



Process Guide

Problem Management

Version: 1.4
CALGARY Release

Table of Contents

1 Introduction	3
1.1 Overview	3
1.2 Process Description	3
1.3 Process Goal	3
1.4 Process Objectives	3
1.5 Relationship with other processes	4
1.6 Principles and Basic Concepts	5
2 Process Roles	7
2.1 RACI Matrix	8
3 Problem Management Activity Description.....	9
3.1 Process Overview	9
3.2 Problem Detection and Logging	11
3.3 Problem Investigation and Diagnosis	14
3.4 Problem Resolution and Recovery	16
4 Process Control	18
4.1 KPIs	18
4.2 Operational Data.....	18
4.3 Reports and Homepages.....	18
Appendix A: Document Conventions	20
Appendix B: Glossary of Terms and Acronyms	20
Appendix C: Problem Categorization	26
Appendix D: Problem Prioritization	27

List of Figures

Figure 1. Process Overview	9
Figure 2. Problem Detection and Logging	11
Figure 3. Problem Investigation and Diagnosis	14
Figure 4. Problem Resolution and Recovery	16

1 Introduction

The concepts described in this guide are aligned with ITIL 2011 and may reference capabilities that are dependent on other ServiceNow applications. These references will be noted by *blue italicized font*.

1.1 Overview

A process is defined as a set of linked activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon objective in a measurable manner. The problem management process definition laid out in this document further breaks down these activities into actions and the role(s) responsible for their execution.

This document describes the problem management process and how it is supported by ServiceNow to detect, record, and classify problems, assign for investigation and diagnosis, document known errors, create knowledge from problems, request changes, and manage through to resolution and reporting.

1.2 Process Description

A *problem* is defined as the underlying cause of one or more incidents. Problem management is the process responsible for managing the life cycle of all problems from first identification through further investigation, documentation, and eventual removal.

1.3 Process Goal

The primary goals of problem management are to:

- Prevent problems and resulting incidents from happening by removing their root cause.
- Eliminate recurring incidents.
- Minimize the impact of incidents that cannot be prevented.

1.4 Process Objectives

The objectives of the problem management process are to:

- Diagnose the root cause of incidents and determine the resolution or permanent solution to those problems to prevent recurrence.
- Maintain information about problems and the appropriate workarounds and resolutions to reduce the number and impact of incidents over time.
- Conduct major problem reviews to determine what could be done better in the future.
- Proactively identify and solve problems and known errors to improve IT services and prevent potential incidents from occurring.

1.5 Relationship with other processes

Process	Relation Description	Input	Output
Incident Management	<ul style="list-style-type: none"> The majority of 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	
	<ul style="list-style-type: none"> Related incident records are automatically updated when the problem is resolved, if the proper business rules have been created. 		X
Change Management	<ul style="list-style-type: none"> Requests for change (RFC) are initiated to remove detected errors in the infrastructure. 		X
	<ul style="list-style-type: none"> Problem Management is informed on the status and the progress of submitted RFCs. 	X	
Configuration Management	<ul style="list-style-type: none"> Configuration item (CI) details and relationship information aids in root cause analysis, impact evaluation, and solution development. 	X	
	<ul style="list-style-type: none"> Problems are linked to relevant CI record(s). 		X
Knowledge Management	<ul style="list-style-type: none"> Problem matching against existing known errors is performed during problem investigation and diagnosis to see if the problem has already been identified. 	X	
	<ul style="list-style-type: none"> Known errors and workarounds are documented and published in the knowledge base. 		X

1.6 Principles and Basic Concepts

Policies

Problem management policies are required to guide all staff in the behaviors needed to make problem management effective. Policy statements will be very dependent on the culture of the organization, but typically address the following:

- Problems tracked separately from incidents.
- Use of a single management system for all problems.
- Problems subscribe to the same categorization schema as incidents.

Incidents vs. Problems

An *incident* is an unplanned interruption to, or reduction in the quality of, an IT service. Incident management activities are focused on restoring services to normal state operations as quickly as possible (often by means of a temporary workaround). Incidents do not *become* problems, however; it is quite common to have incidents that are a symptom of problems. The rules for invoking problem management during an incident can vary and are at the discretion of individual organizations. See [Promoting an Incident to a Problem](#) in the ServiceNow Wiki for a description of how to use ServiceNow functionality to initiate a problem from an incident.

Reactive vs. Proactive Problem Management Activities

The difference between *reactive* and *proactive* problem management lies in how the process is triggered:

- **Reactive:** triggered in reaction to an incident that has taken place.
- **Proactive:** triggered by activities seeking to improve services (examples: trend analysis of incident history, notification by vendor of software bug).

Better IT service is provided when more effort is applied to *preventing* incidents rather than *reacting* to incidents.

Problem Categorization and Prioritization

Problems should be categorized and prioritized in the same manner as incidents. This allows for problems and incidents to be more readily matched and for more meaningful management information to be obtained.

