University of Padua

Master in Computer Science

23/01/2023

CASE STUDY ON SLA BREACH IN A BANK

Authors:

Marco Nardelotto
2044588
marco.nardelotto@studenti.unipd.it

Andreas Roennestad
2037142
andreas.roennestad@studenti.unipd.it

Jeanette Hue Nhu Tran
2045647
jeanettehuenhu.tran@studenti.unipd.it

Table of Contents

List of Acronyms 3

Introduction 4

Analysis Of The Failure 4
- Problems 4
- Processes 7
  - Integration Process 7
  - Supplier management 8
  - Portfolio maintenance 8
  - Knowledge, Configuration and Information security management 8
    - Information Security Management 9
    - Knowledge Management 9
    - Configuration Management 9
  - Service Level Management 10
    - Where SLA breach occurred 10
  - Customers involvement 11
  - Deployment management 12
  - Problem management 12
  - Ordering process 13

New Processes Design 15
- Problem Management 15
- Supplier Management 16
- Knowledge, Configuration and information security Management 18
  - Knowledge Management 18
  - Information Security Management 19
  - Configuration Management 21
- Service Level Management 22
- Customers Involvement 23
- Portfolio Management 24
- Integration Process 26
- Deployment Management 27
- Ordering Process 29

RACI table 30

Rollout Plan 30
- Problem Management 30
- Supplier Management 31
- Knowledge, Configuration and information security Management 33
  - Knowledge Management 33
  - Information Security Management 34
  - Configuration Management 35
- Service Level Management 36
- Customers Involvement Process 37
- Portfolio Management 38
- Integration Process 41
- Deployment Management 43
- Ordering Process 44

List of Acronyms

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CI	Configuration Item
CIO	Chief Information Officer
CMDB	Configuration Management Database
ESP	External Service Provider
HQ	Headquarters
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicators
MI	Management Information
RACI	Responsible, Accountable, Consulted and Informed
RFC	Request For Change
SDA	Service Desk Agent
SLA	Service Level Agreement
SLM	Service Level Management
SVC	Service Value Chain

Introduction

The analyzed expanding bank is looking to integrate its businesses and share its services with recently acquired banks. The bank has already started selling and providing its services in these markets. The bank's strategy is to take the lead in these partnerships to design and develop new banking services and to sell them to the bank's own customers.
In the bank, there are eight divisions, each with a divisional director reporting to the CEO. The company's divisions are

- Banking divisions: retail banking, customer delivery, industry liaison, financial products, and global banking
- Non-banking divisions: marketing, shared services, and security

The bank has recently had problems with the SLA, as there have been problems with a request to replace a monitor by an end user of the bank, who will have to wait longer than necessary before returning to work normally as the monitor requested by him will not arrive on time due to problems related to the replacement process.

Analysis Of The Failure

Problems

The analysis carried out on the specific case proposed by the bank highlighted the problems and consequently the errors that arose, which made the entire process of replacing the monitor for the end user not congruent with what should be specified in the SLA between customer and company.
The analysis contains the problems during this process, which include all parties involved in it (e.g. Service Desk, Service Management tool, Support Group, External Provider). The problems are cataloged according to the paragraph defined in the case study.

Company Structure

- In the three company's non-banking divisions are present the *Shared services division* and the *Security division,* which contains IT Security and IT management respectively. These two IT-related divisions should be separated and contained within a specific division to handle all IT-related matters, to obtain:
    - More cooperation between the IT divisions.
    - Simpler handling of problems and incidents..

    - An administrative department of IT, with the possibility to create subdivisions inside it.
- CIO used to report to CFO, but now they both report to the CEO via the shared services divisional director.

Challenges, Issues, and Risks

- When globalization is taken into consideration, the new companies with different cultures attached within the bank and all new employees should be integrated with the internal policies of the bank.
- There are currently organizational and cultural issues depicting different levels of expectation for IT support in the different countries and companies acquired, the idea is to have a level of expectations that are fair for all divisions and that can be monitored.
- There have been issues with the integration of management information across the business units, this involves taking information and problems in obtaining them, but above all a correct integration of the data between all the business units allows you to always keep the data to be analyzed under control.
- It is indicated that all IT Hardware maintenance within the HQ country is outsourced to a single supplier which was not profitable in the last financial year. It can therefore be understood that the supplier of the infrastructure is not very reliable and it can be necessary to enter a stricter agreement with it or to obtain a secondary provider.

IT Infrastructure

- Some direct management of the branch IT infrastructure remains with the customer delivery division. Some direct management of the overseas banks' IT infrastructure remains with the overseas banks within the global banking division. This leads to an unnecessary division of IT infrastructure management since there is no explanation that defines the principles for which this division is necessary and it is not clear why some branches are managed by the *Customer delivery division* and others by the *Global banking division.*

ITSM Situation

- Service Strategy:
    - The service portfolio is not formally maintained, so the customer can't understand if a service is available or not, or which service it is. The portfolio must be maintained.

    - Only limited information is known as to the detailed cost of individual IT services and the usage by each customer, which makes it difficult to maintain an overview for reaching quarterly targets.
- Service Design:
    - About 60% of the work of IT service design is delivered by short-term contract staff, limiting the overview of the system and creating problems of knowledge of the environment on the part of workers, it can also lead to problems regarding long-term goals to maintain these in good quality you have to have workers that stay there for a longer time and who therefore have adequate knowledge of company processes.
    - The negotiation for Service Level Agreements begin during the service design stage and extend through the service transition stage; it would be better if correct metrics for SLA are defined at an early stage.
- Service Transition:
    - Once the internal customers have specified what they want, they expect the IT department to deliver the IT service without their further involvement. This is a problem of continual improvement and dialogue with the customer because customers must be an integral part of the development and release process, and this process should be constantly improved.
    - There is no formal change evaluation process to provide support for changes, it is, therefore, appropriate for the change management team to involve customers more.
    - Software testing is almost totally focused on software functionality and must provide tests also for integration with the systems.
    - The incident and problem teams do not feel that the data from automated discovery tools help them to diagnose issues easily. It is necessary to review the data acquired by service asset and configuration management, perhaps the CIs are not properly documented, and relevant data are not acquired
    - Problem with deployment management, because two updates on security update and management information were done at the same time and resulted in significant problems like
        - Maybe lost some information in MI when doing the update
        - Problem with the knowledge management because people do not have the technical competence to use the new updated software
- Service Operation:
    - Problem management tends to be reactive rather than proactive. That is the main problem of the case study since it should be proactive so that you have

a plan for solving problems before they arise, instead of coming up with a plan when problems occur.
    - There is a process to manage service requests that enable the direct ordering of certain service catalog items by business users. They must be reviewed because there are problems in ordering catalog items. Also, this process should maybe be available for all users, not only for business users.
    - Management is focusing more on IT operations rather than integrating the new companies acquired with the bank's processes and with the staff already present.

Case Study

- There is no appropriate control of the external provider that provides the monitors, no agreements have been made to manage the maximum refueling time and above all the response time of the external provider (which responded to the request, two days later).
- Communication problems between different parts of the monitor replacement process.

Processes

Integration Process

During the acquisition of new companies and banks outside the bank's country of origin (HQ country), difficulties were encountered in integrating these acquired companies, with the inclusion in existing business processes. To solve these problems it is necessary to review (or create anew in this case) the integration process of the acquired companies, within the bank.

The process must review policies for

- Integrate the new staff with the existing one, also take into account cultural diversity
- Define a level of expectations for IT support that is fair and common to all business divisions that are created with acquisitions, and identify metrics to monitor this level.
- Integrate existing processes in acquired companies, modifying them appropriately until they become an integral part of the company.
- Establish a plan to manage the knowledge of newly acquired employees to more easily integrate them into business processes.

Supplier management

In the process of management, interaction, and choice of suppliers, reference is made to one of the 4 dimensions of ITIL4, namely *Partners and Suppliers.*
This dimension defines that every organization is a provider and a consumer of services, so an organization needs partners and suppliers to help deliver its services. The way in which an organization integrates suppliers into its SVC varies depending on in-house capabilities, sourcing biases, and regulatory requirements. With reference to the dimension defined previously, the process of choosing and integrating suppliers with the bank is not optimal because many aspects of the choice of supplier have not been carefully evaluated, in fact there are problems related to:

1. **Performance:** as defined in the case study's document "*the single supplier was not profitable in the last financial year",* this problem is caused by the lack of tracking of the supplier's performance.
2. **Strategy:** understand if the right strategy for the bank is to have a single supplier for the supply of monitors and other IT hardware or if it is convenient to have more than one for emergencies like this defined in the case study.
3. **Relationships:** it is necessary to understand if there are still good relations with the supplier to understand if it is possible to modify the conditions of the contract so that it becomes more efficient or if it is necessary to completely change supplier.

Portfolio maintenance

Actually, the portfolio of the available services is not kept consistent with the services offered by the bank. This causes problems for customers who may not have a clear idea of the services the bank offers. The process of maintaining the portfolio of services is lacking from the point of view of the acquisition of resources and the processes of portfolio management in primis change management and deployment management that must be reviewed to allow the changes to be approved and then be directly available and updated to customers.

Knowledge, Configuration and Information security management

Information and knowledge within the bank is not properly managed, among the main problems of the information management process are:

- The information taken does not seem relevant to some sectors of the bank (incidents and problems teams).
- Only limited information is known as to the detailed cost of individual IT services and the usage by each customer.

- Lost some information in MI when doing the update of the software.
- There have been issues with the integration of management information across the business units.

To solve these problems it is, therefore, necessary to review the internal process of data acquisition, transmission and security and for this reason, the practices relating to Knowledge Management, Configuration Management, and Information Security Management must be reviewed.

