Problem Management Process

Document name	Process_Design_Document_PB_V0.1.docx
Version	0.1
Status	☒ In progress ☐ Approved ☐ Validated
Update date	2025/05/02
Owner	Syensqo - Infrastructure
Level of confidentiality	☐Public ☒Internal ☐Limited ☐Confidential

Document Control

CHANGE HISTORY:

AUTHOR(s)	VERSION	DATE	CHANGES
Coralie CHAUDIER	V0.1	2025/05/02	Document creation

APPROVAL

ROLE	NAME	DATE
Foundation Office Lead	Li-Kang KUANG	2025/07/07

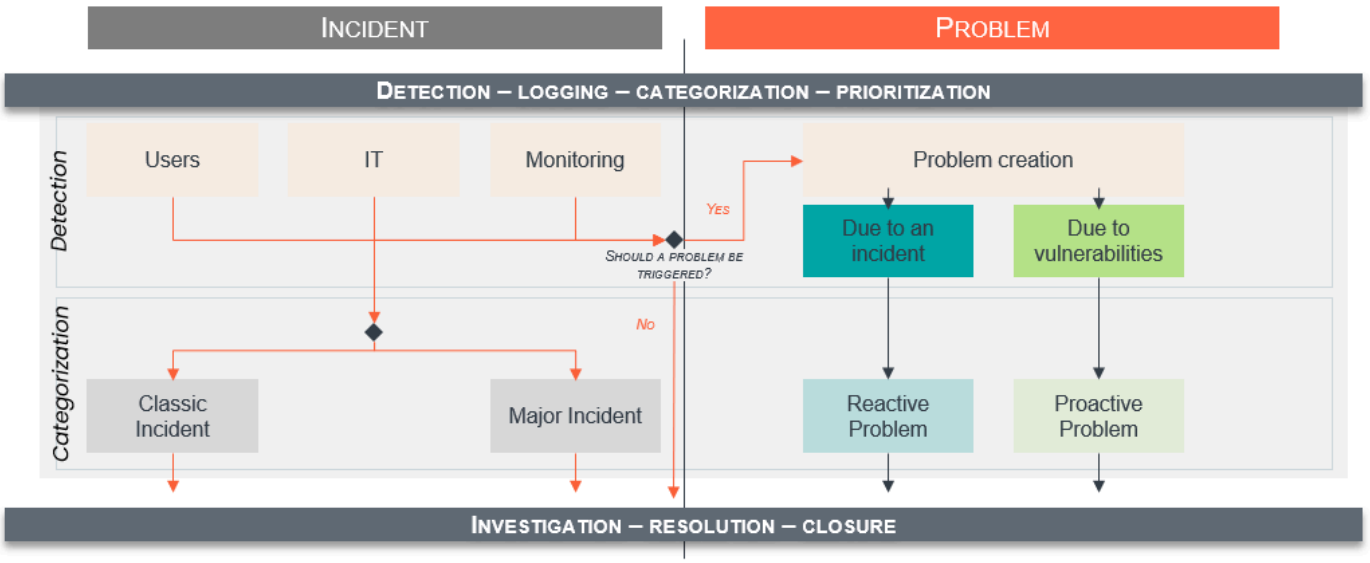
Table of Contents

1. Introduction

1.1. Main definition

Incident and Problem management are similar since they have almost the same stages: logging, categorization, prioritization, investigation, resolution closure. Problems are related to incidents, but they should be distinguished as they are managed in different ways:

- Incidents have an impact on users or business processes and must be resolved so that normal business activity can take place.
- Problems are the **cause or potential causes** of one or more incidents. They require **investigation and analysis to identify the root causes** with the objective of implementing a permanent resolution. This process may involve validating existing workarounds or recommending more effective long-term solutions. This reduces the number and impact of future incidents. Only designated persons can validate a ticket problem creation



Links and differences between incident and problem – Problem Management

A temporary way to restore service failures to a usable level is called a **workaround**. It is a solution that reduces/eliminates the impact of an incident/problem for which a full resolution is not yet available. Some of them reduce the likelihood of incidents

The **root cause analysis (RCA)** is an approach for identifying the causes of problems and responding to them. During this phase the workarounds are reviewed and validated to determine whether they can serve as a permanent solution or if a more robust and sustainable fix is required.

A **known error** is a problem that has been analysed, documented, with generally a workaround but for which a permanent resolution has not yet been implemented. They are created and managed throughout their lifecycle by problem management and are used to categorize and evaluate incidents. All known errors are recorded in the known error database.

Example:
Incident: *An application malfunctions and stops without warning.*
Problem: *This malfunction appears repeatedly creating recurring incidents, more investigations are required.*
Root Cause: *This appears because of an OS security update.*
Workaround: *A temporary solution can be to roll back (if possible) or Temporarily disable or bypass the specific security feature introduced by the OS update that is causing the application to crash, only for affected systems or users, while maintaining overall system security. Otherwise, it can have no workaround, and the teams will have this issue until a new app migration. All those solutions must be documented.*
Known error: *The root is identified and the known error is created and documented (Id, problem description, root cause description, impact, workaround if available, status, assignation)*

1.2. Reactive versus proactive problem

Problem management deals with two kinds of problems:

- **Reactive problem management**: is concerned with solving problems in response to one or more incidents. Problem management activities are performed in reaction to specific incident situations. (more detailed paragraph 2.1)
  Major incidents, recurring incidents will always trigger a problem. Other incidents may also trigger problems if they need further investigation (this will be dealt with on a case-by-case basis).

Example:
Description of a ***reactive problem:*** *Users in multiple departments are unable to send or receive emails via Gmail.*
This problem has been raised because of a high number of incidents reported to HelpDesk and a major incident has been raised.

- **Proactive problem management** is concerned with identifying and solving problems and known errors before further incidents related to them can occur (more detailed paragraph 2.1)

Example:

*Description of a **proactive problem:** Email server logs show increasing latency in sending emails through Gmail SMTP servers*

This problem has been raised because of latency trend analysis and early alert on external mail delivery performance

1.3. Objectives, challenges & benefits

The purpose of the problem management practice is to **reduce the likelihood** and **impact of incidents** by identifying **actual and potential** causes of incidents and managing workarounds and known errors (with sometimes a removal).

This process aims to manage the lifecycle of all problems from first identification through further investigation, documentation and eventual removal.

The implementation of the problem management process allows the IT department to:

- Reduce or eliminate recurring incidents by identifying and eliminating the root causes of incidents
- Improve the quality of IT services by preventing service disruptions
- Avoid costly incident which will save money, time and pain
- Increase team productivity with a quicker resolution time thanks to:
    - less incident/problem ticket to focus on higher value-added task
    - better teamwork organization and experience
- Improve decision-making with problems analysis (trends, frequency, impact) that enable Syensqo to anticipate risks and improve IT strategies
- Maintain information about problems and appropriate workarounds to reduce the number and impact of incidents over time
- Conduct regular problem reviews to determine what could be improved in the future
- Increase Customer satisfaction: better problem management leads to fewer incidents, and happier customers. Alternatively, customer patience wears thin when they notice the same incident happening multiple times. Decreasing the occurrence of repeat incidents builds customer trust and improves users' perception of IT services.

1.4. Actors

The Main actors (with standard designation and Syensqo designation) in the problem management process are:

1. **Problem requestor**

He is an IT resource that identifies problems and requests the creation of a problem ticket

2. **Problem Manager** (from the Global IT Support : computa center specialist - with a specific role regarding problem)

He is responsible for creating or approving the problem ticket and checking that all information is available. He assesses, prioritizes the problem and assigns it to the relevant team. The Problem Manager assumes full responsibility for managing the problem throughout its entire lifecycle, from investigation to resolution and closure.

3. **Technical Expert**

He is focused on resolving technical & functional issues, organized into several levels. Is responsible for investigating assigned problems, identifying root cause, proposing solutions and workaround and implementing corrective actions

ITIL role: Support L2/L3

4. **Delivery Manager (DM)**

He is responsible for centralization of information (to improve the knowledge base). He is the business representative, involved in assessing the risks and impacts of issues on business activities and in helping to prioritize corrective actions to undertake.

ITIL role: Problem Coordinator

5. **Service Owner (SO)**

He coordinates the technical resolution of the problem and ensures communication towards their managers and the other teams involved.

ITIL role: Technical Coordinator

6. **Delivery Lead**

He is accountable for the overall design, performance and continual improvement of the Problem Management process. He has the ability to ensure the process is rolled out and used by all stakeholders.

ITIL role: Problem Process Owner

2. Process description

2.1. Process trigger, inputs, outputs

1. Triggers - *What initiates the process ?*

The creation of problems highlights the need to restore or improve the quality of a service. They are triggered by several inputs, depending on whether they are proactive or reactive.

With **reactive problem management**, problems can be triggered in relation to:

- **Recurring incidents**: multiple similar incidents over time often signal an underlying problem that requires root cause analysis
- **Major incidents**: high-impact incidents trigger post-incident reviews, which lead to problem record creation to prevent recurrence
- **Other incidents** when:
    - the cause of an incident was not removed and may cause other incidents
    - a high percentage of similar incidents are resolved after target resolution time

With **proactive problem management**, problem records can be triggered in relation to:

- **Patterns and proactive trends** identified in incidents when reviewing historical incidents records and all incidents' data (a high percentage of similar incidents are resolved after target resolution time, etc.)
- **Monitoring alerts / technical audits**: system or service monitoring may detect anomalies or degraded performance not yet reported by users
- **Supplier or vendors** through the notification of potential faults in their products or services
- **Developers or designers:** issues in the versions currently deployed to the live environment have been identified during testing but have not been fixed
- **Non Syensqo users** (other organizations) detect issue using the same versions of systems and components

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

A problem ticket logged into ITSM platform (BMC Helix) will formally enter the process, it is the main **input**. It must contain as much information as possible to allow the investigation.

Typical input elements:

- Requester name, contact information, and role.
- Incident linked to the problem (if it is a reactive problem)
- service(s) or application(s) impacted by the issue
- description of the problem (summary, date of the first report, location,
- impact and urgency
- mitigation actions (steps taken to address or contain the issue)

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

The process delivers two main **output**:
The problem record (or postmortem) that contains all the information needed to effectively document and resolve the problem.
Typical output elements:

- problem id (the identifier automatically assigned by the ITSM Tool)
- impact, urgency and the associated priority
- references to related incident (if applicable)
- chronological assignation, actions, status, resolution details and communication (if applicable)
- details of the root cause
- workaround (if applicable)
- user feedback (if possible)
- closure reason

The known error documentation to avoid other teams spending time diagnosing the same problem and to directly provide a workaround when possible.
Typical output elements:

- Known error id
- references to related problem
- problem description and its root cause
- impact
- Workaround
- Status
- Team responsible for the known error
- Result of the monitoring (if applicable)

2.2. Process activities

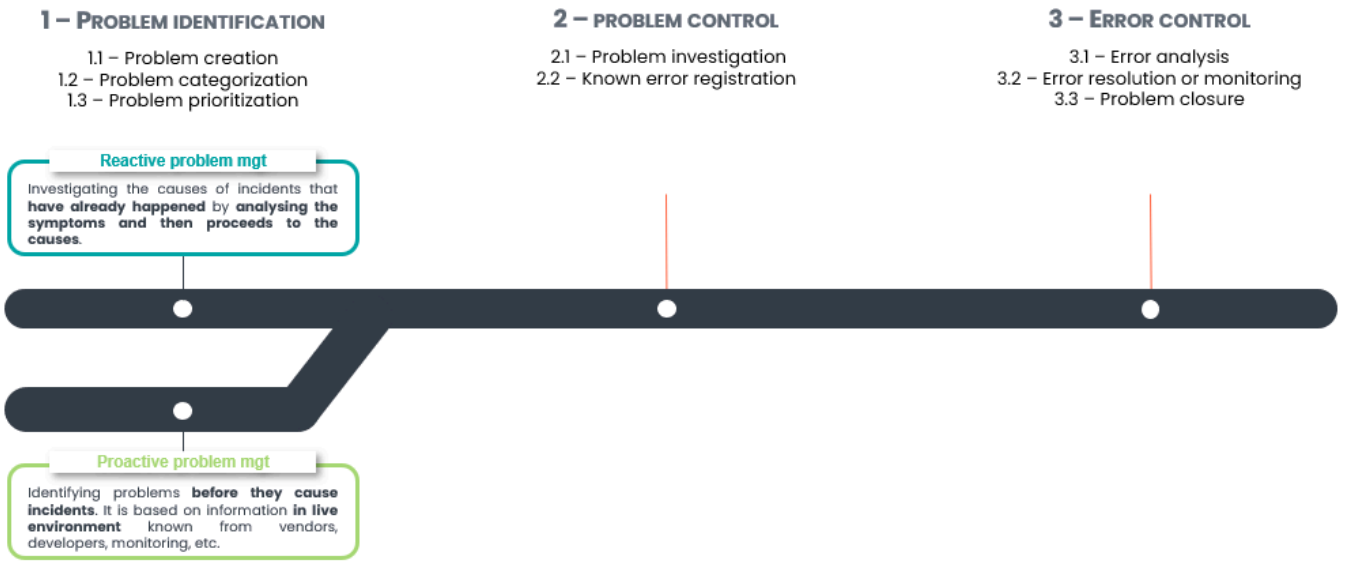
The problem management activities include three distinct stages:

1. **Problem identification**
   - 1.1. Identify all necessary conditions that may require a problem and creation of the ticket in the ITSM Tool (linked to recorded incidents or not)
   - 1.2. categorization and assessment of the problem: evaluation of the risks related to it
   - 1.3. prioritization of the ticket based on the impact and urgency and determine the assignation of the ticket to the relevant team (several team may be concerned)
2. **Problem control**
   - 2.1. Collection and analysis of the related information using problem solving techniques (5 whys, Kepner and Fourie, fault tree analysis). Investigation of the problem to find the root cause
   - 2.2. Registration of the known error when a permanent fix solution is not available. If a permanent solution is found, it should be implemented and the process end without going through the stage 3
3. **Error control**
   - 3.1. Analysis of the known error
   - 3.2. Choice of the mitigation approach to resolve or monitor the known error
   - 3.3. Closure of the problem

Not every problem goes through all three phases. Some can be dismissed at the identification phase (as duplicates). Others may be closed at the problem control stage because their impact has changed during the investigation, they need no further attention or because a permanent fix solution has been found and implemented.

Each phase has its **own timeline**:

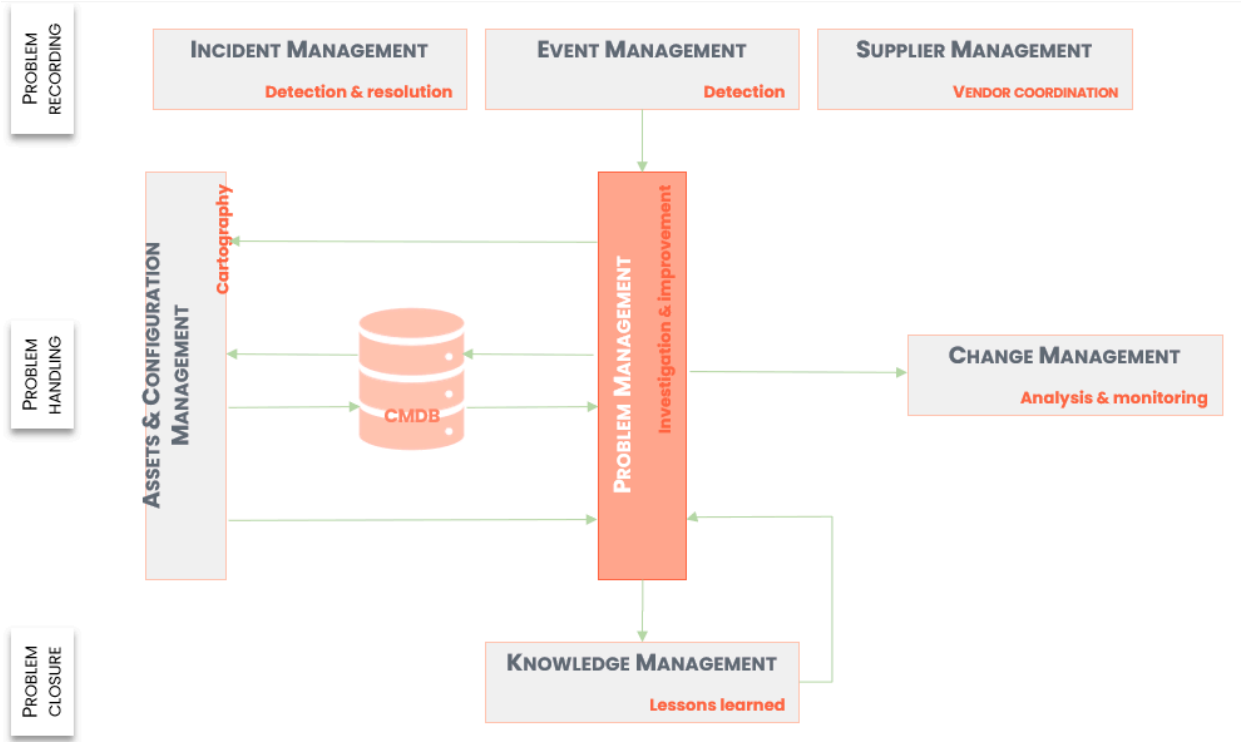
- Problem identification is a relatively quick workflow, although it can be preceded by a long period of data collection and processing.
- In the problem control phase, service providers can influence the speed of investigation by assigning additional resources or by prioritizing the investigation over other tasks. The duration is also influenced by the difficulty of the investigation.
- The timeline of error control timeline can vary significantly. When there is a known problem solution to be implemented, the implementation can be planned with high certainty but still may take a long time. If there is no reasonable way to resolve the problem, it may remain open for a long time, especially if there are effective ways to mitigate its impact. In this case the problem remains open and undergoes periodic reviews to confirm or change the way the error is managed.



Macro activities description – Problem Management

2.3. Link with other ITSM processes.

The problem Management process is closely connected with the following ITSM practices:



Main interdependencies – Problem Management

- **Event Management:** events and alerts can trigger proactive problem investigation before users are impacted, supporting early root cause identification.

- **Incident Management:** problem Management analyzes recurring or major incidents to identify root causes. In return, known errors and workarounds from Problem Management support faster incident resolution.

- **Supplier Management:** Problem Management may involve third-party vendors when the root cause of a problem lies within external services or products. A strong link ensures proper escalation, contract alignment (e.g. under an Underpinning Contract), and tracking of supplier-related issues.

- **Change Management:** solutions to problems often require changes to the IT environment. Problem Management submits change requests to implement permanent fixes once root causes are identified.

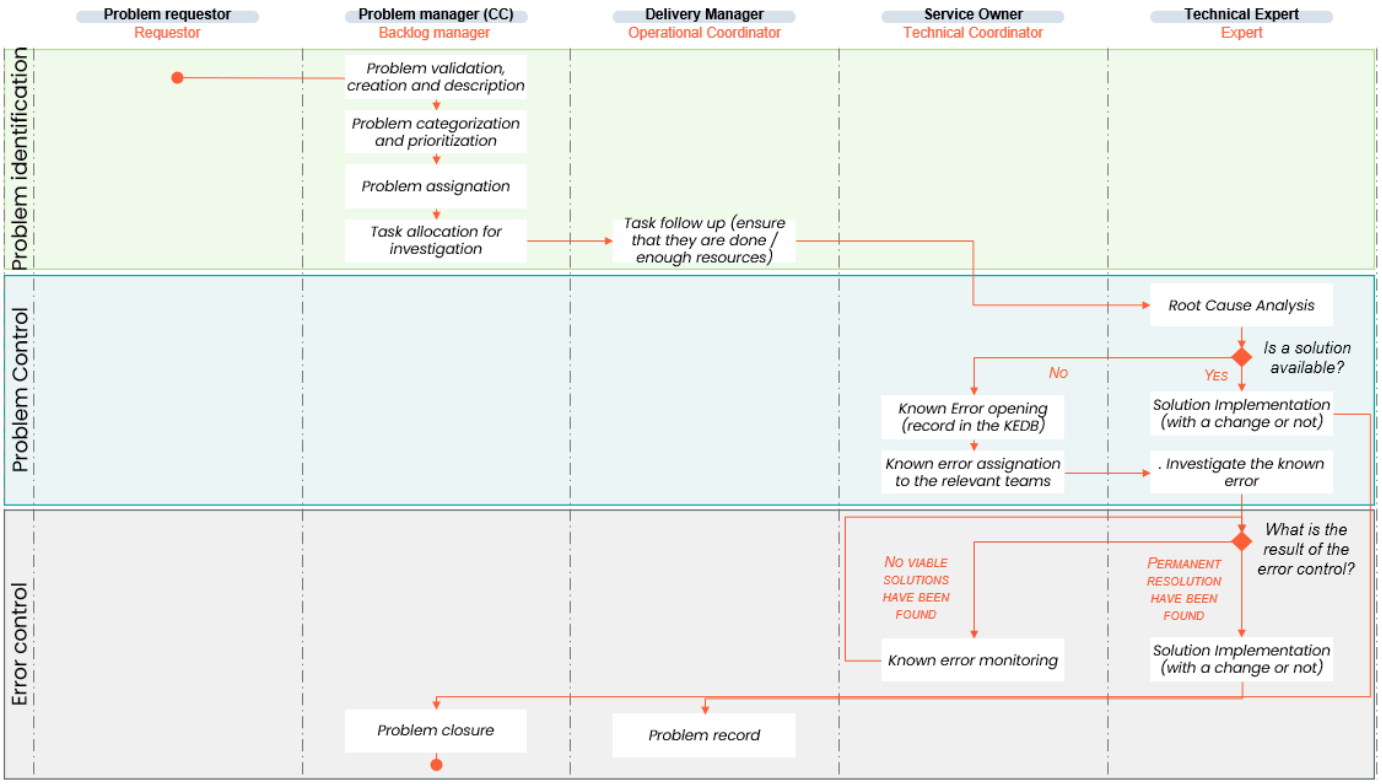
- **Asset & Configuration Management (CMDB):** Accurate configuration data is essential for effective root cause analysis. Problem Management relies on the CMDB to understand relationships between components and identify potential points of failure.

- **Knowledge Management:** Problem Management contributes to the knowledge base by documenting known errors and their workarounds, supporting both incident resolution and continuous learning.

Other processes are linked with problem management to a lesser extent such as request management, service level management, risk management, continuous Service Improvement management, etc.

3. Process Workflow

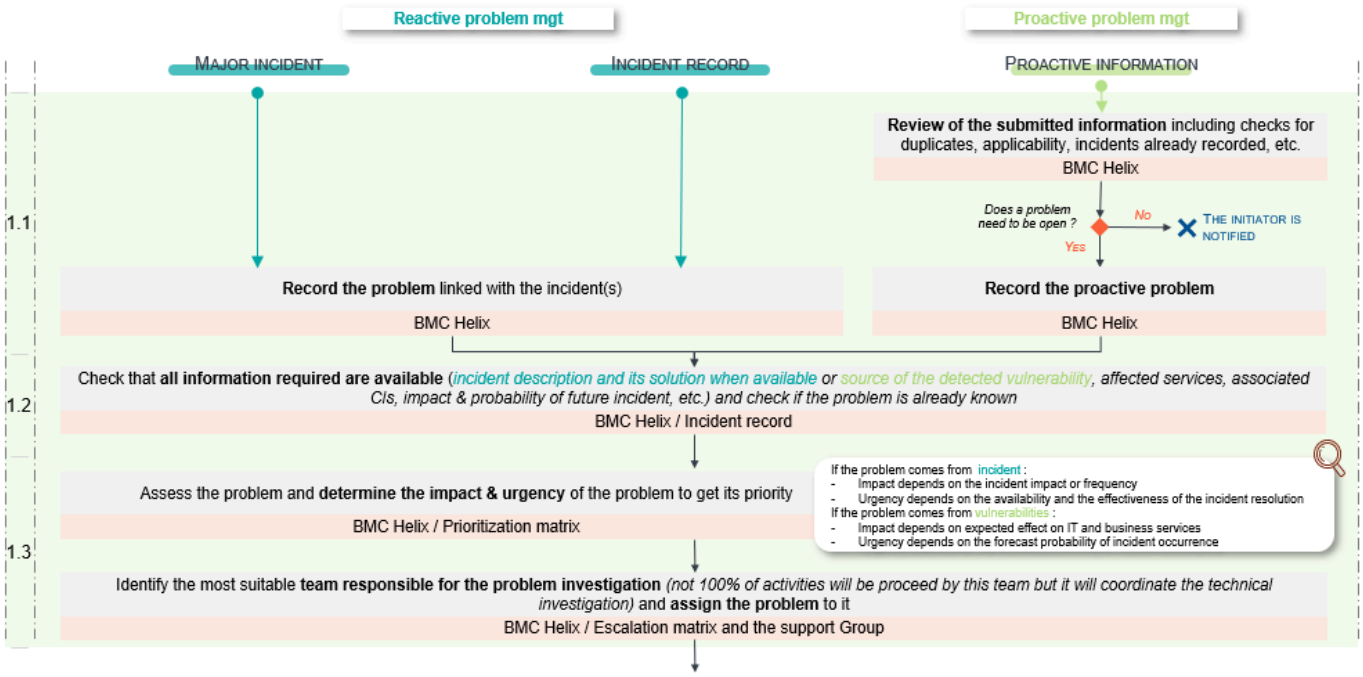
The flowchart below provides a global view of all activities handled during problem management.



Global flowchart – Problem Management

The flowcharts in the next chapters provide a detailed view of how the process works through a **detailed description of the activities** (grey part) and **means used** (pink part)

3.1. Problem identification – Stage 1



Detailed activities description – Stage 1 – Problem Management

Potential problems can be identified by **various players in the IT Department**, in different activities, corresponding to the processes for managing operations and availability, as well as incident management. It can also be identified by suppliers or other organizations when we speak about proactive problems

When a problem is **detected and saved as a draft**, the problem manager validates its creation and checks if all information required is available *(1.1 stage)*. Each problem is detailed in the ITSM tool, which describes, among other things (when available):

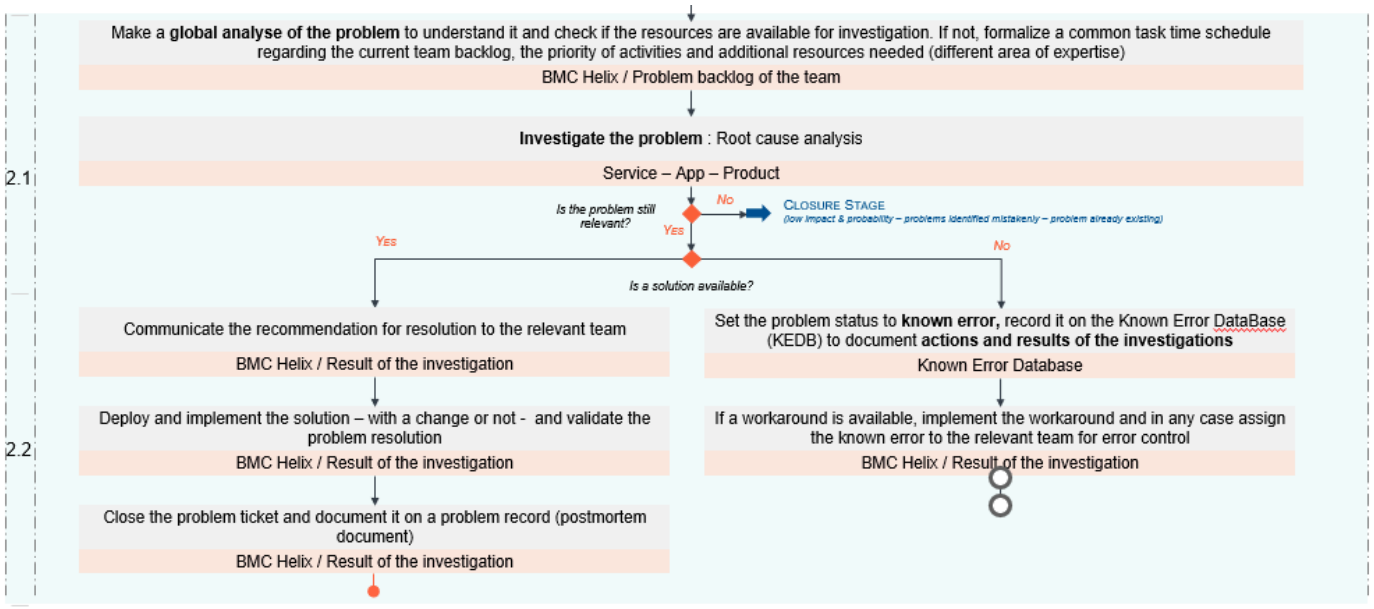
- Symptoms of the problem
- Business impact, criticality
- Related incidents
- Responsibility and players
- Workarounds (when available: reactive problems)

Please note that only the **Problem Manager and the Major Incident Manager** (when it is related to a major Incident) is able to validate a problem ticket creation.

A first level of analysis is carried out directly by the problem manager to identify, via the knowledge base, whether another identical or very similar problem has already been documented and is likely to provide elements of a response (Particularly for proactive problems to identify workarounds) *(1.2 stage)*.

With all the information the problem manager determines the **impact & urgence,** prioritize the problem (using the prioritization matrix, available on the appendices) and **assign** it to the relevant team *(1.3 stage).* A problem with the priority critical (P1) will require a call to align all stakeholders.

3.2. Problem control – Stage 2



Detailed activities description – Stage21 – Problem Management

Further investigations and diagnostics will be carried out by the team responsible for the investigation. The **identification of the necessary skills** will be supported by the delivery manager with the help of service owners.

The **prioritization** of problems will determine the timetable for the different stakeholders involved in the problem investigation.
Problems are mostly managed in project mode, the investment in resources being directly linked to their criticality. The various steps involved in diagnosing the problem, analyzing its causes, developing workarounds and finding a definitive solution are all recorded in the ITSM tool. *(2.1 stage)*

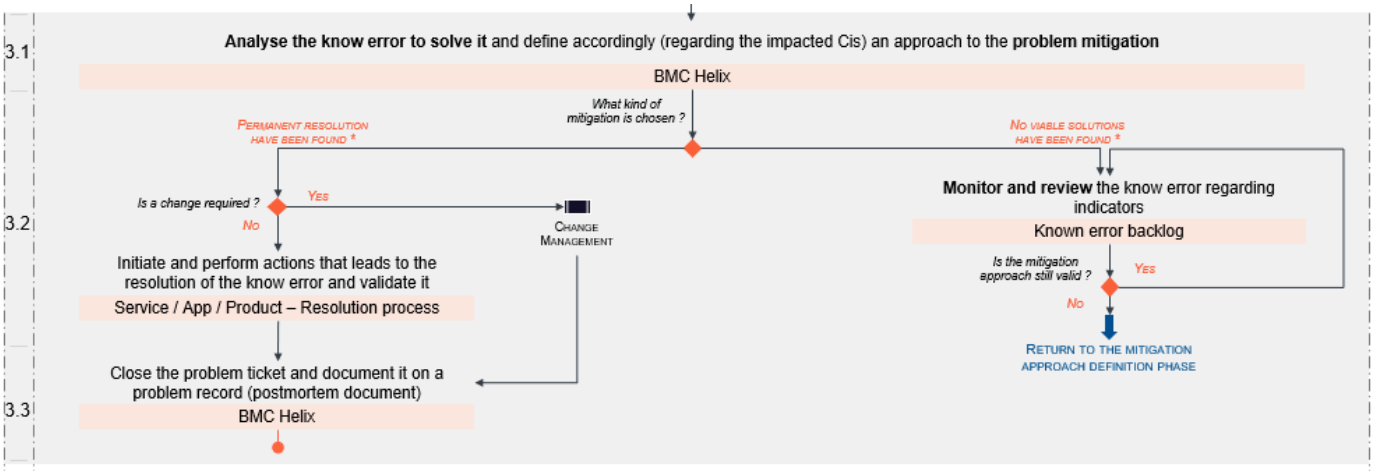
When the root cause of the problem is found, two solutions are possible:

- If a permanent solution is found, it is implemented so that the problem ticket can be closed.
- Or no permanent solution is found, so the problem is considered as a known error and registered in the known error database with all information needed. When a workaround is available, it is implemented. This solution may evolve over time as a more effective or less cumbersome solution is identified (e.g. instead of restarting a server, only an EAR in a JVM

could be restarted).

