

Internal and Confidential

Netradyne Problem Management Process

v1.1

Table of Contents

[Netradyne Problem Management Process 0](#_Toc170117402)

[Document Control 3](#_Toc170117403)

[1 Purpose 4](#_Toc170117404)

[2 Scope 4](#_Toc170117405)

[3 Roles and Responsibilities 4](#_Toc170117406)

[4 Procedure 5](#_Toc170117407)

[4.1 Process Goals 5](#_Toc170117408)

[4.2 Problem Management Benefits 5](#_Toc170117409)

[4.3 Policies 5](#_Toc170117410)

[4.4 Key Contacts & Escalation Matrix 6](#_Toc170117411)

[4.5 RACI 6](#_Toc170117412)

[4.6 Activities 6](#_Toc170117413)

[4.6.1 Weekly Activities 6](#_Toc170117414)

[4.6.2 Monthly Activities 7](#_Toc170117415)

[4.7 Problem Management – Workflow & Process 7](#_Toc170117416)

[4.7.1 Workflow 7](#_Toc170117417)

[4.7.2 Problem Detection 7](#_Toc170117418)

[4.7.3 Problem Logging: Categorization & Prioritization 8](#_Toc170117419)

[4.7.4 Problem Assignment & Analysis 8](#_Toc170117420)

[4.7.5 Problem Investigation & Diagnosis 8](#_Toc170117421)

[4.7.6 Root Cause Identification 9](#_Toc170117422)

[4.7.7 Workaround Identified 9](#_Toc170117423)

[4.7.8 Root Cause, Known Error & Resolution Identification 9](#_Toc170117424)

[4.7.9 Review Draft Document 9](#_Toc170117425)

[4.7.10 Root Cause Approval 9](#_Toc170117426)

[4.7.11 Problem/Error Resolution (CA Processing) 9](#_Toc170117427)

[4.7.12 Final RCA Document 9](#_Toc170117428)

[4.7.13 Monitoring, Continual Service Improvement & Process Maturity 9](#_Toc170117429)

[4.8 Problem Management – Roles & Responsibilities 10](#_Toc170117430)

[4.8.1 Problem Source 10](#_Toc170117431)

[4.8.2 Problem Initiator 10](#_Toc170117432)

[4.8.3 Problem Manager 10](#_Toc170117433)

[4.8.4 Root Cause Owner (SME) 11](#_Toc170117434)

[4.8.5 RCA Approver 11](#_Toc170117435)

[4.8.6 Knowledge Management / Known Error 11](#_Toc170117436)

[4.9 Root Cause Analysis – RCA 11](#_Toc170117437)

[4.10 Work Level Instruction 12](#_Toc170117439)

[4.10.1 Problem Detection 12](#_Toc170117440)

[4.10.2 Problem Logging and Closure 12](#_Toc170117441)

[4.11 Interface with ITSM Process 15](#_Toc170117442)

[4.12 Problem Management: KPI & Process Control 16](#_Toc170117443)

[4.12.1 Key Performance Indicators 16](#_Toc170117444)

[4.12.2 Process Control 17](#_Toc170117445)

[5 Conduct 17](#_Toc170117446)

[6 Exception 17](#_Toc170117447)

[7 Terms/Acronyms 17](#_Toc170117448)

[8 References 18](#_Toc170117449)

[Policies 18](#_Toc170117450)

[Process/Procedures 18](#_Toc170117451)

[9 Appendix A: Document RACI Matrix 18](#_Toc170117452)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDPM202401 |
| **Document Name** | Netradyne Problem Management Process |
| **Document Status** | Released |
| **Document Released Date** | 25-Mar-2024 |
| **Document Author** | Priyesh Parashar |
| **Document Content Contributors** | Priyesh Parashar |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Priyesh Parashar |
| **Document Version** | v1.1 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 25/Mar/2024 | Initial Version | Priyesh Parashar |
| v1.1 | 24/Feb/2025 | Annual Revision | Priyesh Parashar |
|  |  |  |  |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 10/Jul/2024 | Saravanan Sankaran | Senior Director, Infosec & IT | Approved |
| 26/Feb/2025 | Saravanan Sankaran | VP, Infosec & IT | Approved |
|  |  |  |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Staff | Netradyne |
|  |  |
|  |  |

# Purpose

This document is a Netradyne Policy/Process/Procedure document.