Information Security Management

Information Security Management is the practice that protects the business and its data from threats. The loss of information caused by the update may have had repercussions on the problem of replacing the monitor as information relating to the number of monitors in the bank's warehouse may have been lost. In this practice we need to improve:

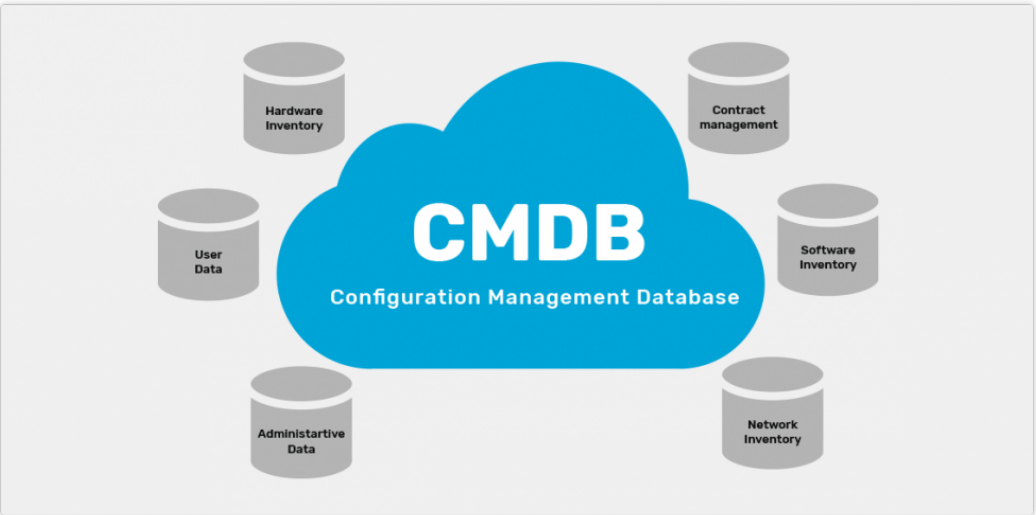
- **Prevention:** ensuring that security incidents don't occur, thinking of new ways to keep resources safe.
- **Correction:** recovering from incidents after they've been detected so as not to lose sensitive data.

Knowledge Management

The purpose of the Knowledge Management practice is to maintain and improve the effective, efficient and convenient use of information and knowledge across the organization. The problem of acquiring non-relevant information in some business areas must be improved by reviewing the knowledge management practice in particular it is necessary to evaluate, together with the employees of the various sectors, the information that should be acquired and that is necessary, also trying to improve the acquisition of information during the analysis of incidents and problems to also improve the process problem management (from reactive to proactive).

Configuration Management

The purpose of Configuration Management is to manage and control assets that make up an IT service. These assets are called Configuration Items (CIs). The problem related to “only limited information is known as to the detailed cost of individual IT services and the usage by each customer” can be solved by improving this practice. It is necessary to review or instantiate a key element of the process, the CMDB, which is used to track all the CIs and the relationships between them.



Service Level Management

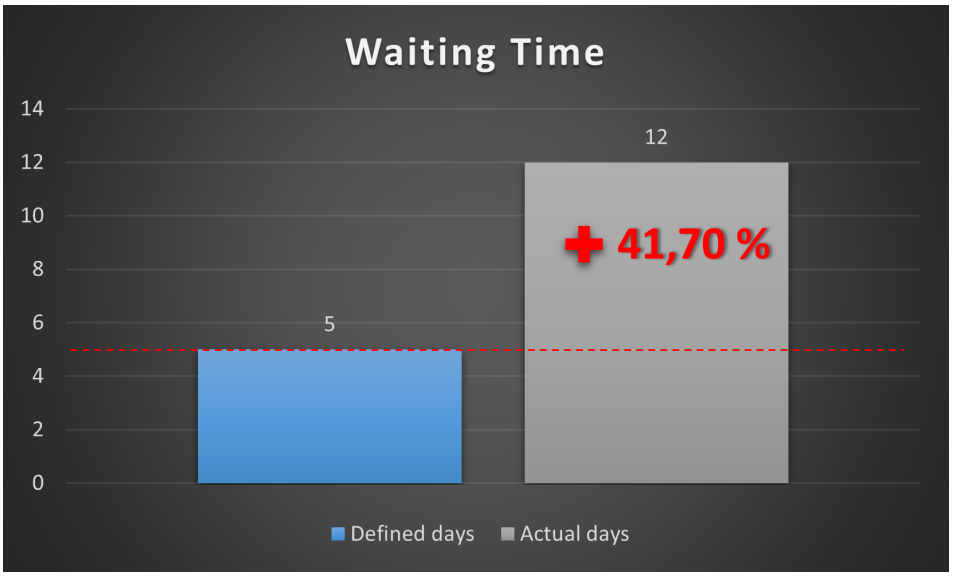
The goal of the SLM approach is to establish specific objectives for service performance that are tied to business needs, in order to efficiently evaluate, track, and control the delivery of the service in relation to those targets. In this practice the SLA is stipulated which is a document that collects the agreements between a service provider and a customer and that identifies both services required and the expected level of service. In this case study one of the main problems that have arisen is the disruption caused to the end user regarding user experience and user support. In fact, in this case it is possible to talk about SLA breach as some agreements between the organization and the customer have not been maintained, based on previously defined metrics.

Where SLA breach occurred

The SLA breach must be reported based on a metric, ITIL4 defines some sample metrics such as:

- **Functionality**: completeness of the functions available
- **Availability**: percentage of availability or permitted downtime
- **Performance**: service throughput
- **Timeliness**: fulfillment of requests within deadline
- **User support**: timeliness of support request processing
- **Accuracy**: number of errors expected
- **User experience**: percentage of interrupted service actions

In this case (taking these metrics as an example) the SLA breach referred to user support and the user experience as, according to the case study, the service desk agent had promised the replacement of the monitor to the end user in 5 working days, but by contacting the external provider the total time required for the arrival of the monitor is at least 12 working days (2 days of waiting for the response from the external provider and 10 days for the actual arrival of the monitor).



Customers involvement

During the service transition step in the document of the case study it is specified that "*Once internal customers have specified what they want, they expect the IT department to deliver the IT service without their further involvement*" this is not a good practice to follow as the customer should be involved throughout the product development and release process to clear up any misunderstandings or to get a more customer-friendly service.
It is therefore necessary to apply first of all the guiding principles defined by ITIL4, in particular the principles:

- Progress iteratively with feedback: to focus attention not on the development of the service as a single block, but on the creation of small parts agreed with the customer in order to facilitate their acceptance;
- Collaborate and promote visibility: which defines that it is necessary to collaborate, to include the customer in the realization of his service and to have clarity with him about what is happening.

The following problem of customer involvement is also linked to the case study reported as, the customer should not be involved only in the development of the service but in the whole

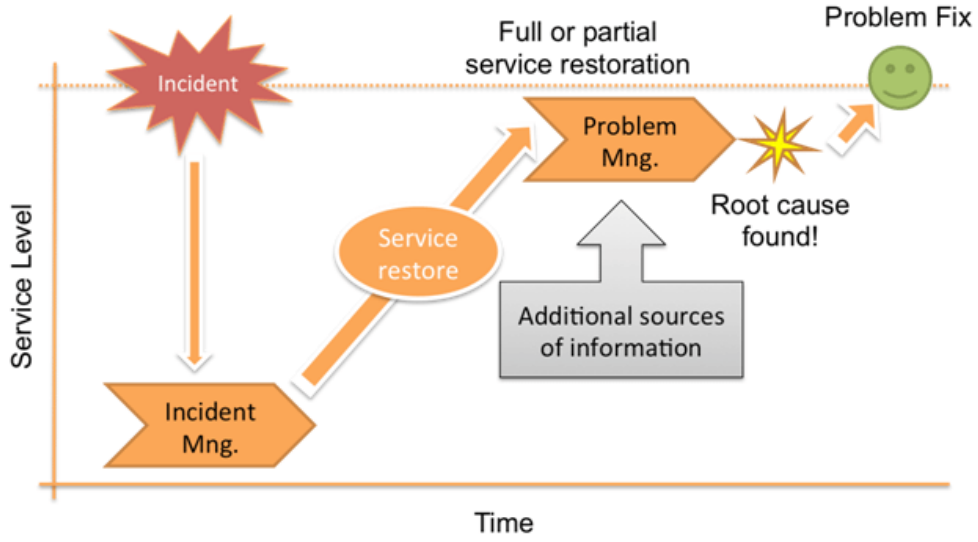
life cycle of it, in this way if the customer had been involved more would be more data was acquired to ensure that the caused SLA breach would not occur.

Deployment management

The deployment process ensures that the releases of services are deployed into production efficiently and effectively. In this case there were several errors in the management of this process, first of all, as defined above, during the execution of the two security updates, which were not properly managed as they were released without any control and without managing the possible problems that have been caused, perhaps by providing a backup of the configuration prior to the upgrade.
Then, there is the problem of the deployment of the services available in the company portfolio. This problem is to be managed together with the updating of the portfolio. Finally, with regard to the case study relating to the SLA breach caused, the deployment process is to be reviewed as the monitor replacement service was not able to maintain the expected quality standards, it is therefore necessary to define the ordering process and replacement and once this is done, provide for a secure deployment and release of this new service offered.

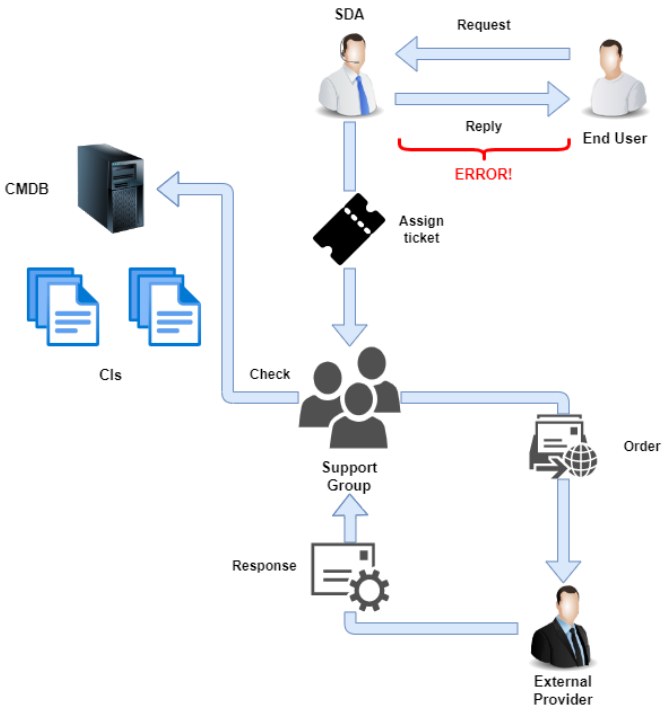
Problem management

As mentioned, one of the main problems identified in the case study is the definition of the problem management in a reactive and not in a proactive way.
Reactive Problem Management reacts to incidents that have already occurred, and focuses effort on eliminating their root cause and reoccurrence. The main focus of Problem Management is to increase long-term service stability and, consequently, customer satisfaction.
The following figure shows the cycle of solving a problem in a reactive way.



