

PECB

When Recognition Matters



WHITEPAPER

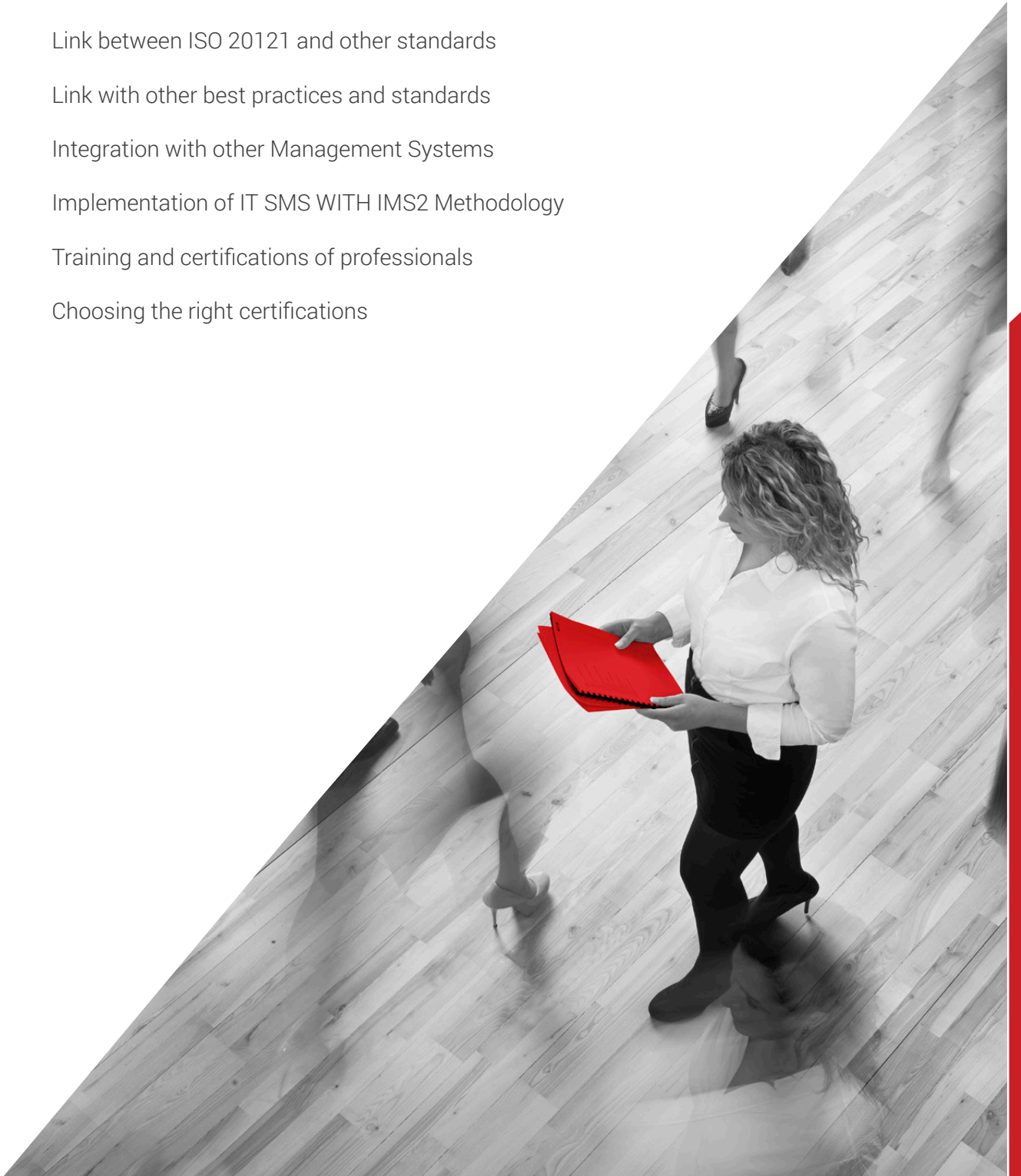
ISO/IEC 20000-1:2011

SERVICE MANAGEMENT SYSTEM REQUIREMENTS

www.pecb.com

CONTENT

- 3 Introduction
- 4 An overview of ISO 20121:20121
- 4 IT Service Management
- 6 Key Clauses of ISO 20121:20121
- 9 Link between ISO 20121 and other standards
- 10 Link with other best practices and standards
- 11 Integration with other Management Systems
- 13 Implementation of IT SMS WITH IMS2 Methodology
- 15 Training and certifications of professionals
- 16 Choosing the right certifications



