Checklist of Mandatory Documentation Required by ISO/IEC 20000-1:2011

WHITE PAPER
# Table of Contents

- Executive summary .................................................................................................................. 3
- Introduction ............................................................................................................................... 3
- Which documents and records are required? ........................................................................... 4
  - Mandatory documents .......................................................................................................... 4
  - Mandatory records ................................................................................................................ 6
- Commonly used non-mandatory documents .......................................................................... 8
- How to structure documents and records .............................................................................. 9
- Conclusion ............................................................................................................................... 21
- Sample documentation templates .......................................................................................... 21
- References .................................................................................................................................. 21
Executive summary

Aspiration for excellence while delivering IT services is the ultimate goal of every competitive IT organization in today’s business world. ISO 20000 provides an excellent framework to achieve exactly that. It describes a set of requirements your organization must fulfill in order to implement a management system that will help you introduce a managed IT service management (ITSM) environment. This white paper is designed to help top management and employees involved in ISO 20000-based Service Management System (SMS) implementation and to clear up any misunderstandings regarding documents required by the standard.

In this document you will find an explanation of which documents are mandatory according to the ISO 20000 standard, and which non-mandatory documents are commonly used in the SMS implementation, in the same order and numbered clauses as in ISO 20000. In addition, you’ll see links to additional learning materials.

Introduction

While trying to fulfill standard requirements, organizations have a tendency to generate too many documents in order to be on the “safe side.” This is counterproductive, because it makes the implemented processes and respective SMS hard to use and maintain, as well as making the SMS a bureaucratic burden. While taking such approach, organizations are missing a chance to improve their ITSM for their own benefit, as well as that of their customers.

In this white paper you will find, explained in plain English, what the minimum ISO 20000 requirements for the documentation are, as well as a list of documents that are commonly in place and can help you make your SMS more efficient.
Which documents and records are required?