In this case the incident is the failure to replace the monitor in time and after having solved the problem or partially contained it to allow the continuity of the service, further information on the problem is acquired in order to identify the root cause and then resolve the error. The whole process is implemented when a problem arises and it is necessary to identify the error, while with a proactive solution when a problem is detected, based on the information already acquired in the past, the error is immediately identified and the problem is solved in a shorter time.

Ordering process

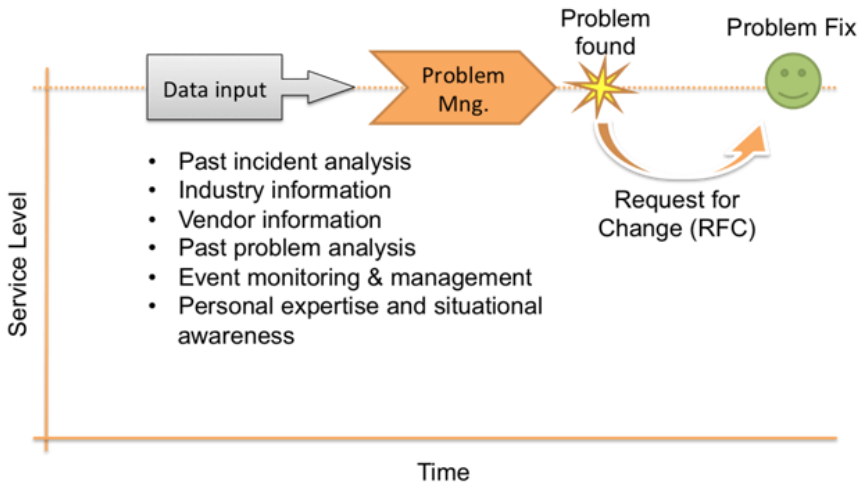


The ordering process for this specific case of monitor replacement, is the process that led to the SLA breach and is the final process on which all the errors present in the other business processes accumulate.
The following errors were found in the analysis of the ordering process:

- The response given by the service desk agent to the end user was given without knowing too much about the real time of issue of the monitor, especially from the delivery by the external provider.
- The information contained in the CIs was not enough to predict in advance that the spare monitors were finished and needed to be ordered in time
- Already knowing that the external supplier was not performing well in the last period, efforts had to be made to replace it or inform them in time that new stocks of monitors were needed.
- As just said, the external provider was not efficient and therefore we could not even expect the bank to have the time scheduled to deliver the monitors in time, in fact the ESP responded to the bank's request with 2 days delay.
- There were clear communication problems between the different parts of the process.
- The SDA defined a waiting time for the monitor for the end user, but failed to ensure that the user could continue to work safely during that time.
- The whole problem that arose in this process was handled in a reactive and non-proactive way, it may be useful in the future to collect information about this error in order to better manage it.

New Processes Design

Problem Management



The problem management process has been redesigned to be proactive rather than reactive. Proactive problem management is a continuous process that doesn't wait for a series of incidents to happen in order to react, but it is always active and relies on other service management components. The focus of this process is now on continuous data analysis and acquisition on a large volume of quality data. So the main purpose of the new problem management process is to anticipate potential problems and prevent them.
The redesigned process includes:

- Initially there is the data acquisition phase where they are analyzed in depth:
    - All past accidents
    - Information relating to the particular sector in which the bank belongs and how other competitors operate
    - All problems analyzed in the past, how they were solved and from which incidents they were caused, in order to obtain a more precise correlation between incidents and problems
    - Monitoring and management events, in order to understand how to monitor the occurrence of such incidents and consequently errors and how to best manage them
    - Personal expertise and how situations leading to problems were understood
- After the entire phase of analysis and data acquisition, all the information processed and acquired is saved in special databases and relationships are created between the data such as the relationships that have been analyzed between accidents and problems resulting from them, or how they have been previously managed these

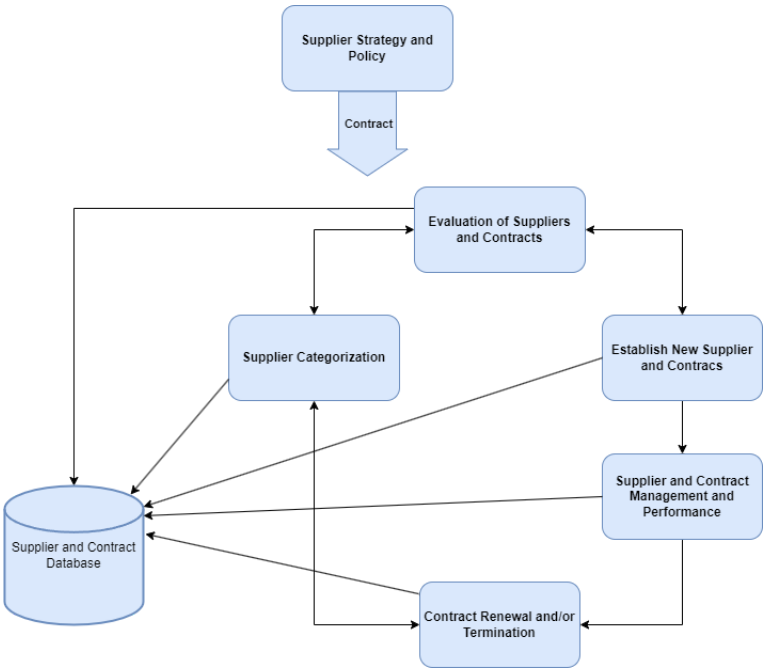
problems and how they should be managed now after the analysis and finally what metrics and methods to use to control the occurrence of incidents and the creation of problems.

- Meanwhile the problem management process is obviously active and whenever a problem occurs the two previous phases are processed, while for the current problem we look at the previously analyzed data and try to solve the problem using this data in order to speed up the recovery of service.
- When the problem has been identified, the changes to be made are defined to solve the problem and allow it not to occur again, once the changes have been defined, a Request For Change (RFC) is made, which once approved allows the problem to be solved and the maintenance of the active service as before.

The data collection and analysis phases will be carried out whenever useful information is detected to prevent problems.

In this process there is therefore a large data collection and a large iteration with other processes such as Incident management and Change management, in order to make the resolution of problems proactively and therefore prevent their causes.

Supplier Management



The supplier management process has been redesigned in order to obtain better performance from the suppliers and obviously to choose the ones most suitable for the bank. Initially, it will be necessary to decide whether, especially for the supply of monitors, to maintain a single supplier or have multiple ones, this will also be applied to other suppliers

for the different areas of the bank. Once this has been decided, the process design in the figure can be applied to each of the two cases.
The stages of the process in the photo are as follows:

1. Initially all the suppliers that compete to be an integral part of the business process are interrogated (including the supplier already present to choose whether it is to be replaced or not).
2. Each supplier defines a contract and its strategy to see if it is in line with the bank's corporate strategy.
3. Subsequently, the evaluation process of the supplier and its contract will take place within the bank in which:
    - The single supplier and his contract are evaluated.
    - Categorize each supplier by keeping the information in a dedicated database.
    - Establish and/or modify classified contracts to gain more control over performance and other details.
    - Precisely define the performances that the supplier must maintain and how to verify these performances related to the SLA.
    - Renewing or terminating contracts as performance and service needs dictate.

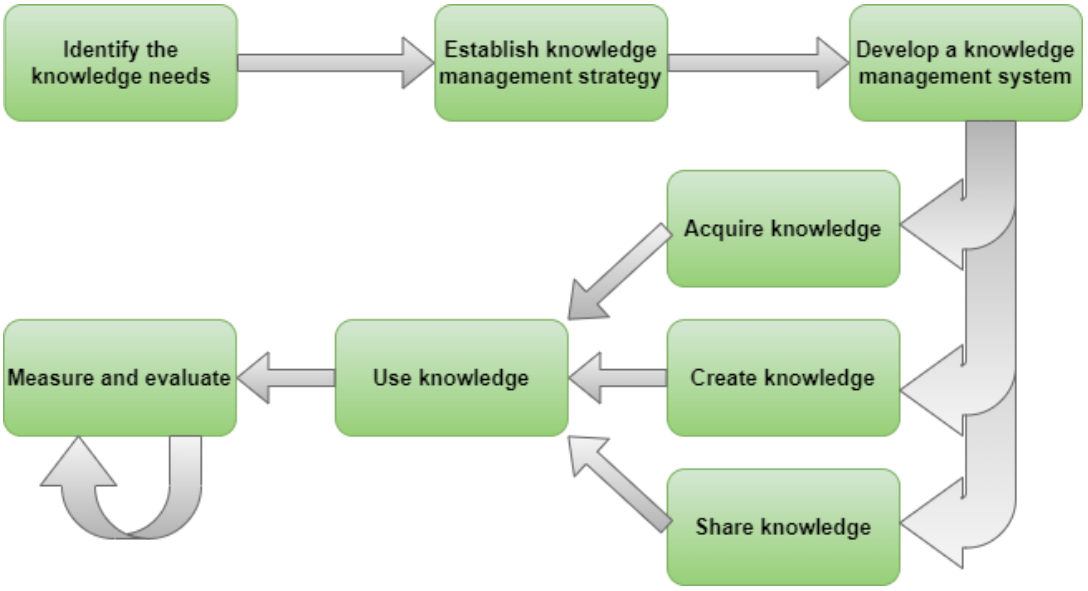
In all phases of this process, the information collected is saved, processed and modified within a dedicated database for the supplier management process, in order to keep the information consistent and always up-to-date and to easily obtain information on the control of performance of the suppliers and their contracts with their obligations towards the bank.
The following process is intended to resolve the issues described in the previous section, primarily based on troubleshooting related to:

- **Performance**: with the new process designed, the parameters to be respected and the metrics with which to evaluate the performance of a supplier are defined and this data is saved in a database.
- **Strategy**: the process makes it possible to acquire suppliers who have an affinity with the bank's strategy in order to have the same progress objectives.
- **Relationships**: the process defines various interactions with the supplier both to maintain and define performance and to review the contractual obligations and to constantly interact with it.

