QCert360

YOUR 360° COMPLIANCE PARTNER

QCERT360 | IMPLEMENTATION GUIDE

ISO/IEC 20000-1:2018

INFORMATION TECHNOLOGY – SERVICE MANAGEMENT SYSTEM

IMPLEMENTATION GUIDE

PLAN

SMS scope, services, risks and objectives

DESIGN

Service portfolio, SLAs, changes and releases

DELIVER

Incidents, requests, suppliers and operations

IMPROVE

KPIs, internal review, corrective action and continual improvement

A practical, clause-by-clause guide for planning, implementing, maintaining and improving an IT Service Management System based on ISO/IEC 20000-1:2018.

Implementation status note

This guide is an implementation aid. It should be used with the official ISO/IEC 20000-1:2018 standard, Amendment 1:2024 climate-action changes, and applicable legal, contractual and organizational requirements.

HOW TO USE THIS GUIDE

This guide has been prepared to help organizations understand the practical implementation of ISO/IEC 20000-1:2018 for an IT Service Management System (SMS). It is suitable for IT service providers, managed service providers, internal IT departments, cloud service providers, helpdesk operations, software support teams and organizations that design, transition, deliver and improve services for customers or internal users.

The guide is written in a practical format. It explains what each clause expects, what evidence usually supports implementation, and which documents or records are commonly reviewed during certification readiness checks.

CONTENTS

1	Understanding ISO/IEC 20000-1:2018
2	Service Management System fundamentals
3	Benefits of implementation
4	PDCA model for IT service management
5	Implementation roadmap
6	Clause 4 – Context of the organization
7	Clause 5 – Leadership
8	Clause 6 – Planning
9	Clause 7 – Support
10	Clause 8 – Operation of the SMS
11	Clause 9 – Performance evaluation
12	Clause 10 – Improvement
13	Documented information toolkit
14	Certification-readiness checklist
15	90-day implementation planner
16	Frequently asked questions

1 UNDERSTANDING ISO/IEC 20000-1:2018

ISO/IEC 20000-1:2018 is a management system standard for service management. It specifies requirements for establishing, implementing, maintaining and continually improving a Service Management System. The SMS helps an organization plan, design, transition, deliver and improve services so that service requirements are met and value is delivered to customers and users.

The standard is not limited to technology infrastructure. It applies to the management of services, including service planning, service catalogue, service levels, supplier management, demand, capacity, changes, releases, incidents, service requests, problems, availability, continuity and information security in the service environment.

Who can implement ISO/IEC 20000-1?

- Managed service providers and IT outsourcing organizations.
- Internal IT departments supporting business users.
- Cloud, SaaS, hosting, data center and network service providers.
- Application support, helpdesk and technical support teams.
- Organizations that need structured ITSM controls for tenders, customer assurance, service governance or continual improvement.

Core implementation principle
The standard expects the organization to define the SMS scope, understand service requirements, control the full service lifecycle, measure service performance, and improve services using evidence. It is compatible with other management system standards and can be integrated with ISO 9001, ISO/IEC 27001, ISO 22301 and ISO 27017 where relevant.

2 SERVICE MANAGEMENT SYSTEM FUNDAMENTALS

A Service Management System is the coordinated set of policies, processes, roles, objectives, resources and records used to direct and control service management. The SMS should not be treated as a folder of procedures. It must operate as a live system that governs how services are planned, agreed, delivered, monitored and improved.

Term	Practical meaning
Service	A means of delivering value by facilitating outcomes for customers without the customer managing specific costs and risks directly.
Service requirement	A documented need or expectation that must be met through service delivery and control.
Service catalogue	Controlled information about live services and, where applicable, services available for deployment.
Service level agreement	A documented agreement describing service targets, responsibilities, reporting, availability, response, resolution and related service commitments.
Configuration item	An item that needs to be controlled to deliver one or more services.
Incident	An unplanned interruption to a service or reduction in service quality.
Problem	A cause or potential cause of one or more incidents.
Change	Addition, modification or removal of anything that could affect services or service components.

