ITIL project

Alessio Trevisan 2057467
Vittorio Schiavon 2057832

April 23, 2023

Contents

List of Figures

1 Abstract

The goal of this document is to describe the process of analysis and improvement of the set of processes applied to the resolution of hardware malfunctioning incidents.
This document and the work described in it have been developed after an official request made by the CIO of our company.
The document is structured into three main sections: the analysis of the critical situation, the evolutionary plan and the rollout plan of how to get the changes successfully applied to production.

2 Analysis of the critical situation

The analysis described in this document is based on a case study that brought to light serious management problems regarding the replacement of malfunctioning hardware.
This section describes all the useful details of the case study, paying particular attention to the succession of events that have been implemented to resolve the incident. After this detailed description, all the processes involved are highlighted and the worst faults have been listed.

2.1 Case study

In the figure below (Figure 1), it is possible to see the flowchart that summarizes what happened in the case study. Every step will be further described later during this section.

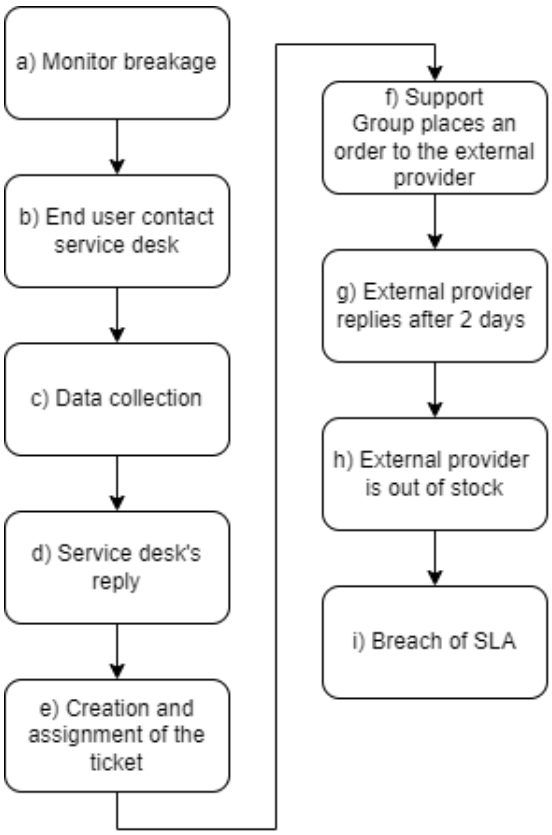

Figure 1: Flowchart of succession of events of the case study

2.1.1 Detailed description of every step

- a) Monitor breakage: the end user has found out that his monitor has a crack. The broken screen, according to the user, is a medium-impact hindrance to his productivity since it is still operating apart from a few unintentional shutdowns. The user expects to be able to continue using the broken screen for a few more days since the time of the request.
- b) End user contact service desk: The user has contacted the service desk via the right channels.
- c) Data collection: the service desk has helped the user to fetch information about the incident and it has captured all necessary details in the Service Management tool.
- d) Service desk's reply: the service desk, based on the set thresholds, responded to the user that the service would be done within 5 working days.
- e) Creation and assignment of the ticket: after data collection a ticket was created and assigned to the appropriate support group.
- f) Support Group places an order to the external provider: The assignee of the Support Group places an order to the external provider who is responsible for managing the supply for all desktop services.
- g) External provider replies after 2 days: the external provider alerts the Support Group after two days that there are no more monitors in stock.
- h) External provider is out of stock: not having spare parts in stock resulted in the provider being able to perform the repair in no less than a week and a half.
- i) Breach of SLA: a service that should have taken a maximum of 5 working days was carried out in more than two weeks. This represents a significant breach of the SLA.

2.2 Bottlenecks and SPOF

The Service Management analyst group has spotted sub-optimal management practices that led to unacceptable handling of the incident. Resolving these errors is necessary to sanitize the management of hardware malfunctioning incidents and apply the correct procedure to minimize the impact on productivity and costs of the incident.
This is the list of major issues encountered in the study case:

- Lack of automated response system with External Provider: the inability to receive a response from the external provider in a timely manner results in the efficiency of incident resolution being unacceptable.

- Lack of hardware request form: the absence of an established method to check hardware support availability hinders the effectiveness of the process.
- Lack of same day hardware solution: many hardware malfunctions severely hinder the productivity of the end user and, when the end user's work is not deferrable, a immediate solution is needed.
- Lack of financial penalty in case of breach in SLA: the case study shows that the breach of the SLA is not punished.
- Total dependence on external services: having an in-house solution to address a breached service level is advisable as solely depending on an external service may result in unacceptable failures and delays.

3 Evolutionary plan

A different, better approach to managing hardware malfunctioning incidents has been conceived and in the following sections, it will be discussed in detail.

3.1 Flowchart object definition

In order to read and comprehend the following flowcharts it is necessary to understand the meaning of their visual objects:

- standard rectangle: when it is at the beginning of a flowchart it contains the name of the sub-process. If the rectangle has a parent object it means that the indicated sub-process needs to be executed first before continuing. It is common to use colors to help the readability of the charts.
- rounded rectangle: it represents a single, atomic activity.
- rhombus: it is an if-then statement. The question or check under the exam usually fires an affirmative or negative response, and based on that the flow of the sub-process changes.
- ellipsis: it represents the closure of a sub-process.

3.2 Definition of a sub-process

To define the process of hardware malfunctioning incidents management, a series of sub-process has been created. To define each sub-process, it has been followed the following structure:

- sub-process flowchart: this figure illustrates the steps to perform to complete the sub-process.
- sub-process scope and objectives: this section tells the objectives of the process and what it aims to achieve.
- sub-process activities: it defines the activities required to deliver the sub-process. It is an in-depth description of every step included in the flowchart.
- sub-process roles and responsibilities: it identifies the roles and responsibilities involved in delivering the process.
- sub-process inputs and outputs: it define the list of inputs required to deliver the sub-process and the expected outputs.
- sub-process performance metrics and continual improvement: it is useful to track the performances of the process and identify and collect the opportunities for improving the sub-process.

3.3 Solution

A better way to manage hardware malfunctioning incidents requires multiple steps, investigations, forms, and many more aspects. To increment the readability of the proposed solution, it has been split into sections that are intended to illustrate the new functioning of a sub-part of the incident management process.

It is important to note that in this evolutionary plan, the team is proposing an improvement regarding the specific type and urgency of the situation proposed.

The evolved hardware malfunctioning incident management process has been split into four different sub-processes:

- Incident management: the general incident management process.
- Resolution and recovery for hardware malfunction tickets: the sub-process that starts the resolution of the hardware malfunction tickets.
- Supplier answer analysis and response: it is the sub-process that receives the answer from the hardware supplier and proceeds with the process accordingly.
- Hardware disposal management: it is the sub-process that manages how the damaged hardware should be disposed.