Problem States

Problems should be tracked throughout their life cycle to support proper handling and reporting. The *state* of a problem indicates where it is in relation to the life cycle and helps determine what the next step in the process might be. The typical uses of the default state values are:

- **Open:** the default value when the record is created.
- **Known Error:** the root cause of the problem has been identified.

- **Pending Change:** the problem has been used to initiate a change request and is awaiting closure of the change request.
- **Closed/Resolved:** the problem is no longer active. A problem can be closed without having been resolved due to the complexity or expense of removing the root cause from the infrastructure.

Major Problem Review

At the closure of every major problem, a review should be conducted to learn any lessons for the future. The review should examine:

- Those things that were done correctly.
- Those things that went wrong.
- What could be done better in the future.
- How to prevent recurrence.
- Whether there has been any third-party responsibility and whether follow-up actions are needed.

A definition of what constitutes a major problem must be agreed and mapped onto the overall problem prioritization scheme.

2 Process Roles

Each role is assigned to perform specific tasks within the process. Within a process, there can be more than one individual associated with each role. Additionally, a single individual can assume more than one role within the process, although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following table describes the typical roles defined for problem management.

Role	Description
Process Owner	<p>A Senior Manager with the ability and authority to ensure the process is rolled out and used by the entire IT organization.</p> <p>Responsible for:</p> <ul style="list-style-type: none"> • Defining the overall mission of the process. • Establishing and communicating the process mission, goals, and objectives to all stakeholders. • Resolving any cross-functional (departmental) issues, including resource availability. • Ensuring consistent execution of the process across the organization. • Reporting on the effectiveness of the process to senior management. • Initiating any process improvement initiatives.
Problem Manager	<p>Responsible for:</p> <ul style="list-style-type: none"> • Managing the day-to-day activities of the process. • Gathering and reporting on process metrics. • Tracking compliance to the process. • Escalating any issues with the process. • Ownership and maintenance of the known error database (KEDB).
Problem Creator	<p>The person who creates the problem record. This is frequently done from within the incident management process.</p>
Problem Support Teams	<p>Responsible for:</p> <ul style="list-style-type: none"> • Investigating assigned problems through to resolution or root cause. • Updating the KEDB with new or updated known errors and workarounds. • Submitting appropriate request(s) for change (RFCs) to resolve problems. • Formally closing all problem records.

2.1 RACI Matrix

ID	Activities	Problem Creator	Problem Manager	Problem Support Teams	Vendor / Third Party Support
PRB 1.0	Problem detection and logging				
PRB 1.1	Detect a problem	A/R	C/I		R
PRB 1.2	Create a problem record	A/R	I		I
PRB 1.3	Categorize problem record	R	A/R		C
PRB 1.4	Prioritize problem record	R	A/R		C
PRB 1.5	Review problem record	I	A/R	C/I	I
PRB 1.6	Assign problem record		A/R	C/I	I
PRB 2.0	Problem investigation and diagnosis				
PRB 2.1	Investigate problem	C	I	A/R	R/C
PRB 2.2	Diagnose problem	I	I	A/R	R/C
PRB 2.3	Document workaround / known error	I	I	A/R	R/C
PRB 3.0	Problem resolution and recovery				
PRB 3.1	Document and submit RFC	I	I	A/R	I
PRB 3.2	Implement resolution or workaround	C	I	A/R	C/I
PRB 3.3	Close problem record	C	C	A/R	C
	R: Responsible, A: Accountable C: Consulted, I: Informed				

3 Problem Management Activity Description

3.1 Process Overview

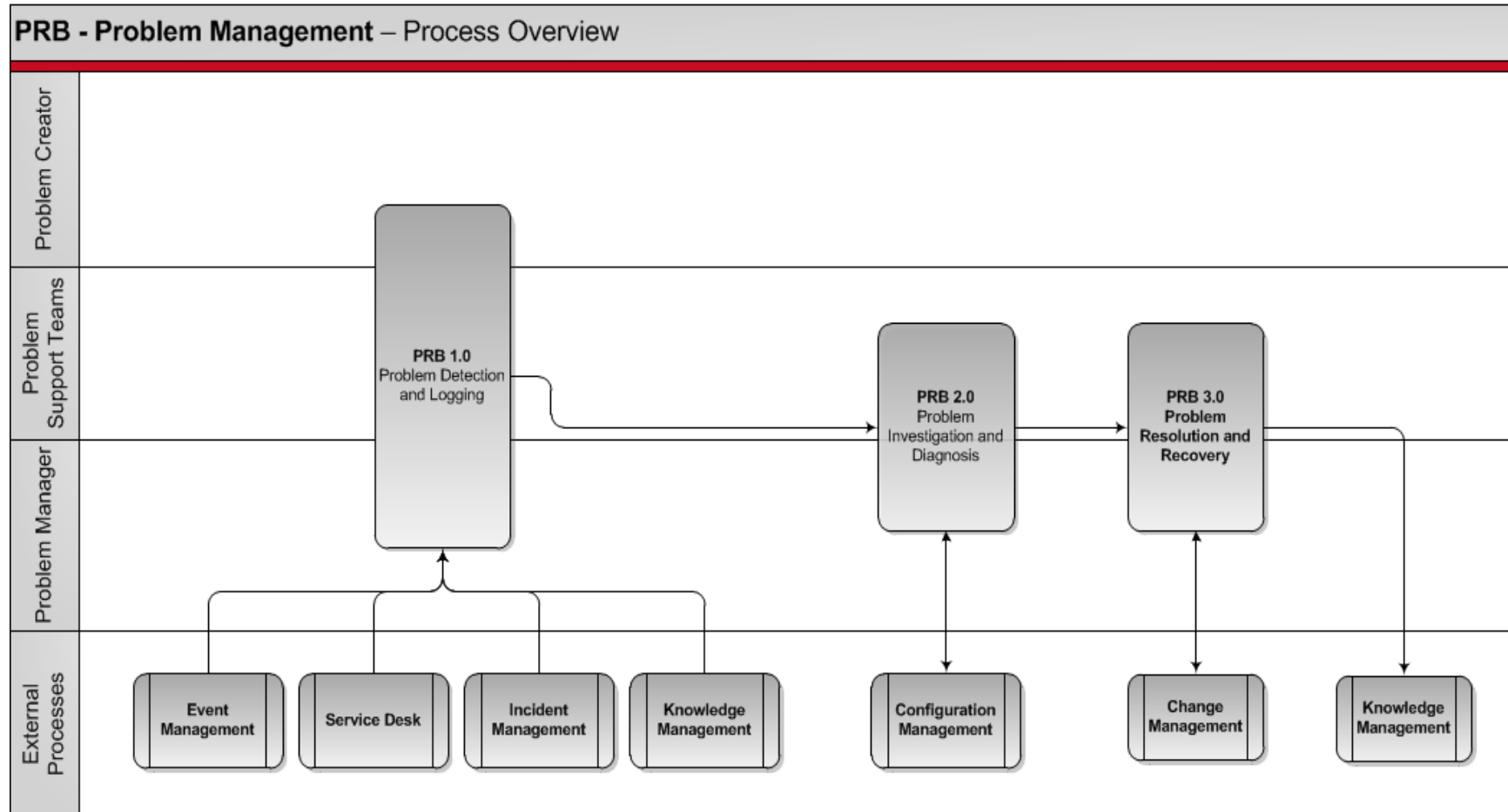


Figure 1.Process Overview

Process Overview Activity Description

ID	Tasks	Description
PRB 1.0	Problem Detection and Logging	<p>Multiple ways of detecting problems exist, including triggers for reactive and proactive problem management. Regardless of the detection method:</p> <ul style="list-style-type: none"> • All relevant details of the problem, including relevant CIs, must be recorded so that the full historic record exists. • The problem record must be <i>related to any incident record</i> from which it was initiated or displays identical symptoms. <p>Problems should be <i>categorized and prioritized in the same way as incidents</i> so that the true nature of the problem can be easily traced in the future and meaningful management information can be obtained. Problem prioritization should also take into account the severity of the problems. Severity in this context refers to how serious the problem is from a service, customer, or infrastructure perspective.</p>
PRB 2.0	Problem Investigation and Diagnosis	<ul style="list-style-type: none"> • Conduct an investigation to diagnose the root cause of the problem. • Document any workarounds to the incidents caused by the problem (either in the problem record or in <i>the related incident record</i>). • When the root cause of the problem has been identified, create a known error record to ensure that if further incidents or problems occur, they can be identified and the service restored more quickly. <ul style="list-style-type: none"> ○ The known error record must be related to the problem record. ○ The known error record should document the status of actions being taken to resolve the problem, its root cause, and workaround.
PRB 3.0	Problem Resolution and Recovery	<p>Once the root cause of a problem has been found and a solution has been developed, it should be applied to resolve the problem.</p> <ul style="list-style-type: none"> • A <i>request for a change</i> (RFC) should be initiated and approved before the solution is applied, if any change in functionality is required. • When a final resolution has been applied successfully, the problem record should be formally closed.

3.2 Problem Detection and Logging

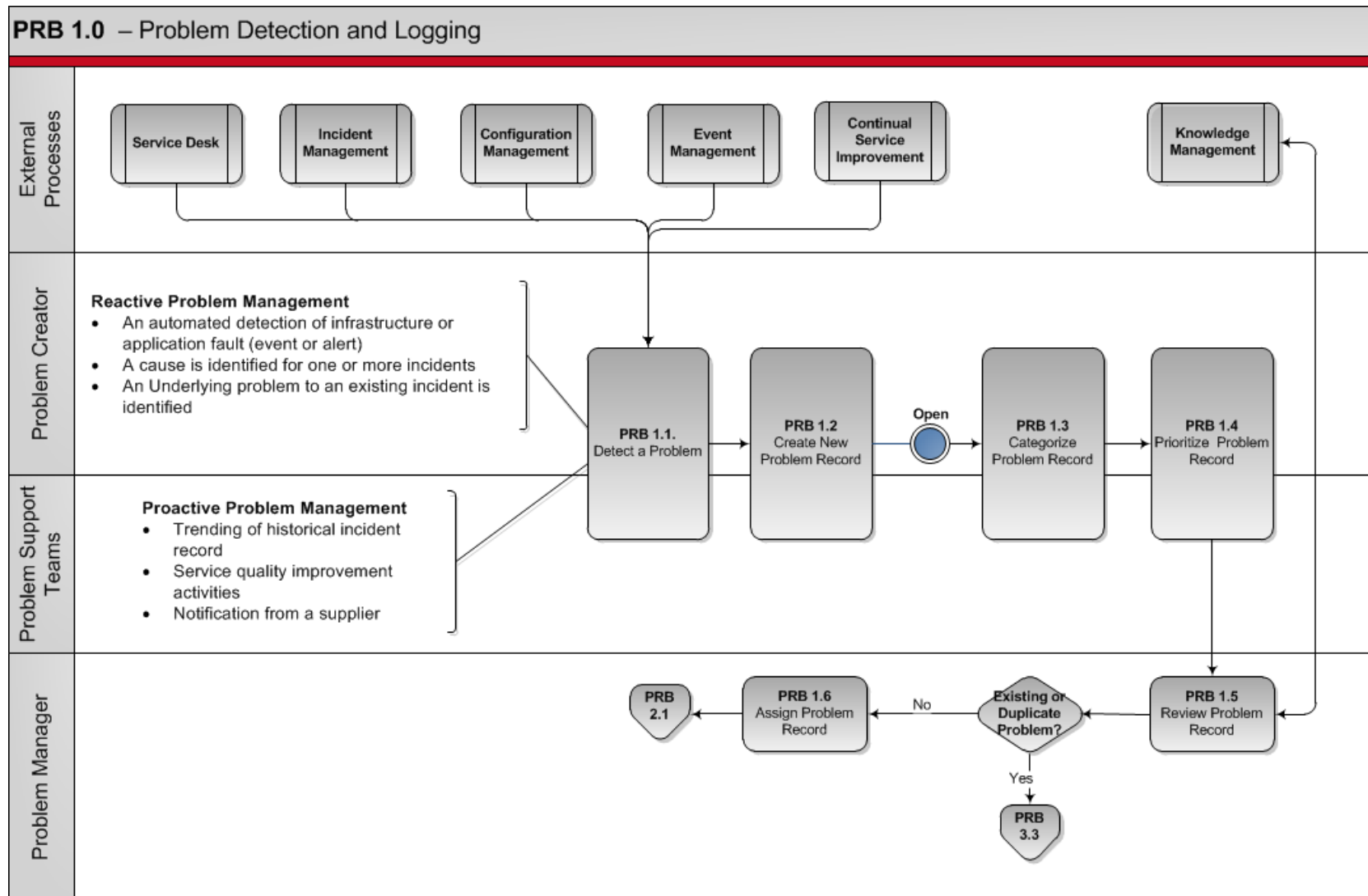


Figure 2. Problem Detection and Logging

Problem Detection and Logging Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
PRB 1.1	Detect a Problem	When a problem is detected, gather all the required information in preparation for creating a new problem record.	Problem Requestor	<ul style="list-style-type: none"> Automated detection of infrastructure or software fault Resolved incident with no identified root cause Cause identified for one or more incidents Known errors that are allowed to transition into the production environment Supplier notification Trend analysis results from historical incident records Service quality improvement activity 	Detected problem
PRB 1.2	Create New Problem Record	Create a new problem record and document all the relevant details of the problem so that a full historical record exists: <ul style="list-style-type: none"> Summarize the problem. Associate related incident(s). Detail all diagnostic or attempted recovery actions. Associate impacted CI(s). 	Problem Requestor	Detected problem	New documented problem record
PRB 1.3	Categorize Problem Record	See Appendix C for categorization techniques.	Problem Requestor	New documented problem record	Categorized problem

ID	Tasks	Procedure	Primary Role	Input	Output
PRB 1.4	Prioritize Problem Record	See Appendix D for prioritization techniques.	Problem Requestor	Categorized problem	Prioritized problem
PRB 1.5	Review Problem Record	<p>Review the problem record to:</p> <ul style="list-style-type: none"> • Ensure it is documented properly. • Confirm problem category and priority are correct; adjust if needed. • Determine if this is problem has occurred previously. • Determine if a workaround or known error exists. <p>Associate to the problem any additional records that may be applicable to investigation and diagnosis activity.</p>	Problem Manager	Prioritized problem	<p>Problem corresponding to an existing known error</p> <p>Or</p> <p>Problem corresponding to an existing active problem</p> <p>Or</p> <p>Reviewed problem record ready to be assigned</p>
PRB 1.6	Assign Problem Record	Assign the problem investigation to the appropriate problem support group or analyst.	Problem Manager	Reviewed problem record	Assigned problem record

3.3 Problem Investigation and Diagnosis

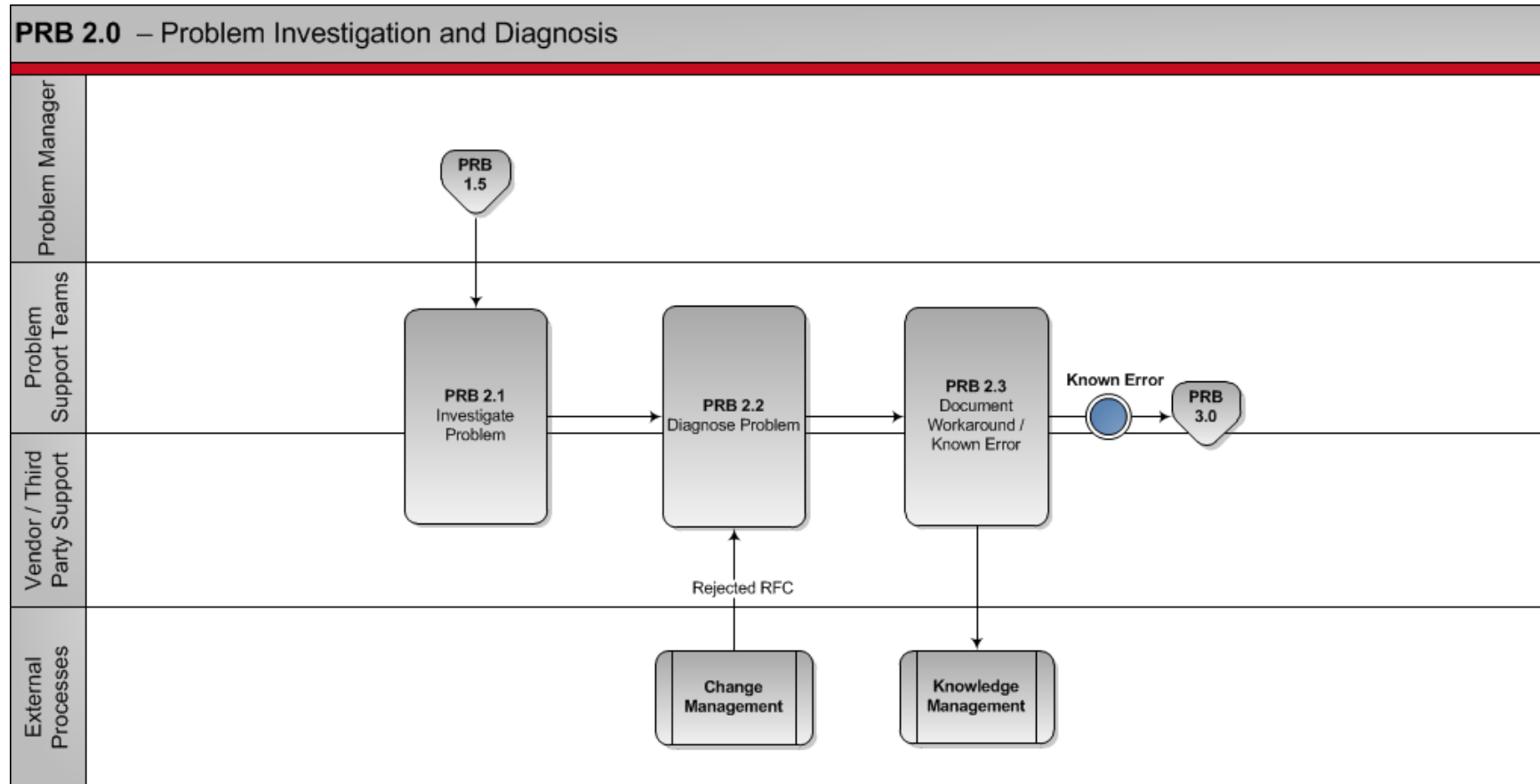


Figure 3. Problem Investigation and Diagnosis

Problem Investigation and Diagnosis Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
PRB 2.1	Investigate Problem	<ul style="list-style-type: none"> Search for any recent changes that might have caused the problem. Review all investigation and diagnosis work notes from associated incident(s). Document all investigation activities and findings. If other resources are required to perform investigation task, create and assign a task to the appropriate resource. 	Problem Support Teams	Assigned problem record Or Alternate solution required for a problem for which a submitted RFC has been rejected Or Permanent solution required for a problem for which only a temporary workaround has been identified	Documented investigation findings
PRB 2.2	Diagnose Problem	When possible: <ul style="list-style-type: none"> Attempt to replicate problem. Identify possible causes and solutions. Test the most probable identified solution or workaround. Validate test results until predefined acceptance criteria are met. Document all diagnosis activities. If other resources are required to perform a diagnosis task, create and assign a task to the appropriate resource or support group. 	Problem Support Teams	<ul style="list-style-type: none"> Documented investigation findings Rejected RFC 	Identified root cause, workaround, or permanent solution
PRB 2.3	Document Workaround / Known Error	<ul style="list-style-type: none"> Document the workaround in the Workaround section of the problem record. If the root cause has been found and a workaround determined, select the Known Error check box within the problem record. 	Problem Support Teams	Tested workaround or solution	Known error submitted for review And/or Communicated workaround