Knowledge, Configuration and information security Management

To better manage the problems reported previously, the three processes relating to knowledge, information and security management have been redesigned, in the next subparagraphs the designs for each process will be defined in detail.

Knowledge Management



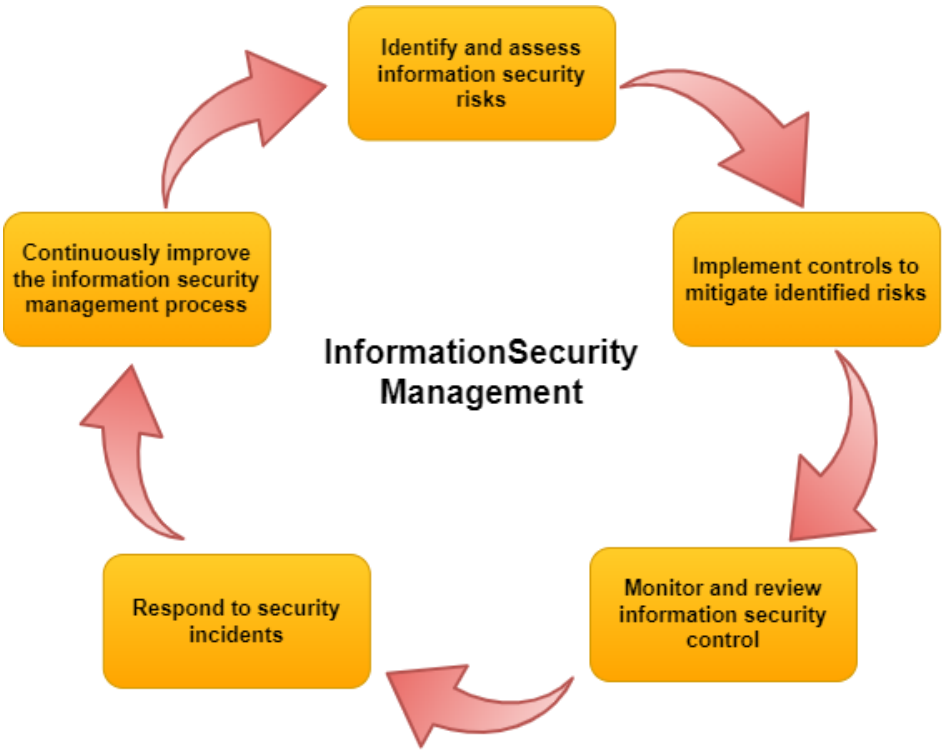
To better manage knowledge within the company, to keep track of it and to increase knowledge, the knowledge management process has been designed as follows:

1. **Identify the knowledge needs of the organization**: This involves identifying the types of knowledge that are necessary for the organization to operate effectively and efficiently, as well as the specific knowledge needs of different business units and individual employees.
2. **Establish a knowledge management strategy**: Based on the identified knowledge needs, a strategy should be developed to guide the acquisition, creation, sharing, and use of knowledge within the organization. This strategy should align with the overall business goals and objectives of the organization.
3. **Develop a knowledge management system**: A system should be developed to support the acquisition, creation, sharing, and use of knowledge within the organization. This may include the use of knowledge management software, as well as the establishment of policies and procedures to support the management of knowledge.

4. **Acquire knowledge**: This may involve purchasing knowledge from external sources (e.i. from the acquired companies), as well as developing internal expertise and capabilities through training and development programs.
5. **Create knowledge**: This involves generating new knowledge through research and development activities, as well as capturing and documenting the knowledge and expertise of employees through various means such as knowledge-sharing sessions, mentoring programs, and other methods.
6. **Share knowledge**: This involves making knowledge available to the appropriate employees and business units through various channels such as knowledge management software, shared databases, and other methods.
7. **Use knowledge**: This involves leveraging the available knowledge to support decision-making, problem-solving, and other activities within the organization.
8. **Measure and evaluate the effectiveness of the knowledge management process**: This involves regularly evaluating the success of the knowledge management process in meeting the needs of the organization and identifying areas for improvement.

This is just a general outline for the knowledge management process, and each phase will be implemented in a more concrete way during the rollout plan.

Information Security Management

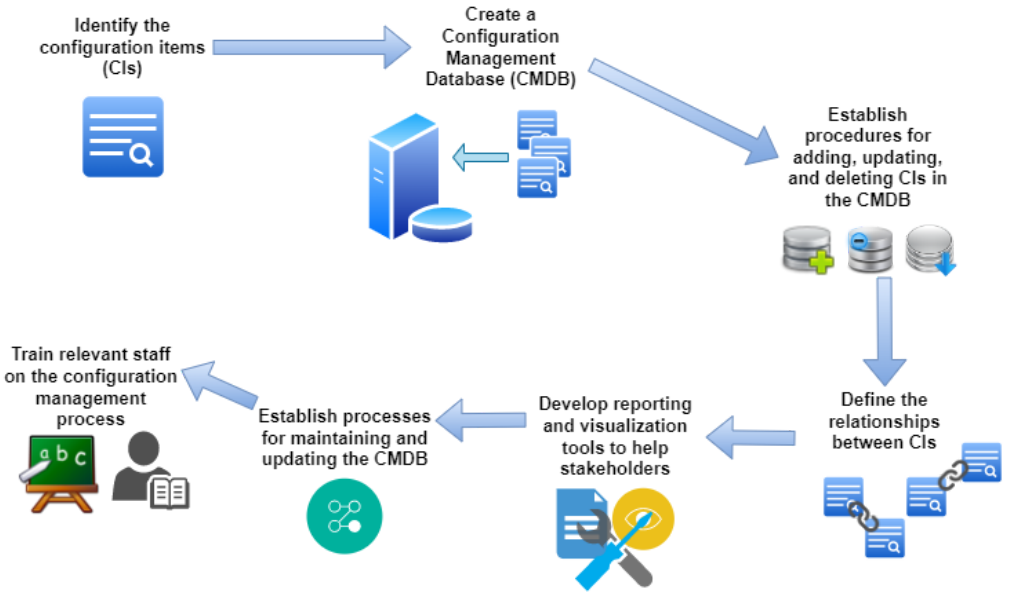


In carrying out the design of the Information security management process, an attempt was made to increase and take into consideration the prevention of information incidents and the correction of any problems.

The information security management process should follow these steps:

1. **Identify and assess information security risks**: The first step in the process is to identify and assess the risks to the organization's information assets. This can be done through various methods such as threat modeling, vulnerability assessments, and penetration testing.
2. **Implement controls to mitigate identified risks**: Once the risks have been identified, appropriate controls should be implemented to mitigate them. These controls can include technical measures such as firewalls and intrusion detection systems, as well as non-technical measures such as security awareness training and policies and procedures.
3. **Monitor and review information security controls**: It is important to regularly monitor and review the effectiveness of the implemented controls. This can be done through regular testing and audits.
4. **Respond to security incidents**: In the event of a security incident, a response plan should be in place to minimize the impact and restore normal operations as quickly as possible. This plan should include procedures for identifying, containing, and eradicating the threat, as well as communication protocols for informing relevant parties.
5. **Continuously improve the information security management process**: It is important to continuously review and improve the information security management process to ensure that it is effective and up to date with the latest threats and technologies. This can be done through regular reviews, training, and incorporating lessons learned from past incidents.

Configuration Management



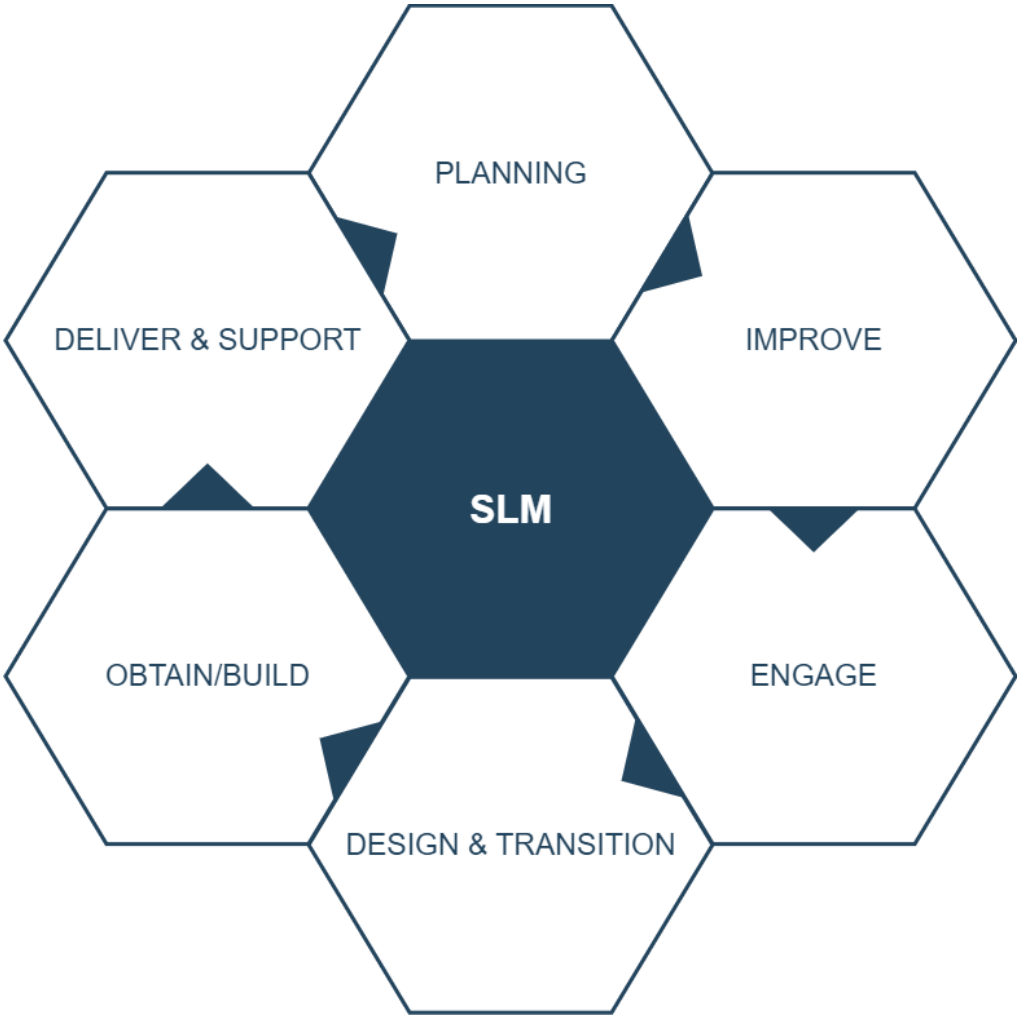
The configuration management process has an important role both in business processes and in the resolution of the defined case study, this is based on the mapping of the bank's configuration items and their management.