In addition to the previous sub-processes, it is necessary to define other two sub-processes that manage the backup hardware warehouse:

- Backup warehouse management analysis: it ensures the warehouse backup satisfies the OLA.
- Periodic backup hardware test: it performs an age, quality, and quantity test on the hardware in the warehouse

3.4 Incident management sub-process

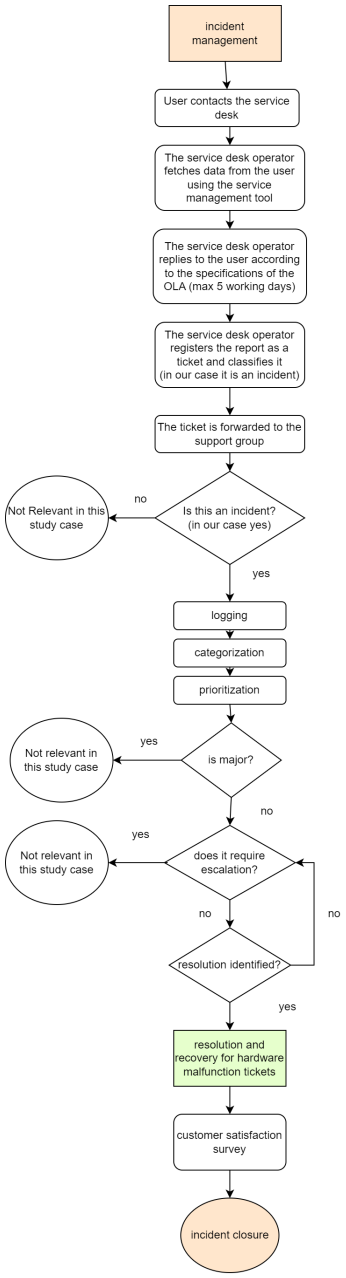

Figure 2: Flowchart of the sub-process "Incident management"

3.4.1 Scope and objectives

The scope of Incident Management is to manage the life cycle of incidents, from detection and logging to resolution and closure. The sub-process is necessary to minimize the impact of incidents and restore normal service operation as quickly as possible, maintain consistency, identify and prevent a recurrence, and continually improve the process.

3.4.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 2.
Here it is a detailed description of every activity:

- User contacts the service desk: as seen in the study case, when a hardware malfunction occurs, the end user can contact the service desk to report the situation.
- The service desk operator fetches data from the user using the service management tool: the SD can collect the information shared by the end user using the service management tool. Important factors such as the type of incident, the urgency of the operation, the cause of the incident, and more are collected using the tool.
- The service desk operator replies to the user according to the specifications of the OLA: the SD can provide the end user useful information about how and when the incident might be resolved. This is doable because the SD assumes the OLA will be respected.
- The service desk operator registers the report as a ticket and classifies it.
- The ticket is forwarded to the support group.
- Question: is this an incident?: check the ticket just created and if the answer is "no", continue with the standard management, while if the answer is "yes", continue with this sub-process.
- Logging: it is an important activity because it captures and records critical information related to incidents, helping to investigate and resolve them, identify trends, and provide a historical record for reporting and analysis.
- Categorization: it analyzes the type of incident.
- Prioritization: this activity aims at assigning the right urgency to the incident. It should be done considering the impact that the incident has on the stakeholders affected by the incident.
- Question: is it a major incident?: if the answer to this question is "yes", carry out the process of major incident management, otherwise, continue with this process.

- Question: does it require escalation?: analyze the incident and, if needed, proceed to manage its escalation, otherwise proceed with this sub-process.
- Question: resolution identified?: if the resolution is known, then continue, otherwise reconsider its escalation.
- Resolution and recovery for hardware malfunction tickets: once the ticket has been analyzed and the resolution is found, proceed with it. In this study case, the resolution is for hardware malfunction and it is defined in the next sub-process.
- Customer satisfaction survey: once the incident is resolved it is a good practice to perform a customer satisfaction survey to assert the level of efficiency of the operation.
- Incident closure: the incident has been analyzed and resolved so the ticket can be closed.

3.4.3 Roles and responsibilities

Please read the RACI matrix section.

3.4.4 Inputs and outputs

The input for this sub-process is the request of the end user to contact the service desk.
The outputs of this sub-process are the customer satisfaction survey and the logs produced during the activities.

3.4.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- response time of the service desk
- resolution time of the incident
- working hours used to resolve the incident
- cumulative working hours lost
- cost of the operation
- end user feedback
- difference between estimated and actual working hours needed

3.5 Resolution and recovery for hardware malfunction tickets sub-process

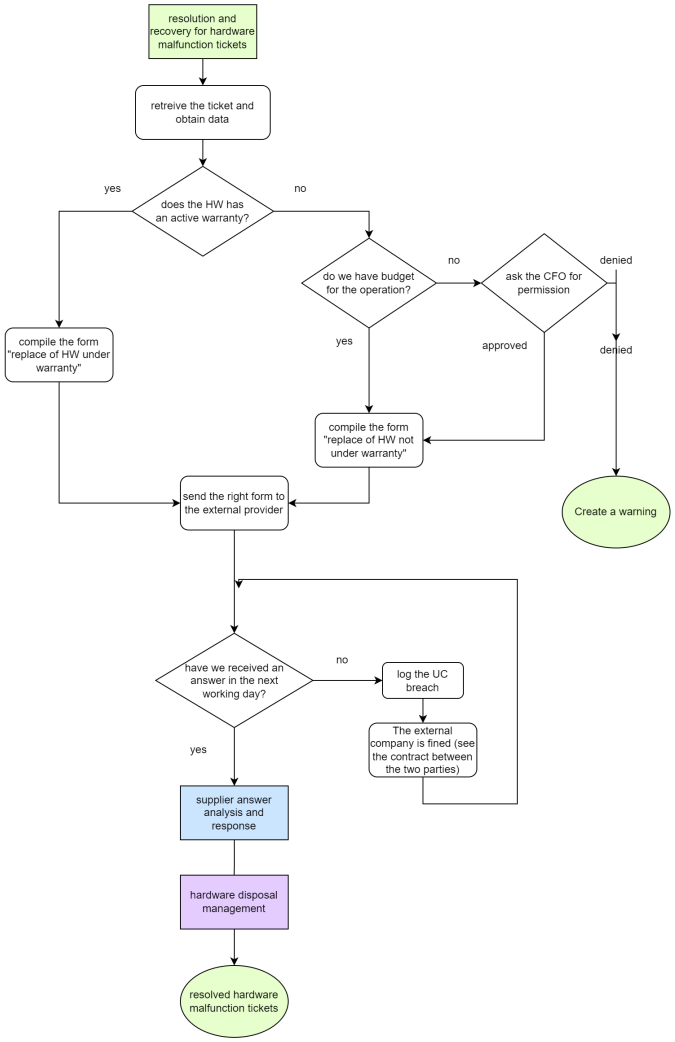

Figure 3: Flowchart of the sub-process "Resolution and recovery for hardware malfunction tickets"

3.5.1 Scope and objectives

The scope of the "Resolution and recovery for hardware malfunction tickets" sub-process is to ensure that hardware malfunctions are resolved efficiently and effectively, minimizing the impact on business operations. To achieve this is important to have solid communication with the external provider responsible for the management of the company's hardware. The main activity is the checking of an active warranty that determines the proper request, expressed as standardized forms, to send to the external provider.

3.5.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 3.
Here it is a description of every activity:

- Retrieve the ticket and obtain data: the input of the activity is the incident ticket with its data.
- Question: does the hardware has an active warranty?: it is a crucial aspect because the financial impact of fixing a piece of hardware strictly depends on weather it is possible to enforce the warranty claim or not.
- Compile the form "replace of HW under warranty": If the answer to the previous question is "yes", then compile the correct form.
- Question: do we have the budget for the operation?: if the answer to the first question is "no", it is crucial to understand if the company has a sufficient available budget to complete the operation.
- Question: ask the CFO for permission: if the company does not have a pre-allocated sufficient budget, then to continue the process it is necessary to have the permission of the CFO. If the CFO approves the operation then proceed, otherwise create a warning and end the process.
- compile the form "replace of HW not under warranty": if the budget for the operation is available or the CFO has confirmed the operation, proceed to fill the form to contact the external provider.
- Send the right form to the external provider: after filling out the right form, which can be "replace of HW not under warranty" or "replace of HW under warranty", send it to the external provider.
- Question: have we received an answer in the next working day? According to the service level agreement between our company and the external provider, it is crucial to receive an answer in a maximum of two working days. For this reason, it is useful to keep track of how many days the external provider takes to provide the support group with an answer.

- Log the UC breach: if the external provider takes more than a working day to answer, log the UC breach.
- The external company is fined: since a UC breach has occurred, the external provider has to face the consequences.
- Supplier answer analysis and response: once the answer from the external provider arrives, proceed to complete the sub-process called "supplier answer analysis and response".
- Hardware disposal management: once the "supplier answer analysis and response" sub-process is completed it is necessary to manage the disposal of the hardware with the sub-process "hardware disposal management"
- Resolved hardware malfunction tickets: the sub-process can be closed successfully.

3.5.3 Roles and responsibilities

Please read the RACI matrix section.

3.5.4 Inputs and outputs

The inputs for this sub-process are the incident ticket and the damaged hardware unit.
The outputs of this sub-process are the compiled form and the logs produced during the activities.

3.5.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- percentage of hardware unit under warranty
- warranty check response
- response time
- request time
- cost of the operation
- percentage of approved operation by the CFO
- percentage of operation that ends in a UC breach

3.6 Supplier answer analysis and response

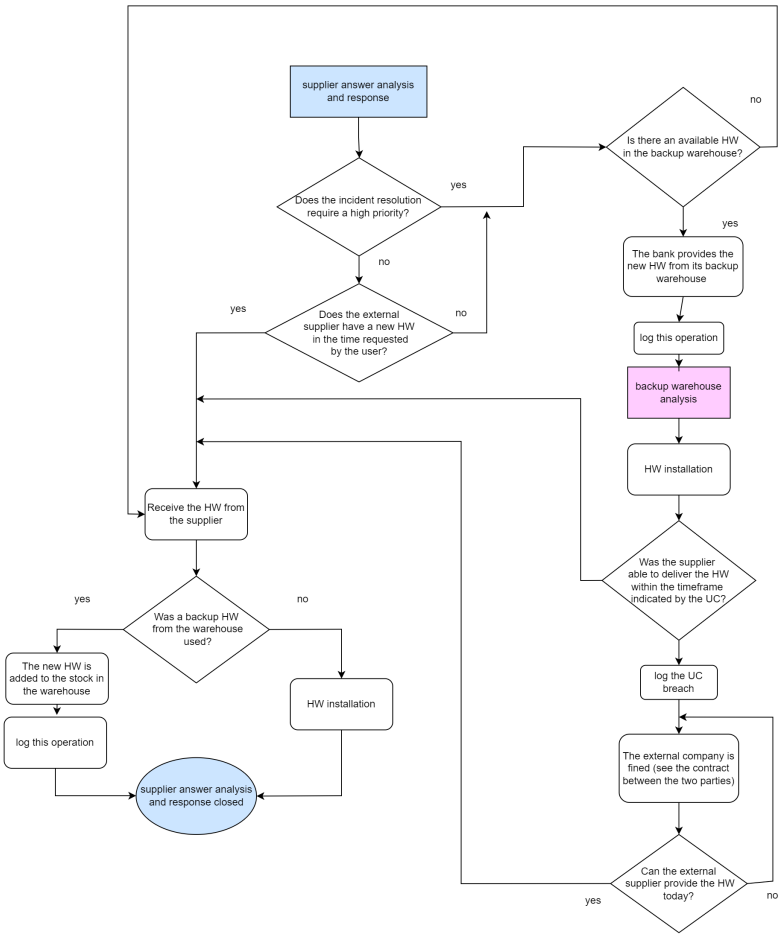

Figure 4: Flowchart of the sub-process "Supplier answer analysis and responses"

3.6.1 Scope and objectives

The scope of "Supplier answer analysis and response" sub-process is to act upon the response of the external provider. The main activity of this sub-process is to mitigate as much as possible the negative impact that an eventual UC breach might have on the productivity of the company.

3.6.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 4.
Here it is a description of every activity:

- Question: Does the incident resolution require a high priority?: the incident ticket shows the urgency of the resolution. The urgency determines the approach the company has to the resolution of the incident because, if the incident is severe, then the company provides backup hardware to ensure business continuity, otherwise it is not necessary.
- Question Does the external supplier have a new HW in the time requested by the user?: if the urgency is not high but the external provider cannot provide working hardware in the time requested by the user, it is mandatory to ensure business continuity by offering backup hardware.
- Question: Is there an available HW in the backup warehouse?: if, for any reason, it is requested backup hardware from the warehouse, the first step is to confirm the availability of the requested piece. If there is no available piece, wait for the hardware sent by the external supplier.
- The bank provides the new HW from its backup warehouse: if the warehouse can provide backup hardware, then proceed.
- Log this operation: keep track of the usage of the hardware.
- Backup warehouse management analysis: start and complete the subprocess. It is useful to maintain the backup warehouse up to standards.
- HW installation: The hardware has to be installed.
- Question Was the supplier able to deliver the HW within the time-frame indicated by the UC?: This check is necessary to log the efficiency and eventual brakes of the UC.
- Log the UC breach: if the supplier has not been able to deliver the hardware in the prefixed timeframe a UC breach has occurred. Log the breach.
- The external company is fined: the external supplier has to be fined for the UC breach.
- Question: Can the external supplier provide the HW today?: repeat the check every day and for each day of delay apply a fine.

- Receive the HW from the supplier: when the company receives the hardware, retrieve it.
- Question: Was a backup HW from the warehouse used?: this check allows us to understand what to do with the new hardware, based on whether we have used backup hardware or not.
- HW installation: if the process did not require backup hardware, the new hardware piece has to be installed.
- The new HW is added to the stock in the warehouse: if the process required backup hardware, the new hardware piece should be sent to the warehouse to replace the backup one used.
- Log this operation: keep track of the operation.
- Supplier answer analysis and response closed: the sub-process can be closed successfully.

3.6.3 Roles and responsibilities

Please read the RACI section.

3.6.4 Inputs and outputs

The inputs for this sub-process are the incident ticket, the requested hardware unit from the supplier, and the backup hardware from the warehouse.
The outputs of this sub-process are the logs produced during the activities.

3.6.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- percentage of high-priority tickets
- percentage of operation utilizing backup hardware units.
- working hours lost due to the operation
- hardware installation time
- supplier delay hours

3.7 Backup warehouse management analysis

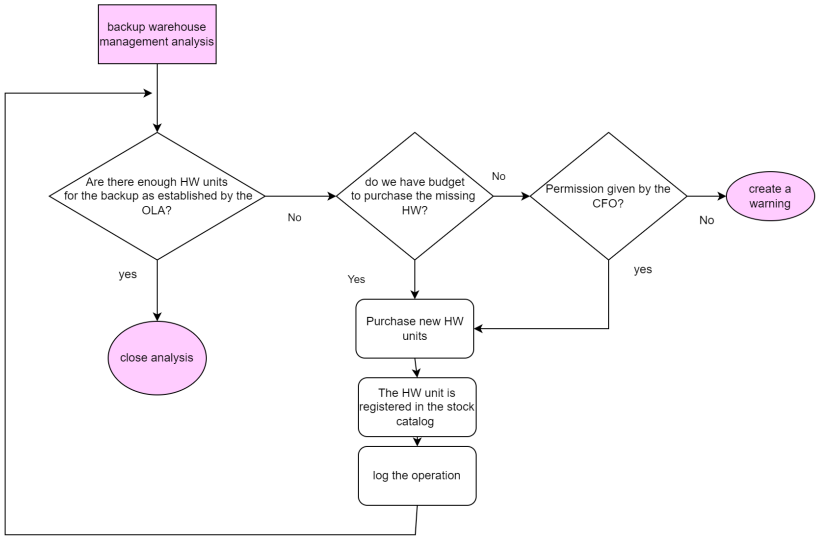

Figure 5: Flowchart of the sub-process "Backup warehouse management analysis"

3.7.1 Scope and objectives

The scope of the "Backup warehouse management analysis" sub-process is to maintain the quality and the quantity of the backup warehouse up to standards and service level agreement.

3.7.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 5.
Here it is a description of every activity:

- Question: Are there enough HW units for the backup as established by the OLA?: check if the quantity of the hardware pieces is enough.
- Question: do we have a budget to purchase the missing HW? If there is a shortage of hardware pieces, check the budget to understand if a purchase is feasible or not.

- Question: was permission given by the CFO?: If there is no pre-defined budget available, ask the CFO if the operation should and can be done. If the answer is "no", close the sub-process and create a warning.
- Purchase new HW units: If there is an available budget, purchase the missing hardware unit(s).
- The HW unit is registered in the stock catalog: update the warehouse catalog.
- Log the operation: keep track of the changes and operations.
- Close analysis: when there are enough units per category, end successfully the analysis.

3.7.3 Roles and responsibilities

Please read the RACI section.

3.7.4 Inputs and outputs

The inputs for this sub-process are the number of minimum hardware units per category, and the process for purchasing new hardware units.
The outputs of this sub-process are the analysis of the status of the backup hardware and the logs produced during the activities.

3.7.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- number of missing hardware units
- type of missing hardware units
- number of purchased hardware units
- types of purchased hardware units.
- money spent to complete the purchasing
- percentage of operation approved by the CFO
- number of warnings

3.8 Hardware disposal management

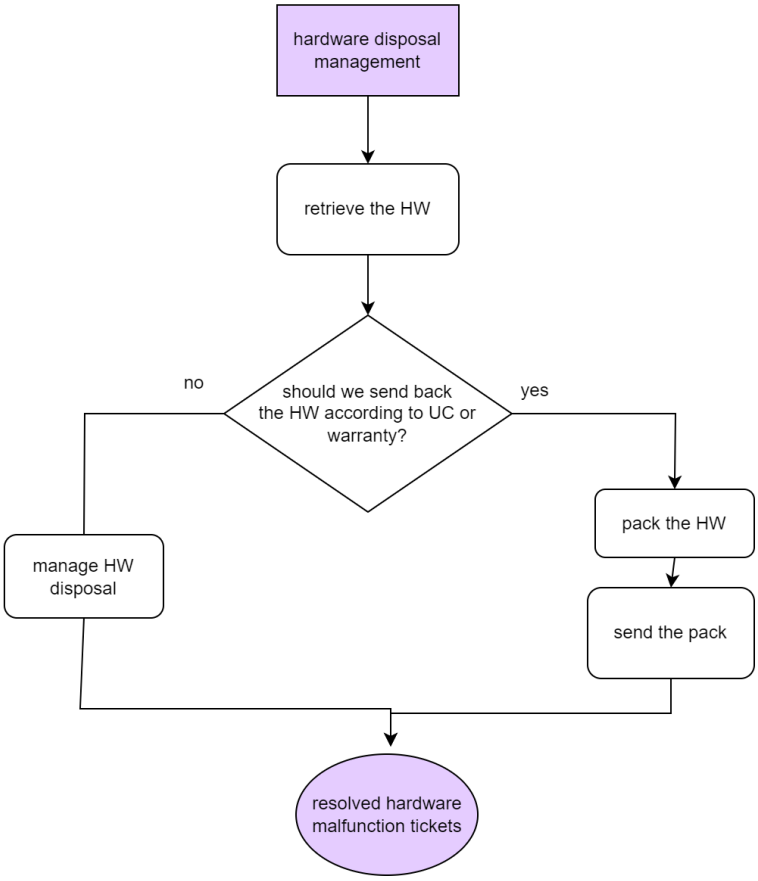

Figure 6: Flowchart of the sub-process "Hardware disposal management"

3.8.1 Scope and objectives

The scope of the "Hardware disposal management" sub-process is to manage the disposal of broken hardware units. This activity depends on whether or not the hardware unit is under active warranty.

3.8.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 6.
Here it is a description of every activity:

- Retrieve the HW: collect the unit.
- Question: should we send it back the HW according to UC or warranty?: check if the external provider requires the damaged hardware to be sent back to them.
- Manage HW disposal: If the hardware unit does not have to be sent back to the supplier, proceed with the standard hardware disposal.
- Pack the HW: If the hardware unit is under warranty, it has to be sent to the external provider. Create a pack safely containing the hardware. Remember to include every piece and necessary data.
- Send the pack: send the pack to the right address of the external supplier.
- Resolved hardware malfunction tickets: close successfully the sub-process.

3.8.3 Roles and responsibilities

Please read the RACI section.

3.8.4 Inputs and outputs

The input for this sub-process is the damaged hardware.
The outputs of this sub-process are the logs produced during the activities.

3.8.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- cost of disposal
- percentage of hardware units sent back to the external provider
- disposal hours used
- number of delivered pack
- number of disposed hardware

3.9 Periodic backup hardware test

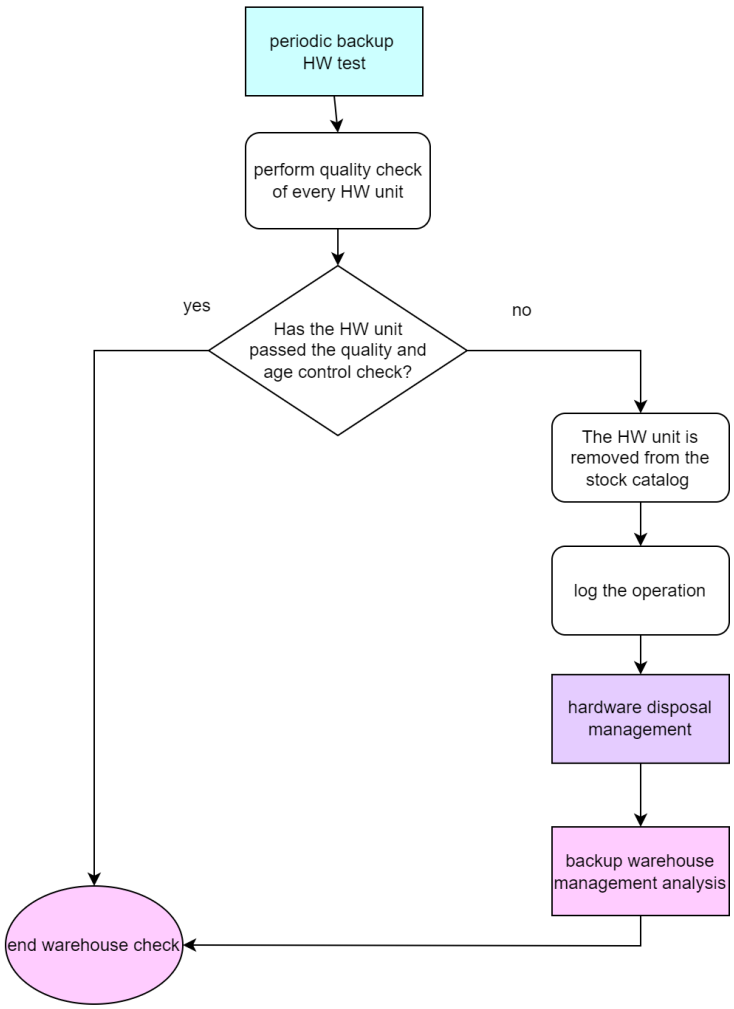

Figure 7: Flowchart of the sub-process "Periodic backup hardware test"

3.9.1 Scope and objectives

The scope of the "Periodic backup hardware test" sub-process is to test the age and quality of the hardware units of the backup warehouse. The test has to be performed periodically.

3.9.2 Activities

The activities to complete this sub-process can be seen in the flowchart of Figure 7.
Here it is a description of every activity:

- Perform quality check of every hardware unit: complete a quality test of every hardware piece contained in the backup warehouse.
- Question: Has the HW unit passed the quality and age control check?: if there are no failed tests, conclude the periodic analysis.
- The HW unit is removed from the stock catalog: remove every damaged or expired hardware unit from the catalog
- Log the operation: keep track of the operation and its specification.
- Hardware disposal management: complete the sub-process dedicated to the hardware unit disposal.
- Backup warehouse management analysis: complete the sub-process dedicated to restoring the quality of the backup hardware warehouse.
- End warehouse check: once every unit passes the control check, close the analysis.

3.9.3 Roles and responsibilities

Please read the RACI section.

3.9.4 Inputs and outputs

There are no inputs for this sub-process. It is a periodic activity.
The outputs of this sub-process are the logs produced during the activities.

3.9.5 Performance metrics and continual improvement

To judge the performance of the sub-process, the following metrics need to be collected:

- percentage of passed test
- number of test performed
- number of expired hardware units

- number of hardware units of insufficient quality
- percentage of expired hardware units
- percentage of hardware units of insufficient quality
- test requested time
- cumulative hours spent to perform the whole test
- number of units removed from the catalog

4 RACI matrix

This section explains the correlation between the various roles and the respective involvement in every task of the redefined processes. The incident management process is a general overview whose incident resolution phase is analyzed more in detail in the Incident resolution and customer satisfaction analysis subsection. A tabular form of the RACI matrix can be consulted at the following link https://docs.google.com/spreadsheets/d/1Nl1igIZ1uTaxF_o3VDkD9SVDvEl-LmRyIFKzwDQod9o/edit#gid=0

- A: accountable (and by consequence also responsible)
- R: responsible
- C: consulted
- I: informed

4.1 Incident management

4.1.1 Incident identification

- *End user - R,C:* the end user responsible for reporting the error and following the instructions given by the Service Desk and he is consulted to retrieve data about the incident
- *Service desk manager - A,R,I:* the service desk manager is accountable for having at least one service desk analyst available in order to address the issue, as accountable he/she is also responsible and must be informed whether an incident occurred
- *Service desk analyst - R,I:* the service desk analyst is responsible for capturing the info related to the incident and identify it, he must be also informed by the end user about the details of the issue

4.1.2 Incident logging

- *End user - C,I:* the end user is consulted for retrieving more information about the incident and he/she is informed about the incident log
- *Service desk manager - R,I:* the service desk manager is responsible for the supervision of the incident management flow and he/she is informed about the incident log
- *Service desk analyst - A,R,I:* the service desk analyst is accountable for creating a new incident log, he is informed about the info required to create the ticket

4.1.3 Incident categorization

- *End user - I:* the end user is informed about the next steps to be taken
- *Service desk manager - C:* the service desk manager is consulted about any possible doubt about the incident classification
- *Service desk analyst - A,R:* the service desk analyst is accountable for classifying an incident according to the information that he/she disposes of

4.1.4 Incident prioritization

- *End user - C,I:* the end user is consulted for retrieving more information about his/her necessities and he/she is informed about the next steps to be taken
- *Service desk manager - C,I:* the service desk manager is consulted in cases of uncertainty and is immediately informed in cases where the priority is strict
- *Incident analyst - C:* he/she is consulted about cases where there is uncertainty about the priorities to be assigned by the service desk
- *Service desk analyst - A,R:* the service desk analyst is accountable for prioritizing all the tickets

4.1.5 Incident investigation

- *End user - R,C:* the end user is responsible for reporting all eventual new symptoms or information related to the incident
- *Incident manager - A,R:* the incident manager is accountable (and responsible) for making sure that all incidents are properly assessed and analyzed by a team and an analyst
- *Incident analyst - R,C,I:* the incident analyst is responsible for investigating the various issues that have occurred in the incident
- *Service desk analyst - C,I:* the service desk analyst is consulted for eventual useful information by the incident analyst and is informed about the status of the investigation
- *Incident resolution team - C,I:* the incident resolution team is consulted in order to find out more about the possible causes of the incident and is informed about the incident that is under investigation
- *Service desk manager - I:* the service desk manager is informed about the beginning of the incident investigation phase

4.1.6 Incident resolution

Referenced by subsection Incident resolution and customer satisfaction analysis

4.1.7 Incident closure

- *End user - I:* the end user is informed about the incident closure
- *Incident manager - I:* the incident manager is informed about the incident closure
- *Service desk analyst - A,R,I:* the service desk analyst is accountable for closing the ticket and is informed about the possibility to close the incident by the incident analyst
- *Incident analyst- R,C,I:* the incident analyst is responsible for communicating the incident closure to the service desk analyst once all the issues of the incident have been addressed, he is consulted by the incident resolution team to understand whether all the issues have been properly fixed and is informed by the same team in order to understand the status of the resolution of one or more issues
- *Incident resolution team - R,C,I:* the incident resolution team is responsible for communicating the status of the issues detected in the incident, it is consulted by the incident analyst in order to let him/her understand the status of the resolution and is informed by the same analyst about the completion of the tasks involved to close the incident
- *Service desk manager - I:* the service desk manager is informed about the incident closure
- *Service level manager - I:* the service level manager is informed about the incident closure in order to let him/her conduct some analysis on the whole incident management process