3 BENEFITS OF IMPLEMENTATION

ISO/IEC 20000-1 implementation gives the organization a structured method for controlling IT services and related service processes. It supports consistency, customer confidence and measurable service improvement.

Better service control

Defined service ownership, service levels, responsibilities and escalation rules reduce ambiguity.

Customer confidence

A certified SMS can support tenders, contractual assurance and customer trust in the organization's service capability.

Stronger operational discipline

Incident, request, problem, change and release controls become consistent and measurable.

Improved supplier governance

Supplier performance, agreements, dependencies and service commitments are better controlled.

Evidence-based improvement

KPIs, service reports, internal review and management review provide evidence for decisions.

Integration with security and continuity

Information security, continuity, availability and service resilience become part of service management.

Typical business outcomes

- Clearer ownership of services and customer requirements.
- Reduced service disruption through improved change, release, incident and problem management.
- Better transparency through service reporting and agreed service targets.
- Improved ability to manage outsourced services and service supply chains.
- A practical framework for service improvement and customer satisfaction monitoring.

4 PDCA MODEL FOR IT SERVICE MANAGEMENT

The ISO/IEC 20000-1 management system follows a Plan-Do-Check-Act approach. This cycle should be applied to the SMS as a whole and also to individual processes such as incident management, supplier management, service continuity and change management.

PLAN

Define SMS scope, service objectives, policies, risks, service requirements, resources and process controls.

DO

Operate the service lifecycle: service catalogue, SLAs, suppliers, demand, capacity, changes, releases, incidents and requests.

CHECK

Monitor service performance, customer satisfaction, SLA achievement, internal review results and management review inputs.

ACT

Correct nonconformities, improve services, update controls and revise objectives based on evidence.

In practice, PDCA prevents the SMS from becoming static. Service performance, user feedback, supplier performance, incidents, changes and risk information should regularly feed back into service planning and improvement.

Management system flow

Context and scope > Leadership and policy > Planning and support > Service operation > Evaluation and improvement

5 IMPLEMENTATION ROADMAP

Step	Focus	Key action
Step 1	Define the SMS scope	Identify services, customers, users, sites, technologies, service providers, suppliers and exclusions.
Step 2	Map services and processes	Prepare service catalogue, process map and responsibility matrix for the service lifecycle.
Step 3	Assess gaps	Compare current practices against Clauses 4–10 and Clause 8 service management requirements.
Step 4	Build SMS controls	Develop policies, objectives, risk controls, SLA controls, supplier controls and service operation procedures.
Step 5	Implement records	Start using live records for incidents, requests, changes, releases, problems, service reports and supplier reviews.
Step 6	Measure performance	Track service level achievement, availability, incidents, capacity, changes, customer feedback and corrective actions.
Step 7	Conduct internal review	Review conformity, performance and implementation effectiveness across the SMS.
Step 8	Complete management review	Top management reviews SMS performance, risks, changes, resources, improvement needs and readiness.
Step 9	Certification readiness	Verify that documented information and implementation evidence are complete before Stage 1 and Stage 2.

6 CLAUSE 4 – CONTEXT OF THE ORGANIZATION

Clause 4 requires the organization to understand its service environment and define the boundaries of the SMS. This includes internal and external issues, interested parties, service requirements and the scope of the SMS.

Implementation actions

- Identify internal issues such as service capability, tools, skills, staffing, process maturity, automation, security posture and service performance.
- Identify external issues such as customer contracts, technology dependency, regulatory requirements, market expectations, supplier dependence and cyber threats.
- Determine interested parties such as customers, users, suppliers, regulators, internal departments, top management, service owners and security teams.
- Determine whether climate change is a relevant issue for the SMS context and whether interested parties have climate-related requirements that may affect service continuity, infrastructure, suppliers, availability or resilience.
- Define the SMS scope, including services, customers, locations, technology boundaries, supplier interfaces and organizational units included.
- Document the service management processes and their interactions.

