White Paper – ISO/IEC 20001-1

Information Security – Service Management System

First published in 2005, ISO/IEC 20000 is the international standard for IT Service Management. It is published by ISO, the International Organization for Standardization, based in Geneva, and has been adopted globally. It describes an integrated set of management processes for the effective delivery of services to the business and customers. Latest version is 2018.

The standard is based on, and supersedes, BS 15000 – a standard developed by the British Standards organization. It aligns with best practice guidance contained within the ITIL framework and is compatible with other IT Service Management frameworks and approaches, including components of ISACA's COBIT® framework.

This is all contained within a quality management system which itself aligns with other pertinent standards such as ISO 9001, ISO/IEC 27001 etc.

The standard comprises several parts. Part 1 is the formal specification and details the requirements for a service management system that enables the service provider to "fulfil service requirements and provide value for both the customer and the service provider".

Part 2 provides guidance on the application of service management systems. It describes the best practices for service management within the scope of ISO/IEC 20000-1. It provides more detail about the process's organizations should follow to achieve the requirements laid out in Part 1.

Part 3 gives guidance on scope definition and applicability of the standard. This is required to help understand the often-complex supply chains involved in IT service management, particularly where many process areas and functions are outsourced.

Part 1 comprises several sections. Many of the process names will be recognized by those familiar with ITIL.

- **Scope – outlining the scope of the ISO/IEC 20000 standards.**
- **Terms & definitions – explaining the terminology used in the requirements.**
- **General requirements for a management system – Similar to other standards such as ISO 9001 and ISO/IEC27001, outlining the detailed management responsibilities, including resourcing, reporting, accountability and documentation.**
- **The general requirements also cover scope and process governance, documenting a formal plan for the overall management system including process integration and continual improvement.**
- **Design and transition of new or changed services – key to enabling the smooth implementation of new services, or major changes to existing services.**
- **Service delivery processes – capacity management, service level management, information security management, budgeting and accounting for IT services, service reporting and service continuity and availability management.**
- **Relationship Processes – supporting business relationship management and supplier management in the end to end supply chain.**
- **Control Processes – configuration management, change management and release and deployment management.**
- **Resolution Processes – incident management and problem management.**

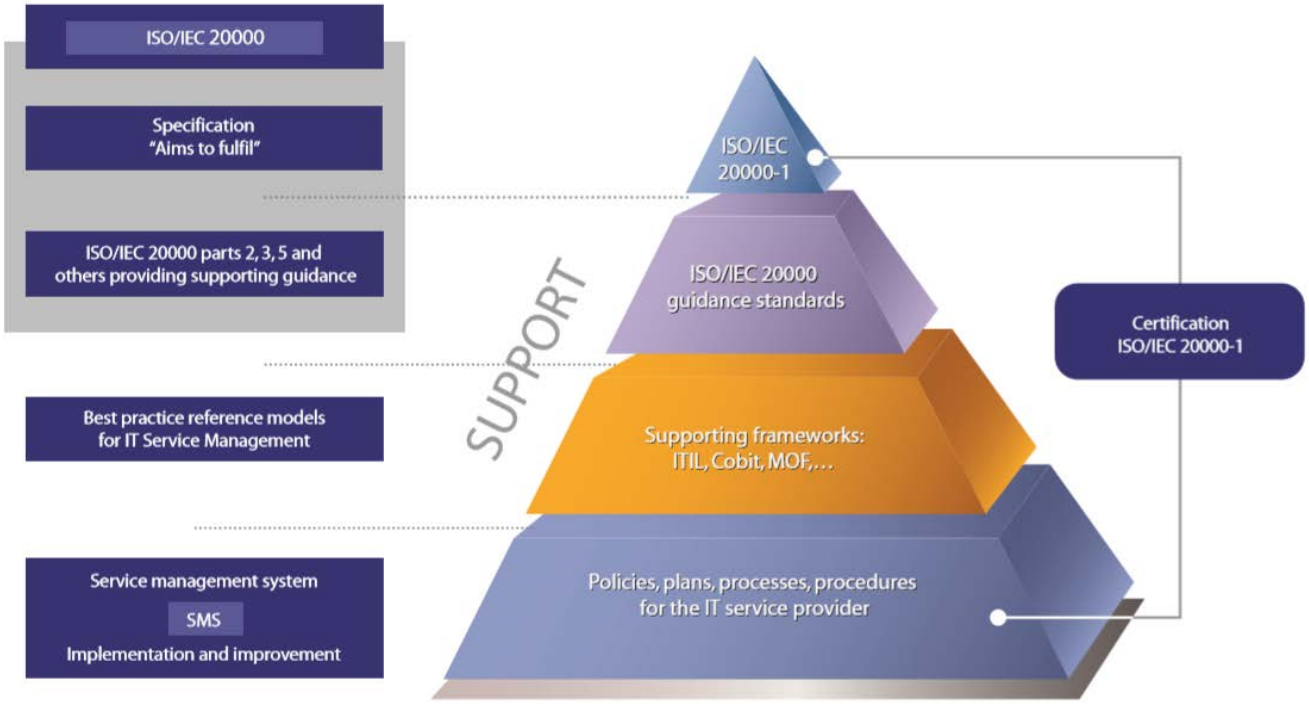
For companies that have already achieved ISO 9001 or ISO/IEC 27001 certification, the management system of ISO/IEC 20000 will be familiar. It follows the same plan-do-act-check methodology, linked to customer/business requirements using business metrics and reinforcing continual improvement.

It demands the implementation of a management structure and system to provide accountability for every element of IT service management including a strong reporting structure, clear personal

PO Box No. 80910, 106, - Al Dana Centre, Maktoum Street, Dubai, UAE
Tel No.: 042235779; Fax No.: 042235886
www.kavzedconsultatns.com , www.iso-dubai-uae.com

responsibility and supporting documentation. And, again following similar standards, it addresses the planning and implementation of the service management system aimed at achieving the goals of improving efficiency and effectiveness, customer satisfaction and continual improvement.

For those companies that have achieved ISO 9001 or similar certification, this core part of ISO/IEC 20000 should be reasonably straightforward, with demonstrable, proven management processes and structures already in place. This does assume, however, that the existing system encompasses the activities of IT Service Management to some degree.



Benefits:

TRANSFORMING PERFORMANCE
So why is ISO/IEC 20000 important? Since only companies that have demonstrated they have implemented all of the service management processes within a quality management system framework can become certified, achieving certification provides clear competitive advantage for companies across many sectors including:

- **Internal IT service provider organizations in any sector**
- **Outsourcers**
- **Application service providers (hosted/cloud solutions) Government contractors.**

Improving IT processes and, critically, the control, audit and documentation of these processes, is a key requirement for the many sectors now subject to tight regulations, including:

- **Banks, Retailers and other merchants: Payment Card Industry Data Security Standard (PCI DSS)**
- **Insurance Companies: Model Audit Rule (MAR) regulation on solvency and corporate governance developed by the National Association of Insurance Commissioners (NAIC).**
- **Organizations needing to conform with Sarbanes-Oxley (SOX) requirements**
- **Utility Companies: Face strict new conformance rules, including Critical Infrastructure Protection (CIP).**

For a business, ISO/IEC 20000 certification enforces a measurable level of effectiveness and creates a culture of continual improvement. It delivers a multitude of benefits that include:

- **Outsource core functions: Once ISO/IEC 20000 is in place, and an organization has created its culture of proactive IT service delivery, it is far easier to outsource the reactive elements to a third party, driving down costs and enabling the IT service delivery team to concentrate on adding tangible corporate value. ISO/IEC 20000 specifies that the interfaces between the outsourcers and the service providers have to be clearly documented and managed.**

- **Competitive differentiation: For outsourcing providers in particular, ISO/IEC 20000 offers a chance to achieve significant competitive differentiation. It also can drive down costs. For example, the integration of incident management with problem management can typically result in a large reduction in incidents. This has a huge impact on costs; increasing profitability in existing customer accounts and enabling more competitive tenders for new business.**

- **Access to key markets: With government, healthcare and military organizations now mandating ISO/IEC 20000 for their IT service providers, any organization wanting to enter this market, or sustain an existing market position, must achieve certification. In the EU, organizations already need ISO 9000 certification; it is likely that a demand for ISO/ IEC 20000 will follow. Organizations from all over the world are increasingly looking at certification as way of differentiating themselves and ensuring high levels of quality.**

- **Streamlined conformance activity: Organizations that adhere to the policies and processes of ISO/IEC 20000, especially the management procedures, have a strong foundation for conformance activity. Indeed, conformance with ISO/IEC 20000 is proven to drive down the cost of conformance to a multitude of regulations, from PCI, DSS to Sarbanes Oxley. For example, one utility company's CIP conformance effort was reduced by 50% because the company was already ISO/ IEC 20000 compliant.**

- **Improved Merger & Acquisition (M&A): Leveraging ITIL practices to achieve ISO/IEC 20000 certification means that companies have a far better insight into the resources in place and what will be required to support both organic growth and any merged organization. The result is that the right resources can be put in place in time, to maximise the success of the M&A activity.**

- **Continual improvement: Companies in this economic downturn want efficiencies now that can be leveraged to support expansion and profitable growth in the future. By enforcing conformance to the requirements, ISO/IEC 20000 drives highly effective and efficient management of IT services and promotes a culture of proactive service delivery that supports continual improvement.**

- **Demonstrable best practice: Internal service provider organizations that have achieved ISO/ IEC 20000 certification are increasingly being heralded as market leaders, with competitors now encouraged to follow suit.**

For the individual: ISO/IEC 20000 qualifications provide an opportunity to build up skills; to evolve beyond generic service management expertise and take companies through the ISO/IEC 20000 process. It enables individuals to leverage ITIL experience and develop new competencies. There is a demand for skilled ISO/IEC 20000 implementers in the market at the present time.

Conclusion:

In this marketplace, organizations need to drive down costs. But they also need to build a solid foundation for the future and achieve competitive differentiation, maximize the opportunities provided by merger and acquisition and ensure access to key markets.

The adoption of ITIL processes over the last decade has undoubtedly transformed the quality, relevance and timeliness of IT service delivery; it has enabled the creation of customer and business focused services and improved the cost/ value equation.
Over 600 organizations globally have already recognized the value of certification to ISO/IEC 20000.

For most organizations the people cost is the biggest burden on the budget. Trained staff who understand the value of a process-oriented culture and work in tightly integrated teams within a recognized quality management system bring great value to the organization. It is the first step to becoming highly effective. The ISO/ IEC 20000 professional qualification will give the organization a head starts in achieving company certification and realizing true value from improved efficiencies and effectiveness.

Which documents and records are required?

Mandatory Documents	ISO 20000 Clause
Service Management System (SMS) Policy	4.3.1.; 4.1.1.a), 4.1.2, 4.1.4
Service Management System (SMS) Plan	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
Procedure for Document and Record Control	4.3.2 and 4.3.3
Communication Procedure	4.1.2.e), 4.1.3.b)
Service Level Requirements	5.2, 6.1
Service Improvement Plan	4.5.5.1, 4.5.5.2
Procedure for Internal Audit	4.5.4.1,4.5.4.2, 4.5.4.3,6.6.1, 6.6.2, 6.6.3
Continual Service Improvement Process	4.5.5.1, 4.5.5.2
Training and Awareness Plan	4.4.2, 4.5.2.l)
Corrective and Preventive Action	6.6.1., 6.6.2, 6.6.3, 4.5.5.1, 4.5.5.2
Risk Assessment and Treatment	6.3.1, 6.3.2, 6.3.3
Service Catalogue	6.1
Service Level Management Process	4.3.1, 5.3.i); 6.1, 5.3.j)
Service Level Agreement	6.1, 8.1
Operational Level Agreement	6.1

Mandatory Documents	ISO 20000 Clause
Design and Transition of New or Changed Services	4.3.1, 5.1, 5.3.a), 5.3.b), 5.3.c), 5.2.b)
Service Continuity and Availability Management Process	4.3.1, 6.3.1 6.3.2, 6.3.3
Budgeting and Accounting for Services Process	4.3.1, 6.4
Capacity Management Process	4.3.1, 6.5
Information Security Management Process	4.3.1, 6.6.1, 6.6.2, 6.6.3
Information Security Management Policy	6.6.1, 6.6.2, 6.6.3
Business Relationship Management Process	4.3.1, 7.1
Supplier Management Process	4.3.1, 7.2
Incident and Service Request Management Process	4.3.1, 8.1, 6.6.3
Problem Management Process	4.3.1, 8.2, 8.1
Configuration Management Process	4.3.1, 9.1, 5.1
Change Management Process	4.3.1, 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
Release and Deployment Management Process	4.3.1, 5.3.a), 5.3.b), 5.3.k), 9.3
Supplier Contract	7.2
Customer Portfolio	7.1

Mandatory Documents	ISO 20000 Clause
Customer Release and Deployment Policy	9.3
Availability Plan	6.3, 6.3.1, 6.3.2, 6.3.3
Capacity Plan	6.5
Change Management Policy	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
Annual Internal Audit Program	4.5.4.1,4.5.4.2, 4.5.4.3,6.6.1, 6.6.2, 6.6.3

Mandatory Records

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

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.