The purpose of this Problem Management document is to provide an end-to-end description of the Standard Operating Procedures (SOP) to manage the Problem Record lifecycle. The primary objectives of Problem Management are:

* To efficiently prevent problems and resulting Incidents from occurring
* To eliminate recurring Incidents
* To minimize the impact of Incidents that cannot be prevented

The objective of this document is to serve as an official document, to be used by the Netradyne Problem Management capability. It defines a process framework which consists of details on all the essential activities required to implement a high-quality process and ensure that it is effective in supporting the business.

The primary audience for this process guide will be the personnel performing the roles defined within the [Roles and Responsibilities](#_Problem_Management:_Roles_1) section of this document.

Note: This document is subjected to regular analysis and assessment, and updated versions may be recorded and released upon approval.

# Scope

The organizational scope of the Problem Management Process includes problems related to Netradyne IT Services.

This document covers both the Reactive and the Proactive aspects of the Problem Management process.

The Reactive Problem Management Process is based on solving problems in response to one or more Incidents or failed changes or Major Incidents.

The Proactive Problem Management process is based on early identification of problems and solving them to prevent incidents from occurring.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

This section covers a brief set of details around Problem Management and the purpose of this document.

## 4.1 Process Goals

A Problem is the unknown underlying cause of one or more (potential or occurring) Incidents. The Problem Management process is responsible for recording and managing the lifecycle of all problems, from identification to further investigation, documentation, and eventual removal. The Problem Management process covers a defined set of activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon objective in a cost-effective and measurable manner.

A robust Problem Management process aims to provide additional stability and reliability to the IT environment, leading to improved availability of Business Services and Customer Satisfaction.

This document elaborates on the Problem Management process on how to detect, record, classify, investigate and diagnose Problems; document Known Errors in the KEDB; and manage all this till resolution.

## 4.2 Problem Management Benefits

The key benefits of the Problem Management process include:

* Higher productivity of IT Operations Service Delivery and the supporting IT staff
* Reduction in cost-of-effort in firefighting or resolving repeat Incidents
* Higher availability of managed infrastructure services
* Reduced expenditure on workarounds or fixes that do not work
* Improved Customer satisfaction

## 4.3 Policies

The Problem Management policies are required to instruct/guide all the stakeholders to make the process effective.

* Every Problem record must be recorded in the ServiceDesk+
* Service Ownership is a critical component to assure the quality of services provided by IT. The Service Owner must be designated for each service to be managed by the Problem Management process. The Service Owner works to ensure that any Problem that may impact their service(s) is controlled.
* The Problem Management team will be responsible for updating Problem Status in the ServiceDesk+
* The Support teams (Root Cause Owner) will be responsible for updating the Problem Record
* Each Problem Record will be assigned a category using the same classification system as the related Incident or Change Record.
* Problem investigations will determine the Root Cause and Configuration Item (CI) at fault
* The Problem Management team will identify the single best solution to the Known Error, based on business requirements.
* The Problem Manager will receive enough resources to perform the task of administrating the process of Problem Management. Resource requirements will be based on the scope of the Problem. Resources from the business and technical analyst teams will be required.
* The Problem Management team may have the need to call on the stakeholders to help identify Root Causes. The Business Service Owner will be responsible for arranging user support for the Problem Management team.
* After executing a successful change resulting in the removal of a Known Error, the Change, and the overall Problem will be evaluated for a fixed period. This is to ensure that the Known Error has been permanently removed from the environment.

## 4.4 Key Contacts & Escalation Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact** | **Email ID** | **Role** |
| Priyesh Parashar | 9845227014 | [priyesh.parashar@netradyne.com](mailto:priyesh.parashar@netradyne.com) | Staff Manager - ITSM |
| Saravanan Sankaran | 9444161422 | [saravanan.sankaran@netradyne.com](mailto:saravanan.sankaran@netradyne.com) | VP - Info Security & IT |

## 4.5 RACI

This section maps the Roles and Responsibilities to the various steps in the workflow.

