process is to make the CMDB accurate and up-to-date as a source of information about the IT environment for decision-making and other ITSM processes. This will be implemented by the *Service Configuration Management* team, directly under the supervision of the *IT Asset Manager*, with inputs from various IT units involved in the transition.

- *Configuration Baseline Establishment*
  - This is the configuration baseline, which captures the state of the information technology infrastructure before, during, and after the transition to the new Token Connectivity service. It serves as a reference point for later changes and audits.
  - In general, it allows for easier tracking of changes, supports rollback procedures if needed, and expresses the clarity of the view that the transformation will entail from decommissioning and implementation of a new service. It then will be controlled by the *Service Configuration Manager*, on approval by the manager, *IT Strategy Unit*, and the *CIO*.
- *Configuration Verification and Audit*
  - Run regular verification and audits on the accuracy and completeness of the configuration information. This will be particularly true during transition when many changes are happening.
  - It helps in the integrity of configuration information, early inconsistency detection, and compliance with regulatory requirements. This is performed by the *Service Quality Unit* in cooperation with the *Service Configuration Management* team. Results are reported to the *IT Asset Manager* and the *CIO*.
- *Configuration Management Process Integration*
  - This process must be integrated with other processes in ITSM: Change Management, Incident Management, and Problem Management. It will ensure uniformity of applying and updating configuration information in all activities.
  - It improves the overall efficiency of ITSM processes, reduces errors caused by inaccurate or obsolete configuration information, and facilitates better decisions across the whole of IT operations. Under the guidance of the *IT Strategy Unit Manager*, collaboration with other ITSM Process Managers on the establishment and maintenance of appropriate integration points.

#### **6.2.5.6. Change Control**

The scope of the *Change Control* practice is strictly defined by each organization, including all of IT infrastructure, applications, documentation and processes of various kinds. It must balance the need to make beneficial changes that will deliver additional value with the need to be protected from the adverse effect of changes. All changes should be assessed by competent patients who have the ability to understand the risks and expected benefits; the changes must then be authorized. Before they are deployed, these should be assessed. This assessment shall not introduce in-built delay.

It's important to handle all types of changes, may it be standard (low-risk, pre-authorized), normal (scheduled, assed, for which there is a normal procedure) and emergency ones (not typically included in a change schedule and they can be implemented quickly and precisely). This is to be done in order according to a schedule so to help planned changes, assist in communication, and assign resources, following relevant change rules.

The following are to be considered the *key activities* to be applied for this practice:

- *Design Change Evaluation*
  - Throughout the development project, there will be inevitable pressures to alter the original design due to technical difficulties, changing business requirements, or new opportunities. All proposed design changes must be properly reviewed. It could include change impact analysis of the user interface, authentication process alteration, or even a change in integration with other bank systems of the Token Connectivity arrangement. Technical feasibility, user experience,

security implications, and strategic alignment to the digital agenda of the bank must be covered during the impact assessment.

- This has the goal to ensure that design changes improve and don't reduce the intended value of the service, and they are coherent with the bank's strategic objectives. The subprocess will be guided by the *Change Advisory Board (CAB)*, supported by the *IT Strategy Unit* and the *Service Design* team.
- *Build Process Change Management*
  - It is envisaged that these development and build processes may potentially change during the progress of the Token Connectivity project for faster delivery, better quality, or closer integration between development and operations teams. These changes may involve new Agile methodologies, further automation testing tools, or changes in the CI/CD pipeline. All of these changes have to be handled with great care to make sure that they actually bring improvement to the development process and are not a cause of instability or inconsistency.
  - It wants to facilitate continuous process improvement in the building, while ensuring stability and consistency for the development of services. This will be led by the *Change Manager* but worked collaboratively with the *Development team* leads and DevOps specialists.
- *Vendor and Technology Selection Changes*
  - The connectivity required by the Token project may require new vendors or technologies not envisioned at the beginning. This may involve new hardware providers, software platforms, or specialized consultancy services. Any change in this realm should be very carefully evaluated and managed. Equally, when a new technology is proposed—a security token type or a new API management platform—the change process has to make sure that this technology is really checked against compatibility with the existing systems and brings real added value for the project.
  - In general, it ensures that any changes to the technology base or supplier relationships are rigorously checked and aligned with the service requirements and bank strategic direction. This will be led by the *Supplier Manager* in conjunction with the *IT Strategy Unit* and subject matter experts from relevant technical teams.
- *Integration Change Coordination*
  - Coordinating changes so to control how integration points are affected between existing Connectivity services and existing bank systems or third-party systems. When changes are made, it has to be ensured they are beneficial to their way of operating, ensuring interoperability across the bank's evolving IT ecosystem.
  - Mitigation of risks associated with other changes needs to be assessed and seen beforehand. This is to be implemented by the Integration team, under the guidance of the *Change Manager*, interfacing with the *Service Architecture* team.
- *Pre-deployment Change Validation*
  - Any new change has to be vigorously validated before being rolled out to the production environment. In the case of the Token Connectivity service, this becomes essential, as it is part of the most central operations at the bank, substantially impacting customer trust and regulatory compliance. Validation may involve a variety of activities, such as peer review of code, automated testing, load performance testing, penetration testing for security, and user acceptance testing.

- It provides integrity in the service build, reducing the likelihood of defects and minimizing rework in the later stages of development. This would be carried out by the *Quality Assurance team* in conjunction with the *Change Manager* and relevant development teams. The CAB would then review the results prior to final approval to integrate.

#### 6.2.6. Deliver & Support

The purpose of this SVC activity is to ensure services are delivered and supported according to agreed specification and expectations, particularly relevant for the presented decommissioning case. It is, therefore, a crucible wherein well-thought-out strategic plans and carefully designed services find the actual implementation test in a real-world setting—that is, facing user adoption and retaining continual improvement over shared value when created with collaborative work between engaged stakeholders. It's inside of this phase promises of enhanced connectivity and improved security meet streamlined operations, translating them into tangible benefits into everyday practices. A balance must be met and preserved between the need to preserve continuity of service with legacy systems, while at the same time making progressive shifts of resources and focus towards the new token connectivity infrastructure.

This SVC activity has a corresponding series of *inputs*:

- Tasks related to user support and information from third-party services “*Engage*”
- New and changed products and services for “*Design and transition*”
- Information on service components and services in design and transition of new and updated services and service components from “*Obtain/build*”
- The “*Obtain/Build*” service components
- Improvement initiatives and improvement status reports from “*Improve*”

It's also important, for this SVC activity, to focus on its corresponding series of *outputs*:

- Services provided to customers/users
- Information regarding the completion of a task for user support tasks in “*Engage*”
- Contract and agreement requirements for “*Engage*”
- Information on the performance of products and services regarding “*Engage*” and “*Improve*”
- Change Requests for “*Obtain/Build*”
- Improvement opportunities for “*Improve*”

##### 6.2.6.1. Service Desk

The *Service Desk* is particularly relevant, since it provides a clear path for users to report issues, queries and requests to acknowledge practices and ensure virtual and factual connection and coordination between different people, may them be users, stakeholders or other general staff. It works on a different number of channels, incorporating mainly the qualities present within Figure 12.





Figure 12: Service desk workflow and qualities

The Service Desk, embodying the qualities illustrated in the figure, acts as both a single point of contact for transition-related issues and a reference for user empowerment. It's where the theoretical benefits of the new Token Connectivity service are translated into practical, day-to-day value for end-users. By leveraging emotional intelligence, empathy, and excellent customer service skills, the Service Desk ensures that users feel supported and heard throughout the decommissioning and transition process.

The following are to be considered the *key activities* to be applied for this practice:

- *User Support and Query Management*
  - It's mainly involved in front line support to users as they transit from Home Connectivity and USB Connectivity to the new Token Connectivity service. This includes attending to queries, troubleshooting, and orienting them on how to use the new system, while offering ready availability of services and problems the correct way.
  - This presumes a smooth transition for their users with minimal fuss and as maximal implementation of the new service as possible. The empathy and emotional quotient of the service desk people handle these concerns and frustrations. These professionals, led by the *Service Desk Manager*, and ably supported by trained Service Desk analysts— who embody these same skills—are shown in the following illustration.
- *Incident Triage and Escalation*
  - The examination and qualification of incidents related to old and new connectivity services are done fast, ensuring a resolution or escalation to the appropriate teams. Exploiting the service desk qualities, a greater ability of reducing low-level work and escalating directly issues so to intervene against problems is an earned capacity from within teams of operations.
  - It minimizes the disruption of services and sustains user productivity during the transition. This task very much depends on the incident analysis and prioritization competences described in the figure. This will be done by Service Desk analysts with defined escalation paths set by the *Service Desk Manager* in conjunction with the technical support teams.
- *Knowledge Base Management*
  - Empower the service desk staff to accurately and consistently support users with self-service opportunities. This works on the premise that the team will understand business priority and that the people in the team are good at communicating. It is being maintained by a dedicated

individual as the Knowledge Manager, the Service Desk team, and with contributions and feedback incorporated into the database from various IT units and the users.

- *User Feedback Collection and Analysis*
  - This involves a systematical gathering and analysis of user feedback on both the decommissioning process and the new Token Connectivity service, so to ensure a good reaching of value and control across all stages of analysis and operations. This can be done both manually and automatically, providing points of contact and understandings.
  - It gives valuable insight into service improvement and identification of any unexpected problems or opportunities. Such a process utilizes the Service Desk's empathy and customer service skills in order to foster the end-users to provide honest and constructive feedback. Led by the *Service Desk Manager*, with analytical support from the *Service Quality Unit*.
- *Transition Communication and Support*
  - It is the main way of communication of updates, instructions and support, when using all relevant channels of information, ensuring a prepared and smooth service transition the correct way.
  - This way, users are well-informed and prepared for change; therefore, it reduces resistance and smooths the transition process. The figure has a dependence on effective communication skills as far as this activity is concerned. Executed by the Service Desk team in close coordination with the Change Management and Communications teams.