Process design contains the following steps:

1. **Identify the configuration items (CIs) that need to be tracked and managed**: In this case, the CIs might include the desktop monitors and other hardware and software components that make up the desktop service.
2. **Create a Configuration Management Database (CMDB) to track and store information about the CIs**: The CMDB should include details such as the type, model, and serial number of each CI, as well as information about its location, owner, and any associated contracts or warranties.
3. **Establish procedures for adding, updating, and deleting CIs in the CMDB**: This might involve processes for acquiring new CIs, retiring or decommissioning old ones, and updating existing CIs with new information as needed.
4. **Define the relationships between CIs**: For example, a desktop monitor might be related to a particular desktop computer or to a specific user. These relationships can help to provide context and make it easier to understand the dependencies and impacts of changes to individual CIs.
5. **Develop reporting and visualization tools to help stakeholders understand and manage the CIs**: This might include dashboards, reports, or other tools that provide insights into the status, health, and utilization of the CIs.

6. **Establish processes for maintaining and updating the CMDB**: This might include regular audits or reviews to ensure that the CMDB is accurate and up-to-date, as well as procedures for correcting errors or discrepancies that are identified.
7. **Train relevant staff on the configuration management process**: This might include providing training on how to use the CMDB and other tools, as well as on the procedures for adding, updating, and deleting CIs (this will also impact the knowledge management process).

Service Level Management

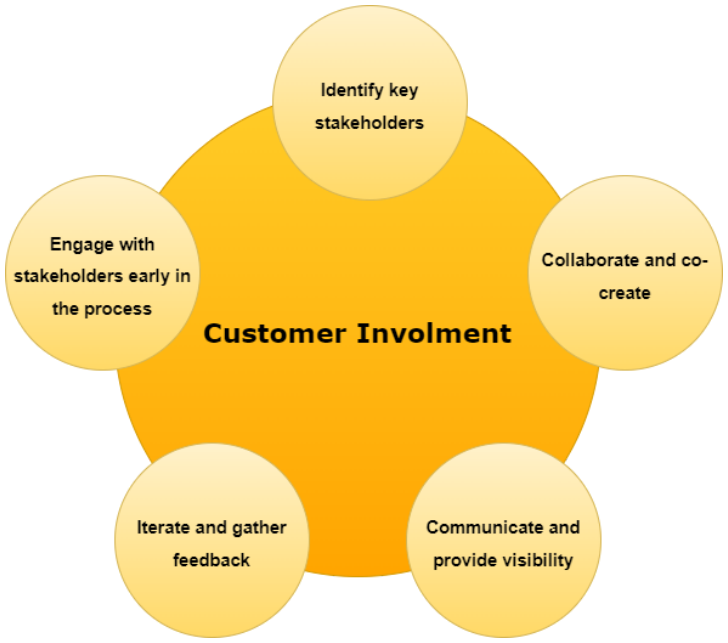


It is impossible to avoid every SLA breach, but improving Service Level management process so the agents resolve their tasks in time will avoid some SLA breaches, and preparing for them will limit the damage.

To perform good service performance and user service, we need to focus on these 6 steps:

1. **Planning:** plan of product, service portfolio and offerings. Setting service internal goals for response and performance. The goal should not be a minimum level and it should be defined for example with the highest waiting time acceptable for the replacement of the monitor for customers so it exceeds the expectations of the customers.
2. **Improve:** review the process of defining and implementing the metrics defined earlier by ITIL 4, simultaneously with the modification of other processes. A good problem management will support the prevention of the SLA breaches.
3. **Engage:** focus and listen to the customers when it comes to their needs, requirements, problems and concerns. Also consider customer feedback when making SLA in terms of for example surveys and customer engagement to get a better understanding in addition to a confirmation about the need being fulfilled
4. **Design & Transition:** the design with new, changed and improved services
5. **Obtain/Build:** Collect objectives for the services and components
6. **Deliver & Support:** support by communicating with the operations and support teams

Customers Involvement



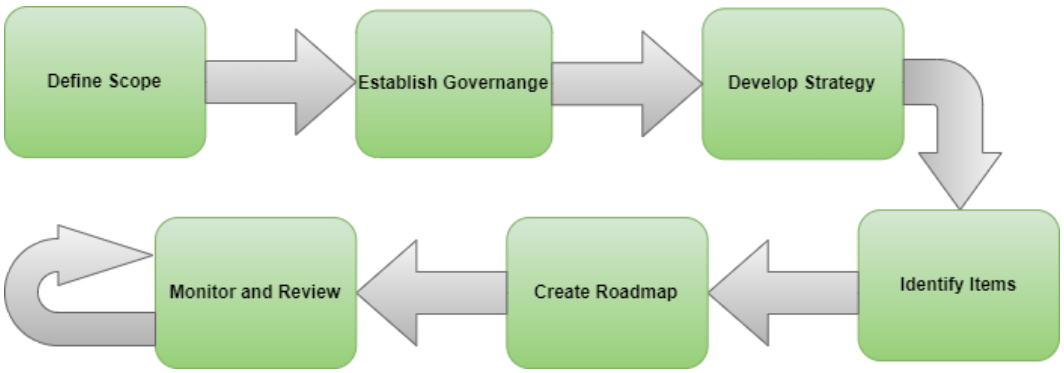
The customer engagement process has been designed to improve it, the following steps have been identified from the design for better customer engagement:

1. **Identify key stakeholders**: The first step in improving customer involvement is to identify the key stakeholders who will be impacted by the service, and to understand

their needs, expectations, and priorities. This could include customers, users, and other internal or external parties.

2. **Engage with stakeholders early in the process**: Once key stakeholders have been identified, it is important to engage with them early in the service development process to ensure that their needs and priorities are understood and taken into account. This could involve gathering feedback and insights through interviews, surveys, focus groups, or other methods.
3. **Collaborate and co-create**: Collaborating with stakeholders can help to ensure that the final service meets their needs and expectations, and can also improve customer satisfaction and loyalty. This could involve co-creating the service with stakeholders, or involving them in the design and development process through workshops, prototyping, or other methods.
4. **Communicate and provide visibility**: Providing regular communication and visibility into the service development and delivery process can help to build trust and confidence with stakeholders, and can also help to identify and resolve potential issues or concerns. This could involve sharing progress updates, soliciting feedback, and being transparent about any challenges or delays.
5. **Iterate and gather feedback**: It is important to continue gathering feedback and insights from stakeholders throughout the service development and delivery process, and to use this feedback to iteratively improve and refine the service. This could involve conducting user testing, gathering feedback through customer satisfaction surveys, or using other methods to gather insights and identify areas for improvement.

Portfolio Management



The service portfolio management process has been redesigned in order to keep the services offered by the bank to its customers and users up-to-date.

The phases that define the design of the new process are:

1. **Define the scope of the portfolio**: This step involves identifying the types of assets that will be included in the portfolio, such as applications, services, and infrastructure components. In our case the main focus would be in services.
2. **Establish portfolio governance**: This step involves defining the roles and responsibilities of the stakeholders involved in managing the portfolio, such as the portfolio manager, portfolio board, and portfolio steering committee.
3. **Develop the portfolio strategy**: This step involves creating a high-level plan for how the portfolio will be managed, including the goals and objectives, key performance indicators, and metrics that will be used to measure success.
4. **Identify and prioritize portfolio items**: This step involves identifying the specific assets that will be included in the portfolio, and prioritizing them based on their strategic value, risks, and opportunities.
5. **Create the portfolio roadmap**: This step involves creating a detailed plan for how the portfolio will be implemented and managed over time, including the timelines, budgets, and resources required to achieve the portfolio's goals.
6. **Monitor and review the portfolio**: This step involves regularly tracking the performance of the portfolio against its goals and objectives, and making any necessary adjustments to ensure that it remains aligned with the organization's strategic direction.

This last phase is the one that will be most considered during the implementation of the process and that will require more attention. In particular, this part will be iterated every time the assets in the portfolio are modified.

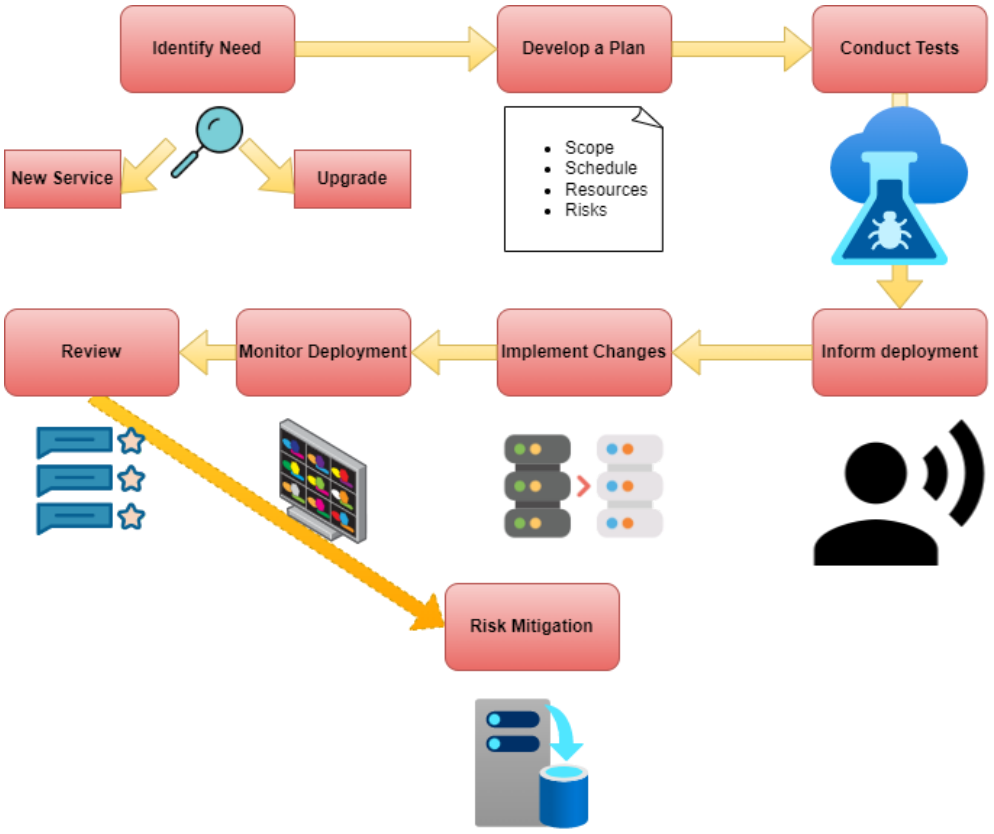
Integration Process

The integration process is reviewed, and new, stricter policies are proposed to ease the integration process when expanding the business and acquiring new companies. Aligned with the principle of continual improvement, the company has failed to continually review and improve the integration process to ensure that it is meeting the needs of the business and customers as the business has expanded internationally. We now structure the policies in place based on their corresponding sections in the problem formulation of the integration process.