4.2 Incident resolution and customer satisfaction analysis

4.2.1 Team assignment

- *Incident manager - A,R,I:* the incident manager is accountable for making sure that a team is assigned to the incident analysis and management and is informed about the availability of the components of the team
- *Service desk analyst - I:* the service desk analyst is informed about the beginning of the investigations about the incident
- *Incident analyst- C,I:* the incident analyst is consulted in order to understand his/her availability and eventually informed about its assignment to the incident

- *Incident resolution team - C,I:* the incident resolution team is consulted in order to understand the availability of its members and eventually informed about its assignment to the incident

4.2.2 Ticket data retrieval

- *Incident manager - I:* the incident manager is informed about the beginning of the incident analysis
- *Service desk analyst - C,I:* the service desk analyst is consulted by the incident analyst for eventual further explanations about the ticket and is informed about the beginning of the incident analysis
- *Incident analyst- A,R,I:* the incident analyst is accountable for retrieving all the relevant data included in the ticket and is informed about eventual updates applied on it
- *Incident resolution team - C,I:* the incident resolution team is consulted by the incident analyst in order to understand whether further information are required to resolve the incident and is informed about the data present in the ticket

4.2.3 Warranty check

- *External provider - R,C,I:* the external provider is informed about the data of the broken device and is consulted about the status of the warranty on it. He/she is also responsible for communicating correct information about the status of the warranty
- *Service level manager - A,R,I:* the service level manager is informed about the data of the device/s that need to go under revision and he is accountable for controlling whether the asset has an active warranty or maintenance agreement on it
- *Supplier manager - R,I:* the supplier manager is responsible for interacting with the external provider and he/she is informed about the results of the warranty check on the provider side
- *Incident analyst- R,C,I:* the incident analyst is responsible for communicating the required data to both the supplier manager and the service level manager and is informed about their responses. He/she is consulted by the other cited figures whether more information is needed.
- *Incident resolution team - R,C,I:* the incident resolution team is responsible for conducting a brief analysis on the device, it is consulted to retrieve the information arising from the inspection and is informed about the responses of the service level manager and the supplier manager

4.2.4 Budget check

- *Capacity manager - C,I:* the capacity manager is consulted in order to understand whether the budget allocated to the warehouse is sufficient in order to provide a backup monitor to the end user and in the meantime purchase a new backup monitor
- *Chief Financial Officer - C,I:* the CFO is consulted about the decisions taken by the management and is informed about any critical issue reported by the IT Financial Manager
- *IT Financial manager - A,R,I:* the IT financial manager is accountable for checking the warehouse budget and is informed about any critical issue related to it by the capacity manager

4.2.5 Permission to instantiate more budget whether not sufficient

- *Capacity manager - C,I:* the capacity manager is informed about the budget modifications on his/her department of administration and is consulted about the current status of the warehouse
- *Chief Financial Officer - A,R,I:* the CFO is accountable and responsible for taking any decision about the modification of the budget for the capacity management and is informed by the IT Financial manager about the motivations and needs to do so
- *IT Financial manager - C,I:* the IT financial manager is consulted by the CFO to understand whether it is necessary and possible to instantiate more budget than the established

4.2.6 Warning creation

- *Capacity manager - C,I:* the capacity manager is consulted to retrieve all the data concerning the warning situation and he/she is informed about the warning creation (that might compromise the management of internal hardware backup)
- *Chief Financial Officer - A,R,I:* the CFO is accountable and responsible for signalling a warning situation to the administrative board (whether there is no possibility to instantiate budget for the capacity management) and he/she is informed by the capacity and the IT financial managers about the critical issues that led to the warning creation
- *Incident manager - I:* the incident manager is informed about the warning creation (that might compromise the possibility to resolve the incident)
- *IT Financial manager - C,I:* the IT financial manager is consulted by the CFO to understand the critical issues that led to the warning creation

- *Service desk manager - I:* the service desk manager is informed about the warning creation (that might compromise the possibility to resolve the incident)
- *Service level manager - I:* the service level manager is informed about the warning creation (that might translate into an OLA breach)
- *Service owner - I:* the service level manager is informed about the warning creation (that might translate into an UC breach)
- *Supplier manager - I:* the supplier manager is informed about the warning creation to understand whether any process with the external provider may be affected by the issues related to the warning
- *Service desk analyst - I:* the service desk analyst is informed about the warning creation (that might compromise the possibility to resolve the incident)
- *Incident analyst - I:* the incident analyst is informed about the warning creation (that might compromise the possibility to resolve the incident)
- *Incident resolution team - I:* the incident resolution team is informed about the warning creation (that might compromise the possibility to resolve the incident)
- *Capacity team - I:* the incident resolution team is informed about the warning creation (that might compromise the management of internal hardware backup)

4.2.7 Proper form request management

- *Capacity manager - C,I:* the capacity manager is consulted about the number of items that need to be purchased or the information about the device that needs to go under repair and is informed about the submission of the form
- *External provider - C:* the external provider is consulted in order to reply to any possible doubt during the form submission
- *Supplier manager - A,R,I:* the supplier manager is accountable and responsible for submitting the proper form to the external provider and is informed about the data that are required to fulfill the form
- *Capacity team - C,I:* the capacity team is consulted about the data that are needed to fulfill the form and is informed about its submission

4.2.8 UC breach management

- *Business relationship manager - R,C,I:* the business relationship manager is responsible for conducting inspections about the customer satisfaction after the UC breach, he/she is consulted about the results of the investigation and is informed about the UC breach
- *Capacity manager - I:* the capacity manager is informed about the breach, especially whether this requires the provisioning of a monitor from the warehouse
- *Chief financial officer - C,I:* the CFO is informed about the UC breach and is consulted in order to understand whether to issue a fine or not (maybe the provider is a strategic link for the company)
- *End user - I:* the end user is informed about the consequences that the UC breach has on the incident resolution
- *External provider - R,I:* the external provider is informed about the breach and is responsible for minimizing the damage and the negative outcomes deriving from the breach
- *Incident manager - C,I:* the incident manager is informed about the breach and is consulted in order to retrieve more details about it
- *IT financial manager - C,I:* the IT financial manager is informed about the UC breach and is consulted in order to understand eventual motivations that can lead to a fine issuing against the external provider
- *Service level manager - A,R,I:* the service level manager is accountable and responsible for logging the UC breach and is informed about the specifications of the breach and eventual fine emissions
- *Supplier manager - R,C,I:* the supplier manager is informed about the breach and is responsible for interacting with the external provider. He/she is consulted by the service level manager to understand the causes that led to the breach from the provider side
- *Service desk analyst - C,I:* the service desk analyst is informed about the breach and is consulted by the service level manager to understand which ticket/s is/are involved in the breach
- *Incident analyst - C,I:* the incident analyst is informed about the breach and is consulted to understand which consequences it has on the incident resolution
- *Incident resolution team - C,I:* the incident resolution team is informed about the breach and is consulted by the incident manager to understand the consequences it has on the incident resolution

4.2.9 Fine management

- *Capacity manager - C:* the capacity manager is consulted to understand whether the external provider finally delivered the required monitors
- *CFO - C,I:* the CFO is informed about the status of the fine payment and is consulted to understand whether to emit the fine or not
- *External provider - R,C,I:* the external provider is responsible for paying the fine and for resolving the breach as soon as possible. It is consulted by the supplier manager to understand its needs and is informed about the fine emission
- *IT financial manager - A,R,I:* the IT financial manager is accountable and responsible for emitting the fine on the behalf of the company and he/she is informed about the status of the fine payment and the breach resolution by the supplier manager
- *Service level manager - C:* the service level manager is consulted about the amount of the fine
- *Supplier manager - C,I:* the supplier manager is informed about the fine emission and is consulted about the service level manager to understand the necessities of the external provider

4.2.10 Backup hardware provisioning

- *Capacity manager - A,R,C:* the capacity manager is accountable for accomplishing a proper backup provisioning to the end user and is consulted about the service desk analyst to understand how long will it take to complete the related operations
- *End user - I:* the end user is informed about the availability of the monitor replacement
- *External provider - R,C:* the external provider is responsible for delivering the needed hardware according to the UC and for repairing the damaged one whether this is covered by a warranty, he/she is consulted about any necessity related to the hardware that was purchased by the warehouse
- *Supplier manager - C,I:* the capacity team is consulted about the data that are needed to fulfill the form and is informed about its submission
- *Service desk analyst - R,I:* the service desk analyst is informed about the ongoing activities for the provisioning of the backup hardware and is responsible for informing the end user
- *Capacity team - R:* the capacity team is responsible for the warehouse management and for the control of the availability of backup devices as required by the end user

4.2.11 Hardware installation

- *End user - I:* the end user is informed about the new hardware installation
- *External provider - C:* the external provider is consulted in case of need for assistance during the hardware installation
- *Service desk analyst - I:* the service desk analyst is informed about the new hardware installation (ticket closure trigger)
- *Incident analyst - I:* the incident analyst is informed about the hardware installation (incident closure trigger)
- *Incident resolution team - I:* the incident resolution team is informed about the hardware installation (incident closure trigger)
- *IT technician - A,R:* the IT technician is accountable and responsible for the installation of the new monitor

4.2.12 Hardware added to the backup stock

- *Capacity manager - A,R:* the capacity manager is accountable for the proper registration of the new hardware delivered by the external provider
- *Supplier manager - I:* the supplier manager is informed about the arrival of the new hardware delivered by the external provider
- *Capacity team - R:* the capacity team is responsible for the management of the catalog of the hardware backups in the warehouse

4.2.13 Damaged hardware retrieval

- *End user:* the end user is informed about the damaged hardware retrieval
- *External provider - C:* the external provider is consulted in case there is need for assistance on the hardware removal
- *Incident analyst - I:* the incident analyst is informed about the damaged hardware retrieval in order to process its later stages of the life cycle (repair or disposal)
- *IT technician - A,R:* the IT technician is accountable and responsible for the removal of the damaged hardware

4.2.14 Damaged hardware disposal

- *Capacity manager - I:* the capacity manager is informed about the monitor disposal (it should not be longer on the asset catalog)
- *External provider - C:* the external provider is consulted about the proper ways to dispose of the broken monitor (if no warranty is pending on it)

- *Service level manager - I:* the service level manager is informed about the beginning of of the operations needed to dispose of monitor
- *Incident analyst - C,I:* the incident analyst is informed about the beginning of the operations needed to dispose of the monitor and is consulted for further information about its disposal
- *Incident resolution team: A,R,I:* the incident resolution team is accountable and responsible for the monitor disposal and is informed about the instructions to be followed for the monitor disposal
- *Capacity team - R,I:* the capacity team is informed about the monitor disposal and is responsible for removing it from the asset catalog

4.2.15 Damaged hardware dispatch (warranty case)

- *Capacity manager - A,R,I:* the capacity manager is informed about the status of the warranty and is accountable for the hardware dispatch to the external provider warehouse
- *External provider - R,C:* the external provider is consulted about the status of the warranty and is responsible for communicating eventual incorrect procedures during the hardware dispatch
- *Service level manager - I:* the service level manager is informed about the beginning of the operations needed to dispatch the broken monitor (and for its replacement)
- *Supplier manager - R,C,I:* the supplier manager is responsible for the interactions with the external provider during the monitor dispatch scheduling and is consulted by the capacity manager, which wants to know the address and the modalities for the hardware dispatch to the external provider warehouse. At last, he/she is informed about the successful delivery of the monitor and any non-compliance with the warranty clauses
- *Service desk analyst: I:* the service desk analyst is informed about the status of the dispatch and the monitor repairing/non-compliance with the warranty (in order to update the ticket)
- *Incident analyst - I:* the incident analyst is informed about the status of the monitor (in order to understand the actual state of the incident after the hardware removal)
- *Capacity team - R,C,I:* the capacity team is responsible for the monitor dispatch (with the related documentation) and is consulted about the status of the dispatch itself. Furthermore, the hardware asset catalog needs to be updated according to the final state of the monitor warranty management. It is informed about the successful delivery or any non-compliance with the warranty

4.2.16 Customer satisfaction questionnaire

- *Business relationship manager - A,R,I:* the business relationship manager is accountable and responsible for interviewing the customer and collecting feedback about the whole incident management. He/she is informed by the service owner or the service level manager about any update of the incident management process related to the customer satisfaction analysis
- *End user - R:* the end user is responsible for providing relatable answers to the business relationship manager
- *Service level manager - I:* the service level manager is informed about the results of the interview to understand whether it is necessary to operate some modifications to the incident management flow (on the aspects that require the external provider interaction)
- *Service request manager - I:* the service request manager is informed about all the possible requests or insights provided by the end users during the interviews
- *Service owner - I:* the service owner is informed about the results of the interview to understand whether it is necessary to operate some modifications to the incident management flow (on the internal departments management)

4.2.17 OLA breach management

- *Capacity manager - C:* the capacity manager is consulted about the availability of backup resources in order to understand whether the current situation is compliant with the OLA
- *Chief Financial Officer - I:* the CFO is informed about the current situation and eventual OLA breaches
- *End user - I:* the end user is informed about the OLA breach in order to let him/her know that the incident resolution will require more time
- *Incident manager - C,I:* the incident manager is informed about the OLA breach and the impact that it can have on the incident resolution and is consulted to retrieve more information about the incident
- *Service owner - A,R,C,I:* the service owner is accountable and responsible for logging the OLA breach and is consulted by the CFO to understand whether the issue came from the absence of the budget. He/she is informed about the details of the breach by the various entities involved in the corresponding process
- *Service desk analyst - R,I:* the service desk analyst is informed about the OLA breach and is responsible for reporting it to the end user