Evidence usually expected

- Context analysis or SWOT/PESTLE relevant to services
- Interested party and requirements register
- SMS scope statement
- Service catalogue or service list
- Process interaction map
- Applicability and interface notes for outsourced or supplier-delivered services

7 CLAUSE 5 – LEADERSHIP

Top management must demonstrate leadership by establishing the SMS policy, ensuring service management objectives are compatible with organizational strategy, assigning roles, supporting resources and promoting continual improvement.

Practical requirements

- Approve a Service Management Policy that is appropriate to the organization and its services.
- Define SMS roles such as service owner, process owner, incident manager, change manager, supplier manager, service desk lead and SMS coordinator.
- Ensure the policy and objectives are communicated and understood.
- Integrate service management into business planning, customer commitments and resource decisions.
- Support customer focus, service quality, risk-based thinking and continual improvement.

Leadership evidence

Evidence	What it should show
Service Management Policy	Commitment to meet service requirements and continually improve the SMS.
Role and responsibility matrix	Clear process ownership and authority.
Objectives approval	Top management involvement in service management direction.
Management review records	Evaluation of SMS performance and decisions for improvement.

8 CLAUSE 6 – PLANNING

Planning connects service requirements, risks, opportunities and measurable service objectives. The organization should determine what could affect the SMS and the services, then plan actions to address these matters.

Risk and opportunity planning

- Identify risks to service delivery, availability, continuity, capacity, supplier performance, information security, change failure, release failure and customer satisfaction.
- Assess risk using defined criteria such as likelihood, impact, detectability, customer effect, legal effect and business continuity effect.
- Define controls, owners, deadlines and effectiveness checks.
- Link risks to service objectives, service continuity plans, capacity plans, supplier reviews and improvement actions.

Service management objectives

Objectives should be measurable, aligned with the policy, monitored, communicated and updated when services or requirements change.

Objective area	Example measurable objective
Incident response	95% of priority 1 incidents acknowledged within agreed response time.
Service availability	Maintain monthly availability above agreed SLA target for critical services.
Change success	Reduce emergency changes and failed changes through improved assessment and testing.
Customer satisfaction	Measure satisfaction quarterly and implement actions for low-scoring services.
Supplier performance	Review critical supplier SLA performance monthly and address repeated failures.

9 CLAUSE 7 – SUPPORT

Support requirements ensure that the SMS has suitable resources, competence, awareness, communication and controlled documented information.

Resources and competence

- Identify resource needs for service desk, monitoring, infrastructure, tools, automation, service reporting, security and continuity.
- Define competency requirements for roles that affect service management performance.
- Maintain records for training, experience, certification, role authorization and competence evaluation.
- Ensure staff understand the Service Management Policy, objectives, procedures, customer commitments and consequences of nonconformity.

Communication and documented information

- Define what needs to be communicated, when, by whom and through which channels.
- Control policies, procedures, service catalogues, SLA records, configuration records, change records and service reports.
- Use document control rules for identification, revision, approval, distribution, access, retention and disposal.
- Protect sensitive service information, customer data, credentials, configuration records and security-related information.

Minimum support records

- Competence matrix
- Training and awareness records
- Communication plan
- Document master list
- Record retention register
- Tool access records
- Internal and customer communication records

10 CLAUSE 8 – OPERATION OF THE SMS

Clause 8 is the operational core of ISO/IEC 20000-1. It covers the planning and control of service management processes and the service lifecycle. Implementation should be supported by live records, not only written procedures.

8.1 Operational planning and control

Plan, implement and control the processes needed to meet service requirements. Changes to the SMS and services should be controlled, and outsourced or supplier activities should be managed where they affect service delivery.

8.2 Service portfolio

- Plan services before they are introduced or changed.
- Maintain a service catalogue with controlled service information.
- Control assets and configuration items that support services.
- Ensure service delivery aligns with service requirements and agreements.
- Define ownership and controls for services delivered by internal or external parties.

Key records

- Service catalogue
- Service portfolio list
- Asset register
- Configuration management database or configuration records
- Service design and transition records
- Service acceptance criteria

8.3 Relationship and agreement

The organization must manage relationships with customers, users and interested parties and ensure service requirements are agreed, monitored and reviewed. Service level management should define targets, responsibilities, measurement methods and reporting arrangements.