1. **Integrating newly hired employees:** The organization implements a comprehensive onboarding program that includes team building activities and mentorship opportunities. This allows for easier onboarding for future employees. Additionally, the bank can establish cross-cultural communication guidelines and make sure that all employees are aware of them. This makes for better integration of employees across cultures and countries.

2. **IT Support:** The organization conducts a survey of current IT support levels across all divisions and uses this data to establish a baseline level of support across branches. Additionally, the bank identifies key metrics to monitor the level of support, such as response time, resolution time, and customer satisfaction rates.
3. **Process Integration:** The organization conducts an audit of the processes at each acquired company and identifies areas with room for improvement. The bank can then work with employees at the acquired companies to modify processes as needed and ensure that they align with the business' overall strategy.
4. **Knowledge of newly hired employees:** To establish a plan to manage the knowledge of newly acquired employees, the organization can set up a knowledge management system that includes relevant resources, such as process documentation, training materials, and practices. Additionally, the newly acquired employees can learn from more experienced colleagues through a mentorship programme as suggested in point 1.

Deployment Management



In the deployment management design, the problems defined in the previous paragraphs were taken into consideration, for this reason we focused more on reducing the risks deriving from the deployment of new upgrades and on correctly distributing the new services

especially within the bank's portfolio to always keep it up to date. In detail, the steps defined by the new process design are:

- Identify the need for a change to your IT services, such as an upgrade or a new service.
- Develop a plan for the deployment, including details about the scope, schedule, resources, and risks.
- Conduct testing to ensure that the changes will work as intended and will not have negative impacts on other services.
- Communicate with stakeholders, including users, customers, and other teams, to inform them of the planned deployment and any potential disruptions or changes to service availability.
- Implement the changes, following the plan and any relevant procedures.
- Monitor the deployment to ensure that it is successful and that any issues are addressed quickly.
- Review the deployment to assess its success and identify any areas for improvement.
- In case, provide risk mitigation plans and methods to reverse the deployed changes.

Ordering Process

This process depends on the other processes, where all the processes have to be designed better for the ordering process to result in better performance. The following steps for a new ordering process are:

1. **Review and update the process:** review the current ordering process and identify any bottlenecks or areas for improvement. Update the process as needed to address these issues.
2. **Improve communication and collaboration**: address the communication problems between different parts of the process by introducing new tools or processes to facilitate better communication and collaboration.
3. **Use automation:** consider using automation to execute the ordering process and reduce the risk of errors or delays.
4. **Investigate the external supplier**: if the external supplier is not performing well, consider replacing them or addressing the issue with them directly. In addition, communicate with the supplier in a frequently to ensure that they are able to meet your needs

5. **Provide training and support:** provide training and support to service desk agents to ensure that they have the knowledge and skills they need to handle requests and issues effectively.
6. **Implement a proactive approach**: instead of handling issues in a reactive manner, try to take a proactive approach to identifying and addressing potential issues before they occur. This may involve regularly reviewing and updating the process, as well as collecting and analyzing data on past issues to identify patterns and trends. This is discussed earlier.

These steps align with the ITIL4 practices of Service Level Management and Service Automation, Continual Improvement, Service Relationship Management, and Knowledge Management.

RACI table

See the file in the shared directory

Rollout Plan

This section explains in greater detail the rollout plan and therefore the implementation of each process designed in the previous phase, taking into consideration how the processes will be introduced and how they will be activated in the bank.

Problem Management

For a reactive problem management, the new process should follow these nine steps:

1. **Define the problem management:** The bank should identify the roles and responsibilities in the problem management team (including a problem manager) and discuss the process that will be used to identify, prioritize and solve problems.
2. **Establish a problem management base:** The bank should have a database used to track all known problems. It can also include customer complaints, issues regarding the system, and violation of regulations.
3. **Develop a strategy to identify problems:** Find a way to identify potential problems before they have a significant impact on the bank. This can include regular review of data (e.g. customer complaints, audit reports).

4. **Establish a strategy for problem prioritization:** Not all problems will have the same impact on the bank's operations, so prioritizing problems based on potential impact is necessary. The problems can impact for example the financial, performance or reputational. The problems must be classified on these factors:
    a. Probability of occurrence
    b. Impact of risk
    c. Time to solve
5. **Develop a strategy for problem solving:** Establish a problem resolution process to solve problems, including prevention of the problem happening again in the future and communication procedures with the stakeholders (customers, other management teams).
6. **Regular reviews and updates of the processes in the management:** The bank should review the problem management often so it remains effective and relevant.
7. **Implement training:** Regular training within the bank will result in the employees having relevant and updated knowledge.
8. **Establish a customer complaint management process:** This bank's team will be responsible for the customer complaints and for solving them, like replacing the monitor in an acceptable time frame in this SLA breach case. This will result in customer satisfaction.
9. **Meet the requirements always:** The bank should have a relationship with the other teams and the regulatory bodies to ensure that the management process meets their requirements.

Supplier Management

The design of the supplier management process for the bank can be implemented as follows:

1. **Identify whether to have a single or multiple suppliers**: The bank could conduct a review of its current IT hardware sourcing strategy, taking into account factors such as cost, reliability, and risk. This could involve gathering data on the performance of the current supplier, as well as exploring options for alternative suppliers.
2. **Evaluate and categorize suppliers**: Once the decision has been made on the number of suppliers to have, the bank can then evaluate and categorize the selected suppliers based on their performance and other relevant factors. This could involve reviewing their financial stability, track record of meeting performance targets, and alignment with the bank's corporate strategy.

3. **Define and monitor performance metrics**: The bank should then work with its suppliers to define clear performance targets and establish a process for regularly reviewing and tracking progress against these targets. This could involve setting up regular meetings or reviews with the suppliers, and using metrics such as on-time delivery and incident resolution rates to measure performance.
4. **Save and process information in a dedicated database**: The bank should set up a dedicated database to store and manage all information related to its supplier relationships. This database should be accessible to relevant staff across the organization and should be regularly updated to ensure that the information it contains is accurate and up-to-date.

With this implementation, the bank should be able to better manage its supplier relationships and avoid SLA breaches like the one described in the case study. Additionally, the bank may want to consider implementing additional measures to mitigate the risk of SLA breaches, such as:

- **Conduct regular supplier reviews**: The bank could conduct regular reviews of its suppliers to ensure that they are meeting their performance targets and fulfilling their obligations under the terms of their contracts. This could involve gathering data on key performance indicators such as on-time delivery rates, incident resolution times, and customer satisfaction levels.
- **Implement a supplier performance improvement program**: If the bank identifies that a particular supplier is not meeting its performance targets, it could implement a performance improvement program to help the supplier improve. This could involve providing additional training or support, setting additional performance targets, or implementing other measures to help the supplier meet its obligations.
- **Establish a process for addressing supplier issues**: The bank should have a clear process in place for addressing issues that may arise with its suppliers. This could involve having regular meetings or check-ins with the suppliers to discuss any issues and identify ways to resolve them.
- **Have backup suppliers in place**: In order to reduce the risk of disruptions caused by issues with a single supplier, the bank could consider having backup suppliers in place for critical items. This would allow the bank to quickly source alternative supplies in the event that an issue arises with its primary supplier.
- **Develop contingency plans**: The bank should also have contingency plans in place to address potential disruptions or issues with its suppliers. These plans could include measures such as identifying alternative sources for supplies, implementing temporary workarounds, or activating crisis management protocols.

By implementing these measures, the bank should be able to better mitigate the risk of SLA breaches and ensure that it is able to continue meeting the needs of its customers in the event of issues with its suppliers.

Knowledge, Configuration and information security Management

Knowledge Management

To solve the problems regarding information and knowledge in the bank, these eight steps from the new process described earlier are necessary to follow for a professional knowledge management within this company:

1. **Identify the knowledge needs of the organization**: The bank should collect information from each sector (especially incident and problem teams) and map all the needs and find out the difference in relevance of information needed for each of them.
2. **Establish a knowledge management strategy**: Find a strategy to accomplish the needs in step 1. Identify the roles and responsibilities in the team and find a strategy to gather, organize, and distribute the information to every sector in the bank.
3. **Develop a knowledge management system**: The bank should implement a strategy for capturing, storing, and organizing the information with all the sectors so the relevant and necessary information is acquired for each sector. Make this system available for each employee in the bank and make it possible to integrate within different managements.
4. **Acquire knowledge**: Procedures for capturing knowledge will include getting information from the different team members, customers and external providers.
    a. The employees should be provided training and development opportunities - it should be encouraged to share knowledge.
    b. The bank must acquire knowledge from customer feedback in case of surveys and complaints.
    c. Acquire knowledge from external sources such as conferences and events - the bank should be informed about trends and best practices.
5. **Create knowledge**: To create knowledge in the bank, we can encouraging employees to share their experiences and expertise through collaboration and teamwork, providing training and development opportunities to help employees acquire new skills and knowledge, facilitating brainstorming sessions and idea

generation workshops to encourage innovation and new thinking or conducting research and development projects to explore new technologies and business models.

6. **Share knowledge**: The bank should share the knowledge with the employees and customers with a knowledge management newsletter that is distributed every week, a portal so each individual can go in and check when they want to, and training sessions. This includes making sure that the individuals do not acquire non-relevant information but organizing and categorizing the knowledge (use of tags, keywords and metadata).
7. **Use knowledge**: The employees in the bank use the relevant data for their decisions and problems. In this step, it includes maintaining knowledge, so the employees need to review, update and achieve information to use this information for later work.
8. **Measure and evaluate the effectiveness of the knowledge management process**: Identify metrics to measure the effectiveness of knowledge management and report regularly to the relevant stakeholders.

Information Security Management

To give this management the best practice and to avoid it having problems such as loss of information, the bank need to improve the security aspect of information with these steps:

1. **Identify cause of the problem:** investigate the cause of the problem to find out how the information was lost (in this case, during an update). This step includes how to prevent this from happening again in the future.
2. **Having a backup and recovery plan:** The bank should develop a plan just in case of a data loss, so they can recover the information. This includes regularly backing up data - creating backups, maintaining backups and test backups to know that they are restored properly, and how to restore the backups.
3. **Security mechanisms to prevent information and data loss:** The bank should have security mechanisms to protect sensitive information from unauthorized access and data loss. The bank must take encryption, firewalls, access controls, and intrusion detection systems in use.
4. **Implement monitoring and auditing:** The bank needs to establish a way to detect unauthorized access or data loss, and can do this by logging and monitoring access to data, and audits of the logs for detecting suspicious activity.
5. **Monitor and review information security controls:** The bank needs to ensure at all times that the procedures are in place. This should be done by regularly auditing and testing.

6. **Establish a security incident response plan:** The bank needs to know how to respond in case of an incident. This includes how to report the event, how to limit the damage, and how to recover from it.
7. **Regularly training:** The employees in the bank should have the updated best practices to keep information from losing and from unauthorized people. Update the employees on how to detect and report incidents, how to use backup and recovery. This should be done by giving them regular courses which result in awareness and more knowledge in the security aspect.

Configuration Management

The implementation of the configuration management process is mainly based on the resolution of the proposed case study and on the improvement of the process itself in general. The steps to be implemented are:

1. **Identify the configuration items (CIs) that need to be tracked and managed:** This can be done by conducting a thorough inventory of all the IT assets in the organization, including hardware and software components. A list of CIs can be created and maintained, with details such as the type, model, and serial number of each item.
2. **Create a Configuration Management Database (CMDB) to track and store information about the CIs:** This can be done by setting up a database system that can store information about the CIs, such as their type, model, and serial number, location, owner, and any associated contracts or warranties. The CMDB should be accessible to authorized personnel and should be updated regularly. This database can be internal to the bank or external to the cloud (more risky).
3. **Establish procedures for adding, updating, and deleting CIs in the CMDB:** This can be done by creating standard procedures for acquiring new CIs, retiring or decommissioning old ones, and updating existing CIs with new information as needed. The procedures should include steps for capturing all necessary information about the CIs and updating the CMDB accordingly. Each change in the CMDB should be approvate using the Change management process.
4. **Define the relationships between CIs:** This can be done by identifying the dependencies and impacts of changes to individual CIs. For example, a desktop monitor might be related to a particular desktop computer or to a specific user. These relationships can be captured in the CMDB and used to understand the context of changes to individual CIs.

5. **Develop reporting and visualization tools to help stakeholders understand and manage the CIs:** This can be done by creating dashboards, reports, or other tools that provide insights into the status, health, and utilization of the CIs. These tools should be accessible to authorized personnel and should be updated regularly.
6. **Establish processes for maintaining and updating the CMDB:** This can be done by creating regular audit and review processes to ensure that the CMDB is accurate and up-to-date, as well as procedures for correcting errors or discrepancies that are identified. The process should also include a procedure for maintaining the security of the CMDB, all this can be managed by competent personnel of the Application Unit Department and the Service Implementation Unit Department.
7. **Train relevant staff on the configuration management process:** This can be done by providing training on how to use the CMDB and other tools, as well as on the procedures for adding, updating, and deleting CIs. The training should be provided to all relevant staff, including IT personnel, service desk agents, and support staff.

Service Level Management

For Service Level management, the bank should follow these steps to avoid SLA breaches and not maintained SLA:

1. **Define the SLM:** Identify the roles and responsibilities of the SLM team and outline the process that will be used to manage service levels between the bank and its customers.
2. **Define service levels**: Identify the specific services that the bank provides to its customers, along with the corresponding service level agreements (SLAs) that are in place.
3. **Establish a strategy for monitoring service levels:** Implement procedures for regularly monitoring and measuring service levels against the SLAs, using tools and systems such as service level reporting and automated monitoring software.
4. **Develop a strategy for reporting and communicating service level performance:** Develop procedures for reporting service level performance to customers and other stakeholders.
5. **Managing SLA breaches:** The bank should establish a process to handle service level breaches and ensure that they are handled in a timely and efficient manner. This process should also include procedures for communication with customers and other stakeholders.

6. **Implement a service level review strategy:** The bank should regularly review the SLAs to ensure that they are still relevant and meet the needs of both the bank and the customer.
7. **Regular training:** Provide training to team members on the SLM process, the use of the tools, and the importance of maintaining service level agreements.
8. **Develop a customer service charter:** A customer charter is telling about the bank's commitment to customer service and what the customers can expect from them. In this way, the agreements between the bank and the customer will be easier to maintain since there are clear promises.
9. **Review and update the Service catalog:** A service catalog is a document that tells the services that the bank provides to its customers. This should be maintained and aligned with the Service Level Agreements.

Customers Involvement Process

The implementation steps to improve the Customer Involvement process are described below:

1. **Identify key stakeholders**: This can be done by conducting research, such as surveys or focus groups, to understand the needs, expectations, and priorities of customers, users, and other internal or external parties that will be impacted by the service. A list of key stakeholders can be created and maintained, with information such as their contact details, roles, and areas of interest.
2. **Engage with stakeholders early in the process**: Once key stakeholders have been identified, it is important to engage with them early in the service development process to ensure that their needs and priorities are understood and taken into account. This can be done by holding meetings, conducting interviews, sending out surveys, or organizing focus groups to gather feedback and insights.
3. **Collaborate and co-create**: Collaborating with stakeholders can help to ensure that the final service meets their needs and expectations, and can also improve customer satisfaction and loyalty. This can be done by involving stakeholders in the design and development process through workshops, prototyping, or other methods. The stakeholders can provide input and feedback on the service, and help in the co-creation of the service.
4. **Communicate and provide visibility**: Providing regular communication and visibility into the service development and delivery process can help to build trust and confidence with stakeholders, and can also help to identify and resolve potential

issues or concerns. This can be done by sharing progress updates, soliciting feedback, and being transparent about any challenges or delays.

5. **Iterate and gather feedback:** It is important to continue gathering feedback and insights from stakeholders throughout the service development and delivery process, and to use this feedback to iteratively improve and refine the service. This can be done by conducting user testing, gathering feedback through customer satisfaction surveys, or using other methods to gather insights and identify areas for improvement.

Portfolio Management

In the rollout plan for the implementation of portfolio management, the implementation of the steps described in the process design itself is defined, including further steps for the initiation of the process in the company, risk management and its maintenance.
The steps followed for the implementation of the process are the following:

1. **Identify the key stakeholders**: the stakeholders who are mostly involved in this process are already defined with their responsibilities in the RACI table, but in particular the stakeholders involved are:
    a. The IT department: This group is responsible for managing the portfolio and ensuring that it aligns with the bank's business goals and objectives.
    b. Business managers from each division: These individuals are responsible for representing the needs and priorities of their respective divisions, and for providing input on which services should be included in the portfolio.
    c. External partners such as suppliers and service providers: These groups may be involved in providing services to the bank, and it is important to include them in the portfolio management process to ensure that their needs and priorities are taken into account.

    By identifying these key stakeholders and involving them in the process, the bank can ensure that the portfolio management process is comprehensive and takes into account the needs of all relevant parties.
2. **Communicating the plan**: is an important step in implementing the service portfolio management process because it helps to ensure that all relevant parties are aware of the process and understand how it will be implemented. In this case, the IT department can communicate the plan in a number of ways:
    a. Sending out a company-wide email introducing the new process and explaining its goals and benefits: This can be an effective way to reach a

large number of people quickly and provide them with basic information about the process.

b. Giving a presentation at a meeting with business managers: This can be a more in-depth way to provide information about the process, and allows for questions and discussion.

By communicating the plan in these ways, the IT department can help to ensure that all relevant parties are aware of the process and understand how it will be implemented. This can help to build support for the process and ensure its success.

3. **Defining the scope of the portfolio**: helps to determine which services will be included in the portfolio. This should be done in collaboration with business managers, who can provide valuable input on which services are most important to the bank's operations and customers.In this case the main scope is to define all the useful service available for the customers and other stakeholders and this may involve reviewing existing services, identifying new services that could be added, and determining which services should be prioritized based on their importance to the bank's operations and customers.
4. **Establish portfolio governance**: it helps to ensure that there is clear responsibility and accountability for managing the portfolio. This typically involves defining the roles and responsibilities of the stakeholders involved in the process, such as the portfolio manager, portfolio board, and portfolio steering committee.
    a. The portfolio manager is typically responsible for day-to-day management of the portfolio, including tracking the performance of the portfolio against its goals and objectives, and making any necessary adjustments to ensure that it remains aligned with the bank's strategic direction.
    b. The portfolio board is responsible for providing high-level oversight of the portfolio, and may include representatives from the IT department, business divisions, and external partners such as suppliers and service providers.
    c. The portfolio steering committee is responsible for providing more detailed guidance on the management of the portfolio, and may include representatives from the IT department, business divisions, and external partners.

    By defining the roles and responsibilities of these stakeholders, the IT department can help to ensure that there is a clear chain of command and that everyone understands their role in the portfolio management process. This can help to ensure that the process runs smoothly and that the portfolio remains aligned with the bank's strategic goals and objectives.