* **R**esponsible: Those who do the work to achieve a task. There is typically one role with a participation type of *Responsible*.
* **A**ccountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom *Responsible* is accountable. Typically, the process owner is *Accountable* for a process, and there must be only one *Accountable* specified for each task or deliverable.
* **C**onsulted: Those who are not directly involved in the process but provide inputs and whose opinions are sought.
* **I**nformed: Those who receive outputs from the process or are kept up to date on the progress, often only on completion of the task or deliverable.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles/Activities** | **Problem Initiator** | **Problem Manager** | **RCA Owner** | **RCA Approver** |
| Problem Detection | R | R, A | C | I |
| Problem Logging | R | R, A | C | I |
| Problem Assignment | I | R, A | C, I | I |
| Problem Investigation and Diagnosis | C | R, A | R | R, C, I |
| Workaround Creation | I | A | R | C, I |
| Root Cause Identification | I | C, I | A, R | C, I |
| RCA Approval | I | A, I | C, I | R |
| Known Error creation | I | A, C, I | R | C, I |
| Problem Resolution | I | R, A | R | C, I |
| Problem Closure | I | R, A | C, I | C, I |
| Continual Improvement | R | R, A | C | C, I |

## 4.6 Activities

### 4.6.1 Weekly Activities

* Weekly RCA Follow up with support teams.
* Create/Close/Update Problem record & Problem tasks.

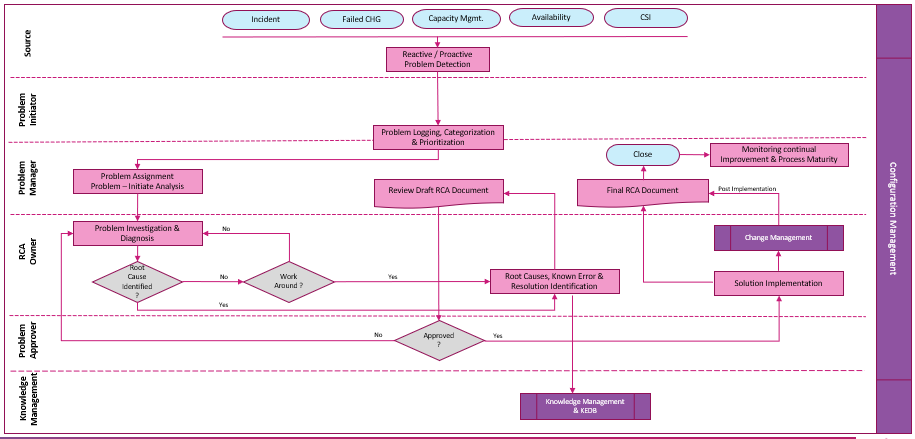
### 4.6.2 Monthly Activities

* Proactive problem analysis
* Trend Analysis/Heat Map
* Monthly Reporting & Review
* Track Corrective & preventive actions

## 4.7 Problem Management – Workflow & Process

### 4.7.1 Workflow

The overall activity flowchart for the Problem Management process is given below. The process flow depicts the Twelve activities associated with the **Problem Management Process**, both Reactive and Proactive, from beginning to end; and, how it integrates with the six **Roles and Responsibility** categories.



### 4.7.2 Problem Detection

**Reactive detection** entails Problem Records being generated by default for:

* All resolved P1 incidents, by the Incident Management team.
* The Change Management team is required to create Problem Records for failed changes to cover the PIR and to document/implement the lessons learnt.
* The Trend Analysis performed by the Problem, Incident, Event Management teams as a part of their daily operational activities.
* Problem Records may also be generated for RCAs of specific incidents as requested by the stakeholders.

**Proactive detection** involves Problem Records being created for issues identified as an outcome of Trend Analysis. This includes:

* The Trend Analyses performed by the Capacity, or the Availability Management teams as a part of their daily operational activities.
* There may also be inputs that arise off the Continuous Service Improvement (CSI) effort.

Once a problem is identified, these respective teams are to create a Problem Record with all the relevant details and assign it to the problem manager’s queue for processing.

| **Problem Detection** | **Description** | **Responsible** |
| --- | --- | --- |
| Reactive Problem Detection | Incident Management: An investigation is initiated by default for all solved P1.  Event Management: The problem was identified through alerts received event. | Problem Manager |
| Change Management: The problem is likely related to an unsuccessful change. | Change Manager |
| Proactive Problem Detection | Event/Availability/Capacity Management: The problem was identified through alerts received for a non-impacting event | Monitoring Team/Asset Manager |
| Proactive Problem Management: The problem was identified through trend analysis of historical incidents (Automated and Manual). | Problem Manager |

### 4.7.3 Problem Logging: Categorization & Prioritization

Problems are logged in a Problem Record. A Problem Record is a compilation of every problem in an organization. This is accomplished via ServiceDesk+ and is done by the Problem Source in liaison with the Problem Manager.

