ISO 27001:2013 vs. ISO 20000-1:2011 matrix

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
0	Introduction		Introduction	
0.1	General	1.1	General	Although there are no sub-clauses in the introduction of ISO 20000-1, both standards state in their introductions the need for a process approach for the planning, establishment, implementation, operation, maintenance, and improvement to fulfill the requirements of an ISO management system (for information security and services, in this case).
0.2	Compatibility with other management systems			There are no similar clauses in ISO 20000-1.
1	Scope	1	Scope	
		1.1	General	Although there are no sub-clauses in the scope of ISO 27001, both standards state here what is included: requirements for the management system, service management (ISO 20000-1), and information security risk evaluation and treatment (ISO 27001). The generality of the standard required (fit for all kinds of organizations, independent of size, type, and nature). Like ISO 27001, ISO 20000-1 does not allow exclusions of clauses.
		1.2	Application	
2	Normative references	2	Normative references	This requirement s identical for both standards, except for references specific for each standard.
3	Terms and definitions	3	Terms and definitions	Both standards list their own “Fundamentals and vocabulary” (ISO 27000 for ISO 27001, and ISO 20000-1 provides its own definitions of the main terms).

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
4	Context of the organization	4.5	Establish and improve the SMS	
		7	Relationship processes	
4.1	Understanding the organization and its context	4.5.1	Define scope	You can use the same document to define the process of identification of interested parties, as well as statutory, regulatory, contractual, and other requirements related to the services to be provided, and responsibilities for their fulfillment. See a sample document here: Procedure for Identification of Requirements You can use the Service Management System (SMS) Plan to map the specific aspects of the Service Management System context and, with a few adjustments, use a similar map to identify information security context aspects of your ISMS.
		7.1	Business relationship management	
4.2	Understanding the needs and expectations of interested parties	4.5.1	Define scope	You can use the same document to list requirements regarding the services to be provided. See a sample document here: List of Legal, Regulatory, Contractual and Other Requirements
		7.1	Business relationship management	
4.3	Determining the scope of the information security management system	4.5.1	Define scope	You can use the same document to define the scope of your SMS. See sample document here: ISMS Scope Document
4.4	Information security management system			There is no exact clause in ISO 20000-1 similar to this ISO 27001 clause, but the following clauses provide some useful detail that can help you to better understand ISO 27001 clause 4.4: • ISO 20000-1 clause 4.5.2 Plan the SMS (Plan) – See details in ISO 27001 clauses 6 and 7. • ISO 20000-1 clause 4.5.3 Implement and operate the SMS (Do) – See details in ISO 27001 clause 8. • ISO 20000 clause 4.5.4 Monitor and review the SMS (Check) – See details in ISO 27001 clause 9. • ISO 20000 clause 4.5.5 Maintain and improve the SMS (Act) – See details in ISO 27001 clauses 6 and 10.

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
5	Leadership	4.1	Management responsibility	
		6.6	Information security management	
5.1	Leadership and commitment	4.1.1	Management commitment	The requirements are the same, and management has to treat both standards the same way regarding implementing the policies, provision of resources, continual improvement, assigning roles and responsibilities, etc.
		6.6.1 a)	Information security policy (communication and the importance of conformity)	This requirement is basically the implementation of an ISMS; so, by performing this clause from ISO 27001 you can get through sub-clause 6.6.1 a) of ISO 20000-1. See sample documents here: Information Security Policy and Service Management System (SMS) Policy
5.2	Policy	4.1.2	Service management policy	The requirements are almost the same, and in theory, they could be met through a single document. However, it is better if the policies are written as separate documents, in which case they must be compatible with each other. See sample document here: Information Security policy and Service Management System (SMS) Policy
		6.6.1	Information security policy (definition of information security management objectives)	This requirement is basically the implementation of an ISMS; so, by performing this clause from ISO 27001 you can get through sub-clause 6.6.1 b) of ISO 20000-1. See sample documents here: Information Security Policy and Service Management System (SMS) Policy
5.3	Organizational roles, responsibilities and authorities	4.1.3	Authority, responsibility and communication	The requirements are the same, so roles, responsibilities, and authorities for both standards can be communicated in the same way. For example, a manager, or managers, must be indicated to oversee service / information security management activities; the same auditor can perform SMS and ISMS audits, etc.
		4.1.4	Management representative	
		4.2	Governance of processes operated by other parties	There are no similar clauses in ISO 27001.

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
6	Planning	4.1	Management responsibility	
		4.5.2	Plan the SMS (Plan)	
		4.5.5	Maintain and improve the SMS (Act)	
		6.6.1 c) and d)	Information security policy (definition of risk assessment approach and risk assessment realization)	This requirement from ISO 20000-1 includes the planning of an ISMS; so, by performing all items from clause 6 of ISO 27001 you can get through sub-clauses 6.6.1 c) and d). See sample document here: Risk Assessment and Risk Treatment Methodology
6.1.1	Actions to address risk and opportunities – general	4.5.5.1	General	Addressing risks can be considered as preventive action, but it cannot be merged in the same document. For ISO 20000-1 preventive actions, see this document: Corrective or Preventive Action Form
6.1.2	Information security risk assessment	4.5.2 j) 4.5.3 d) 6.6.1 c) 6.6.2	Approach to be taken for the management of risks and the criteria for accepting risks	The general approach can be the same, but oriented to service risks. See sample document here: Risk Assessment and Risk Treatment Methodology
6.1.3	Information security risk treatment			
6.2	Information security objectives and planning to achieve them	4.1.1 6.6.1 b)	Management commitment	Objectives for both standards, and plans for their realization, can be placed in one document. See sample document here: Service Management System (SMS) Plan
7	Support	4	Service management system general requirements	
		5.2	Plan new or changed services	
		6	Service delivery processes	