3.4 Problem Resolution and Recovery

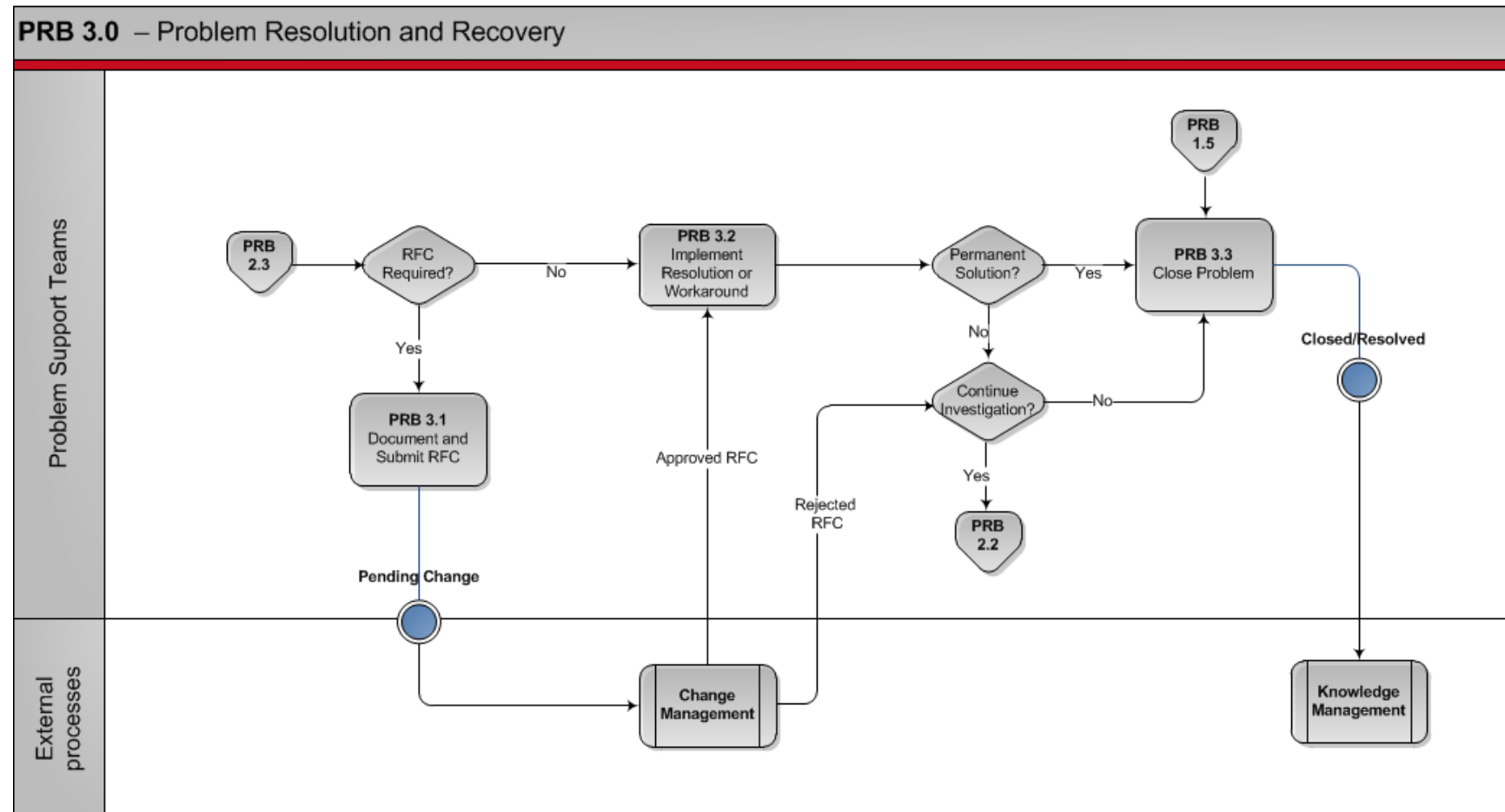


Figure 4. Problem Resolution and Recovery

Problem Resolution and Recovery Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
PRB 3.1	Document and Submit RFC	<ul style="list-style-type: none"> From the problem record, initiate a new request for change (RFC). Submit the RFC. Change the Problem state to Pending Change. <p>If the RFC is rejected, determine whether an alternate solution needs to be identified. If so, return to PRB 2.1 – Investigate Problem.</p>	Problem Support Teams	<p>Documented known error</p> <p>And/or</p> <p>Communicated workaround</p>	RFC submitted to change management process
PRB 3.2	Implement Resolution or Workaround	<p>Implement the resolution or workaround.</p> <p>If a workaround has been implemented and a permanent solution is required, return to PRB 2.1 – Investigate Problem.</p>	Problem Support Teams	<ul style="list-style-type: none"> Identified solution or workaround Approved RFC 	<p>Temporary workaround</p> <p>Or</p> <p>Permanent solution implemented</p>
PRB 3.3	Close Problem	<ul style="list-style-type: none"> The problem and any associated known error record are reviewed and closed. Related incidents where State is Awaiting Problem can be automatically closed. See Closing Related Incidents from a Problem in the ServiceNow Wiki for a description of how to use this feature. 	Problem Manager	<ul style="list-style-type: none"> Problem with existing known error Permanent solution successfully implemented Updated known error 	Closed problem record