* **Categorization**: Problem categorization should match the related Incident or Change categorization. Problem categorization involves assigning a main and secondary category to the issue.
* **Prioritization**: The Problem priority is determined by its impact on users and on the business and its urgency. This must match the priority of the associated Incident(s) or Change.

The up-to-date details on the associated Configuration Item (CI) should also be present in the CMDB and associated to the Problem Record in the ServiceDesk+. If the CI information is not available or accurate, the Asset Manager is to be engaged to update the CMDB/Asset Register.

### 4.7.4 Problem Assignment & Analysis

The Problem Manager analyses the incidents that led to the Problem Detection and updates the Problem Record with all the relevant initial information.

**Assign Problem:** The Problem Manager assigns the Problem to the support SME for further analysis.

### 4.7.5 Problem Investigation & Diagnosis

The speed at which a problem is investigated and diagnosed depends on its assigned priority. High-priority issues should always be addressed first, as their impact on services is the greatest. The Problem Manager, together with the support SME will use Problem Analysis Methods to diagnose the symptoms and arrive at the Root Cause, Workaround, Known Error, and the Resolution Activities (CAPA).

### 4.7.6 Root Cause Identification

After the investigations, it needs to be established if the SME can provide the Root Cause information. If, however, it is not possible to identify the root cause, the next step will be to identify a workaround.

### 4.7.7 Workaround Identified

In case the Root Cause identification is not possible, the investigation goes on till there is at least a step-by-step work around identified.

### 4.7.8 Root Cause, Known Error & Resolution Identification

Once the Root Cause, Known Error and Workaround are identified, the same must be documented in the draft RCA document and provided to the Problem Manager for review.

### 4.7.9 Review Draft Document

The Problem Manager will review the Draft RCA document for quality and completeness, ensuring that all the relevant details are present. The Draft RCA document is then sent across to the stakeholders for review and approval.

### 4.7.10 Root Cause Approval

The stakeholder for respective stream is the Approver for RCAs. For every RCA, a draft will be provided to be reviewed and approved. If, in case the Draft RCA document is found to need changes, the feedback is provided to the Problem Owner and subsequently, an updated draft will be released for approval. Once approved, the Problem Owner will give the go ahead for the implementation of the Problem/Error resolution.

### 4.7.11 Problem/Error Resolution (CA Processing)

On approval of the draft RCA document from the SPOC, the Problem Manager will enable the SME to initiate steps for Problem / Error Resolution, using the ServiceDesk+. Problem Resolution activities, when available, will resolve the underlying cause of a set of incidents and prevents those incidents from recurring. Some resolutions may require the Change Management process.

### 4.7.12 Final RCA Document

Post successful implementation of the solution, the Problem Record is resolved and closed. The stakeholder is provided with the Final RCA document and notified of the closure.

### 4.7.13 Monitoring, Continual Service Improvement & Process Maturity

Problems Records are tracked and updated throughout their lifecycle to support proper handling and reporting. In addition, the information in Problem Records is used to develop reporting for governance and to periodically show the status and the overall effectiveness of the Problem Management process.

Reporting and Continual Improvement provide visibility into the performance of the Problem activity underway. By providing information and visibility to the rest of the organization, decisions can be made, and focus can be maintained on solving issues.

By recognizing Opportunities for Improvement (OFIs) and leveraging Continual Service Improvement, the level of maturity increases, and the impact and benefits provided by Problem management are kept current and relevant.

## 4.8 Problem Management – Roles & Responsibilities

The Problem Management process activities are broken up over six roles, with specific responsibilities. Each role is assigned to perform specific tasks. Within the process, there can be more than one individual associated with a specific role. Additionally, a single individual can assume more than one role within the process although typically not at the same time.