INTRODUCTION

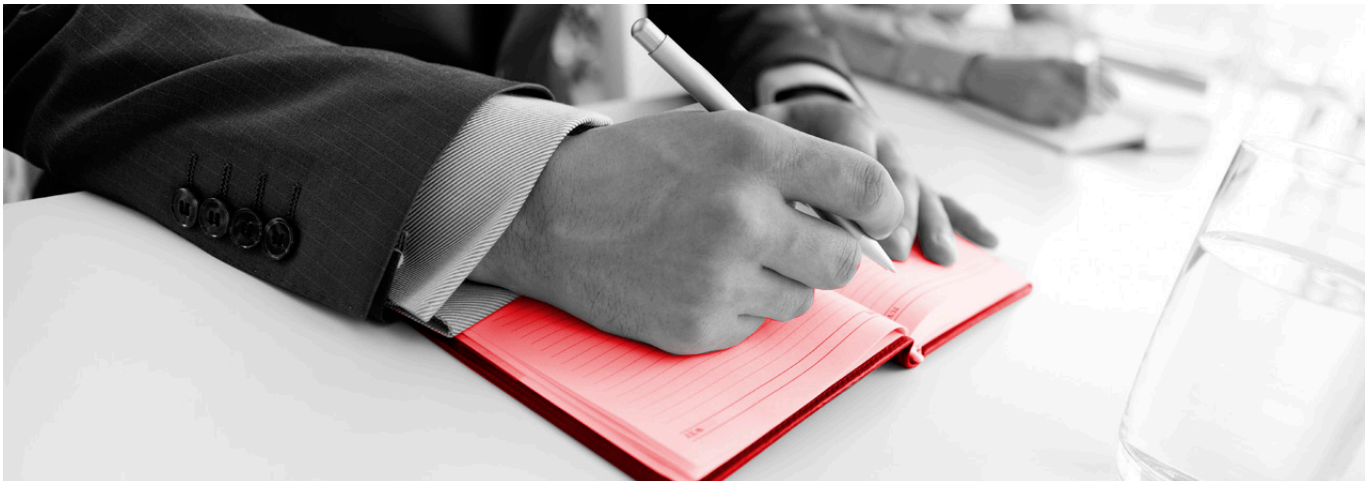
Because ITIL® qualifications were only available for individuals, it was impossible for an IT organization to prove that it was working along the ITIL recommendations.

In order to fill this gap, two organizations itSMF (The IT Service Management Forum) and BSI (British Standards Institution), initiated the ISO/IEC 20000:2011 standard.

The standard is modeled upon the principles of ITIL® and allows IT organizations to be certified as IT Service Management.

It has to be noted that there is no formal relationship between ISO 20000 and ITIL®, even though ISO 20000 is based on ITIL® principles.

ITIL® provides a suitable basis for developing an ISO 20000 compliant process.



There are additional parts of this standard, which provide the following guidelines:

- **ISO/IEC 20000:2012, Part 2:**
Provides guidance on the application of service management systems (SMS) based on ISO/IEC 20000-1. It aims to enable organizations and individuals to interpret ISO 20000-1 more accurately and use it more effectively.
- **ISO/IEC 20000:2012, Part 3:**
Provides practical guidance on scope definition, applicability and demonstration of conformity to the requirements in ISO/IEC 20000-1.
- **ISO/IEC TR 20000:2010, Part 4:**
Aims to facilitate the development of a process assessment model according to ISO/IEC 15504 process assessment principles.
 - ISO/IEC 15504-1 describes the concepts and terminology used for process assessment.
 - ISO/IEC 15504-2 describes the requirements for the conduct of an assessment and a measurement scale for assessing process capability.
- **ISO/IEC TR 20000:2010, Part 5:**
Displays an exemplar implementation plan that provides guidance to service providers on how to implement a service management system to fulfil the requirements of ISO/IEC 20000-1, or for service providers who are planning service improvements and intending to use ISO/IEC 20000 as a business goal. It could also be useful for those advising service providers on how to effectively achieve the requirements of ISO/IEC 20000-1.

AN OVERVIEW OF ISO 20000-1:2011

This part of ISO/IEC 20000 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil service requirements.

All requirements in this part of ISO/IEC 20000 are generic and are intended to be applicable to all service providers, regardless of type, size and the nature of the services delivered.

Exclusion of any of the requirements in Clauses 4 to 9 is not acceptable when a service provider claims conformity to this part of ISO/IEC 20000, regardless of the nature of the service provider's organization.

What is a Service Management System?

SMS is a management system to direct and control the service management activities of the service provider.

IT SERVICE MANAGEMENT STANDARDIZATION IS IMPROVED WITH ISO/IEC 20000 BY CORRESPONDING TO THE FOLLOWING:

- Implementing a framework for working through the definition and implementation of a set of processes;
- Attaining recognition from a third party on the level of maturity reached by the organization;
- Preserving a demonstrated service quality;
- and Preserving better alignment between business objectives and IT.



