digital space

Problem Management Policy

1. Document

Control

This document is controlled and maintained according to the documentation standards and procedures of Digital Space. All requests for changes to the document should be sent to the document owner. Any new issues will be sent to the recipients as defined within the distribution list maintained by the document owner. Requests for additional copies of this document should be sent to the document owner to ensure that alterations or amendments to the distribution list are properly controlled.

Version control

Version	Description	Editor	Date
1.0	Revision and publication of Problem Management policy	Problem, Proactive and Change Team Manager	29/12/2022

Review period

This document shall be reviewed at least annually to ensure that the document remains relevant. Any changes will be recorded in the version history above.

2. Document purpose

This document outlines the Problem Management policy expected to be adhered to by all employees of Digital Space.

3. Problem Management policy summary

The primary objectives of Problem Management (PM) are to prevent incidents from happening and to minimise the impact of incidents than cannot be prevented.

Problem Management works in conjunction with other Digital Space policies related to ITIL and IT Service Management (ITSM).

The goals of the Digital Space Problem Management policy include establishing a standard process for identifying, recording, analysing, and resolving issues which may create unexpected breaks in service.

The owner of this policy is the DS Problem, Proactive and Change Team Manager.

4. Key Problem Management policy steps

5. Roles

Roles	Description
Problem Manager	Ensures that the PM procedure is followed across the business
Solution Owner	Provides specialist technical input for the investigation and resolution of problems
Major Incident Manager	Assesses whether Problem ticket is necessary to resolve major incident

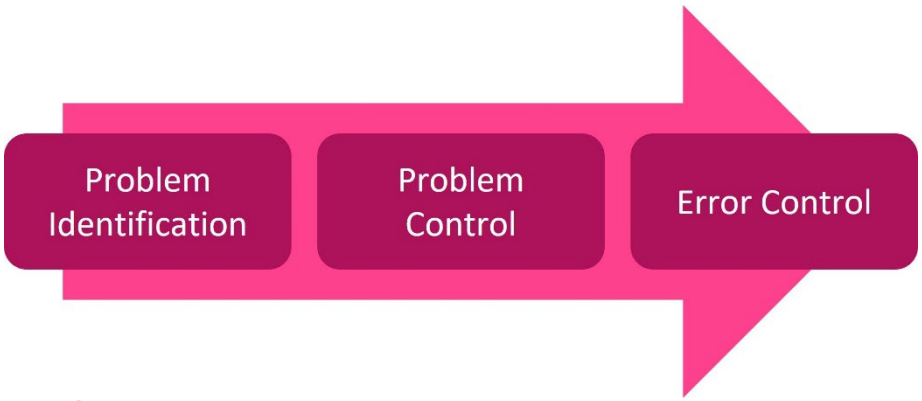
6. Terminology

Term	Definition
Error Control	Error control activities manage known errors and may enable the identification of potential permanent solutions
Known Error	A problem that has a documented root cause but is not yet resolved
Problem	A cause or potential cause of one or more incidents

Problem Control	Problem control covers multiple steps including prioritization, investigation, analysis, and documentation of known errors and workarounds.
Problem Identification	Problem identification detects underlying issues through data analysis or as an output from the major incident management process. Formal recording of problems is a further part of this activity.
Problem Management	A methodology for reducing the likelihood and impact of incidents by identifying their actual and potential causes, and managing workarounds and known errors.
Root Cause Analysis	Root cause analysis (RCA) is a systematic process for finding and identifying the root cause of a problem.
Workaround	A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available.

7. Problem Management Lifecycle

Digital Space follow ITIL 4 guidance in the lifecycle of addressing problems. In doing so, three phases of activity are broadly adopted.



Problem Identification

Problem identification activities initially detect candidate problems through a variety of inputs

- Performing trend analysis of incident tickets
- Detecting duplicate and recurring issues
- As part of the resolution of a major incident
- Analysis of information received from suppliers and partners
- Analysis of information highlighted by internal staff including service delivery, project management and 1st line teams

Once an issue is confirmed as a problem, which could be the root cause of multiple incidents, its details are logged to the corporate ITSM system.

Problem Control

Problem control includes activities including prioritization, investigation, analysis and documenting known errors and workarounds. In evaluating problems, a technical specialist uses information about the product architecture and configuration to identify configuration items that are likely to cause the relevant incidents or

alerts. The analysis is not limited to configuration items but may include other considerations, such as user behaviour, human error and procedural inaccuracies.

Problems are prioritized based on the risk they pose in terms of probability and impact to services. Focus is given to problems that have highest risk to services and service management.

The Solution Owner, with advice from the Problem Manager and any other necessary technical resources, conducts an in-depth and detailed root cause analysis. If the problem ticket was triggered because of a Major Incident, then the Major Incident Report (MIR) is used as an input to the conduct of an RCA.

The following parameters are used in conducting an RCA:

- Source of the Problem
- Symptoms
- Impact details
- Any dependencies

When a problem cannot be resolved quickly, attempts are made to find and document a workaround for future incidents, based on an understanding of the issue. Workarounds are documented in problem records, which can be done at any stage without necessarily having to wait for RCA to be complete. However, if a workaround has been documented early in problem control, then this is reviewed and improved after problem analysis is finalised.

When a problem has gone through this analysis step, it is now termed a known error. Known errors are documented in the knowledge base as articles so that workaround details are captured and shared across the organization.

Error Control

Error control activities manage known errors and may enable the identification of potential permanent solutions. Where a permanent solution requires change control, this is assessed from the perspective of cost, risk and benefits.

Error control also regularly re-assesses the status of known errors that have not been resolved, taking account of the overall impact on customers and/or service availability, and the cost of permanent resolutions, and effectiveness of workarounds.

Once the Problem Manager ensures that all the necessary steps in the workflow have been completed, the problem ticket is closed as either resolved or the risk of leaving a workaround in place accepted. Should the problem not be resolved, an entry in the appropriate risk register is made, detailing the potential impact of the issue together with the reasoning why it could not be addressed.

If a user is directly involved in asking for a problem analysis, they are informed by the Problem Manager of details of the outcome of closure.

8. Expected Problem Management inputs and outputs

Inputs

- Results of Proactive Problem Management
- The occurrence of a Major Incident (Reactive Problem Management)
- Any unknown issue
- Change Implemented
- Workarounds
- Known errors arising from the IT development teams and test environments
- Configuration Management
- Service Level Management
- Incident Management
- Availability Management

Outputs

- Request for Change (RFC)
- Resolution for the problem
- Knowledge Articles
- Trigger to Change Management
- Entry in customer or DS risk register