- Maintain customer and user communication channels.
- Define service level agreements or service commitments.
- Review service performance against agreed targets.
- Manage complaints, satisfaction, service changes and customer feedback.
- Control supplier performance where suppliers support the service.

8.4 Supply and demand

The SMS should include controls for budgeting and accounting for services, demand management and capacity management. This helps ensure that services are financially understood, demand is forecast, and capacity is sufficient to meet agreed requirements.

Area	Implementation focus	Records
Budgeting and accounting	Understand service costs, budgets and charging where applicable.	Cost reports, budget records, service cost model
Demand management	Forecast demand and manage usage patterns.	Demand forecasts, trend reports, business plans

Area	Implementation focus	Records
Capacity management	Ensure service capacity meets current and future requirements.	Capacity plan, utilization reports, capacity actions

8.5 Service design, build and transition

Changes to services and service components must be controlled. The organization should evaluate risks, impacts, resources, testing, acceptance criteria, deployment steps and rollback arrangements before a change or release is implemented.

- Use a change management process with request, assessment, authorization, testing, implementation and review stages.
- Plan service design and transition for new or changed services.
- Control release and deployment to reduce service disruption and protect customer commitments.
- Maintain evidence of approvals, test results, release notes, communication and post-implementation review.

8.6 Resolution and fulfillment

Incident management, service request management and problem management help restore service, fulfill user needs and remove root causes of recurring issues.

Incident management	Service request management	Problem management
Restore normal service as quickly as possible and minimize adverse impact.	Handle standard user requests through controlled request models and fulfillment rules.	Identify causes, known errors and permanent actions to prevent recurrence.

8.7 Service assurance

Service assurance requirements help ensure that services remain available, resilient and protected. The organization should align these controls with service requirements, risk assessment and customer commitments.

Availability management

- Define availability requirements for services.
- Monitor uptime, downtime, planned maintenance and service interruption trends.
- Analyze availability incidents and implement actions to improve reliability.

Service continuity management

- Identify continuity requirements for critical services.
- Prepare service continuity plans aligned with business impact and customer needs.
- Test continuity arrangements and record results.

Information security management

- Identify security requirements related to services and service data.
- Implement controls for confidentiality, integrity and availability of information.
- Manage security incidents and link security controls with service continuity, supplier controls and access management.

Evidence examples

- Availability reports
- Continuity plans and test records
- Security policy and incident records
- Access review records
- Backup and recovery evidence
- Service monitoring logs

11 CLAUSE 9 – PERFORMANCE EVALUATION

Performance evaluation verifies whether the SMS is working as intended. The organization must monitor and measure service performance, conduct internal reviews, evaluate customer satisfaction and complete management review.

Monitoring and measurement

KPI area	What to monitor
SLA achievement	Percentage of services meeting agreed targets.
Incident performance	Response and resolution against priority targets.
Change performance	Successful changes, failed changes, emergency changes and rollback trends.
Service availability	Availability by service and cause of downtime.
Customer satisfaction	Feedback scores, complaints, compliments and improvement actions.
Supplier performance	Supplier SLA achievement, issues and corrective actions.

Internal review and management review

- Plan internal reviews at defined intervals based on process importance, previous results and service risks.
- Report findings to responsible managers and track actions to closure.
- Hold management review to evaluate policy, objectives, service performance, risks, changes, resources, nonconformities and improvement opportunities.

12 CLAUSE 10 – IMPROVEMENT

Improvement ensures that the SMS remains suitable, adequate and effective. Nonconformities, incidents, service failures, customer feedback, supplier issues and internal review findings should be converted into corrective actions and service improvements.

Corrective action process

- Record the nonconformity, service failure or improvement issue.
- Contain the immediate impact where required.
- Analyze root cause using methods such as 5 Whys, fault tree or incident trend analysis.
- Define corrective action with owner and target date.
- Verify whether the action was effective.
- Update risks, procedures, training, service plans or controls where necessary.