### 4.8.1 Problem Source

The Problem Source provides a clear description of the trigger, based on an event or analysis. Depending on the source, Problems can either be Reactive or Proactive in nature.

| **Problem** | **INPUT SOURCE** | **DESCRIPTION OF SOURCE** | **MODE OF INPUT** |
| --- | --- | --- | --- |
| Reactive &  Proactive | Incident | * Identified by Service Desk/Capabilities team, in response to a solved P1 Incident. * Problem identified through a non-impacting event. * Trend Analysis of historical Incidents revealed an underlying problem. | Service Desk / Support team/Problem Manager |
| Failed Change | Identified by the Change Manager in response to an unsuccessful change. | Change Manager |
| Continuous Service Improvement | Determined through service improvement activities. | Problem Manager/Process Owner |
| Capacity Management | There is a problem with capacity causing repeat incidents. | Asset/Capacity Manager |
| Availability Management | The problem was identified as related to Availability and Up-Time of services in scope. | Monitoring Team / Support Teams |

### 4.8.2 Problem Initiator

The Problem Initiator is the person who raises/logs the Problem Record in the ServiceDesk+. The Problem Record must be raised by the Problem Source, in liaison with the Problem Manager. It also needs to be ensured that the Problem Record reflects the Categorization and Priority of the associated Incident or Change. The current details on the associated Configuration Item (CI) should also be present in the CMDB. If the CI information is not available or accurate, the Asset Manager is to be informed to update the CMDB.

### 4.8.3 Problem Manager

The Problem Manager is responsible for managing all Problem Records through the Problem Management Lifecycle.

The Problem Manager / Owner is responsible for:

* Reviewing the initial classification and prioritization of the Problem Records.
* Assign the Problem Record to the appropriate Root Cause Owner in a timely manner.
* Track the progress of all Problem Records to ensure they are actively moving through the Problem Management Lifecycle.
* Validate that the implemented solution has resolved the Problem.
* Perform closure assessments of Known Errors and Problem Records.
* Communicate the RCA and overall status of the problems to all required stakeholders.

### 4.8.4 Root Cause Owner (SME)

The Root Cause owner is the support team SME that is working on the investigation and diagnosis of the problem.

The SME is responsible for:

* Investigation and diagnosis of the Root Cause.
* Identifying the workaround or Known Error.
* Working with the Problem Manager to add the Known Error details to KEDB.
* Providing the error resolution and its implementation schedule (liaise with Change Management if needed).

### 4.8.5 RCA Approver

The RCA Approver will be stakeholder. For every RCA, a draft will be shared which needs to be reviewed and approved. If, in case the Draft RCA document needs changes, the feedback is provided to the Problem Owner and subsequently, an updated draft will be released for approval. Once approved, the Problem Owner will give the go ahead for the solution implementation.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Contact** | **Email ID** | **Role** |
| Saravanan Sankaran | 9444161422 | [saravanan.sankaran@netradyne.com](mailto:saravanan.sankaran@netradyne.com) | VP - Info Security & IT |

### 4.8.6 Knowledge Management / Known Error

This process involves the activities including the Knowledge article uploads, article changes, deletion, and review request.

This process also involves the archiving of the articles. Maintaining and managing the database provides value by ensuring accuracy and relevance for those using this resource.

Problem matching against existing known errors is performed during problem investigation and diagnosis to see if the problem has already been identified.

Post Problem closure, Known Errors and workarounds are documented and published in the knowledge base on a real time basis.

## 4.9 Root Cause Analysis – RCA

## Final RCA will be submitted within 5 business days for all problem tickets. Below SLA will be followed for all reactive and proactive problem tickets.

|  |  |
| --- | --- |
| **Problem Type** | **Duration** |
| Proactive/Reactive | 5 Business Days |

## 4.10 Work Level Instruction

This section describes the step by step process to carry out the Problem Management activities in ServiceDesk+, as per the section [**4.7 Process Workflow**](#_4.7_Problem_Management)**,** to be carried out by the various stakeholders described in the [**4.8 Problem Management: Roles and Responsibilities**](#_4.8_Problem_Management)

### 4.10.1 Problem Detection

For Reactive and Proactive Problem Detection, each contributing capability has a documented process, introduced in section [**4.7.2 Source**](#_Source).