**Mandatory documents**

<table>
<thead>
<tr>
<th>Mandatory Documents</th>
<th>ISO 20000 Clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Management System (SMS) Policy</td>
<td>4.1.1.a), 4.1.2, 4.1.4</td>
</tr>
<tr>
<td>Service Management System (SMS) Plan</td>
<td>4.1.1, 4.1.4, 4.2, 4.3.1, 4.4.1, 4.4.2, 4.5.1, 4.5.2, 4.5.3, 5.3.h), 6.2</td>
</tr>
<tr>
<td>Procedure for Document and Record Control</td>
<td>4.3.2 and 4.3.3</td>
</tr>
<tr>
<td>Communication Procedure</td>
<td>4.1.2.e), 4.1.3.b)</td>
</tr>
<tr>
<td>Service Level Requirements</td>
<td>5.2, 6.1</td>
</tr>
<tr>
<td>Service Improvement Plan</td>
<td>4.5.5.1, 4.5.5.2</td>
</tr>
<tr>
<td>Procedure for Internal Audit</td>
<td>4.5.4.1,4.5.4.2, 4.5.4.3,6.6.1, 6.6.2, 6.6.3</td>
</tr>
<tr>
<td>Continual Service Improvement Process</td>
<td>4.5.5.1, 4.5.5.2</td>
</tr>
<tr>
<td>Training and Awareness Plan</td>
<td>4.4.2, 4.5.2.l)</td>
</tr>
<tr>
<td>Corrective and Preventive Action</td>
<td>6.6.1., 6.6.2, 6.6.3, 4.5.5.1, 4.5.5.2</td>
</tr>
<tr>
<td>Risk Assessment and Treatment</td>
<td>6.3.1, 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Service Catalogue</td>
<td>6.1</td>
</tr>
<tr>
<td>Service Level Management Process</td>
<td>4.3.1, 5.3.i); 6.1, 5.3.j)</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>6.1, 8.1</td>
</tr>
<tr>
<td>Operational Level Agreement</td>
<td>6.1</td>
</tr>
<tr>
<td>Mandatory Documents</td>
<td>ISO 20000 Clause</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Design and Transition of New or Changed Services</td>
<td>4.3.1, 5.1, 5.3.a), 5.3.b), 5.3.c), 5.2.b)</td>
</tr>
<tr>
<td>Service Continuity and Availability Management Process</td>
<td>4.3.1, 6.3.1 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Budgeting and Accounting for Services Process</td>
<td>4.3.1, 6.4</td>
</tr>
<tr>
<td>Capacity Management Process</td>
<td>4.3.1, 6.5</td>
</tr>
<tr>
<td>Information Security Management Process</td>
<td>4.3.1, 6.6.1, 6.6.2, 6.6.3</td>
</tr>
<tr>
<td>Information Security Management Policy</td>
<td>6.6.1, 6.6.2, 6.6.3</td>
</tr>
<tr>
<td>Business Relationship Management Process</td>
<td>4.3.1, 7.1</td>
</tr>
<tr>
<td>Supplier Management Process</td>
<td>4.3.1, 7.2</td>
</tr>
<tr>
<td>Incident and Service Request Management Process</td>
<td>4.3.1, 8.1, 6.6.3</td>
</tr>
<tr>
<td>Problem Management Process</td>
<td>4.3.1, 8.2, 8.1</td>
</tr>
<tr>
<td>Configuration Management Process</td>
<td>4.3.1, 9.1, 5.1</td>
</tr>
<tr>
<td>Change Management Process</td>
<td>4.3.1, 4.3.2.d), 5.1, 5.2, 5.3, 5.4, 6.1, 6.2, 6.3.2,</td>
</tr>
<tr>
<td></td>
<td>6.4, 6.5, 6.6.3, 7.1, 7.2, 8.2, 9.1, 9.1.g), 9.2, 9.3</td>
</tr>
<tr>
<td>Release and Deployment Management Process</td>
<td>4.3.1, 5.3.a), 5.3.b), 5.3.k), 9.3</td>
</tr>
<tr>
<td>Supplier Contract</td>
<td>7.2</td>
</tr>
<tr>
<td>Customer Portfolio</td>
<td>7.1</td>
</tr>
<tr>
<td>List of Services</td>
<td>4.5.2.f), 7.1</td>
</tr>
<tr>
<td>Configuration Management Database (CMDB)</td>
<td>9.1</td>
</tr>
<tr>
<td>Release and Deployment Planning</td>
<td>9.3</td>
</tr>
<tr>
<td>Service Design Package</td>
<td>5.1, 5.3.c), 5.3.d), 5.2</td>
</tr>
<tr>
<td>IT Service Continuity Plan</td>
<td>6.2, 6.3.1, 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Mandatory Documents</td>
<td>ISO 20000 Clause</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Customer Release and Deployment Policy</td>
<td>9.3</td>
</tr>
<tr>
<td>Availability Plan</td>
<td>6.3, 6.3.1, 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Capacity Plan</td>
<td>6.5</td>
</tr>
<tr>
<td>Change Management Policy</td>
<td>4.3.2.d), 5.1, 5.2, 5.3, 5.4, 6.1, 6.2, 6.3.2, 6.4, 6.5, 6.6.3, 7.1, 7.2, 8.2, 9.1, 9.1.g), 9.2, 9.3</td>
</tr>
<tr>
<td>Annual Internal Audit Program</td>
<td>4.5.4.1, 4.5.4.2, 4.5.4.3, 6.6.1, 6.6.2, 6.6.3</td>
</tr>
</tbody>
</table>

## Mandatory records

<table>
<thead>
<tr>
<th>Mandatory Records</th>
<th>ISO 20000 Clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Report</td>
<td>6.1</td>
</tr>
<tr>
<td>IT Service Continuity Plan Test and Review Report</td>
<td>6.3.1, 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Customer Complaint Report</td>
<td>6.2, 7.1</td>
</tr>
<tr>
<td>Internal Audit Report</td>
<td>4.5.4.1, 4.5.4.2, 4.5.4.3, 6.6.1, 6.6.2, 6.6.3</td>
</tr>
<tr>
<td>Management Review Minutes</td>
<td>4.5.4.3, 4.1.2</td>
</tr>
<tr>
<td>Availability Measurement Report</td>
<td>6.3.3</td>
</tr>
<tr>
<td>Corrective and Preventive Action</td>
<td>6.6.1, 6.6.2, 6.6.3, 4.5.5.1, 4.5.5.2</td>
</tr>
<tr>
<td>Supplier Performance Report</td>
<td>7.2</td>
</tr>
<tr>
<td>Incident Record</td>
<td>8.1, 6.6.3</td>
</tr>
<tr>
<td>Service Request Record</td>
<td>8.1</td>
</tr>
<tr>
<td>Known Error Record</td>
<td>8.2</td>
</tr>
<tr>
<td>Mandatory Records</td>
<td>ISO 20000 Clause</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Request for Change and Change Record</td>
<td>9.2</td>
</tr>
<tr>
<td>Problem Record</td>
<td>8.2</td>
</tr>
<tr>
<td>Service Performance Review Report Template</td>
<td>7.1</td>
</tr>
</tbody>
</table>

These are the documents and records that are required to be maintained for the ISO 20000 Service Management System, but you should also maintain any other records that you have identified as necessary to ensure your management system can function, be maintained, and improve over time.

The number of documents can vary due to the fact that several documents can be combined into a single one.

Records can be recorded as documents, but also as records in the scope of the ITSM tool.
Commonly used non-mandatory documents

<table>
<thead>
<tr>
<th>Documents</th>
<th>ISO 20000 Clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAC Template</td>
<td>5.4, 5.2.i)</td>
</tr>
<tr>
<td>Test Plan</td>
<td>5.2.h), 5.4</td>
</tr>
<tr>
<td>Business Impact Analysis and Recovery</td>
<td>6.3.1, 6.3.2, 6.3.3</td>
</tr>
<tr>
<td>Budgeting and Controlling Template</td>
<td>6.4</td>
</tr>
<tr>
<td>Capacity Measurement Report</td>
<td>6.5</td>
</tr>
<tr>
<td>Customer Satisfaction Survey</td>
<td>6.2, 7.1</td>
</tr>
<tr>
<td>Supplier Agreement Portfolio</td>
<td>7.2</td>
</tr>
<tr>
<td>Incident Catalogue Template</td>
<td>8.1, 6.6.3</td>
</tr>
<tr>
<td>Major Incident Report Template</td>
<td>8.1</td>
</tr>
<tr>
<td>Service Request Catalogue Template</td>
<td>8.1</td>
</tr>
<tr>
<td>Problem Catalogue Template</td>
<td>8.2</td>
</tr>
<tr>
<td>Minutes of Meeting CAB</td>
<td>9.2</td>
</tr>
<tr>
<td>Change Schedule</td>
<td>9.2</td>
</tr>
</tbody>
</table>
How to structure documents and records

Service Management System (SMS) Policy

The SMS Policy is usually a short, top-level document describing the purpose of the SMS. In this document you should define the purpose, direction, principles, and basic rules for IT Service Management in your organization.

Find out more in the article: SMS Policy – How to create it according to ISO 20000.

Service Management System (SMS) Plan

This is the main document where you will define how the SMS will be established. The aim of this document is to define the scope, requirements, responsibilities, and resources needed to run the services. Although the standard’s requirements regarding the SMS Plan are extensive, this document is usually four to five pages long and references to other stand-alone documents.

Procedure for Document and Record Control

This is usually a stand-alone procedure. The purpose of this procedure is to ensure control over the creation, approval, distribution, usage, and updates of documents and records (stored in any possible form – paper, audio, video, etc.) used in the Service Management System (SMS).

If you have already implemented some other standard, e.g., ISO 9001 or ISO 27001, you can use the same procedure for all the management systems.

Communication Procedure

The Communication Procedure doesn’t need to be extensive, but it should define communication relevant to the SMS (e.g., who communicates which topics, how often, and to whom), how it is implemented (usually – which technology supports different kinds of communication), and how it is used.

Read the articles: IT Service Management communication according to ISO 20000 and Communication inside IT Service Management team – setup of joint vocabulary and criteria to learn more.
Service Level Requirements

This is the document where all requirements for a particular service should be documented. This document is relevant for the service throughout its lifecycle. Therefore, the Service Level Requirements document should capture all details of the service in order to build, test, deploy, maintain, and improve the service. It can be in the form of a document or spreadsheet.

Find out more in the article: Service Level Requirement (SLR) as origin of the SLA content.

Service Improvement Plan

Although a mandatory requirement according to the standard, this document will enable you to track all improvement initiatives. It shouldn’t be extensive, but it must include all available information about the improvement initiative, applicable (implementation) milestones, responsibilities, etc.

Find out more in the article: Service Improvement Plan – For the sake of improvements.

Procedure for Internal Audit

This procedure is, usually, a stand-alone document that can be two to three pages long, and has to be written before the internal audit begins. Similar to the Procedure for Document Control, one Procedure for Internal Audit can be used for all management systems.

Learn more in the article: ISO 20000 internal audit – What is it and why is it important?

Continual Service Improvement Process

The standard requires a procedure and a policy for the maintenance and improvement of the SMS. However, since they are not necessarily extensive documents, they could be combined into a single document with the common goal of defining the purpose, scope, principles, and activities of the Continual Service Improvement (CSI) process.

For more information about the Continual Service Improvement Process, see the following articles:

- ITIL® Continual Service Improvement – the never-ending story
- ITIL® Continual Service Improvement – don’t lose the momentum
- ITIL® CSI 7-step improvement process: What is it all about?
- ITIL® CSI 7-step improvement process: How to analyze and present findings
- ITIL® CSI 7-step improvement process: Start gathering the data
- Improvements in ISO 20000 vs. CSI in ITIL®
Training and Awareness Plan

This is the document that will help you to keep control over planned trainings and awareness campaigns inside the SMS. The Training Plan is usually made together with the HR department.

Read this article to learn more: How to perform ISO 20000 training and awareness.

Corrective and Preventive Action Form

This is the document that will help you track activities related to corrective and preventive actions. It should be a simple, one-page document, which includes a description, actions to be taken, roles and responsibilities relevant to the corrective or preventive action, etc.

Risk Assessment and Treatment

This is the document that will enable risk assessment and definition of risk reduction measures. It could be written in a table (spreadsheet) form.

Service Catalogue

The Service Catalogue lists all the services in one place – this includes customer-facing as well as internal services. Customer-facing services are written in business language (understandable by the customer), and internal (or supporting services) use more technical vocabulary. One of the approaches could be to create a spreadsheet in order to easily define dependencies between services and service components.

For more details about service catalogues, see the following articles:

- How to overcome barriers while implementing the Service Catalogue according to ITIL®
- Choosing four main inputs for the ITIL®/ISO 20000 Service Catalogue to avoid bureaucracy
- Service Catalogue – Defining the service
- Service Catalogue – a window to the world

Service Level Management Process

The aim of this document is to define the purpose, scope, principles, and activities of the Service Level Management (SLM) Process. Besides setting up the process and its activities, as well as roles and responsibilities, this document defines service providers’ relationships with the customer (documented in the Service Level Agreement) and internal supporting groups.
Read these articles to learn more about the Service Level Management Process:

- What is the relationship between Service Level Management and the Service Catalogue in ISO 20000?
- ITIL® Service Level Management – making sure that what you want is what you get
- Who is your ideal ITIL®/ISO 20000 Service Level Manager?

Service Level Agreement

This document defines the relationship between the IT service provider and the customer. It contains all relevant parameters in order to manage service delivery according to customers’ requirements. This document contains common legal parameters typical for legally binding documents and, in agreement with the customer, it contains measurable service level parameters.

Read more about the Service Level Agreement here:

- What’s the content of an ITIL®/ISO 20000 SLA?
- ITIL® – Service Level Agreements: Designing frameworks

Operational Level Agreement

This document defines the relationship between the service provider and another part of the same organization. It contains more technical descriptions of the service and it’s not a legally binding document.

Read the article SLAs, OLAs and UCs in ITIL® and ISO 20000 to learn more.

Design and Transition of New or Changed Services

This process descriptions are a cornerstone of a new or change service that needs to be implemented. Therefore, all necessary details related to planning, design, and transition to a new service should be included.

Read more here: Design and transition of new or changed services in ISO 20000.

Service Continuity and Availability Management Process

This document covers both IT service continuity and IT service availability in one document. It includes a policy and all relevant activities in order to achieve the required continuity and availability of the services. The length of the document depends on the business requirements. The document content is related to the IT Service Continuity and Availability Plan.
Read more about the Service Continuity and Availability Management Process in these articles:

- IT Service Continuity Management – waiting for the big one
- Availability Management – calculating for improvement

**Budgeting and Accounting for Services Process**

In this document you can include the Financial Management Policy, but you should certainly define budgeting and accounting activities with related roles and responsibilities.

Read more here:

- Financial Management for IT services – theory and practice
- ITIL® Financial Management – Charging as a moment of truth

**Capacity Management Process**

In this document you should include all activities of the Capacity Management Process and related roles and responsibilities. The Capacity Plan is, usually, a stand-alone document.

Read more in the article: ITIL® and ISO 20000 – How to set up the Capacity Management process

**Information Security Management Process**

If you have implemented ISO 27001 – you have almost all of the requirements fulfilled. Otherwise, this document should define security-related policies, activities, and controls (applied to manage security risks) and their relationships with other processes.

Learn more in these articles:

- Security incidents – How to approach them using ITIL® and ISO 20000
- If anything shouldn’t be taken for granted... it’s Information Security Management

**Information Security Management Policy**

This is the main document for information security and is written as a stand-alone document. The policy defines security objectives that need to be achieved and refers to security requirements, risk management, and internal audit.
Business Relationship Management Process

The process description can also include a policy, and should include a description of activities, roles, and their responsibilities to establish relationships with customers, users, and interested parties.

Read more here:

- Taking care of relationships with ISO 20000
- Business Relationship Management, Service Level Management... Too much management?

Supplier Management Process

ISO 20000 sets clear responsibilities towards IT service provider suppliers and their sub-suppliers. This process document ensures that this relationship is controlled and managed, as well as confirming that agreements and monitoring are in place.

Find out more in these articles:

- ISO 20000 Supplier Management – You lead the game
- ITIL® Supplier management – the third party you depend on
- ITIL® Supplier Management and Service Level Management – How to put the two in balance

Incident and Service Request Management Process

The Incident and Service Request Management Process is the most exposed process towards users and customers. Besides fulfilling the standard’s requirements, it is important to include all relevant activities and parameters to have a functional and well-managed process.

Learn more in these articles:

- ISO 20000 Incident and Service Request Management – Increasing efficiency with information flow
- How to choose an ITIL/ISO 20000 Incident Manager: 5 main characteristics
- 5 biggest challenges while setting up the Incident Management process
- Major Incident Management – when the going gets tough...
- ITIL® Request Fulfillment: a quick win for customer satisfaction

Problem Management Process

The Problem Management Process document should define problem identification and activities (both proactive as well as reactive ones) in order to manage problem resolution and minimize the impact of incidents and problems.
Read more in these articles:

- How to resolve the problem ticket/record according to ITIL®/ISO 20000
- How to avoid unsatisfied customers by managing problems and incidents according to ISO 20000
- ITIL® and ISO 20000 Problem Management – Organizing for problem resolution
- ITIL® Reactive and Proactive Problem Management: Two sides of the same coin

Configuration Management Process

Since Configuration Management is the basis for most of the ISO 20000 processes, particular care should be taken while setting up this process. Therefore, this document can be more detailed, but it should at least define the purpose, scope, principles, and activities of the Configuration Management Process.

Learn more in these articles:

- What is the role of the Service Asset and Configuration Manager according to ITIL®/ISO 20000?
- Knowing your herd – Service Asset and Configuration Management (SACM)

Change Management Process

Changes are one of the most prevailing sources of incidents. Therefore, the Change Management process should include regulations, authorities, descriptions of activities, roles, responsibilities, measurements, and metrics for the process. The Change Policy could be a stand-alone document, but that doesn’t necessarily need to be so.