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
7.1	Resources	4.4.1	Provision of resources	The organization has to determine and provide necessary resources for process execution in order to meet requirements for both standards. You can use the same processes to fulfill the requirements, such as a purchasing process. See sample document here: Service Management System (SMS) Plan
7.2	Competence	4.4.2	Human resources	ISO 27001 divides competence and awareness and emphasizes awareness more than ISO 20000-1. However, you can use one training plan for both standards to reduce records. See sample document here: Training and Awareness Plan
7.3	Awareness			
7.4	Communication	5.2 c)	Communication with interested parties	Communication to interested parties must be established for both standards. See sample document here: Communication Procedure
		6.2	Service reporting	
7.5	Documented information	4.3	Documentation management	You can apply the same procedure to meet the requirements of both standards and establish a documentation system. See sample document here: Procedure for Document and Record Control
8	Operation	4.5.3	Implement and operate the ISMS (Do)	
		6.3	Service continuity and availability management	
		6.6	Information security management	
8.1	Operation and planning control	4.5.3 e)	Manage service management processes and interfaces	The key performance indicators (KPIs) can be set for processes of both standards and described in the same document.

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
8.2	Information security risk assessment	4.5.3 d)	Identify, assess, and manage service management risks	The general approach can be the same, but oriented to service risks. See sample document here: Risk Assessment and Risk Treatment Methodology
		6.3.1	Service continuity and availability requirements	Although the first step of this specific topic of ISO 20000-1 is in the field of business continuity (see this sample document: Business Impact Analysis Methodology), the risk assessment step can use the same general approach used by information security risk assessment, but oriented to service risks. See sample document here: Risk Assessment Table
8.3	Information security risk treatment	4.5.3 d)	Identify, assess, and manage service management risks	The general approach can be the same, but oriented to service risks. See sample document here: Risk Treatment Table
		6.3.2	Service continuity and availability plans	Although the first step of this specific topic of ISO 20000-1 is in the field of business continuity (see these sample documents: Business Continuity Strategy and Business Continuity Plan), the risk assessment step can use the same general approach used by information security risk assessment, but oriented to service risks. See sample toolkit here: ISO 27001/ISO 22301 Risk Assessment Toolkit
		6.6.2	Information security controls	These two ISO 20000-1 clauses can be fulfilled exactly by the items of ISO 27001 clause 8. See sample document here: Risk Assessment and Risk Treatment Methodology
		6.6.3	Information security changes and incidents	
9	Performance evaluation	4.5.4	Monitor and review the SMS (Check)	
		6.3	Service continuity and availability management	
		6.6	Information security management	
		4.5.4.1	General	There are no similar clauses in ISO 27001.

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
9.1	Monitoring, measurement, analysis and evaluation	4.5.4.1	General	The organization must demonstrate the effectiveness of the system through monitoring of parameters that the organization identified as important for process realization. Although briefly described in ISO 20000-1, these requirements are better detailed in ISO 27001 and both standards can be met through the same document, e.g., Balanced Scorecard or Matrix of Key Performance Indicators.
		6.3.3	Service continuity and availability monitoring and testing	You can use the same document to determine the frequency and methods of testing in order to assess the feasibility of measures and arrangements for service continuity, and to establish necessary corrective actions. See sample document: Exercising and Testing Plan The organization must demonstrate the effectiveness of the services provided through monitoring of parameters that the organization identified as important for service delivery. Although briefly described in ISO 20000-1, these requirements are better detailed in ISO 27001 and both standards can be met through the same document, e.g., Balanced Scorecard or Matrix of Key Performance Indicators.
9.2	Internal audit	4.5.4.2	Internal audit	The same procedure for internal audit can be applied for both standards. See sample document here: Internal Audit Procedure
		6.6.1 e)	Information security policy (internal audit)	This requirement from ISO 20000-1 is similar to the internal audits required for an ISMS; so, by performing clause 9.2 from ISO 27001 you can get through sub-clause 6.6.1 e) of ISO 20000-1. See sample document here: Internal Audit Procedure

Copyright ©2015 27001Academy. All rights reserved.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
9.3	Management review	4.5.4.3	Management review	Although the requirement is the same, input elements of management review are different. The same document can be used for both standards, but it has to contain separate input elements for both standards. See sample document here: Management Review Minutes
		6.6.1 f)	Information security policy (audit results review)	This requirement from ISO 20000-1 includes the review of the results of the ISMS audits; so, by performing clause 9.3 from ISO 27001 you can get through sub-clause 6.6.1 f) of ISO 20000-1. See sample document here: Management Review Minutes
10	Improvement	4.5.5	Maintain and improve the SMS (Act)	
10.1	Nonconformity and corrective action	4.5.5.1	General	The requirements are almost the same (ISO 27001 does not explicitly require preventive actions), but both can be met through the same procedure. See sample document here: Procedure for Corrective Action
10.2	Continual improvement	4.5.5.2	Management of improvements	Like every management system, the emphasis is on continual improvement, which is conducted through a joint procedure for corrective actions.
		8	Resolution processes	There are no similar clauses in ISO 27001.
		9	Control processes	There are no similar clauses in ISO 27001.

Copyright ©2015 27001Academy. All rights reserved.

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

20000 Academy
ITIL and ISO 20000 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
Ul. Vladimira Nazora 59, 10000 Zagreb
Croatia, European Union

Email: support@iso27001standard.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

Copyright ©2014 27001Academy. All rights reserved.