4 Process Control

4.1 KPIs

KPIs are best represented as trend lines and tracked over time. They provide information on the effectiveness of the process and the impact of continuous improvement efforts.

KPI/Metric	Purpose
Percentage of problems resolved within target time by priority.	Measure of how well problem SLAs are achieved.
Total number of open problems.	A control measure that reflects the workload of problem management.
Total number of incidents.	Incidents are frequently caused by problems. The reduction of this measure is the prime means of establishing the effectiveness of the problem management process.
Number and percentage of incidents resolved by known errors.	Measures the effectiveness of problem management in supporting the timely resolution of incidents.

4.2 Operational Data

Active problems that require visibility, oversight, and possible management intervention are best tracked on a dashboard or homepage that is monitored by the Problem Manager.

Item	Purpose
List of active <i>major problems</i> .	Provides high visibility to major problems in progress.
List of active problems that have missed target resolution time.	Provides quick view of problems that need attention to prevent further delay of resolution.
Aged list of backlogged problems.	Provides visibility to unassigned work.
Top 5 incident categories reported for the period (pie chart).	Provides assistance in proactively identifying trends and possible problem areas for further analysis.


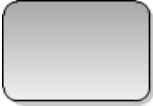






4.3 Reports and Homepages

There are numerous reports available in the base ServiceNow system that can be used to generate charts, can be published to a URL, or can be scheduled to run and distributed at regular intervals. Users can also create custom reports. See [Creating Reports](#) in the ServiceNow Wiki for more detail on this capability.

In addition to reports, each user can create a personal homepage and add gauges containing up-to-the-minute information about the current status of records that exist in ServiceNow tables. See [Customizing Homepages](#) in the ServiceNow Wiki for details.

Appendices

Appendix A: Document Conventions

Symbol	Description
	Process start / end point: Represents the starting and ending point of the process.
	Process Activity/Task: Presents an activity or task that needs to be accomplished to produce a specific outcome.
	Predefined external process or organization: Indicated a contribution from an external process or organization.
	Decision: Indicates that a question needs to be answered in order to determine the in order to identify the following Activity/task in the process. The answers are indicated on the different connectors attached to the decision box. Every answer is linked to an associated Activity/task.
	Off-page reference: Indicates a reference to another diagram within the same process. The number of the referenced diagram is indicated in the shape.
	On-page reference: Indicates a link to another activity within the same diagram.
	Association: Represented by a dotted or dashed line, it indicates an association or a relation between the connected, processes, tasks or activities.
	Sequence flow: Is represented with a solid line and arrowhead, and shows in which order the activities are performed.

Appendix B: Glossary of Terms and Acronyms

Term	Acronym	Definition
Alert		A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.
Assessment		Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Attribute		A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in the configuration management database (CMDB).
Back-out		An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful.
Baseline		<p>(ITIL <i>Continual Service Improvement</i>) (ITIL <i>Service Transition</i>) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:</p> <ul style="list-style-type: none"> ▪ An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan ▪ A performance baseline can be used to measure changes in performance over the lifetime of an IT service ▪ A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails.
Category		A named group of things that have something in common. Categories are used to group similar things together.
Change		The addition, modification, or removal of anything that could have an effect on IT services.
Change Advisory Board	CAB	A group of people who support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties such as suppliers.
Change Management	CHG	The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

Term	Acronym	Definition
Change Record		A record containing the details of a change. Each change record documents the life cycle of a single change. A change record is created for every request for change.
Change Request		See Request for Change.
Configuration Record	CI Record	A record containing the details of a configuration item. Each configuration record documents the lifecycle of a single configuration item. Configuration records are stored in a configuration management database and maintained as part of a configuration management system.
Configuration Type	CI Type	A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, and user.
Classification		The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, incidents, problems, and changes are usually classified.
Closed		The final status in the life cycle of an incident, problem, or change. When the status is closed, no further action is taken.
Closure		The act of changing the status of an incident, problem, or change to closed.
Configuration Item	CI	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 life cycle by service asset and configuration management.
Configuration Management Database	CMDB	A database used to store configuration records throughout their life cycle. The configuration management system maintains one or more CMDBs. Each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management System	CMS	A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS also includes information about incidents, problems, known errors, changes, and releases. It may contain data about employees, suppliers, locations, business units, customers, and users. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.