Continual improvement sources

- Service performance reports
- Customer satisfaction results
- Repeated incidents or service requests
- Problem records and known errors
- Supplier performance reviews
- Change and release reviews
- Internal review findings
- Management review decisions

Practical note
Continual improvement does not mean changing everything at once. It means using evidence to improve the SMS, services and service management processes in a controlled and measurable way.

13 DOCUMENTED INFORMATION TOOLKIT

The exact documented information depends on the organization's services, size, complexity, customer commitments and regulatory environment. The following list is a practical starting point.

Document group	Examples
SMS core documents	SMS scope, Service Management Policy, process map, objectives, risk register, roles and responsibilities, communication plan.
Service portfolio documents	Service catalogue, service descriptions, service plans, asset register, configuration records.
Relationship and agreement records	SLAs, OLAs, customer communication records, satisfaction records, supplier agreements, supplier reviews.
Operational records	Incident log, service request log, problem log, change records, release records, capacity records, availability reports.
Assurance records	Continuity plans, continuity test records, security incident records, access reviews, monitoring logs.
Evaluation and improvement records	Internal review programme and reports, management review minutes, corrective action log, improvement plan.

14 CERTIFICATION-READINESS CHECKLIST

#	Readiness item	Status
1	SMS scope approved and aligned with services under certification	Yes / No
2	Service Management Policy approved and communicated	Yes / No
3	Interested parties and service requirements identified	Yes / No
4	Service catalogue controlled and current	Yes / No
5	Service management objectives defined and monitored	Yes / No
6	Risk and opportunity register completed	Yes / No

#	Readiness item	Status
7	Incident, request, problem, change and release records available	Yes / No
8	Supplier performance records available	Yes / No
9	Availability, capacity and continuity evidence available	Yes / No
10	Information security controls linked to services	Yes / No
11	Internal review completed	Yes / No
12	Management review completed	Yes / No
13	Corrective actions tracked to closure	Yes / No
14	Records are controlled, retrievable and retained	Yes / No

15 90-DAY IMPLEMENTATION PLANNER

The timeline below is indicative. Actual implementation time depends on service complexity, number of locations, outsourcing arrangements, existing ITSM maturity and availability of records.

Days 1–15	Define scope, interested parties, service list, SMS policy, roles and implementation plan.
Days 16–30	Develop risk register, objectives, service catalogue, process map and document control structure.
Days 31–45	Implement incident, request, problem, change, release, supplier and service level controls.
Days 46–60	Prepare availability, capacity, continuity, security and service reporting evidence.
Days 61–75	Conduct internal review, correct gaps, complete corrective actions and verify records.
Days 76–90	Complete management review, readiness check, final document review and certification preparation.

Before Stage 1

- Confirm scope and service catalogue.
- Ensure required SMS documents are approved and controlled.
- Prepare records showing the SMS has been implemented, not only drafted.
- Verify internal review and management review records are complete.

16 FREQUENTLY ASKED QUESTIONS

Is ISO/IEC 20000-1 only for IT companies?

No. It is for organizations that manage services. Many users are IT service providers or internal IT departments, but the focus is the service management system and service lifecycle.

Can ISO/IEC 20000-1 be integrated with ISO/IEC 27001?

Yes. Information security management is a service assurance requirement and many organizations integrate ISO/IEC 20000-1 with ISO/IEC 27001 for stronger IT governance.

Is a service catalogue mandatory in practice?

A controlled service catalogue is a key operational document because it defines service information, ownership, commitments and service boundaries.

How much implementation evidence is needed?

Enough to show the SMS is operating. This usually includes records for incidents, service requests, changes, releases, supplier reviews, service reports, objectives and management review.

Can outsourced services be included?

Yes, but interfaces and responsibilities must be clearly controlled. The organization remains responsible for controlling parties involved in the service lifecycle where they affect service delivery.

Important note
This guide is intended for implementation planning and awareness. It does not reproduce the full ISO/IEC 20000-1:2018 standard or Amendment 1:2024. Organizations should use the official standard and applicable statutory, regulatory, customer and contractual requirements when implementing and preparing for certification.