Read more in these articles:

- How to overcome barriers while implementing the ITIL®/ISO 20000 Change Management process
- ITIL®/ISO 20000: What is the job of the Change Manager?

Change Management Policy

The Change Management Policy is a mandatory document according to the standard, and it should provide defined Configuration Items (CIs) that are under the control of Change Management, as well as criteria to determine changes with the potential to have major impact on services or customers. Additionally, this document regulates the authorization of various types of changes.

Find out more in these articles:

- 5 benefits of ITIL® Change Management implementation
- How to manage Emergency Changes as part of ITIL® Change Management
- ITIL® V3 Change Management – at the heart of Service Management
Release and Deployment Management Process

This process relies on Configuration Management and Change Management, and is an executable process for the implementation of new or changed services. Therefore, clear interfaces to other processes, activities, and roles and responsibilities should be defined.

Supplier Contract

This document is the basis for an IT service provider to define its relationship with its supplier. Because it’s a legally binding document, respective clauses must be present. From the document’s content, responsibilities of both parties should be clear.

Learn more in these articles:

- ITIL® Release and Deployment Management Part I – General principles and service testing
- ITIL® Release and Deployment Management Part 2 – deployment methods and early life support

Customer Portfolio

This is the list of all customers, their contracts, the services they use, contact partners and business relationship managers inside the organization. For easier maintenance and a clear overview, this document could be in a spreadsheet form.

Training and Awareness Plan

Usually, this plan is made together with HR and presents an annual plan of needed education and training. It’s usually made in a table form in order to have a clear overview.

Read more about training and awareness in the article: How to perform ISO 20000 training and awareness.

List of Services

This is the list of services that needs to provide an overview of provided services and the customers who are using them. It’s usually made in a spreadsheet form.

Read the article: Service Portfolio Management – Services, where do they come from? to learn more.
Configuration Management Database (CMDB)

If you are not using an ITSM tool, then this spreadsheet can help you to record the required and most important parameters of CIs in one place.

Learn more here: Knowing your herd – Service Asset and Configuration Management (SACM).

Release and Deployment Planning

This is the formal plan for a particular release. In order for the release to be deployed in a controlled manner, many details need to be planned. This document keeps track of all necessary details for a particular release.

Service Design Package

The Service Design Package (SDP) is a document where all aspects of a new or changed service are documented. It helps to document all service-related information in one place. Depending on the service, it could be quite extensive.

To learn more, read the article: ITIL® Service Design Package – everything under one roof.

IT Service Continuity Plan

After IT service continuity is set (using a process description), a detailed plan should be developed and tested. This is the document with a detailed description of how to achieve the agreed IT service continuity.

Customer Release and Deployment Policy

Based on the release and deployment process (and related policy), a plan for a particular service, i.e., customer, should be made. This document contains all the necessary details for release and deployment planning in order to ensure that releases for a particular customer are planned, built, tested, and deployed through an established process.

Availability Plan

Availability of the service is one of the basic service requirements, often part of the SLA and reports sent to customers. Therefore, careful planning regarding how to fulfill requirements is needed. This is a document that ensures that existing and future availability requirements are provided cost effectively, availability of current services is improved, and availability level of new services is defined.

Read more in the article: ITIL® Availability Plan – A document you need, but probably don’t have.
Capacity Plan

The Capacity Plan should define how to manage resources needed to deliver IT services, analyze data, and define a long-term approach to satisfy capacity requirements for services.

Learn more about the Capacity Plan in the article: ITIL® Capacity Plan – A document you need, but probably don’t have.

Annual Internal Audit Program

Internal audits should be planned. This document provides a timetable of internal audits, auditor names, scope, objectives, etc. To maintain a clear overview, it’s advisable to create a program in table form.

Learn more about the audit checklist (needed for an audit) in the article: How to create an ISO 20000 internal audit checklist.

Service Report

ISO 20000-1:2011 emphasizes measurement and reporting in several places. This template should be used to report service-related measurements. Various parameters should be measured to give a clear overview of service performance.

Learn more about measurements in these articles:

- Service Reporting: get the picture, big and small
- Facing reality – measurements in ITIL®

IT Service Continuity Plan Test and Review Report

IT Service Continuity Plans need to be tested regularly. As proof of performed test activities you should create a report that contains a testing description, testing results, and reporting.

Customer Complaint Report

Customers are receiving value through the services delivered. If value is not received according to customer expectations, they will complain. Therefore, an official communication channel for customer complaints should exist. This template should contain information about the affected service, business impact, actions performed (as a result of the complaint), and related responsibilities.

Find out more in the article: ITIL® Customer satisfaction – Design driven by outcomes.
Internal Audit Report

Once the internal audit is finished, a report must be made. The Audit Report documents the audit trail, results, nonconformities, and recommendations for improvements.

Management Review Minutes

This is, usually, in the form of minutes of the management review meeting and needs to include all the materials that were involved at the management meeting, as well as all the decisions that were made. The minutes can be in paper or digital form.

Read the article: What should be on the SMS management review agenda according to ISO 20000? to learn more.

Availability Measurement Report

The Availability Measurement Report gives a clear picture of what was defined in the Availability Plan for a particular service. The document could also be in spreadsheet form and should contain measurement and report data.

Corrective and Preventive Action

Corrective and Preventive Action, as well as opportunities for improvement, shall be documented. This record should contain details about corrective and preventive actions.

Supplier Performance Report

In addition to IT service provider reports to the customer, the supplier’s performance also needs to be measured and reported. This report includes a summary for all suppliers, particular supplier performance reports, and a supplier satisfaction survey (which is optional, but provides valuable inputs for the organization).

Incident Record

In order to manage incident resolution and service availability, incidents need to be managed and resolved. The Incident Record is documented information about a particular incident and the activities that led to its resolution. If you don’t have an ITSM tool, you can use a spreadsheet-based document, but you should include (in addition to all required information) all details needed to efficiently manage the opened incident.
Service Request Record

Just as for incidents, service requests need to be documented and fulfilled. The Service Request Record fulfills the standard’s requirements and enables service request management up to its fulfillment.

Known Error Record

In order to improve the organization’s learning and improve ITSM performance, knowledge related to resolved incidents and problems needs to be documented. This document should enable the recording of all relevant information that will help lead to faster incident and problem solving.

Learn more in the article: Known Errors – repetitio est mater studiorum? Not in this case.

Request for Change and Change Record

Once you have a Change Policy and Change Process description in place, you should define the Request for Change and Change Record. The Request for Change contains all details needed to classify, assess, evaluate, and approve the change. The Change Record provides an overview of all changes in order to plan implementation, create reports, and use knowledge for closed changes.

Read this article to get more details: ITIL®/ISO 20000 Request for Change – Your steering wheel throughout the change lifecycle.

Problem Record

The Problem Management Process defines activities, roles, and responsibilities needed to resolve problems. The Problem Record should be a tool where all information relevant for a particular problem is recorded. If you don’t use an ITSM tool, you can create a spreadsheet-based document that will fulfill the standard’s requirements and record other relevant information.

Service Performance Review Report

This is the document that records customer feedback, exceptional situations, and improvement initiatives that were defined. It could be spreadsheet-based, and should contain a service-relevant report and an overview of the performance of all services in place.
Conclusion

ISO 20000 implementation shouldn’t be a complex task if you set it up correctly right from the beginning. Documentation that is required by the standard, extended by non-mandatory documents, forms a significant part of the SMS implementation. Knowing what the standard requires as mandatory documentation helps the organization to be well prepared for the certification audit. On the other side, having non-mandatory documents in place helps the organization to run the SMS effectively. Implementing both mandatory and non-mandatory documents in an optimal scope increases efficiency of the SMS and creates benefits for both the organization itself and its customers. Who would wish for more than that?

Sample documentation templates

Here you can download a free preview of the ISO 20000 Documentation Toolkit – in this free preview you will be able to see the Table of Contents of each of the mentioned policies and procedures, as well as a few sections from each document.

References

20000Academy

International Organization for Standardization

ITIL® Official site

ITIL® is a registered trade mark of AXELOS Limited
Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Fax: +385 1 556 0711