### 4.10.2 Problem Logging and Closure

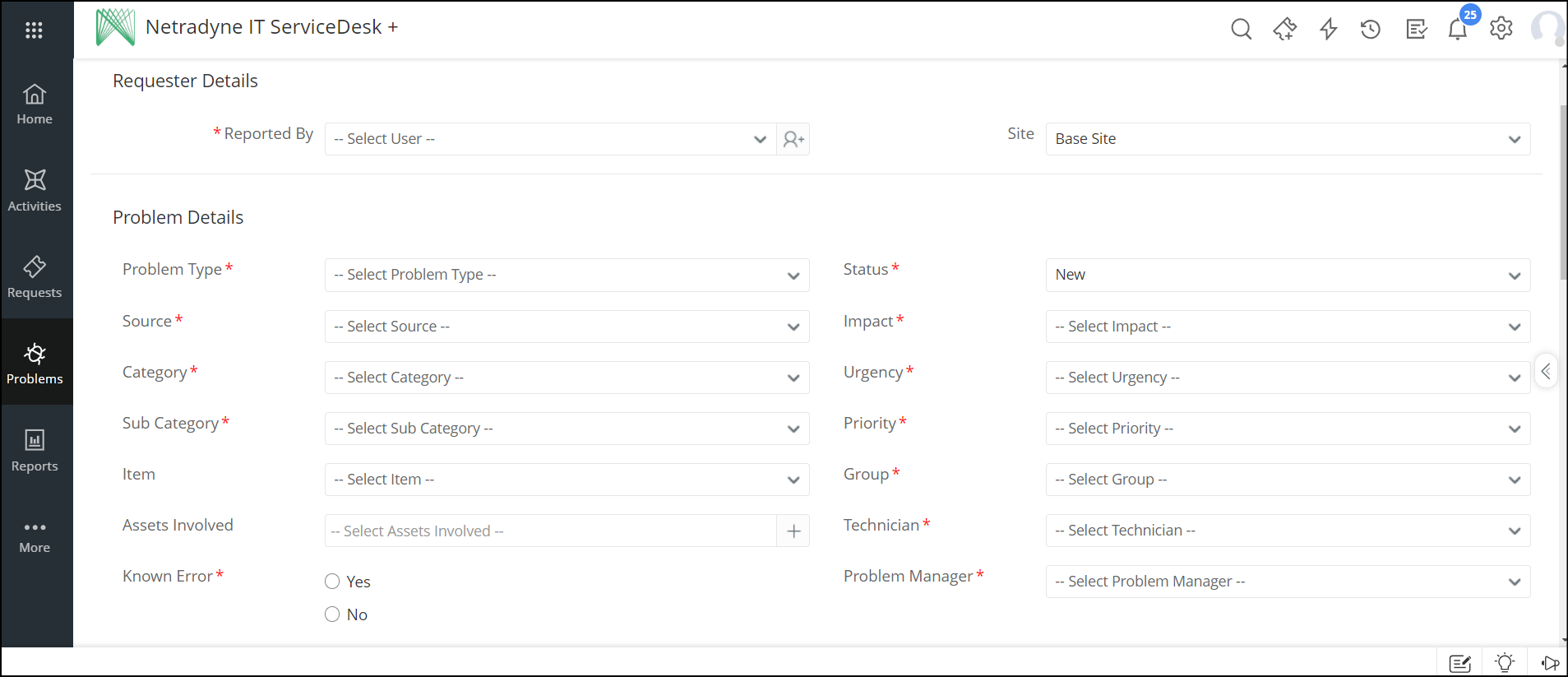
This section describes the Problem Logging and Assignment to initiate the next step in the flow.

* This activity lies under the scope of the Problem Source.
* To generate a Reactive Problem Record from a Major Incident or non-Major Incident, ensure that the Incident is in the resolved state.

A screenshot of a computer

Description automatically generated

* Once the Problem Record has been logged by the Problem Source, it will be in the “New” state, and in the “Problem Categorization and Prioritization” stage (top of the Problem Record).
* Verify below fields should be updated correctly:
  + Source
  + Problem Type
  + Impact, Urgency and Priority based on the Incident/Change associated.
  + Category, Subcategory and Item.
  + The CI information is correct.
  + Known Error – If permanently solution is applied then select yes or else select no



* Update the title and description on the problem record.
  + Title – Short and crisp input on the problem record
  + Description – Detailed description of the issue occured

A screenshot of a computer

Description automatically generated

Below fields will be updated by the problem manager as per the input provided by the SME/Problem Owner

* Business Impact
* Impact Analysis
* Preventive Action
* Corrective Action
* Workaround
* Restoration Activities

A white text box with black lines

Description automatically generated

Problem Closure input will be updated by Problem manager based on the outcome from RCA.