Term	Acronym	Definition
Configuration Record		A record containing the details of a configuration item. Each configuration record documents the life cycle of a single configuration item.
Continual Service Improvement	CSI	Ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness, and cost effectiveness.
Customer		Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees to the service level targets. The term is also sometimes used informally to mean user, for example, 'This is a customer-focused organization.'
Diagnosis		A stage in the incident and problem life cycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.
Effectiveness		A measure of whether the objectives of a process, service, or activity have been achieved. An effective process or activity is one that achieves its agreed objectives. <i>See also</i> Key Performance Indicator.
Efficiency		A measure of whether the right amount of resource has been used to deliver a process, service, or activity.
Emergency Change		A change that must be introduced as soon as possible, for example to resolve a major incident or implement a security patch. The change management process normally has a specific procedure for handling emergency changes.
Employee Self Service	ESS	A module in ServiceNow that allows users to make requests, view articles, log incidents, and search the knowledge base through a user-friendly website called the Employee Self-Service Portal (ESS Portal).
Event		A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool.
Impact		A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
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.

Term	Acronym	Definition
Key Performance Indicator	KPI	A metric that is used to help manage an IT service, process, plan, project, or other activity. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	KE	A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their life cycle by problem management. Development groups or suppliers may also identify known errors.
Major Incident		The highest category of impact for an incident. A major incident results in significant disruption to the business.
Metric		Something that is measured and reported to help manage a process, IT service, or activity.
Policy		Formally documented management expectations and intentions. Policies are used to direct decisions and to ensure consistent development and implementation of processes, standards, roles, activities, IT infrastructure, and so on.
Post-implementation Review	PIR	A review that takes place after a change or a project has been implemented. It determines if the change or project was successful and identifies opportunities for improvement.
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. For example, the SLA may state that priority 2 incidents must be resolved within 12 hours.
Problem		A cause of one or more incidents. The cause is not usually known at the time a problem record is created. The problem management process is responsible for further investigation.
RACI	RACI	A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted, and informed.
Release		One or more changes to in IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, process, and other components.
Request for Change	RFC	A formal detailed proposal for a change to be made. The term is often misused to mean change record or the change itself.
Restore		Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.

Term	Acronym	Definition
Risk		A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
Role		A set of responsibilities, activities, and authorities assigned to a person or team. A role is defined in a process or function. One person or team may have multiple roles. For example, a single person may carry out the role of configuration manager and change manager.
Root Cause		The underlying or original cause of an incident or problem.
Root Cause Analysis	RCA	An activity that identifies the root cause of an incident or problem. Root cause analysis typically concentrates on IT infrastructure failures.
Service		A means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks.
Service Desk		The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and also handles communication with the users.
Service Level		Measured and reported achievement against one or more service level targets.
Service Level Agreement	SLA	An agreement between an IT service provider and a customer. A service level agreement describes the IT service; documents service level targets, and specifies the responsibilities of the IT service provider and the customer.
Service Request		A formal request from a user for something to be provided, for example, a request for information or advice; to reset a password; or to install a workstation for a new user.
Stakeholder		A person who has an interest in an organization, project, or IT service. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, or others.
User		A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.
Workaround		Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available, for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

Appendix C: Problem Categorization

Problem categorization can be used to drive assignment in the problem management process as well as establish trends (incident types/frequencies) for use in proactive problem management, supplier management, and other ITSM activities. Problem categorization can occur several ways:

- *Automatically categorize and assign the problem based on the incident* that initiated the problem.
- Manually select the **Category** from predefined lists. This method is identical to the method used in the Incident application.
 - See [Categorizing Incidents](#) in the ServiceNow Wiki for a list of the category values provided in the base system.
 - See [Assigning Incidents](#) in the ServiceNow Wiki for a description of how to automate assignment based on categorization.
- *Automatically categorize and assign the problem based on the CI* that is identified in the problem record. With this technique, the problem management process inherits the same categorization schema as CIs maintained through the configuration management process, and the category of a problem is automatically determined once the affected CI is identified in the problem record. This technique ensures more accurate and consistent categorization of problems and supports a CI-centric approach to IT service management.

Appendix D: Problem Prioritization

Problems should be prioritized in the same way incidents are prioritized. ITIL suggests that priority be made dependent on impact and urgency where:

- **Impact** - The effect on business that a problem has
- **Urgency** - The extent to which the problem's resolution can bear delay.

Priority is generated from urgency and impact according to the following table:

	Urgency High	Urgency Medium	Urgency Low
Impact High	Priority 1	Priority 2	Priority 3
Impact Medium	Priority 2	Priority 3	Priority 4
Impact Low	Priority 3	Priority 4	Priority 5

Problem prioritization should also take into account the frequency and impact of related incidents and can consider the difficulty of the proposed solution. Difficulty can be determined by considering:

- Can the system be recovered or does it need to be replaced?
- How much will the solution cost to implement?
- How many people, with what skills, will be needed?
- How long will it take?
- How extensive is the problem (for example, how many CIs are affected)?