#### 6.2.6.2. Incident Management

*Incident management* ensure to minimize negative impacts of changes and incidents, defined as unplanned interruptions to services and reduction of their quality. Incident logging, prioritization, and resolution are very critical facets in the delivery of excellent customer and user experiences. Every incident that may arise—be it from the legacy systems or teething issues with the new service—ought to be logged and managed to make sure it gets resolved within time frames that meet customer and user expectations. This requires good practice design, which can offer appropriate management and allocation of resources to incident types, from low-impact issues needing efficient handling to larger impact incidents needing more sophisticated management and resources.

In our context, the incident management practice will have to be quite agile so that it works with equal ease on old and new connectivity services. This may involve teams from the service desk, technical support, application support, and external vendors that might get engaged in the implementation of Token Connectivity. An appropriate tool storing incident records, preferably with links to relevant CIs, changes, problems, and known errors, will support the quick and effective diagnosis and recovery of incidents.

The following are to be considered the *key activities* to be applied for this practice:

- *Incident Detection and Logging*
  - This revolves around fast identification and recording of any service disruptions or anomalies across both the legacy connectivity services and the new Token Connectivity platform, using automated monitoring tools, user reports channeled through the Service Desk, and self-help records.
  - Ensures that no event goes undetected; hence, it gives a comprehensive view of service health during this transition period. Each record of incidents should give complete information about symptoms, business impact, affected CIs, completed actions, and planned actions; all these with

timestamps and details of persons involved in the same. It's led by the *Incident Management Team* but will work in close collaboration with the *Service Desk* and the *Operations Management Unit*.

- *Incident Categorization and Prioritization*

- Systematic categorization of incidents according to nature and impact, with special consideration to those issues that may affect the decommissioning process or the implementation of Token Connectivity. Prioritization of incidents to ensure that the ones with the greatest business impact are addressed first.
- The process facilitates efficient resource allocation and permits realistic resolution times to be set. Should be agreed upon, documented, and communicated to all relevant parties. Executed by *Incident Managers* with contributions from the *Service Desk* and applicable technical teams.

- *Investigation and Diagnosis*

- That is, detailed analysis of incidents to identify the root cause, which may be due to legacy system problems, transition-related issues, or even due to new service teething troubles. Supplementing it by scripts for gathering information from users at first contact, for the diagnosis and resolution of simple incidents becomes a must in order for this process to be important and relevant.
- In general, it assists in fast resolution and reduces down-time and user frustration. This activity, for the more complex incidents, is heavily dependent on knowledge and expertise rather than procedural steps. This may also include swarming techniques for the more complex issues, led by *Incident Managers* and carried out by specialized technical teams.

- *Resolution and Recovery*

- This process wants to implement the solutions to solve incidents and restore normal service operation, both on legacy systems and on the new Token Connectivity service. This can be escalated to a number of groups, depending on the level of complexity: self-help of the users, resolution by the service desk, escalation to a support team, or even invocation of disaster recovery plans at the extreme end.
- It also ensures the continuity of essential services throughout the period of transition and builds user confidence in the new system. This is where effective communication and collaboration between teams is very vital. Carried out by technical support teams, coordinated by an *incident manager*, intermediated with periodic updates to the *Service Desk*, and perhaps third parties being brought in.

- *Incident Closure and Reporting*

- Formal closure of resolved incidents after confirmation with the affected users; production of reports totaling incident trends and resolution success. Capture of which specific self-help records used for measurement and improvement activities.
- Here, it's important to keep an eye at valuable data for continual service improvement and identification of any systemic issues in transition process. This information shall form a key input to any Improvement activity, prioritized both by frequency and severity of Incident. These are managed by Incident Managers, and user satisfaction will be confirmed by the Service Desk.

### 6.2.6.3. Infrastructure and Platform Management

The *Infrastructure and Platform Management* practice is designed to manage and control the components of IT infrastructure that enable the delivery of services to the business. Ensuring IT infrastructure—hardware and software—is fit for purpose, maintained, and operated in an efficient manner for the business needs and service delivery.

Technology should be sufficiently provided in order to support the activities able to create value for the organization and its stakeholders. This can include being ready to adopt new technologies but also to consider how the organization develops its own strategy to achieve intended outcomes without any type of platform or infrastructure, optimizing business goals to be reached efficiently and with the intended service quality. This will also involve the management of the existing infrastructure components and the new ones to ensure that the operations during and after the decommissioning are smoothly done.

The following are to be considered the *key activities* to be applied for this practice:

- *Infrastructure Monitoring and Maintenance*
  - This includes the monitoring of all components of the infrastructure, such as servers, networks, and storage systems, in both new and legacy connectivity services. It shall include reactive maintenance to forestall breakdowns and ensure optimal performance.
  - In general, it ensures that IT services remain stable and reliable during transition. This activity is led by the *Infrastructure Management Team* with help from the *Operations Management Unit*, and potential external vendors in respect to specialized components. Monitoring tools are used, across with technologies, skilled personnel able to interpret and act on monitoring data.
- *Capacity Planning and Optimization*
  - It will involve assessing how infrastructures are currently used, and the infrastructures' future needs will be forecasted. Also, planning for appropriate capacity to support the new Token Connectivity service and managing the phase-out of legacy systems is necessary. This is held to be necessary to achieve efficient resource allocation and cost optimization.
  - In this case, relevant capacity planning tools are involved, with the help of historical data and analytical skills, able to reach goals and satisfy a correct business understanding. It's typically executed by *Capacity Planners* with input from *Infrastructure Managers* and relevant business units. It may involve consultations, in the future, with technology vendors for future planning.
- *Technology Refresh and Upgrade Management*
  - It manages the process of introducing new components of infrastructure for the Token Connectivity service and supervises the gradual phase-out process of the legacy infrastructure. These include the planning of upgrades, implementation supervision, and management of procurement, while change management skills are involved with different impacting service delivery processes and capabilities, while updating and introducing new technologies.
  - This involves ensuring that updates to the infrastructure are made and kept in a state capable of supported the evolving business needs. This is coordinated by the *Infrastructure Managers* with the help of the *Procurement Teams* and the involvement of the *Technical Specialists* for specific components.

- *Security Patch Management*

- This means identifying, testing, and applying security patches in all infrastructure components, specifically taking care of the maintenance of security during the transition period. Focusing on maintaining secure and up-to-date systems is the key, since security expertise might be one of the most important aspects to touch and contribute to overall risk management processes, keeping strict collaboration with relevant stakeholders and software vendors.
- It is an activity usually led by *Security Specialists* in coordination with *System Administrators*, directly overseen by the *Infrastructure Manager*, and essential to the security posture of the infrastructure.

- *Configuration Management of Infrastructure Components*

- This involves detailed record-keeping for all components of the infrastructure in terms of configuration and interdependency. The same is very crucial during transition to ensure all legacy and new components are accounted for.
- In general, this process focuses on relevant configuration management tool, databases and the correct people to give and keep attention to detail and system knowledge. This is managed by Configuration Managers with input from various technical teams, both internal and external. Tracking details over system knowledge and implementation might share even more value when attached to relevant vendor-supplied components and their configurations.

#### 6.2.6.4. Monitoring and Event Management

The purpose of the *monitoring and event management* practice is to observe services and service components and record important events, keeping control and systematic observation of services able to impact CIs and underpinning services, which can be done actively or passively. Monitoring comes from multiple activities and acting on events may be a reactive step to intervene and establish action over different kinds of events.

The processes and procedures needed in this context will be instrumental in managing the transition from the legacy connectivity services to the new Token Connectivity platform. It will be responsible for monitoring not only existing but also new infrastructure components to ensure its smooth operation and detection of issues that may arise during this process. Bringing a different range of perspective is needed in successful monitoring and event management, so to correlate events and leveraging the available expertise at all times. Only needed data should be required, in order to make provision for explicitly defined contracts and agreements.

An ideal logical schema for this practice would be like the one present in Figure 13:

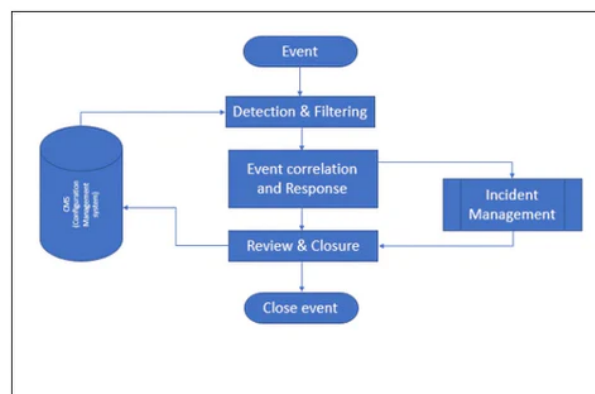


Figure 13: Monitoring and event management logical workflow

The following are to be considered the *key activities* to be applied for this practice:

- *Event Detection and Filtering*
  - This means continuous monitoring of all IT services and infrastructure components, which covers not only legacy systems but also the new Token Connectivity Service. This shall provide the set-up of appropriate monitoring tools and thresholds that shall identify significant events.
- *Event Correlation and Prioritization*
  - Inevitably, once events are detected, they will have to be analyzed in context. This activity is really critical in understanding the real impact of events during a transition period when the IT environment is in flux. Correlation identifies relationships between multiple events that may be symptoms of some larger issue. Prioritization comes equal in ensuring that the most critical events get immediate attention.
  - This ensures that any potential issues that may affect the delivery of service are detected early. The activity is led by the monitoring team in collaboration with the *infrastructure management team* and *service desk*.
- *Response Selection and Execution*
  - This involves identifying the right action to be taken for every event identified. The reaction may be as simple as recording the event for future reference or even triggering major incident procedures. In the transition to Token Connectivity, response processes will have to be changed to address new scenarios.
  - The *Event Management Team* should have a close relationship with other teams to ensure that responses are coordinated and effective. In view of this shifting IT landscape, this may mean developing new, or changes to existing, escalation paths.
- *Review and Closure*
  - It considers reviewing the handling of major events, especially those realized from the decommissioning process and the new Token Connectivity service. This includes the updating of event records and knowledge bases that feed continuously inside relevant continual improvement processes while gaining feedback at all stages.
  - Important in the continuous improvement process of managing events and their evolution impacting different parts and components of an organization. The whole process of this activity is usually driven by the event managers in close cooperation with service owners and technical teams.
- *Reporting and Performance Improvement*
  - It involves the generation of reports on trends in events, with a special focus on events relevant to the transition process. It also entails the identification of monitoring and event management process areas for improvement.
  - Supports the decision-making process and continual improvement, while using different reporting and analytics tools, careful data analysis and presentation skills. This will be managed by the *Event Managers* in consultation with various stakeholders.

#### 6.2.6.5. Service Level Management

The practice of *Service Level Management* allows for the setting of clear business-based targets regarding service levels and ensures that service delivery will be correctly assessed against those targets, thus being monitored and managed. This practice is instrumental in establishing, maintaining, and improving relations between the service provider and its customers by assuring that agreed service levels shall be met consistently.

Consistent agreements should be made as tools to both measure performances but also as a simply-written/easy-to-understand language in use for all parties. Service providers need to be in line with service level metrics requested from the final product, in order to continuously support outputs and avoid watermelon SLA effect, so to have customers dissatisfied from the actual real product. Activities of engaging and listening provide a tremendous opportunity to establish improved relations and concentrate on what really has to be delivered. Additionally, this will provide service delivery staff with experience-based insight into the day-to-day work being done with their technology, thus enabling delivery of a more business-focused service.

The following are to be considered the *key activities* to be applied for this practice:

- *Service Level Agreement (SLA) Development and Maintenance*
  - It involves crafting agreements that clearly define the expected service levels for both the legacy connectivity services and the new Token Connectivity platform. During this transition period, SLAs will need to be particularly flexible and adaptable. They may need to include clauses that account for potential service disruptions during the migration process, while also setting clear expectations for the performance of the new Token Connectivity service.
  - Warrants clear expectations for service delivery during the transition period. This activity is led by the *Service Level Manager* in collaboration with *Customer Relationship Managers* and *Service Owners*. Service management tools for SLA documentation are needed to fully coordinate teams/ service knowledge and SLAs with service providers.
- *Service Performance Monitoring*
  - It doesn't mean that once SLAs are in place, monitoring can stop; rather, it becomes regular to ensure the continual meeting of the agreed service levels. This activity gains added importance during the transition period since it is going to provide vital feedback on how well both legacy and new services perform. Monitoring will have to be all-encompassing, starting from the technical performance metrics to user satisfaction levels in service delivery.
  - This activity helps in identifying any service level breaches or trends. It's typically executed by *Service Level Analysts* with input from *Technical Teams* and *Monitoring Systems*. All kinds of monitoring should be needed to preserve performance and coordinate problems first-hand and supporting adequately processes, both on the people and technological side
- *Service Review and Reporting*
  - Reviews shall be critical during the transition to ensure that everything is open and clear to the customer. These reviews could provide a forum for discussing service performance against agreed-upon specifications, discussing any issues or concerns, and aligning expectations regarding the ongoing migration to Token Connectivity. Reports for these reviews need to clearly show performance against SLAs for legacy and new services. They might include trend analysis to show how service levels are evolving over time as the transition progresses.

- Ensures ongoing communication and alignment with customer expectations. This is coordinated by the *Service Level Manager* with involvement from *Customer Relationship Managers* and relevant *Technical Teams*. Reporting and presentation tools are used and presented coherently, involving also joint reviews, analyze data and feed accordingly continual service improvement processes.
- *Service Improvement Planning*
  - This activity is oriented towards the identification and implementation of improvements to service delivery in line with insights emanating from performance monitoring, service reviews, and customer feedback. Planning for improvements assumes greater importance during the process of transition to Token Connectivity. It could be attending to tackling problems in the new service or how best to optimize the integration between old and new systems, or even how to speed up the actual migration process with minimum disruption.
  - Critical for maintaining and improving service quality. This activity is typically led by the *Service Level Manager* in coordination with *Service Owners* and *Continual Improvement Managers*. Strategic thinking and problem-solving skills are to be introduced at all levels and improve initiatives across various processes.
- *Operational Level Agreement (OLA) and Underpinning Contract (UC) Management*
  - This process oversees the internal agreements (OLAs) and external contracts (UCs) that back the delivery of services to the customer. This can be quite complex during transition to Token Connectivity because it may involve renegotiation of existing agreements and establishment of new agreements. It also makes sure that, with the phasing out of the legacy services, related OLAs and UCs are wound down or terminated appropriately.
  - Supports the achievement of SLAs by ensuring proper support from all service components. This is managed by the *Service Level Manager* with input from *Internal Support Teams* and *Supplier Managers*. Contract management and negotiation involves management of supplier relationships and contracts, so to carry out roles and responsibilities in a coordinated and precise way

#### 6.2.6.6. Release Management

*Release Management* practice aims to plan, schedule, and control the movement of releases to test and live environments. This practice ensures that the integrity of the live environment is protected and that the correct components are released, making new and changed services and features available for use.

In our context, Release Management will play a critical role in managing the rollout of the new Token Connectivity service while gradually decommissioning the legacy connectivity services. It will need to coordinate releases for both the new service implementation and any necessary changes to existing systems during the transition period.

An ideal release management workflow would work like the one present in Figure 14:

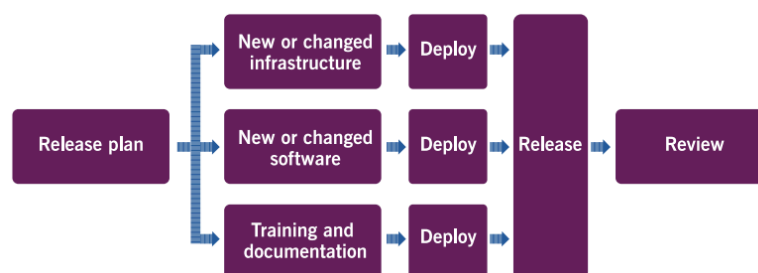


Figure 14: Release management in an Agile workflow



As showed, it strictly depends on the model being used, commissioned and used in delivering the product while supporting it continuously. An ideal product delivery would follow phased, step-by-step approaches, so to enter into production environments when functionalities are analyzed, tested, studied and available in a correct way. The approach followed by the Bank would follow an ideal continuous integration/continuous delivery (CI/CD) approach, so record release and maintain relevant information about them.

The following are to be considered the *key activities* to be applied for this practice:

- *Release Planning*
  - Release planning is one of the most critical activities that paves the way for the whole release process. This activity, already complex in itself, is even more so in the case of a connectivity Token transition, which needs consideration of the rollout for a new service and the gradual decommissioning of legacy systems. In this regard, the release plan should sequence carefully the introduction of the new Token Connectivity components with the retirement of the old connectivity services. This might involve multiple releases over a longer period, each of which would add features of Token Connectivity while retiring certain aspects of the legacy systems.
  - Ensures that changes are implemented in a controlled manner. This activity is led by the *Release Manager* in collaboration with the *Change Managers, Project Managers, and Technical Teams*. The coordination demands planning and coordinating skills when coordinating between different teams and project management processes.
- *Release Build and Configuration*
  - This is the activity consisting of the actual assembly and configuration of all the components to be included in the release. In Token Connectivity, this would be complex for both setting up new systems and reconfiguring existing ones. The build of a Token Connectivity release may involve activities like configuring new network components, setting up authentication systems, and the user management database. This becomes very important in a hybrid environment where legacy and new systems are supposed to coexist and interact.
  - It guarantees that all the components are well prepared for deployment. It is usually executed by *Release Engineers* with inputs from *Development Teams* and *Infrastructure Teams*. While a good software development lifecycle needs to be in act, build and configuration management automated tools should integrate stakeholders and customer direct ideas.
- *Release Testing and Validation*
  - Testing at depth is necessary to ensure that every release works as expected and does not introduce any new problems. In the case of the Token Connectivity transition, testing becomes more challenging because it must address not only the new service but also its interactions with the legacy systems and the impact caused by decommissioning activities. Testing should also include functional testing of the token connectivity features, performance testing to check that this is at least as good as, if not better than, the capabilities of legacy systems, and integration testing to confirm that new and old components will interact without problems. More specifically, User Acceptance Testing (UAT) is important for involving representatives from different user groups to ensure that the new service is in line with their requirements, and for making the new service intuitive.
  - Ensures that the release realizes quality standards and business requirements. This shall be organized by *Test Managers* with involvement from *Quality Assurance Teams* and *User*

*Acceptance Testers.* Assurance processes shall consider knowledge of testing tools and environments in business processes, including third-party testing services.

- *Release Deployment*

- In the deployment stage, the well-planned and tested release is actually pushed to production. For the Token Connectivity project, this will likely be a phased deployment rather than a single big-bang deploy. Early deployments may involve setting up the core of the Token Connectivity infrastructure and the migration of a small pilot group of users. Subsequent deployments would then be gradually expanded to the user base and feature set while bringing down parts of the legacy systems. Each deployment needs to be carefully orchestrated to minimize disruption to business operations.
- Critical to ensure smooth transition with minimal disruption to the service. This activity is usually led by the *Release Manager* in coordination with the *Change Managers*, *Infrastructure Teams*, and the *Service Desk*. Integrations between the processes of change management and incident management shall be used, which involves coordination with external service providers for deployment activities using relevant tools and techniques.

- *Post-Implementation Review*

- After every release, a review of the same is necessary in order to know the success or failure and learn from it. In a project as long and complex as the Token Connectivity transition, this is even more necessary. Reviews shall be against the objectives of the release, considering technical as well as business results. This can include metrics of system performance, user adoption rate, or any other promotion in business processes. Feedback should be collected from all types and classes of stakeholders, including the end-user, support staff, and business leaders.
- Supports the continual improvement of the release process and informs future releases. The *Release Manager* manages this with input from various stakeholders, including *Service Owners*, *Technical Teams*, and *End Users*. Analytical and communication skills feed into continual improvement processes and gathering feedback from external partners.

#### **6.2.6.7. Service Configuration Management**

The following are to be considered the *key activities* to be applied for this practice:

- *Configuration Identification*

- This activity is important at the very beginning of the project since all the CIs that are going to be impacted by, or are part of, the transition should be identified and documented. They will come from both the existing sets of CIs resulting from the connectivity services to be replaced or removed, and new CIs to be introduced with Token Connectivity. This may involve an end-to-end audit of legacy systems to ensure that all their components are captured, including hardware, software, documentation, and service level agreements. This is quite important since over time, some CIs might have been added or modified without proper documentation.
- It is intended to provide an organization-wide view of the IT environment. The *Configuration Manager* will lead this activity in collaboration with *Service Owners* and *Technical Teams*. Discovery tools should be supported, and good management of internal and external providers should be kept over the change and asset management processes in the best possible way.

- *Configuration Control*
  - Control is most complex during the Token Connectivity transition because it needs to manage changes affecting both old and new systems—quite often, simultaneously. In legacy systems, more configuration control would be focused on the gradual decommissioning process. This may include tracking hardware that has been removed or repurposed, archiving data, and updating documentation to reflect that these services are being wound down. Configuration control over the process of introducing new CIs for token connectivity has to be in place to ensure that every new component is correctly recorded and its relationship with other CIs properly mapped. Since new features and capabilities will be introduced from time to time, this will, therefore, be a continuous process.
  - This activity ensures changes to the CIs are properly authorized and documented. It is typically executed by *Configuration Analysts* with inputs from *Change Managers* and *Technical Teams*. Attention to detail and integration is kept with the main adherence to tools and management configurations where relevant.
- *Configuration Status Accounting*
  - It provides status accounting for the present and previous state of all CIs through their lifecycle. This will be a very important tool in managing the complex, changing IT landscape in support of the Token Connectivity transition. For legacy systems, status accounting must follow all aspects of the gradual decommissioning process, which may include capturing time frames when some components are taken offline, when data is migrated, or when the support contracts are terminated. Accomplishment accounting for token connectivity will be necessary to keep track of the rollout of new components, including when they are introduced, when operational, and any problems or changes they undergo in the early stages of deployment.
  - It provides an understanding of the status of the IT environment during transition. This is coordinated by the *Configuration Manager* with involvement from *Service Owners* and *Operations Teams*. To this respect, CIs reporting, with different data analyses running across various IT processes, involves visibility, set targets, and metrics. Communication at all levels works.
- *Configuration Verification and Audit*
  - Regular audits are even more important in times of major transition—like the one that will involve moving to token connectivity. Such audits help to guarantee that what is happening in the rapidly changing IT environment is properly represented within the Configuration Management Database. For legacy systems, audits can ensure that components decommissioned are recorded as such and that no ‘zombie’ systems continue to run unnecessarily. These could involve physical audits of server rooms or network closets to ensure that hardware is removed consistent with record. For connectivity by tokens, audits will have to confirm that all new elements are properly recorded in the CMDB, including their specifications, locations, and relationship with other CIs.
  - Critical for maintaining the integrity of configuration data. This activity is typically led by *Configuration Auditors* in coordination with *Service Owners* and *Technical Teams*. Overall data quality and compliance processes, when involving verifying configuration data from external providers means collaboration and integration with physical asset checks

- *Configuration Information Management*

- This activity is focused on the management of the CMDB itself to ensure it remains a reliable and up-to-date source of information throughout the transition of Token Connectivity. During this time period, the amount and complexity of the information stored in the CMDB are likely to grow tremendously. It will have to keep information about the old and the new systems, track their relationships with each other as they change, and show clearly exactly what progress is being made on the transition process. The CMDB may need redesigning or extending to take on board new types of CIs brought in by token connectivity. There could very well be a need for access to configuration information at differing levels to differing teams.
- This provides accurate configuration data to support effective decision-making. *Configuration Manager* does this, although many IT teams give inputs. Correct management of the CMDB and protection of this data are good data governance and database management skills involved and underpinned in the process. This shall call for managing configuration data related to external services.

## 7. Metrics, performance and maturity

### 7.1. Continual improvement

The retirement of the Home Connectivity and USB Connectivity services provides a very good opportunity to apply ITIL's principle of continual improvement. The process allows our IT service management practice to stay up-to-date with changes in the business and technological environment. We will use KPIs (Key Performance Indicators) and CSFs (Critical Success Factors) to effectively measure and drive this improvement. ITIL benchmark metrics are tools useful in measuring the performance of IT service management processes against recognized standards or previous performance data.

KPIs use metrics to measure the CSFs. Therefore, KPI would simply be a metric that has a linkage or relationship with a target to say whether we have met or not met our CSF. Usually, KPI means how far above or below a predefined target.

#### 7.1.1. Critical Success Factors (CSFs)

These CSFs are the critical elements that must be achieved if our decommissioning project is to be successful. They represent the key areas in which satisfactory results will ensure successful competitive performance. These can be defined as the limited number of areas in which satisfactory results will ensure successful competitive performance for the individual, department or organization and are the areas which must go right for the business to continue working well.

Such contribute on the definition of indicators, which are to be based by the ones given in this subsection, so to further complement and implement indicators into successful operation for the decommissioning project. For each CSF found, a high-level overview and a textual description will be provided, in order to make the analysis further precise and scope the decommissioning carefully.

- *Comprehensive inventory of IT assets*
  - Ensures accurate scope and scale understanding
  - Enables effective planning and execution
  - Prevents assets from being overloaded or underused
  - Identifies all dependencies

This lays the foundation for the entire project, given without a clear understanding of the scope and scale of the assets involved, it would be impossible to plan and execute the decommissioning effectively. This inventory must be accurate, complete and up-to-date, ensuring no asset is overlooked, particularly when multiple assets work together and so all dependencies must be accounted for.

- *Effective stakeholder communication and engagement*
  - Impacts end users, stakeholders, external partners and senior management
  - Manages expectations and addresses concerns
  - Builds project support
  - Requires a transparent, reactive and tailored approach

The stakeholders who will be impacted by the decommissioning project include a broad base of end-users, IT staff, external partners, and senior management. Very clearly, setting lines of communications and engaging in such accordingly will help the project team manage expectations

and alleviate concerns for the purpose of securing support for the project. Such engagement needs to be reactive, open, and based on needs and preferences of each stakeholder group.

- *Robust risk management*
  - Identifies, assesses, and mitigates any potential issues.
  - Covers risks in data security, service continuity, and compliance
  - Reduces the chance of occurrence and the impact of adverse events
  - Requires a systematic and continuous process

Given the complexity and potential risks associated with decommissioning IT services, such practice is to be considered essential. This CSF involves reactively identify, assess and mitigate risks so to be prepared for unexpected disruptions, anticipating and addressing potential issues related to different aspects of operations, may them be service continuity, compliance, and likelihood/impact of adverse events. This requires a systematic and ongoing process of risk assessment, prioritization and treatment.

- *Seamless user transition to Token Connectivity service*
  - It calls for careful planning, testing, and support
  - It includes end-user training and resources
  - It minimizes disruption of the user's work
  - Uses a phased and iterative approach with feedback loops

To achieve this CSF, the project team must ensure the migration process is carefully planned, thoroughly tested and well-supported in all of its points. This involves providing comprehensive training, resources, assistance to end-users so preserve working operations and smooth adoptions of new services. Such process should be phased, agile, iterative with wide opportunities for feedback and improvement over feedback loops.

- *Compliance with security policies and regulations*
  - Non-negotiable requirement given bank's sensitive operations
  - It covers all aspects of the project, particularly asset disposal
  - Conforms to applicable standards and guides
  - This will involve the cooperation of compliance experts and stringent documentation

This CSF is considered non-negotiable, since the sensitive nature of operations conducted by the bank are essential to the project success, particularly the disposal of IT assets, adhering to relevant standards and guidelines. This requires a precise understanding of applicable regulations, close collaboration with compliance experts, both internal and external, with rigorous documentation over assessments conducted and procedures to take.

- *Effective project management and timely completion*
  - Underpins the entirety of the decommissioning effort
  - Sets clear objectives and defines roles and responsibilities
  - Closely monitors the progress and costs
  - Uses best practice: status updates, risk tracking, change control
  - Ensures on-time, within-budget, and quality delivery

- Regular project status reviews conducted
- Project milestones met according to change schedule and baselines established
- Budget adherence throughout all project lifecycle

This underpins the entire decommissioning effort, since it involves clear goals, objectives, clear roles and responsibilities to be defined and updated, so to control issues, tracking them, ensure correct changes (change enablement), ensuring correct usage of all kinds of resources within budget and required quality standards.

- *Service quality maintenance*

- New Token Connectivity service meets or exceeds previous service levels
- Performance metrics continuously monitored and re-evaluated
- Rapid response to any service quality issues

It's important to ensure that the new Token Connectivity service provides a quality of service as good as, or better than, that of the services being turned down. Appropriately set service level targets, with regular measurement of performance against those targets, are key to the speedy resolution of any issues arising. Continuous monitoring and improvement of the new service will help to maintain user satisfaction and business continuity.

- *Knowledge management and transfer*

- Lessons learned, documented and assessed throughout the project working
- Knowledge base created for future reference
- Training materials developed for ongoing use

Effective knowledge capture and transfer is important for the decommissioning project's long-term success and future projects. This should include proper documentation of lessons learned, reusable knowledge base, and training materials development. The organization will be better equipped to improve its IT service management practices and deal with similar efforts in the future if these experiences and insights are appropriately preserved and passed on.

### **7.1.2. Key Performance Indicators (KPIs)**

KPIs are quantifiable targets that measure the performance and progress of our decommissioning project. They provide objective data for evaluating how well we are achieving our goals.

The IT helps deliver operating efficiency, development innovation, and value delivery to customers and other stakeholders of the business. Therefore, effective management of IT services becomes significant. This is where your ITIL KPIs come into play. Some critical business parts that should ensure the ITIL KPIs will include technology—developing the backbone of all IT solutions; processes—defining the way in which IT services should be delivered and managed; and services—concrete IT offerings that businesses rely on.

The implementation of ITIL KPIs into organizations provides insightful metrics for driving continuous improvement, ensuring that IT becomes a resilient enabler of organizational success. Such represent particular values to be reached and achieved and are used in conjunction with CSFs, with target being percentages, ratios, indexes or composite averages. Defining adequate KPIs highly depends on the successful project execution, so to establish correctly specific indications which can be measured and defined.

In the following parts, many will be explored, taking as main reference the application for the relevant ITIL processes. For each one, a definition will be given, followed by a measurement frequency, the target to be reached and formula/measure (where present/relevant).

- IT Asset Inventory KPIs
  - *Percentage of assets inventoried within the planned timeframe*
    - Definition: Proportion of IT assets related to the retired services, which have been properly inventoried and documented in the timeframe planned for it
    - Measurement frequency: Weekly
    - Target: 100% within the first month of the project
    - Formula:  
$$\left( \frac{\text{Number of Assets inventoried}}{\text{Total Number of Assets to be inventoried}} \right) \times 100$$
  - *Accuracy of asset inventory*
    - Definition: The percentage of assets correctly identified and documented in the inventory
    - Measurement frequency: Monthly
    - Target: 98% Accuracy
    - Formula:  
$$\left( \frac{\text{Number of assets documented accurately}}{\text{Total number of inventoried assets}} \right) \times 100$$
- Stakeholder Engagement KPIs
  - *Communication plan implementation percentage in terms of informing and engaging all stakeholders*
    - Definition: Percentage of the identified stakeholders who are informed and engaged as per the project's communication plan
    - Measurement frequency: Bi-weekly
    - Target: 95% of the identified stakeholders would be engaged within the first two weeks
    - Formula: 
$$\left( \frac{\text{Number of stakeholders informed and engaged}}{\text{Total number of identified stakeholders}} \right) \times 100$$
  - *Stakeholder satisfaction score*
    - Definition: Average score of satisfaction of the stakeholders based on surveys or feedback collected
    - Measurement frequency: Monthly
    - Measure: Average satisfaction score
    - Target: 4 out of 5
    - Measurement method: 5-point Likert scale-based stakeholder surveys
- Risk Management KPIs
  - *Number of identified risks mitigated successfully*
    - Definition: Number of risks identified to have been mitigated through the implementation of risk management strategies
    - Measure frequency: Monthly



- Target: 90% identified risks mitigated
- Formula: Count of mitigated risks
- *Percentage of high-impact risks addressed by project midpoint*
  - Definition: The percentage of high-impact risks addressed as of the midpoint of the project timeline
  - Measure frequency: One-time, at project midpoint
  - Target: 100% high impact risks addressed
  - Formula:  $\left( \frac{\text{Number of high-effect risks addressed}}{\text{Total number of high-effect risks identified}} \right) \times 100$
- User Transition KPIs
  - *Percentage of users migrated to the Token Connectivity service*
    - Definition: The percentage of users that are moved to the new service of Token Connectivity
    - Measuring frequency: Weekly
    - Target: 98% of the users have been migrated by the end of the project
    - Formula: Number of users successfully migrated / total no. of users to be migrated)  $\times 100$
  - *Number of transition-related support tickets*
    - Definition: Number of user-raised tickets specifically relating to the transition to the new service
    - Frequency: Daily during transition, weekly thereafter
    - Target: Less than 1 ticket per 20 users transitioned
    - Formula: Count of transition related support tickets
- Compliance KPIs
  - *Percentage of the retired assets in line with security and regulatory policies and procedures*
    - Definition: the proportion of retired assets that were disposed in line with the prevailing security and regulatory policies and procedures
    - Frequency: Monthly
    - Target: 100%
    - Formula:  $\left( \frac{\text{Number of retired assets in compliance}}{\text{Total number of the retired assets}} \right) * 100$
  - *Number of non-compliance incidents*
    - Definition: Number of incidents whereby the decommissioning process has been identified not to follow applicable standards or regulations
    - Measurement frequency: Monthly
    - Target: 0 incidents
    - Formula: Number of incidents of non-compliance

- Project Management KPIs
  - *On-time achievement of project milestones*
    - Definition: The percentage of project milestones achieved within the scheduled timeline
    - Measurement frequency: Monthly
    - Target: 95% of milestones achieved on schedule
    - Formula:  $\left( \frac{\text{Number of milestones achieved on time}}{\text{Total number of milestones}} \right) * 100$
  - *Actual project costs versus budgeted costs*
    - Definition: Difference between the actual costs incurred by the project and the budgeted costs
    - Measurement frequency: Monthly
    - Target: The actual cost should be within 5% of the budgeted cost.
    - Formula:  $\frac{\text{Actual project costs} - \text{Budgeted project costs}}{\text{Budgeted project costs}}$
- Service Quality KPIs
  - *Percentage of availability of the service*
    - Definition: Proportion of time the Token Connectivity Service is available and operational
    - Measurement frequency: Monthly
    - Target: 99.9% Availability
    - Formula:  $\left( \left( \frac{\text{Total service up time}}{\text{Total time in measurement period}} \right) * 100 \right)$
  - *Average response time of service request*
    - Definition: The average time taken to acknowledge and resolve service requests related to the Token Connectivity Service
    - Measurement frequency: Monthly
    - Target: Acknowledge within 1 hour, resolution within 4 hours
    - Formula:  $\frac{\text{Sum of response times}}{\text{Number of service requests}}$
  - *Subscription Satisfaction with New Service*
    - Definition: Percentage of subscription users satisfied or very satisfied by Token Connectivity
    - Measurement frequency: Quarterly
    - Target: 90% of subscription users are satisfied or very satisfied
    - Method of Measurement: User satisfaction survey
- Knowledge Management KPIs
  - *Project documentation completion*
    - Definition: Percent of required project documentation, including key deliverables, decisions, and lessons learned, that are complete
    - Measurement frequency: Monthly
    - Target: 100% of key documents complete at project end
    - Formula:  $\left( \left( \frac{\text{Number of completed documents}}{\text{Number of total required documents}} \right) * 100 \right)$

- *Knowledge base article utilization*
  - Definition: Month over month growth in the number of views or accesses to knowledge base articles related to the decommissioning project
  - Measurement frequency: Monthly
  - Objective: Increase article views by 10% month over month
  - Formula:  $\left( \frac{\text{Current month article views} - \text{Previous month article views}}{\text{Previous month article views}} \right) * 100$
- *Percentage of staff trained on new processes and tools*
  - Definition: The percentage of relevant staffs trained on the new processes and tools related to the decommissioning project
  - Measurement frequency: Monthly
  - Goal: 95% relevant staffs trained at project completion
  - Formula:  $\left( \frac{\text{Number of staff trained}}{\text{Total number of relevant staff}} \right) * 100$

### 7.1.3. KPI/CSF Mapping

The following table presents how each CSF is mapped to its corresponding KPIs. Clearly, this table, as shown in Table 3, presents how the success of each CSF would be measured throughout the decommissioning project. This was realized to further help visualization and comprehension of ITIL application for such decommissioning project.

This mapping will allow the project team to monitor effectively and assess the progress of the project in terms of making sure that all critical areas are being tackled and that the overall objectives of the project remain on track. These KPIs should be regularly reported on to facilitate data-driven decision-making and to support the process of continual improvement, one of the core principles underpinning the ITIL framework.

The relevant table is to be displayed inside of the following page.

Critical Success Factors (CSFs)	Key Performance Indicators (KPIs)
Comprehensive inventory of IT assets	Percentage of assets inventoried within the planned timeframe Accuracy of asset inventory
Effective stakeholder communication and engagement	Percentage of stakeholders informed and engaged according to communication plan Stakeholder satisfaction score
Robust risk management	Number of identified risks successfully mitigated Percentage of high-impact risks addressed by project midpoint
Seamless user transition to Token Connectivity service	Percentage of users successfully migrated to Token Connectivity service Number of support tickets related to transition
Compliance with security policies and regulations	Percentage of assets disposed of in compliance with security and regulatory standards Number of non-compliance incidents
Effective project management and timely completion	Percentage of project milestones achieved on time Actual project costs compared to budgeted costs
Service quality maintenance	Percentage of service availability Average response time for service requests User satisfaction with new service
Knowledge management and transfer	Percentage of project documentation completed Usage of knowledge base articles Percentage of staff trained on new processes and tools

Table 3: Mapping of CSFs to KPIs

## 7.2. Feedback mechanisms

The following are feedback mechanisms that shall be adopted to ensure continuous improvement and satisfaction of stakeholders throughout the decommissioning project. Their format resemble what was present above regarding KPIs description, to maintain coherence in their presentation and user comprehension, describing for each frequency, implementation, method of usage, outcomes, purposes and other relevant information to be discussed here.

- *User questionnaires*
  - Frequency: Before, during and after transition
  - Method: Online questionnaire tool with both quantitative and qualitative questions
  - Analysis: Project team analyzes the results and publishes those among stakeholders
  - Purpose: Understand the user's feelings about the transition process and the new service
- *Service Desk feedback system*
  - Implementation: Feedback option embedded into the Service Desk ticketing system
  - Frequency: Right after every interaction
  - Analysis: Service Desk management reviews feedback on a weekly basis
  - Purpose: Immediate capture of the user experience; periodic issues are noticed
- *Stakeholder review meetings*
  - Frequency: Monthly
  - Participants: IT, business units, management
  - Outcome: Action Items and Improvement Initiatives Identified
  - Purpose: Ensure alignment with business objectives; Address Concerns
- *Automated user experience monitoring*
  - Tool: User experience monitoring software implementation
  - Metrics: Application performance, network latency, user behavior
  - Analysis: Real-time Dashboards, Weekly Reports
  - Purpose: reactively identify and address performance issues
- *Focus group sessions*
  - Frequency: Quarterly
  - Participants: Representative sample of users from different departments
  - Outcome: In-depth insights into the user experiences and suggestions
  - Purpose: Get qualitative feedback and understand user needs rigorously
- *Anonymous suggestion system*
  - Implementation: Online anonymous submission platform
  - Review: By the project team once a week
  - Action: Feasible suggestions that get implemented as part of improvement plans
  - Purpose: Encourage open feedback/ innovative ideas
- *Post-implementation review*
  - Timing: One month after the completion of the project
  - Participants: All teams involved and main stakeholders
  - Outcome: A detailed report about the outcome of the project, lessons learnt, and recommendations for the future.

- Purpose: Review overall outcome of the project and areas of future improvement

### 7.3. Ongoing review and optimization process

To be able to continuously improve during but also beyond the decommissioning project, we will set up the following review and optimization process. This part follows a structure similar to the previous ones: a descriptive purpose, outcomes expected, the timing of application and other relevant data, like method, participants, etc.

- *Monthly KPI review*
  - Timing: Last week of every month
  - Participants: Project team and key stakeholders
  - Outcomes: Performance report and action items for improvement
  - Purpose: Regular check on project progress and identify areas that require special attention
- *Quarterly maturity assessment*
  - Timing: End of every quarter
  - Method: Self-assessment questionnaires and external audit
  - Outcomes: Maturity level report and improvement roadmap
  - Purpose: Process maturity progress monitoring and identification of areas for improvement
- *Continual Improvement Register*
  - Implementation: An online database, open to all members of the team
  - Content: Idea of improvement, Status, Priority, and Responsibility
  - Review: The project team will review this bi-weekly for updating and prioritizing initiatives
  - Purpose: To document and track initiatives for improvement throughout the project life-cycle
- *Review of effectiveness of feedback mechanism*
  - Timing: Bi-annual
  - Method: Quantity, quality, and actionability of the feedback received in these six months will be assessed
  - Outcome: Feedback collection and its analysis process will be improved
  - Purpose: Ensure that feedback mechanisms are effective and yielding valuable insights
- *Annual comprehensive review of the project*
  - Timing: At the end of every project year and at project closure
  - Participants: All project stakeholders, including senior management
  - Output: Detailed report on the progress of the project, challenges, successes, and strategic recommendations
  - Purpose: Holistic evaluation of project performance and strategic alignment
- *IT Asset Management practice updates*
  - Frequency: Quarterly
  - Method: Review of asset management processes, tools, and policies

- Output: Updated IT Asset Management guidelines and procedures
- Purpose: Continue the effectiveness of asset management practices on project goals
- *Optimize the Token Connectivity service*
  - Frequency: Monthly
  - Method: Analysis of service performance data and user feedback
  - Expected outcome: Service improvement initiatives and technical optimizations
  - Purpose: Further optimize the new service based on real-world performance and user experience

In this regard, the establishment of these comprehensive metrics, performance, and maturity framework ensures that our decommissioning project is in full compliance with ITIL 4, mostly for continual improvement and value co-creation. This will enable the adequate measurement of progress against objectives and areas where some improvement may be needed, thus optimizing such in bank's processes all through the entire operation lifecycle.

KPIs, CSFs, feedback mechanisms, maturity assessments, and review processes all combined help in building upon this framework for managing and improving such a decommissioning project. Only then do we stand a chance to achieve our immediate goals with regard to the project at hand and lay a proper foundation for long-term improvement in our IT service management practices.

## 8. Timeline, milestones and baselines

### 8.1. Overview

The decommissioning of the Home Connectivity and USB Connectivity services, coupled with the actual transition to Token Connectivity, represents a significant undertaking for the considered Bank of the use case. To ensure a clear establishment and success of the actual implementation, it's important to establish a comprehensive timeline with clear milestones and established baselines, mostly aligned with ITIL 4 practices and meeting carefully strategic objectives defined and the logical order of action present inside of the SVC.

This timeline spans a period of 28 weeks, divided into *four phases*, each of which contains milestones guiding our progress, so to allow guidance on progress, continuous adjustments and regular assessments of the progresses. This, in essence, involves breaking the actual implementation project down into manageable phases, with clear milestones, to allow for the delivery of incremental value along the way and gathering of feedback so that, at any given moment in the project life cycle, necessary adjustments can be made.

Baselines will be established with the setting of clear milestones, delivering incremental value at each step, gathering feedback and making necessary adjustments throughout the whole project lifecycle. This helps in having established baselines for key metrics such as user counts, operational costs, actual services performance, etc. In order to actually make continual improvement, these baselines will serve as reference points to measure the project's impact, the success upon completion and possible suggestions of improvement. According to ITIL Guiding Principles, the following sections are intended to be flexible guides and not rigid constructs, regularly reviewing them and updating them as part of an operational commitment, guaranteeing continual improvement when necessary and accurately aligned with ITIL 4 best practices described in detail above.

In the next subsections, we define project phases, key milestones, and baselines that have been established, all of which will be presented on a visual timeline of our project. Only such a structured approach will enable us to manage the decommissioning and transition process effectively to minimize disruption to the Bank's users and maximize the value given to the organization.

### 8.2. Project phases

The transition and the rollout plan is a complex undertaking and that requires a structured and careful approach. To manage such complexity and ensure a gradual but smooth transition, a phased approach was thought in implementation: this not only helps in managing the project's complexity, but also allows for better risk management, better resource allocation and stakeholder engagement, providing clear checkpoints of evaluation and course correction and adapting to any challenge or change of requirements which may arise. Failing to plan means planning to fail; this approach wants to be precise and defined beforehand for this specific reason. The actual decommissioning will be rolled out in four distinct phases, each with its own objectives and deliverables,;

- *Phase 1: Initiation and Planning (Weeks 1-6)*

This phase presents a base to the whole project. It has three major emphases: defining project scope, project objectives, and project approach. During this phase, it's relevant to consult with key stakeholders to make sure that their needs and concerns are noted down at the very beginning. The risk assessment done at this phase will inform mitigation strategies to be taken throughout the project life cycle. The key activities here include:

- Development and approval of the project charter
- The detailed analysis of stakeholders



- Thorough risk assessment and planning
- Development of the communication plan
- Finalization of the project plan and securing relevant approvals

Since this phase lays the foundation of the entire project, the “Plan” activity of the SVC is emphasized here. It deals with the description of the project scope, objectives, and approach. Some key ITIL 4 practices applied in this phase include:

- Strategy Management: Development of the project charter and alignment to organizational goals.
- Risk Management: Risk assessment and detailed planning
- Relationship Management: Conducting a detailed stakeholder analysis
- Organizational Change Management: Designing the communication plan

- *Phase 2: Design and Preparation (Weeks 7-12)*

Now that the groundwork has been laid in Phase 1, Phase 2 will be centered on detailed design in relation to the token connectivity service and transition preparation. It would be of prime importance to have a full understanding of the user’s requirements and to design a solution that not only caters to replacing the existing services but also improves user experience. The following activities are to be considered inside of this phase:

- Collect and gather detailed requirements for the Token Connectivity service
- Design the architecture of the new service
- Develop end-user and support staff training materials
- Create and prepare test plans for the new service
- Initial communication with users regarding the change to come

This phase is built upon Phase 1 and focuses on the “Design and Transition” activity of the SVC. The focus here is to understand user requirements and design a solution which not only replaces the existing services but gives added user experience. ITIL 4 practices prominent in this phase include:

- Service Design: Architectural design for the new Token Connectivity service
- Knowledge Management: Preparing training materials
- Continual Improvement: Building on lessons learned from current services into the new design.

- *Phase 3: Implementation and Transition (Weeks 13 - 24)*

This is the most intensive phase of the project, since planning and preparation are put into action. A lot of time is apportioned to this phase to ensure a smooth, measured transition with the least disruption to our users. During this phase, the following activities would ensue:

- A pilot group will be migrated to test the transition process
- Progressive migration of users in waves: 25%, 50%, 75%, 100%
- Gradual decommissioning of old services as users are migrated
- Continuous and constant support and troubleshooting
- Regular progress reports shall be produced and distributed to stakeholders

This is the intensive phase where our planning will come into action, embodying the “Obtain/Build” and “Deliver and Support” activities of the SVC. The design is for a careful, measured transition that brings minimal disruption to users. The key ITIL 4 practices in this phase include:

- Change Control: Managing the rollout in waves
- Service Validation and Testing: This process of transition would be tested with a pilot group
- Incident Management: Provide uninterrupted support and troubleshooting
- Monitoring and Event Management: A function that generates regular progress reports
- *Phase 4: Closure and Review (Weeks 25-28)*

Though this is the last stage of a project, it is highly important for a project in the long term and further improvements. This phase is mainly concerned with sticking the transition, gathering insights, and preparing for ongoing operations. The final phase includes the following activities:

- Post-Implementation Review
- Lessons learned are to be documented
- The final decommissioning of old services will be complete
- Producing and approving the project closure report
- Transition to ongoing operations and support for Token Connectivity

This final activity of this project is one of the most critical to long-term success and continuous improvement. It turns out to be one of the core activities from the “Improve” practice in the SVC. This in effect is the activity where final preparation for transition take place, observations and experiences documented and then gathered in readiness for Day 2 operations. This is where concentration of ITIL 4 practices would be, to include:

- Continual Improvement: Conduct post implementation reviewing, and document Lessons learned
- Service Level Management: Moving into ongoing operation and support
- Information Security Management: Ensuring a secure decommissioning of legacy services

### **8.3. Key milestones**

In this subsection, the key milestones to be reached will be documented, to have an immediate idea of what to implement here:

- *Phase 1: Initiation and Planning (Weeks 1-6)*
  - Project charter approved (Week 2)
  - Stakeholder analysis complete (Week 3)
  - Risk assessment and mitigation plan finalized (Week 4)
  - Communication plan developed (Week 5)
  - Project plan approved (Week 6)

Key participants for this phase:

- Change Manager
- CIO

- IT Asset Manager
- Supplier Manager
- Availability Manager
- Incident Manager
- Service Desk Manager
- Problem Manager
- Service Level Manager
- Service Owner

The following are key activities:

- Changes to IT Asset Management, Supplier Management, Availability Management, and Incident Management practices should be announced
- Introduce new software for IT Asset Management and Supplier Management
- Develop the project charter and communication plan
- Conduct Stakeholder and Risk Analysis

Checkpoint: Each manager briefs his team about the upcoming changes.

- Phase 2: Design and Preparation (Weeks 7-12)
  - Gathering detailed requirements for the Token Connectivity solution (Week 8-9)
  - New service architecture design approved (Week 10)
  - Development of training materials (Week 11)
  - Test plans finalized and approved (Week 12)

Key participants for this phase:

- IT Asset Management team
- Supplier Management team
- Availability Management team
- Incident Management team
- Release Management team
- Service Configuration Management team
- Knowledge Management team

The following are key activities:

- Train IT Asset Management team on new software
- Train Supplier Management team on new software
- Installation and configuration of new software and tools
- Develop training materials for end-users
- New service architecture design

Checkpoint: Meet the team managers to take feedback on new software applications and the training process.