* Cause Code – Reason for the issue occurred.
  + **Environment Disaster** – This harm could result from various causes such as industrial accidents, pollution incidents, natural disasters, or human activities that degrade ecosystems and natural resources.
  + **Vendor Issues** - Any problem or complication arising from the interaction with a supplier, seller, or external service provider.
  + **Hardware Issues** – Issue/incident occurred due to hardware failure or malfunction.
  + **Software Issues** - Issue/incident occurred due to software failure or malfunction.
  + **People/Process/Documentation** – Issue/incident occurred due to deviation from the defined process.
  + **Others** – If the above reasons are not relevant then others option can be selected.
* Closure Code – closure code should be selected based on the RCA input.
  + - Permanently Fixed – If the issue is fixed permanently.
    - Risk Accepted – If the issue is not fixed permanently and need to be worked as per given workaround.
    - Cancelled – If the problem record is not required and requester has requested for cancellation.
    - Duplicate – If already a similar problem record and logged then please select this.

A screenshot of a computer

Description automatically generated

**Note** – PDF copy of the RCA needs to be attached to each problem record.

* **RCA Statement -** [**Netradyne RCA Statement**](https://netorg726775.sharepoint.com/:w:/r/sites/ITTEAM259/Shared%20Documents/General/IT%20Process%20and%20Policy%20Documents/IT%20Process/Problem%20Management/Netradyne%20RCA%20Statement.docx?d=wd70a6719e1974322b6576e1d738b8dc9&csf=1&web=1&e=iSjt2D)
* **RCA – 5 why technique will be used for performing the RCA**

A screenshot of a computer

Description automatically generated

### 4.11 Interface with ITSM Process

Throughout the lifecycle of a Problem, there are multiple instances where the Problem Manager will need to interface with members of other Service Management Capabilities.

| **Process** | **Relation Description** | **Input** | **Output** |
| --- | --- | --- | --- |
| Incident Management | Most problems records are triggered in reaction to one or more incidents.  Incident history helps identify trends or potential weaknesses as part of proactive problem management. | X |  |
| Related incident records are automatically updated when the problem is resolved, if the proper business rules have been created. |  | X |
| Change Management | Problem Management is informed on the status and the progress of submitted RFCs. | X |  |
| Requests for change (RFC) are initiated to remove detected errors in the infrastructure. |  | X |
| Configuration Management | Configuration item (CI) details and relationship information aids in root cause analysis, impact evaluation, and solution development. | X |  |
| Problems are linked to relevant CI record(s). |  | X |
| Knowledge Management/  Known errors | This process involves the activities including the Knowledge article uploads, article changes, deletion, and review request. This process also involves the archiving of the articles. Maintaining and managing the database provides value by ensuring accuracy and relevance for those using this resource.  Problem matching against existing known errors is performed during problem investigation and diagnosis to see if the problem has already been identified.  Known errors and workarounds are documented and published in the knowledge base. | X |  |
| Event Management | Proactive analysis of event data can be potential source for proactive problem management | X |  |
| Capacity Management | Proactive analysis of event data can be potential source for proactive problem management | X |  |
| Release and Deployment Management | Acceptable known errors captured during release review | X |  |
| Availability Management | Proactive analysis of event data can be potential source for proactive problem management | X |  |

### 4.12 Problem Management: KPI & Process Control

### 4.12.1 Key Performance Indicators

To ensure the success of the Problem Management Process, KPI’s need to be tracked over time as trend lines. They provide information on the effectiveness of the process and the impact of continuous improvement efforts. KPIs are ideally to be reviewed every six months to measure efficiency and identify improvement areas.

Critical Success Factors are elements that are necessary for a process to achieve its mission and establish its intended benefits. To achieve the goals there needs to be awareness about each Success Factor and related internal KPIs.