5. **Develop the portfolio strategy**: the IT department works with the stakeholders to define the overall strategy for managing the portfolio. This includes setting clear goals and objectives for the portfolio, as well as identifying the key performance indicators (KPIs) and metrics that will be used to measure the success of the portfolio. This may include metrics such as cost savings, service level agreements (SLAs), and customer satisfaction.
6. **Identify and prioritize portfolio items**: to implement this step, the IT department and business managers can follow these steps:
    a. Create a list of all the services offered by the bank. This list should include all the services that are currently being offered, as well as any new services that are being planned or developed.
    b. Assess the strategic value of each service. Consider factors such as the service's contribution to the bank's overall goals and objectives, its importance to customers and users, and its potential to generate revenue.
    c. Assess the risks associated with each service. Consider factors such as the service's complexity, its reliance on external partners or suppliers, and its potential impact on the bank's operations if it fails or is disrupted.
    d. Assess the opportunities associated with each service. Consider factors such as the service's potential for growth, its ability to drive innovation, and its potential to increase customer satisfaction and loyalty.
    e. Prioritize the services based on the results of the strategic value, risk, and opportunity assessments. This will help the IT department and business managers focus on the most important services and allocate resources accordingly.
    f. Document the prioritization of the services in the portfolio management plan. This will provide a clear understanding of which services should be given the most attention and resources.
7. **Create the portfolio roadmap**: for this the IT department will need to:
    a. Define the timeline for implementing the portfolio. This should include the start and end dates for each phase of the process, as well as any key milestones that need to be achieved along the way.
    b. Estimate the budget required to implement the portfolio. This should include the costs of resources such as staff time, hardware, and software, as well as any external service providers or consultants that may be needed.
    c. Identify the resources needed to implement the portfolio. This could include personnel, equipment, and other assets required to deliver the services in the portfolio.

    d. Develop a plan for how the portfolio will be rolled out to users. This could involve creating training materials, communicating with users about the changes, and providing support to ensure a smooth transition.
    e. Define the processes and procedures that will be used to manage the portfolio. This should include details on how the portfolio will be monitored and reviewed, how decisions will be made about adding or retiring services, and how risks and issues will be identified and addressed.
    f. Establish a system for tracking the progress of the portfolio. This could involve using project management software or creating a dashboard to monitor key performance indicators and other metrics.
    g. Review and update the portfolio roadmap on a regular basis to ensure that it remains aligned with the organization's goals and objectives.
8. **Train staff on the new process**: in order to effectively implement the new portfolio management process, it is important to ensure that all relevant staff are properly trained on how to use it. This may include:
    a. Providing an overview of the new process, including its goals and benefits, and explaining how it differs from any previous portfolio management processes.
    b. Detailing the steps involved in the process, including how to identify and prioritize portfolio items, how to create the portfolio roadmap, and how to monitor and review the portfolio.
    c. Demonstrating how to use any tools or systems that will be used to support the process, such as a portfolio management software platform.
    d. Providing hands-on practice or exercises to help staff gain a better understanding of how to apply the process in their day-to-day work.
    e. Ensuring that staff have access to resources and support to help them learn and understand the new process, such as training materials or an internal knowledge base.
9. **Launch the process**: the portfolio management process is finally launched and monitored to respect the metrics defined.

Integration Process

The following steps, corresponding to the points describing the revised process, are conducted as the revised Integration process is deployed:

Onboarding program:

1. First, the bank makes sure that all current employees are aware of cultural differences and how to work effectively with people from different backgrounds by launching a cultural sensitivity program.
2. Guidelines for cross-cultural communications are developed. Procedures should be in place to make sure all employees are aware of them.
3. A comprehensive onboarding program for new staff that includes team building activities and mentorship opportunities is implemented.
4. The effectiveness of the onboarding program is monitored and evaluated by conducting surveys and gathering feedback from new staff. Adjustments are made when needed.

IT Support:

1. A survey of current IT support levels across all divisions is conducted to establish a baseline level of support that will be helpful in making sure standards are met across the divisions..
2. Key metrics to monitor the level of support are identified. These are metrics such as response time, resolution time, and customer satisfaction rates.
3. The new level of expectations for IT support are communicated to all banking divisions and it is made sure that employees understand what is expected of them.
4. The level of IT support provided by each division is monitored, and the identified metrics are utilized to evaluate performance.
5. Areas for improvement are identified and necessary changes are made.

Process integration:

1. A thorough audit of the processes at each branch of the business is conducted.
2. Areas for improvement are identified and a plan to modify processes as needed is developed.
3. The existing divisions work with employees at newly acquired companies to implement the new processes.
4. The effectiveness of the new processes is monitored and adjustments are made as needed.
5. It is investigated whether the new processes align with the bank's overall business objectives.

Knowledge management:

1. A knowledge management system that includes a database of relevant information and resources is implemented. Relevant information can be process documentation, training materials, best practices, etc..
2. A mentorship program is established, where newly acquired employees can learn from more experienced colleagues.
3. Training and resources are provided to help new employees understand the bank's processes and culture.
4. The effectiveness of the knowledge management system is monitored and adjustments are made as needed.
5. The knowledge management system is continuously updated with the newest information and resources.

Deployment Management

For the bank to deploy their services in best way, the following steps need to be followed:

1. **Define the deployment management:** Identify which steps and workflows are included in the deployment process and the roles and responsibilities to each team member of the management. This includes the goal of the deployment which clarifies the scope.
2. **Develop a change strategy:** A strategy for how to manage changes regarding services and systems so the bank is prepared in case of a change. This should include testing and validation of changes before deployed into production. The bank must test the performance and the functional of each service and system.
3. **Implement a rollback plan:** The bank should have the possibility to roll back from the changes in case of problems or failures. The tools must be in place in this step to be possible to roll back from a new change.
4. **Report the changes:** First, it includes an analysis or a monitoring of the performance of the new changes of the services after deploying, and second, report this performance if any problems occur to the stakeholders that are relevant.
5. **Manage the portfolio of services:** The bank should manage the portfolio of services offered by the bank, including regular reviews, updates and retirements of services.
6. **Review the deployment as related to the SLA breach:** Review the deployment process for the monitor replacement service and identify any issues or problems that contributed to the SLA breach. Make changes to the process as needed to ensure that the service can be deployed and maintained at the expected quality standards.

7. **Make sure the ordering process and the deployment process are aligned:** Check the ordering process, for example the monitor replacement service, is aligned with the deployment process so that the services can be deployed and result in efficientely and effectively maintained.
8. **Implement the deployment**
9. **Regular training:** The bank should provide training so the team members of this management are up-to-date with information and tools.
10. **Identify improvement areas:** Review the process if it could proceed better and how. Report to relevant stakeholders.

Ordering Process

The rollout plan for the ordering process to it will avoid breaches and the other errors found in the analysis, the bank needs to follow these steps:

1. **Define the ordering process:** Identify the specific steps involved in the ordering process, from receiving an order to delivering the product or service.
2. **Identify the key stakeholders:** Determine who will be involved in the ordering process, including customers, service desk agents, purchasing teams, shipping and logistics teams, and external providers.
3. **Establish order management system:** The bank can have a computer-based system, and it should be designed to streamline the ordering process, provide transparency and automate processes where possible. It should include a real-time monitoring system, like real-time issue of the monitor in our case, and delivery status of external providers.
4. **Establish a process for order fulfillment:** Develop a process for fulfilling orders, including shipping and logistics, and ensuring that orders are delivered on time and in the correct condition. Take measures to have a plan B in case of delay of an external provider.
5. **Develop a process for communication:** The service desk agent should have a process for communicating with both external provider and the end user to give updates, information and confirmations. In this way, the agent can be effective and efficient with the end-user, especially regarding delays.
6. **Regular training:** The bank should provide regular training for the agents and other team members in this process, so they are up-to-date with both tools, the process and the information.
7. **Measure the performance of the management and report it**

8. **Continuous improvement:** The bank should establish a process for analyzing and collecting data from the order process to check the errors, potentially low performance, and improvements.

References

1. The power points (Training Course Materials part 1, part 2, part 3 and part 4)
2. The 4 Dimensions of ITIL 4: Partners & Suppliers - IFS Blog [4th of October 2022]
3. ITIL Reactive and Proactive Problem Management: Two sides of the same coin [4th of October 2022]
4. Service Portfolio Management | IT Process Wiki [5th of October 2022]
5. Configuration Management in ITIL4 – ITIL Docs [6th of October 2022]
6. Service Asset and Configuration Management | IT Process Wiki [6th of October 2022]
7. How To Define, Handle & Avoid SLA Breaches – BMC Software | Blogs [8th of October 2022]
8. Service Level Management in ITIL 4 – BMC Software | Blogs [8th of November 2022]
9. ITIL® Release and Deployment Management – BMC Software | Blogs [10th of November 2022]
10. The customer journey and ITIL 4 | Axelos [10th of November 2022]
11. Understanding ITIL Service Design | Lucidchart Blog [28th of November 2022]
12. Knowledge Management Design Principles | APQC [8th of January 2023]
13. Design & the Implementation of Knowledge Management System [8th of January 2023]
14. A Complete Overview of Supplier Management in ITIL [9th of January 2023]
15. Supplier Management | IT Process Wiki [9th of January 2023]
16. What is Supplier Management from an ITIL perspective? : ITILNews.com [9th of January 2023]
17. Why and how to Implement Supplier Management? [9th of January 2023]
18. Problem Management: 8 Steps to Faster Incident Resolution • Asana [10th of January 2023]
19. 8 Steps to Implementing a Knowledge Management Program at Your Organization - Sirius Edge [10th of January 2023]
20. The successful knowledge management rollout | SABIO [10th of January 2023]
21. How to Implement an Information Security Program in 9 Steps - BARR Advisory [10th of January 2023]
22. Configuration Management Plan: Purpose and Components | Indeed.com [10th of January 2023]

23. Implementing Service Level Agreements - IT Service Desk | Giva [10th of January 2023]
24. The Ultimate Guide to Customer Engagement in 2021 [12th of January 2023]
25. 17 Ways to Engage & Re-Engage Your Customers [+ Sample Letter] [12th of January 2023]
26. The customer journey and ITIL 4 | Axelos [12th of January 2023]