- Phase 3: Implementation and Transition (Weeks 13-24)

- Pilot group migration complete (Week 15-16)
- 25% of users migrated (Week 17)
- 50% of users migrated (Week 19)
- 75% of users migrated (Week 21)
- 100% of users migrated (Week 23)
- Old services fully decommissioned (Week 24)

Key participants for this phase:

- IT Asset Management team
- Supplier Management team
- Availability Management team
- Incident Management team
- Release Management team
- Change Control team
- Service Desk team
- Problem Management team

The following are key activities:

- Begin using newly implemented software
- Implement new workflows
- Conduct pilot group migration
- Execute phased user migration
- Provide continuous support and troubleshooting

Checkpoint: Conduct surveys with involved staff to gather feedback on new software applications and training received.

- Phase 4: Closure and Review (Weeks 25-28)

- Post-implementation review conducted (Week 26)
- Lessons learned documented (Week 27)
- Project closure report approved (Week 28)

Key participants for this phase:

- Change Manager
- IT Asset Manager
- Supplier Manager
- Availability Manager

- Incident Manager
- Problem Manager
- Service Level Manager
- Service Owner
- Continual Improvement Manager

The following are key activities:

- Conduct post-implementation review
- Document lessons learned
- Finalize decommissioning of old services
- Produce and approve project closure report

Checkpoint: Managers communicate the successful implementation of changes to their respective teams.

In all stages:

- The Service Configuration Management team will be responsible for maintaining and updating the CMDB as changes occur
- The Knowledge Management team shall document new processes and lessons learned, disseminating them accordingly
- The Information Security Management team will be responsible for security aspects during the transition

#### **8.4. Baselines of CSFs and KPIs**

To effectively measure the project's progress and success, we establish the following baselines at the project's outset, based on the key metrics defined into the relevant chapter, consider for each CSFs defined and relevant KPIs, so to track current and desired situation precisely for each area:

- IT Asset Inventory Baselines:
  - Current percentage of assets inventoried within planned timeframe: 85%
  - Current accuracy of asset inventory: 92%
- Stakeholder Engagement Baselines:
  - Current percentage of stakeholders informed and engaged: 70%
  - Current stakeholder satisfaction score: 3.6 out of 5
- Risk Management Baselines:
  - Current number of identified risks: 27
  - Current percentage of high-impact risks addressed: 75%
- User Transition Baselines:
  - Current percentage of users on Home Connectivity: 30% (3000 users)
  - Current percentage of users on USB Connectivity: 70% (7000 users)
  - Current number of transition-related support tickets: 450 per month

- Compliance Baselines:
  - Current percentage of assets disposed in line with security and regulatory policies: 75%
  - Current number of non-compliance incidents: 5 in the past year
- Project Management Baselines:
  - Current on-time achievement of project milestones: 80%
  - Current project costs vs budgeted costs: 105% (5% over budget)
- Service Quality Baselines:
  - Current percentage of service availability for Home Connectivity: 99.5%
  - Current percentage of service availability for USB Connectivity: 99.3%
  - Current average response time for service requests: 6 hours
  - Current user satisfaction with existing services: 78%
- Knowledge Management Baselines:
  - Current percentage of required project documentation complete: 65%
  - Current number of views of knowledge base articles: 1200 per month
  - Current percentage of staff trained on existing processes and tools: 82%

These provide overall starting positions from which to measure the project's impact and success. They are related to specific KPIs defined earlier in your Metrics chapter, thus permitting a more relevant assessment of improvements throughout the decommissioning of Home Connectivity and USB Connectivity services, as well as the implementation of Token Connectivity as wanted.

By regularly comparing the metrics of the project against these baselines, progress can be tracked, areas of improvement can be spotted, and one can see that a project really is able to provide value for the organization. This supports the principle of continual improvement and allows data-driven decision-making throughout the project lifecycle.

## 8.5. Gantt rollout chart

Figure 15 provides a clear visual representation of the project timeline, including phases, milestones and key activities to be followed given the structure considered up until now. This chart is intended as reference for the actual foreseen implementation, then updated regularly to reflect the project's progresses and any necessary adjustments when needed.

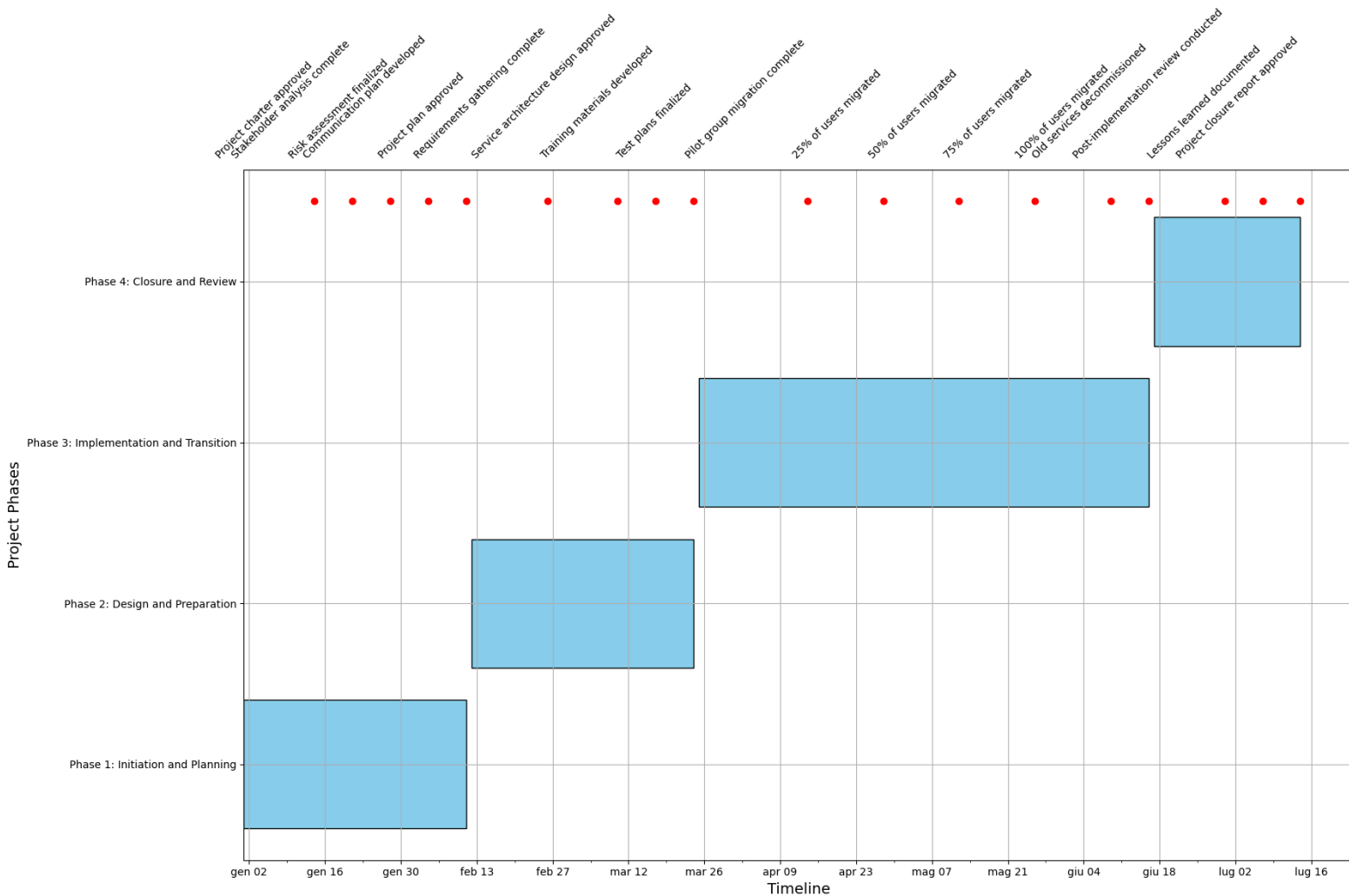


Figure 15: Gantt chart of the discussed planning

## 9. Conclusions

### 9.1. Summary of key recommendations

In this section, the recommendations below are proposed based on the detailed analysis and planning documented here in each section and chapter. Each tries to incorporate as overview at a high-level the entire meaning of the project:

1. Detailed inventorying of all IT assets relevant to the services that are to be turned off for obtaining a comprehensive understanding of scope and dependencies
2. Developing and executing a robust stakeholder communication and engagement plan in order to set expectations, resolve concerns, and secure continued support throughout the project
3. Establish a structured risk management process to identify, assess, and mitigate potential issues related to data security, service continuity, and compliance
4. Design a phased iterative approach to transition users to the Token Connectivity service, while providing comprehensive training and support
  - Ensure tight control over security policies and regulations, especially concerning the disposal of IT equipment, by close interaction with compliance experts and hard follow-up on documentation
  - Ensure successful project management: setting clear goals and roles, monitoring progress, establishing change control, and assuring quality delivery within budget and time constraints
5. Establish service quality metrics and monitoring processes to ensure the new Token Connectivity service attains or surpasses previous service levels
  - Introduce practices for knowledge management to capture and share the experiences learned in creating reusable knowledge assets for the continuation of training materials
  - Track progress by defined KPIs, CSFs, feedback mechanisms, and review processes to identify areas for improvement and drive data-driven decision making
6. Build upon the ITIL 4 framework with respect to guiding principles, the Service Value Chain, and the Continual Improvement model to demonstrate how alignment with best practice can support long-term success

### 9.2. Expected benefits and outcomes

Provided that the execution of the roadmap enclosed in the document regarding the decommissioning plan and transition to the Token Connectivity service goes according to plan, the following will be the main advantages and deliverables for the Bank:

- *Simplified IT service portfolio:* The Bank will be retirement-bound with legacy Home Connectivity and USB Connectivity services, hence making the IT landscape less complex and redundant
  - It will significantly reduce the cost of hardware, software licenses, support contracts, and operational expenses related to these services
- *Security Posture:* As indicated earlier in this document, this change to the token connectivity service will enhance, overall, the security posture of the Bank, as this reduces the risk of a data breach since these servers will be decommissioned in accordance with the security policy.
  - The new Token Connectivity service will provide users with a more flexible, reliable, and user-friendly connectivity solution that allows improving productivity and satisfaction.



- *Improved agility and scalability:* Thanks to the leaner IT service portfolio and the implementation of Token Connectivity, the Bank will be able to respond to changing business needs more agilely and to scale its operations, particularly in the context of its international expansion strategy.
- *Closer alignment with the business strategy:* this initiative will show that IT is able to reactively align with and support the overall business strategy of the Bank, further positioning IT as a strategic enabler of growth and innovation.
- *Improved IT governance and compliance:* strict application of best practices according to ITIL 4 and attention paid to compliance through the course of this project will improve the Bank's framework of IT governance and assurance of compliance with regulatory requirements.
- *Improved IT service management capabilities:* This complex project will bring lessons learned and experience to be had that will help in enhancing the Bank's IT service management capabilities for overall improvement in general and laying the ground for future success.

By following this comprehensive plan outlined in this document, grounded on the theory of the ITIL 4 best practices and framework, the Bank can successfully navigate this complex changing, realizing tangible benefits and laying the foundation for long-term success in the digital age, so to overcome with good planning and careful revision its entire framework of operations.

## 10. Appendix A: References & Sources

In this appendix, bibliography, webliography and sources are inserted, following a chapter-by-chapter logic, so to allow for easier consultation.

### 10.1. General ones

These are to be intended as guidance for the entire file:

- ITIL® Foundation: ITIL 4 Edition (2019) Book by AXELOS Limited
- The official ITIL website: <https://www.axelos.com/certifications/itil-service-management>
- 2023-2024 ITIL Training Material slides - ITSM STEM Moodle: <https://stem.elearning.unipd.it/course/view.php?id=6993>
- AXELOS resource hub for practices application: <https://www.axelos.com/resource-hub/practice>

### 10.2. Chapter 1 & Chapter 2

- Pages 3 to 7 of “2024 ITIL project work test 4”; image at page 9 of - “2024 ITIL project work test 4”
- BMC’s ITIL 4 Guide: <https://www.bmc.com/blogs/itil-4/>
- Gartner’s IT Glossary for banking industry terms: <https://www.gartner.com/en/information-technology/glossary>
- McKinsey & Company’s insights on digital banking: <https://www.mckinsey.com/industries/financial-services/our-insights>
- “The Future of Banking: A Vision for 2030” by Deloitte (2020)

### 10.3. Chapter 3

- “IT service management (ITSM) situation” section of “2024 ITIL project work test 4”
- ITIL Processes: [https://wiki.en.it-processmaps.com/index.php/ITIL\\_Processes#ITIL\\_Processes\\_according\\_to\\_ITIL\\_2011](https://wiki.en.it-processmaps.com/index.php/ITIL_Processes#ITIL_Processes_according_to_ITIL_2011)
- Service Transition Processes: [https://www.hci-itil.com/ITIL\\_v3/books/3\\_service\\_transition/service\\_transition\\_ch4\\_4.html](https://www.hci-itil.com/ITIL_v3/books/3_service_transition/service_transition_ch4_4.html)
- Ensure correct decommissioning of applications and servers: <https://www.itilfromexperience.com/How+to+ensure+that+applications+and+servers+are+decommissioned>
- ITIL4 Change Management: <https://digital.ai/catalyst-blog/understanding-the-itil-4-change-management-process-and-how-automation-can-enhance-it/>
- What is IT Governance: [https://www.youtube.com/watch?v=M\\_8-o-Mvb64](https://www.youtube.com/watch?v=M_8-o-Mvb64)
- Service Design and Building the IT Service Portfolio: <https://www.ciscopress.com/articles/article.asp?p=2873378>
- Impact Of IT Portfolio Management on Organisational Performance in the Automotive Industry: <https://www.linkedin.com/pulse/impact-portfolio-management-organisational-performance-nipo-khan-tnlcc/>

### 10.4. Chapter 4

- The ITIL Four Dimensions of Service Management: <https://itsm.tools/the-itil-four-dimensions-of-service-management/>
- ITIL®4 Four Dimension Model of IT Service Management: <https://www.knowledgehut.com/tutorials/itil4-tutorial/itil-four-dimensions-it-service-management>

- Behavior and ITIL 4: <https://stem.elearning.unipd.it/mod/url/view.php?id=489058>
- ITIL 4 Foundation: a universal guide to service management: <https://stem.elearning.unipd.it/mod/url/view.php?id=491499>
- The Service Value System: <https://stem.elearning.unipd.it/mod/url/view.php?id=491507>
- What is the ITIL 4 Service Value System: <https://www.theknowledgeacademy.com/blog/itil-service-value-definition/>
- ITIL® 4: Service Value System - from opportunity to value: <https://www.alvao.com/en/blog/itil-4-service-value-system-opportunity-value>
- Materials on Moodle Stem section of the course on topics and definition: <https://stem.elearning.unipd.it/course/view.php?id=6993>

## **10.5. Chapter 5**

- Planning of asset disposal <https://www.linkedin.com/advice/0/how-do-you-plan-execute-asset-disposal>
- CSR (focus on value): <https://www.investopedia.com/terms/c/corp-social-responsibility.asp>
- ITIL Change Management Types: <https://faddom.com/itil-change-management-types-standard-vs-normal-vs-emergency/>

## **10.6. Chapter 6**

- ITIL 4 Service Value Chain Defined: <https://youtu.be/J3RoUVFDdQ0>
- Value Stream example: <https://youtu.be/mmPirGAnC04>
- ITIL 4 Service Value Chain Explained: <https://www.bmc.com/blogs/itil-4-service-value-chain/>
- ITIL 4 Practices and the Service Value Chain: <https://www.axelos.com/resource-hub/blog/itil-4-practices-and-the-service-value-chain>
- Implementing ITIL 4 Practices: <https://www.bmc.com/blogs/itil-4-practices/>

## **10.7. Chapter 7**

- ITIL: CSF & KPIs: <https://www.learnovita.com/itil-csf-kpis-article>
- CSF's, KPI's, Metrics, Outcomes and Benefits: <https://www.itsmsolutions.com/newsletters/DITYvol6iss5.htm>
- Guide on ITIL Change Management KPI: <https://www.ocmsolution.com/itil-kpis/>
- CMMI Levels of Capability and Performance: <https://cmmiinstitute.com/learning/appraisals/levels>
- Key Performance Indicators for IT Service Management: <https://www.itsmprocesses.com/Wiki/Englisch/ITIL%20KPI.htm>
- ITIL v4 Big Picture: <https://www.youtube.com/watch?v=1ZqhiwEAtTA>
- ITIL Continual Improvement Model: <https://www.youtube.com/watch?v=xxwYqJ6zpPI>
- Lean IT: <https://www.youtube.com/watch?v=NFrwxzUhfNA>
- Continual Improvement in ITIL 4: <https://www.axelos.com/resource-hub/blog/itil-4-and-the-co-creation-of-value>
- ITIL v4 Other Stakeholders in Value: <https://youtu.be/aYEwVmtcKsg>
- ITIL 4 Metrics and Reporting: <https://www.bmc.com/blogs/itil-metrics-kpis-reporting/>

- Measuring Success in ITIL 4: <https://www.axelos.com/resource-hub/blog/measuring-success-in-til-4>
- Anatomy of Value Stream: [https://youtu.be/\\_cgIOD09DaY](https://youtu.be/_cgIOD09DaY)

## **10.8. Chapter 8**

- How do you manage configuration baselines and versions across different environments: <https://www.linkedin.com/advice/3/how-do-you-manage-configuration-baselines>
- Baseline (configuration management): [https://en.wikipedia.org/wiki/Baseline\\_\(configuration\\_management\)](https://en.wikipedia.org/wiki/Baseline_(configuration_management))
- Gantt chart in Project Management: <https://www.projectmanager.com/guides/gantt-chart>
- ITIL Rollout – Practical Tips for Optimum Business Outcomes: <https://www.linkedin.com/pulse/til-rollout-practical-tips-optimum-business-outcomes-arumanayagam/>
- ITIL Concepts for OE9 MIDDLEWARE ROLLOUT PROCESS (used as an example on how to structure logic, schema and Gantt): [https://indico.egi.eu/event/3/contributions/6752/attachments/6543/7693/service\\_transition\\_v0-1.pdf](https://indico.egi.eu/event/3/contributions/6752/attachments/6543/7693/service_transition_v0-1.pdf)

## **10.9. Chapter 9**

- Lessons Learned in Project Management: <https://www.pmi.org/learning/library/lessons-learned-next-level-communicating-7991>
- Ensuring Benefits Realization in IT Projects: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value>

## **11. Appendix B: Acronyms**

The following sections of this appendix incorporate, for a reader, a brief list sorted by alphabetical order, the relevant acronyms used within this document, so to ensure a common glossary across all documents, used as quick reference, as the official AXELOS book does. Single terms were not considered to be inserted here, since their meaning is often clarified within the same chapter, section and subsection accordingly. This is to be intended as a clarification step for a quick reader.

### **11.1. A**

- API: Application Programming Interface
- ATM: Automated Teller Machine

### **11.2. C**

- CAB: Change Advisory Board
- CCA: Call Center Agent
- CEO: Chief Executive Officer
- CFO: Chief Financial Officer
- CI: Configuration Item
- CI/CD: Continuous Integration/Continuous Delivery
- CIR: Continual Improvement Register
- CMDB: Configuration Management Database
- CRM: Customer Relationship Management
- CSF: Critical Success Factor
- CSR: Corporate Social Responsibility

### **11.3. D**

- DSL: Digital Subscriber Line

### **11.4. H**

- HR: Human Resources

### **11.5. I**

- ISP: Internet Service Provider
- IT: Information Technology
- ITIL: Information Technology Infrastructure Library
- ITAM: IT Asset Management
- ITSM: IT Service Management

### **11.6. O**

- OLA: Operational Level Agreement

### **11.7. K**

- KPI: Key Performance Indicator

### **11.8. U**

- UAT: User Acceptance Testing
- UC: Underpinning Contract
- USB: Universal Serial Bus

### **11.9. V**

- VPN: Virtual Private Network

### **11.10. W**

- WFH: Work From Home

### **11.11. R**

- RFID: Radio-Frequency Identification
- RFC: Request for Change
- RFP: Request for Proposal

### **11.12. S**

- SLA: Service Level Agreement
- SMART: Specific, Measurable, Achievable, Relevant, and Time-bound
- SVC: Service Value Chain
- SVS: Service Value System

### **11.13. V**

- VoIP: Voice over Internet Protocol