* Higher productivity of IO Service Delivery and the supporting IT staff
  + Number of process changes/updates initiated through CAPA for other capabilities.
  + Reduction in Automated Alerts and Incidents.
* Efficiency of Problem management through Known errors/strong Knowledge base
  + In case of repeat incidents, the MTTR goes down.
  + Number of records available in the KEDB for use by SD and MIM.
  + Effective KEDB articles.
* Higher availability of managed infrastructure services
  + Availability Management Reports.
  + No repeat occurrences save downtime over the months.
* Improved Customer satisfaction
  + Less Major incidents/Outages.
  + Reduction in repeated incidents.

### 4.12.2 Process Control

To maintain continuous improvement of the Problem Management process, frequent reviews are essential. The process review is held between Process Owner, Problem Manager and Stakeholders on a yearly basis. These reviews should take place to ensure quality is maintained or even improved.

The following steps should take place for each review.

1. Gather data and information from the Support tool, Customer Satisfaction Surveys, and input from Problem Management staff. Input for the process review should be pro-actively sought from stakeholders by the Process Owner.
2. Analyse the data looking at areas such as, customer satisfaction, suggestions from staff and process metrics.
3. From the above analysis identify opportunities for improvement and put forward the suggestions.

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| **CAPA** | Corrective Actions Preventive Actions |
| **Capability** | The ability of an organization, person, process, application, IT service or other configuration item to carry out an activity. Capabilities are intangible assets of an organization. |
| **CI** | Configuration Item: Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements. |
| **CSF** | Critical Success Factor |
| **CSI** | Continuous Service Improvement |
| **CSIP** | Continuous Service Improvement Program |
| **Incident** | An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set. |
| **IO** | IT Operations |
| **IT** | Information Technology |
| **ITSM** | Information Technology Service Management |
| **KEDB** | A database containing all known error records. This database is created by problem management and used by incident and problem management. The known error database may be part of the configuration management system or may be stored elsewhere in the service knowledge management system. |
| **Known Error** | A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their lifecycle by problem management. Known errors may also be identified by development or suppliers. |
| **MTTR** | Mean Time To Resolve |
| **OFI** | Opportunity For Improvement |
| **Production** | Production Environment, Live Environment: A controlled environment containing live configuration items used to deliver IT services to customers. |
| **Px** | Priority x |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **WLI** | Work Level Instructions |

# References

* **RCA Statement -** [**Netradyne RCA Statement**](https://netorg726775.sharepoint.com/:w:/r/sites/ITTEAM259/Shared%20Documents/General/IT%20Process%20and%20Policy%20Documents/IT%20Process/Problem%20Management/Netradyne%20RCA%20Statement.docx?d=wd70a6719e1974322b6576e1d738b8dc9&csf=1&web=1&e=iSjt2D)

## Policies

[Netradyne Information Security Policy & Procedure.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Policy%20%26%20Procedure.pdf?csf=1&web=1&e=mRSIq4)

[Netradyne Information Security Exception Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Information%20Security%20Exception%20Process.pdf?csf=1&web=1&e=RbfEhO)

[Acceptable Usage Policy.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Acceptable%20Usage%20Policy.pdf?csf=1&web=1&e=2jMnrk)

## Process/Procedures

[NETRADYNE DISASTER RECOVERY PROCESS.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20DISASTER%20RECOVERY%20PROCESS.pdf?csf=1&web=1&e=xTyHtp)

[NETRADYNE BUSINESS CONTINUITY PLAN.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NETRADYNE%20BUSINESS%20CONTINUITY%20PLAN.pdf?csf=1&web=1&e=eCZUy6)

[Netradyne Vulnerability & Patch Management Process.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/Netradyne%20Vulnerability%20%26%20Patch%20Management%20Process.pdf?csf=1&web=1&e=N697w0)

[NetradyneSecurityIncidentResponsePlan.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/ISMS%20Published%20Documents/ISMS%202023/NetradyneSecurityIncidentResponsePlan.pdf?csf=1&web=1&e=Nzo34K)

[Netradyne IT Incident Management.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/ITTEAM259/Shared%20Documents/General/IT%20Process%20and%20Policy%20Documents/IT%20Process/Incident%20Management/Netradyne%20IT%20Incident%20Management.pdf?csf=1&web=1&e=H0T8Rm)

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |