ISO/IEC 20000-1
IT Service Management System

Self-assessment questionnaire

How ready are you for ISO/IEC 20000-1:2011?

This document has been designed to assess your company's readiness for an ISO/IEC 20000 IT Service Management System. By completing this questionnaire your results will allow you to self-assess your organization and identify where you are in the ISO/IEC 20000 process. If you would like us to do this analysis for you, please complete the questionnaire (including your contact details), save and email it to us at certification.sales@bsigroup.com

---

Information provided will not be disclosed and will be destroyed immediately after use. Please mark your answers ✓ **for Yes** and **leave blank for No**. To order a copy of ISO/IEC 20000-1:2011 please visit **www.bsigroup.com/SE20000**

Contact: ..... Job title: .....

Company: ..... No. of employees: .....

Address: ..... Town: .....

County: ..... Postcode: .....

Telephone (*inc. dialing code*): ..... Email: .....

1. Service management system

Are senior management committed to all aspects of implementing the service management system, including:

a) The establishment of scope, policy, objectives, plans, processes and procedures ☐

b) Communicating the importance of fulfilling service and legal and statutory requirements, and meeting contractual obligations ☐

c) Definition of service management authorities and responsibilities, and provision of competent resources ☐

d) Ensuring risks to services have been identified and are being managed ☐

Is there accountability and governance for any service management processes, or process components, operated by other parties – internal and/or external? ☐

Are the documents and records related to the management system managed and controlled according to defined procedures? ☐

Have the human, technical, information and financial resources for the service management system been determined, and have the required human resource competencies been defined? ☐

Is there a service management plan to define the service requirements, the approach to service delivery, the management of risks, and how services will be monitored and measured for effectiveness? ☐

Are internal audits and management reviews conducted at planned intervals? ☐

Is there a formal process for identifying improvements to the service management system and services, for assigning priorities and actions, and for evaluating whether improvements have been achieved? ☐

Continued >>

2. Design and development of new or changed services

Is there a process in place to ensure that new or changed services are planned, designed and developed, tested and transitioned into the live environment efficiently and effectively?

Have the changes that fall within the scope of the new and changed services process been determined and agreed?

Are service requirements identified, designed and documented during the planning and design phases of the new and changed services process, and are outputs reviewed and accepted/rejected?

Are new and changed services tested to verify that they fulfil service requirements and meet the agreed acceptance criteria, prior to release and deployment to the live environment?

Following completed transition of new and changed services, is the achievement of the expected outcomes evaluated and reported?

3. Service delivery processes

Have all services to be delivered been defined, agreed and documented in a catalogue of services and supported by service level agreements that have been reviewed and agreed with the customer?

Have the risks to service continuity and availability been assessed and documented, and have plans that include the procedures and requirements for recovery been developed?

Are the service continuity and availability plans monitored and tested to ensure that they meet targets and requirements?

Is there a budget and account for the cost of service provision, and is there an interface to financial management processes?

Are capacity plans that consider human, technical, information and financial resources in place to ensure agreed capacity and performance requirements are met?

Is there an information security policy and a defined approach for the management of information security risks?

Have physical, administrative and technical information security controls been implemented to address identified risks?

Are changes analysed for potential security risks and impact, and are security incidents managed by formal procedures?

4. Relationship process

Are there designated responsibilities for managing the customer relationship and customer satisfaction?

Is the performance of services reviewed at planned intervals with the customer?

Is there a definition of a service complaint and is a procedure in place for managing customer complaints, including escalation?

Are there designated responsibilities for the management of the relationship, contract and performance of suppliers?

Are the requirements, scope, levels of service and communication processes to be provided by the supplier(s) documented in service level agreements, or other documents, and agreed by all parties?

5. Resolution processes

Are there documented procedures for the management and resolution/ fulfilment of incidents and service requests?

Is there an agreed and documented definition of a major incident with the customer of the service(s) and are top management informed/involved?

Are there documented procedures to identify problems, and minimize the impact of incidents and problems?

Are data and trends on incidents and problems analysed to identify the root cause and the required preventive actions?

Is up-to-date information on known errors and problem resolution available for the management of incidents?

6. Control processes

Is there a definition of each type of configuration item and its description and status, including the relationship with other configuration items and service components?

Are all configuration items uniquely identifiable and recorded in a CMDB to which update access is strictly controlled?

Are changes to configuration items traceable and auditable, and is a baseline taken before release to the live environment?

Is there a change policy that defines change to controlled configuration items and outlines the criteria to determine changes that can have a major impact?

Is there a documented procedure to record, classify, impact assess, approve and schedule changes, and a defined procedure for managing emergency changes and their release?

Are changes reviewed for effectiveness and analysed at planned intervals to detect trends and identify opportunities for improvement?

Is there a release policy agreed with the customer stating the frequency of releases?

Are releases planned and is there an interface to provide information about the release to the change, incident and problem management processes?

Are releases built and tested within a controlled acceptance test environment prior to deployment, using defined and agreed acceptance testing criteria?

Are the activities required to rectify a failed release planned, and is the success/failure of releases monitored and reported in order to identify opportunities for improvement?

For BSI to complete the analysis on your behalf, please click the submit button below or email a saved copy of your completed questionnaire to:
certification.sales@bsigroup.com

Save Submit

BSI/UK/197/SC/0413/en/BLD
© BSI Group

+44 845 080 9000
certification.sales@bsigroup.com
bsigroup.com

ISO/IEC 20000-1 Information Technology Service Management

The trademarks in this material (for example the BSI logo or the word "KITEMARK") are registered and unregistered trademarks owned by The British Standards Institution in UK and certain other countries throughout the world.