- *Incident analyst - C:* the incident analyst is consulted by the service owner to retrieve more information about the causes of the breach
- *Incident resolution team - C:* the incident resolution team is consulted by the service owner to retrieve more information about the causes of the breach
- *Capacity team - C:* the capacity team is consulted by the service owner to retrieve more information about the causes of the breach

4.3 Backup quality control assessment

4.3.1 Warehouse budget check

- *Capacity manager - C,I:* the capacity manager is consulted about the conformity of the budget allocated for the warehouse, especially regarding the amount of backup devices available (and their conformity with the OLA) and is informed about any variation of budget
- *Chief Financial Officer - C,I:* the CFO is consulted by the IT Financial manager to understand whether the situation of the company may require a budget revision and is informed about any critical situation going on in the warehouse due to budget lack
- *IT financial manager - A,R,C,I:* the IT financial manager is accountable and responsible for conducting inspections and conformity checks on the budget allocated for the warehouse and is consulted by the CFO to understand the status of the warehouse on the financial aspect

4.3.2 Permission to instantiate more budget whether not sufficient - Warehouse side

- *Capacity manager - I:* the capacity manager is informed by the IT financial manager about any update on the budget for the warehouse
- *Chief Financial Officer - A,R:* the CFO is accountable and responsible for any update permission on the warehouse budget
- *IT financial manager - C,I:* the IT financial manager is consulted by the CFO to understand the status of the warehouse on the financial aspect after the budget update and is informed by the capacity manager for eventual issues risen after the updates
- *Service owner - I:* the service owner is informed about the budget updates

4.3.3 Warning creation - warehouse side

- *Capacity manager - C,I:* the capacity manager is consulted about the issues that led to the warning creation and is informed about the impact that this has on the warehouse management

- *Chief Financial Officer - A,R,I:* the CFO is accountable and responsible for signaling a warning situation to the administrative board (whether there is no possibility to instantiate budget for the warehouse backup stock management) and he/she is informed by the capacity and the IT financial managers about the critical issues that led to the warning creation
- *IT financial manager - C,I:* the IT financial manager is consulted by the CFO to understand the critical issues that led to the warning creation
- *Service owner - I:* the service owner is informed about the warning creation
- *Capacity team - I:* the capacity team is informed about the warning creation for what concerns the warehouse backup stock management

4.3.4 Backup quality control check

- *Capacity manager - A,R,C,I:* the capacity manager is accountable and responsible for managing the teams assigned to the quality control check, he/she is consulted by the capacity team to understand which pieces need to go under revision and when and he/she is informed about the results of the evaluation
- *Service owner - C,I:* the service owner is consulted about the OLA KPIs that report the expected quality of the backup and is informed about the results of the evaluation
- *Capacity team - R:* the capacity team is responsible for conducting the review of the backup stock

4.3.5 Backup catalog management

- *Capacity manager - A,R,I:* the capacity manager is accountable and responsible for maintaining an updated catalog of all the backup stock available in the warehouse and is informed by the capacity team about the catalog updates
- *Service owner - C,I:* the service owner is consulted about the OLA KPIs that report the expected amount of backup pieces and is informed about the results of the evaluation
- *Capacity team - R:* the capacity team is responsible for conducting the review of the backup stock, updating the catalog once a piece is discarded/a new piece arrives

4.3.6 Inadequate backup disposal

- *Capacity manager - A,R,I:* the capacity manager is accountable and responsible for making sure that all the backup hardware that is not compliant with the OLA KPIs gets properly disposed and replaced. He/She is informed about the effective disposal of some hardware stock

- *External provider - C:* the external provider can be consulted in order to understand how to properly manage the disposal of some devices
- *IT financial manager - I:* the IT financial manager is periodically informed about the disposal of non compliant devices and the cost of their replacements
- *Service owner - C,I:* the service owner is consulted about the OLA KPIs that report the expected amount of backup pieces and is informed about the update of the catalog
- *Capacity team - R:* the capacity team is responsible for making sure that every piece that is not compliant with the OLA KPIs gets disposed correctly

5 Rollout Plan

The refactoring of the processes that is reported at section 3.3 necessarily carries out the necessity of establishing a proper road-map which allows to establish a proper sequential path among the various tasks that will be needed.
First of all, the rollout plan will necessarily require the establishment of the goals and objectives for which it is carried out. Usually this activity is carried out by the administrative board of the company, which is accountable and responsible for the mission and the objective setup according to the core values that build up the company. These intents need to be properly set and written down on the vision statement. These objectives need to be identifiable, measurable and plausible (according to the current situation of the company).
Once the vision statement has been properly checked (or updated), the objectives that have been declared need to be properly assessed during their development and completion phase. Consequently, they need to be evaluable through the establishment and assessment (or eventual update if already present) of KPIs (Key Performance Indicators) reported in the OLA and in the UC. This step needs to involve the various managers of the departments, the service level manager, the service owner and also the external provider to the extent of establishing plausible but efficient metrics to ensure that the service performance is compliant with the expected level of quality, both for what concerns internal and external efficiency and effectiveness. The KPIs also need to take into consideration the budget that is allocated for that specific department, so the cooperation with the financial department is necessary to pursue this scope.
Specifically for this case, which is a normal change, a change advisory board needs to be formed in order to review and authorize the changes by evaluating them through the 7R of change enablement. Then, the change manager needs to provide a suitable change schedule and a projected service outages (if any service interruption is required to implement the changes.
The main changes that should be implemented in this specific scenario should guarantee:

- the establishment of an internal process to manage more efficiently the provisioning of backup devices to the end users
- the improvement of the communications between the service desk and the end users
- the improvement of the communications between the company and the external provider
- the improvement of the delivery time of new hardware
- a major awareness of the various stakeholders regarding the activities to which their intervention is needed

The section 3.3 explains a possible proposal plan for the requirements described above. In parallel, the various stakeholders and employees need to be warned

about the changes and properly trained through dedicated courses and assisted during the various stages of the processes.

6 Conclusions

The evolutionary plan and the rollout plan provided in this document are adequate to resolve every critical error listed in section 2.2.
The next list shows how every error listed in section 2.2 has been fixed:

- Lack of hardware request form: in the sub-process called "Resolution and recovery for hardware malfunction tickets sub-process", explained in section 3.5, the support group has to fill two different types of forms to communicate in a standard, precise way with the external provider.
- Lack of automated response system with External Provider: one of the main benefits of hardware request forms is the ability to receive a fast and automated response from the external provider.
- Lack of same day hardware solution: the in-house backup warehouse is a fit solution to tackle the urgent incidents and resolve them in matters of hours without relying on external services.
- Lack of financial penalty in case of breach in SLA: in the sub-processes called "Supplier answer analysis and response" and "Resolution and recovery for hardware malfunction tickets sub-process" there are repetitive checks to ensure that no SLA breaches occur or, when they do occur, the external service is accordingly fined.
- Total dependence on external services: the existence of the backup warehouse is a robust solution to avoid the total dependence on the hardware external provider. If the external provider fails to resolve the incident as defined in the service level agreement, the end users productivity can be ensured by the usage of backup hardware units.