(2.2 stage)

3.3. Error control – Stage 3



The known error is analyzed by either the same team or assigned to another team if relevant for **investigation** *(3.1 stage)*. Two solutions are possible:

- Either a permanent solution is found and implemented
- Or no viable solution has been found (the costs of problem resolution may be higher than the costs of living with known errors and effective incident management: typical for problems associated with third-party components). The known error is regularly monitored

(3.2 stage)

When a solution is implemented, the problem can be closed in the ITSM tool *(3.3 stage)*

3.4. Necessary rules for a correct implementation of the process

For incident management to be successful, some rules need to be taken into account:

- Key roles of the Problem Management Process should follow and validate mandatory **trainings IT**
- All problems must be **tracked separately from incidents** in the ITSM Group but links can be done and seen on the dashboard space
- A **problem record** must be raised for each Major Incident that occurs.
- The known errors must all be **documented in the known error database**. Every documented workaround should include a clear **definition of the symptoms to which it applies**.
- All problems must be categorized and prioritized within the unique qualification matrix

4. Roles & responsibilities

The RACI matrices below define the roles and responsibilities of the key actors involved in the problem process. It ensures clarity on who is Responsible, Accountable, Consulted, and Informed at each major step of the lifecycle, with strict adherence to the principle of single accountability per activity.

The Incident Management process is led by the actors presented on chapter 1.3:

		Problem requestor	Problem manager (Global IT Support)	Technical Expert	Delivery Manager	Service Owner
1.1	**Problem creation**	C	A, R	I	I	I
1.2	**Problem Categorization**		A, R		I	C
1.3	**Problem prioritization**		A, R			
2.1	**Problem Investigation**		A, I	C	C	R
2.2	**Known Error registration**		I	I	A	R
3.1	**Problem Solution Development**		A, I	C	C	R
3.2	**Monitoring**		A, I	I	C	R
3.3	**Problem Closure**	I	R	I	A	C

Roles & Responsibilities –Problem Management

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

5. Process reporting

5.1. Process Success Factors and their KPIs

To monitor the effectiveness of the Problem Management process and ensure it delivers both operational performance and business satisfaction, **two process success factors (PSFs)** have been identified. Each PSF is supported by a set of specific **Key Performance Indicators (KPIs)** that enable regular measurement, process control, and continuous improvement.

PSF 1 – Identifying and understanding the problems and their impact on services

Effective problem management starts with the ability to detect problems early, to analyze their root cause and to understand errors that can affect business services quality and customer satisfaction. The problem identification contributes to the continual improvement whether it is performed reactively (easier) or proactively

Associated KPIs (Weekly & monthly)**:**

KPI	Description	Calculation mode
Average time to take into account a problem	Time needed for the problem manager to approve a problem (from the request/draft to the assignation)	(Sum of all the time spent from a problem ticket to go through the status "draft" to the status "assign"/Number of problems tickets over the period)
Percentage of problems identified via incidents (major, recurring, others)	Proportion of problem linked with incident → réactive problem	(Sum of problem linked with incident / Number of problems tickets over the period) x 100
Percentage of problems identified via proactive approach	Proportion of proactive problem	(Sum of problem not linked with incident / Number of problems tickets over the period) x 100
Percentage of problems with documented root cause	Proportion of problem with an investigation that leads to a determined root cause	(Sum of problem with a root cause documented/ Number of problems tickets over the period) x 100
Mean Time to Diagnose (MTTD)	Average time to identify root cause	(Sum of all time to diagnose each problem / Total number of diagnosed problem over the period)

It would also be interesting to get when an history is available the reduction in incident recurrence linked to identified problems

PSF 2 – Optimizing problem resolution and mitigation

Once a problem is identified, it is essential to implement timely and effective permanent solutions or mitigating actions (e.g., workarounds). Identification without resolution is less valuable for organization & customers. This minimizes business risk, reduces operational noise, and improves service reliability over time. A balanced approach must be defined for problem mitigation considering the associated costs, risks, and impact on service quality

Associated KPIs (monthly)**:**

KPI	Description	Calculation mode
Percentage of problems resolved with a permanent fixed solution	Proportion of problem completely resolved	(Sum of problem with the status "closed"/ Number of problems tickets over the period) x 100
Mean Time to resolve (MTTR)	Average duration from problem creation to problem resolution	(Sum of all the time to resolve each problem/ Number of problems tickets over the period)
Percentage of problems with a documented known error and workaround	Proportion of known error registered	(Number of known error opened/ Number of problems tickets over the period) x 100
Average ages of problems that remain open in the backlog at any given time	N/A	(Total elapsed time since creation for all open problem tickets/number of open problem tickets over the period)
Number of known errors that remain open – average ages of them	N/A	(Total elapsed time since creation for all open known error/number of open known error over the period)

It would also be interesting to get the number of incident resolved with solution provided by problem investigation

This is an initial list of KPIs, needed for the September Go-Live, they will be completed during the continuous build period according to the business and IT needs

5.2. Risks indicators

Risk scenarios can be defined and the associated indicators monitored to minimize malfunctions.

A lack in **risk assessment** for identified problems related to major incidents and/or a lack in action plan definition and its execution leads to the recurrence of major incidents and impacts on business activities

Risk indicator:

- Percentage of problems older than a month with no calculated risk
- Percentage of problems older than a month with no problem task
- Percentage of problems older than a month without a defined root cause
- Percentage of problems whose resolution due date has been modified

IT department not properly trained leads to **poor problem management** and a lack in weaknesses identification and action plan definition

Risk indicator: Percentage of the IT team department managing problems without being properly trained

This is an initial list risks indicators, they will be completed during depending on the progressive process set-up

6. Governance

Problem Management governance relies on two committee types: operational and continuous improvement. Each has a specific scope, rhythm, and ownership. The following tables outline their purpose, cadence, key participants, and designated animators to ensure clear accountability and structured decision-making.

6.1. Operational Committees

Committee	Objective	Frequence	Animator	Participants	Input (←) /Output (→)
Problem backlog review	• Conduct a peer review of problems backlog and problems escalation	Weekly (30min)	Problem Manager	Problem Manager Delivery manager	← Problem backlog → Problem ticket / action plan
Problem management committee	• Analyse on-going problem • Review the resources capabilities/workload/ backlog • Analyse the steering indicators	Monthly (1h)	Problem Manager	Problem Manager Delivery Manager	→ Monthly KPIs / Problem stock
Major Incident Review (Included in the incident management) [1]	• Carry out feedback regarding what happened during the M.I	After each major incident (1h)	MIM	Problem manager Major Incident Manager Change manager (if needed) DM / SO / Technical Experts involved	← MI record / postmortem → KM articles:

Governance – Problem Management

[1] This committee is not under the problem management scope but the problem manager needs to be involved and informed about the Major Incident.

6.2. Continuous improvement Committees

Committee	Objective	Frequence	Animator	Participants	Input (←) /Output (→)
Review of the problem management process	• Evaluate the overall performance of problem management • Discuss KPIs and suggest improvements.	Quaterly (1h)	Problem Manager	Problem manager Delivery Lead Delivery Managers Major Incident Manager (MIM) & Change manager if needed	→ Overall KPIs / SLAs → Action plan for improvement

Governance – Problem Management

This problem management governance must be completed by committees above through all IT departments to review operational performance of applications and IT services.

7. Tools and deliverables

7.1. The ITSM tool

To ensure consistency, traceability, and efficient collaboration, the Problem Management process relies on one main tool: the ITSM platform (BMC Helix).

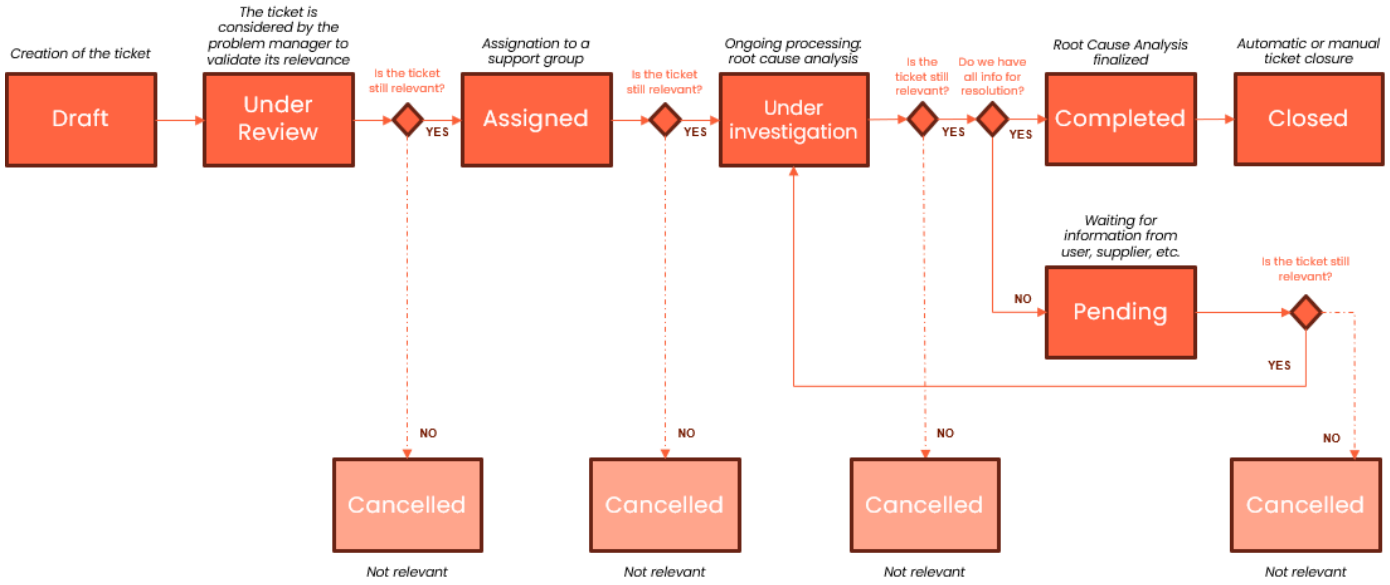
The table below outlines the modules used along with their respective functions in the end-to-end process.

Tool/Module	Description of use in the process
BMC Helix – Problem Module	Submission, categorization, prioritization, assignment, investigation, closure . *The User Guide describes how to use the module.*
BMC Helix – Known Error Module	Submission and follow up of a known error *The User Guide describes how to use the module.*
BMC Helix - Incident Module	Creation of a link between incidents and a ticket problem to help in the investigation
BMC Helix - CMDB	Identification of impacted CIs, support for impact analysis, and problem traceability.
BMC Helix - Knowledge Module	Storage of lessons learned from Problem Record and Known Error Database for cross-domain reuse and continuous improvement.

The problem manager will manage the whole problem backlog within the Syensqo ITSM Tool. It is possible to:

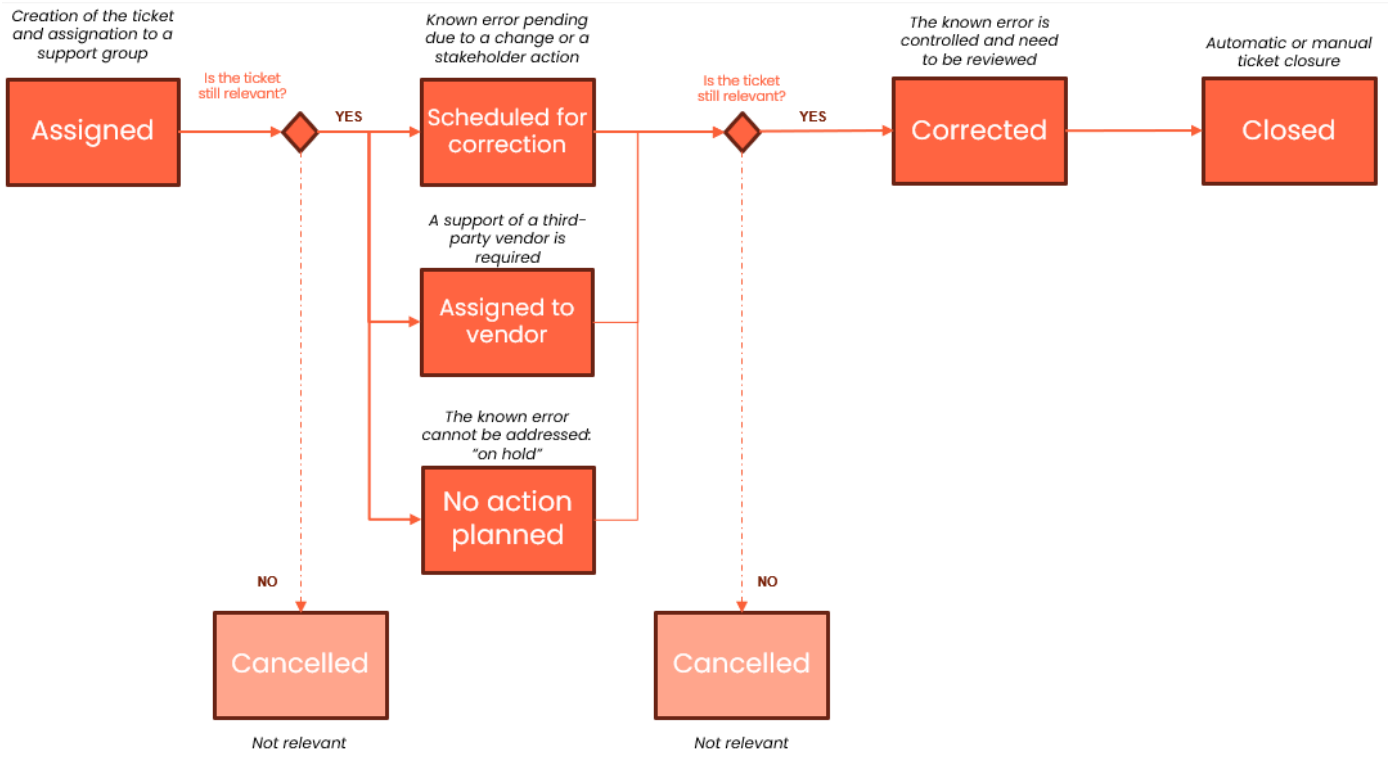
- create a problem from the beginning when an IT agent or monitoring tool suggest a ticket creation
- edit a ticket created through the ITSM Tool (BMC Helix)
- create a known error ticket
- edit a known error ticket

The diagrams below represent the **standard lifecycle of a problem ticket** and of a **known error ticket** managed in the ITSM tool BMC Helix. It illustrates the different statuses a ticket may go through until final closure. This structured workflow ensures traceability, proper validation, and consistent communication throughout the entire process. The User Guide will provide more details.



Problem ticket status lifecycle – Problem Management

Once the ticket status is "completed", the Root Cause Analysis has been performed and either a permanent solution is implemented or a known error is created.



Known error ticket status lifecycle – Problem Management

7.2. Deliverables

The Problem Management practice produces several key deliverables that support effective service restoration, process control, reporting, and continuous improvement:

- **Problem records:** contain all the details related to the problem analysis and its resolution until closure.
- **Known error database:** knowledge base entries documenting symptoms and related problems analyzed or being analyzed, including workarounds when they exist.
- **Risk Acceptance Form:** is used to justify the risk acceptance of a known remaining deficiency that has been agreed not to eradicate as part of Problem Management activities.
- **Communication** to all stakeholders involved in the associated problem. It consists on providing regular updates on the progress of the problem analysis and its action plan leading to resolution.
- **Operational problem management reporting** details the daily aspects of operations, used as the support basis for rapid decision making.
- **KPIs and continuous Improvement Plan:** A set of identified KPIs and improvement actions, based on metrics analysis and IT department feedback (the one who experimented the process), to enhance process efficiency. These deliverables will be the basis of the committee dedicated to the review of the problem management process.
- **Training and Onboarding Materials:** Guides and materials for onboarding new support staff or training existing teams on problem handling procedures and tools

8. Appendices

8.1. Glossary

Term	Definition
Known error database	A record containing the details of a known error: the lifecycle of a known error, including the status, root cause and workaround.
Major incident	The highest category of impact for an incident. A major incident results in significant disruption to the business
Priority	A category used to identify the relative importance of an incident, problem or change. Priority is based on impact and urgency and is used to identify required times for actions to be taken.
Proactive problem management	Part of the problem management process. It is the process of identifying and resolving problems before incidents occur, by analyzing trends, monitoring systems, and using data to detect potential issues that could lead to service disruptions.
Problem record	A record containing the details of a problem. Each problem records the lifecycle of a single problem.
Reactive problem management	Part of problem management that solves problems in response to one or more incidents. Problem management activities are performed in reaction to specific incident situations.
Resolution	Action taken to repair the root cause of an incident or problem, or to implement a workaround.
Root Cause	Cause of problems
Syra	Syensqo ITSM platform
Workaround	A solution that reduces/eliminates the impact of an incident/problem for which a full resolution is not yet available. Some of them reduce the likelihood of incidents

8.2. Prioritization matrix

The prioritization matrix is made of **four levels of priority** (P1 = critical incident to P4 = low priority). Priority **P1 and P2 will lead to major incidents**. The following prioritization matrix is a first version and would evolve according to the maturity of the process:

			IMPACT			
			Widespread within the organization	Large within the organization	Limited within the organization	Localized within the organization
			Extensive	Significant	Moderate	Minor
URGENCY	Total loss of service to a complete group of End Users, impacting ability to conduct business (no work-around)	Critical	P1	P1	P2	P2
	Total loss of service to a group of End Users, impacting their ability to conduct business. A work-around is available to the End User(s).	High	P2	P2	P3	P3
	The issue is bothering the End User but is not affecting their work	Medium	P3	P3	P3	P4
	End User can still do their work	Low	P4	P4	P4	P4

EXAMPLES

P1 **No employee in the whole company** has access to Google Workspace (Gmail, Drive, Calendar, etc.) during working hours. **All internal and external communication is disrupted**.

P2 **The sales team** cannot access Google Calendar with their mobile devices or their computer (no workaround). They have multiple client meetings scheduled throughout the day and **are unable to confirm times or join video calls via Calendar links**. Email and other apps are still functional.

P3 Google Sheets is experiencing **slow performance** for **some users,** affecting productivity.

P4 **An employee** is unable to use his webcam **during all his meeting**. He still can No urgent action is required but

Prioritization matrix with examples