ISO/IEC 20000 can be used by:

- a) An organization seeking services from service providers and requiring assurance regarding their service requirements fulfillment;
- b) An organization that requires a consistent approach by all its service providers, including those in a supply chain;
- c) A service provider that intends to demonstrate its capability for the design, transition, delivery and improvement of services that fulfil service requirements;
- d) A service provider to monitor, measure and review its service management processes and services;
- e) A service provider to improve the design, transition and delivery of services through effective Implementation and operation of an SMS;
- f) An assessor or auditor as the criteria for a conformity assessment of a service provider's SMS to the requirements in this part of the ISO/IEC 20000.

This part of the standard requires the application of the methodology known as “Plan-Do-Check-Act” (PDCA) for all parts of the SMS and the services. The PDCA methodology, as applied in this part of ISO/IEC 20000 can be briefly described as follows:

- **PLAN:** establishing, documenting and agreeing to the SMS. The SMS includes the policies, objectives, plans and processes to fulfill the service requirements.
- **DO:** implementing and operating the SMS for the design, transition, delivery and improvement of the services.
- **CHECK:** monitoring, measuring and reviewing the SMS and the services against the policies, objectives, plans and service requirements and reporting the results.
- **ACT:** taking actions to continually improve performance of the SMS and the services.





KEY CLAUSES OF ISO 20000-1:2011

ISO 20000-1 is organized into the following main clauses:

- Clause 4: Service management system general requirements
- Clause 5: Design and transition of new or changed services
- Clause 6: Service delivery processes
- Clause 7: Relationship processes
- Clause 8: Resolution processes
- Clause 9: Control processes

Each of these key activities is listed below.

CLAUSE 4: SERVICE MANAGEMENT SYSTEM GENERAL REQUIREMENTS

Top management shall provide evidence of its commitment to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the SMS and the services by:

- establishing and communicating the scope, policy and objectives for service management;
- ensuring that the service management plan is created, implemented and maintained in order to adhere to the policy, achieve the objectives for service management and fulfil the service requirements;
- communicating the importance of fulfilling service requirements;
- communicating the importance of fulfilling statutory and regulatory requirements and contractual obligations;
- ensuring the provision of resources;
- conducting internal audits and management reviews at planned intervals;
- and assuring that risks to services are assessed and managed.

GOVERNANCE OF PROCESSES OPERATED BY OTHER PARTIES

The service provider shall identify all or parts of processes in clauses 5 to 9, which are operated by other parties (i.e. an internal group, a customer or a supplier). The service provider shall demonstrate governance of processes operated by other parties.

DOCUMENTATION MANAGEMENT

The service provider shall establish and maintain documents, including records, to ensure effective planning, operation and control of the SMS.

RESOURCE MANAGEMENT

The service provider shall determine and provide the human, technical, information and financial resources needed to establish, implement and maintain the SMS. In addition, the personnel shall be competent on the basis of appropriate education, training, skills and experience.

ESTABLISH AND IMPROVE THE SMS

The steps that the service provider shall take to establish and improve the SMS are:

- Defining the scope
- Planning the SMS (Plan)
- Implementing and operating the SMS (Do)
- Monitoring and reviewing the SMS (Check)
- Maintaining and improving the SMS (Act)

CLAUSE 5: DESIGN AND TRANSITION OF NEW OR CHANGED SERVICES

Operating businesses and organizations will always have the need for new and improved services. All these changes shall be part of the change management process.

The following processes shall be considered for the design and transition of the new changed service:

- Planning new or changed services – Identifying the service requirements for the new or changed service;
- Designing and developing of new or changed services – Designing and documenting the new or changed service;
- Transition of new or changed services – Testing the new service for verification to the service requirements fulfilments and documented design.

CLAUSE 6: SERVICE DELIVERY PROCESSES

The service provider shall consider the following processes for service delivery:

Service level management: is a series of activities including:

- Creating a service catalogue;
- Establishing one or more SLAs for each service;
- Monitoring the service levels;
- Reporting on results; and
- Reviewing service levels.

Service reporting: The description of each service report, including its identity, purpose, audience, frequency and details of the data source(s), shall be documented and agreed by the service provider and interested parties.

Service continuity and availability management: The service provider shall assess and document the risks to service continuity and availability of services. The service provider shall identify and agree with the customer and interested parties service continuity and availability requirements. In addition, the service provider shall create, implement and maintain a service continuity plan(s) and an availability plan(s). Availability of services shall be monitored, the results recorded and compared with agreed targets.

Budgeting and accounting for services: Costs shall be budgeted to enable effective financial control and decision-making for services delivered.

Capacity management: The service provider shall identify and agree capacity and performance requirements with the customer and interested parties. The objective is to ensure that the service provider has sufficient capacity to meet current and future needs of the customers.

Information security management: Management with appropriate authority shall approve an information security policy taking into consideration the service requirements, statutory and regulatory requirements and contractual obligations. Information security management ensures that the service providers effectively manage security within all service activities.

CLAUSE 7: RELATIONSHIP PROCESSES

The two relationship processes regarding IT service management are:

1. **Business relationship management** - The objective of the business relationship management is to establish and maintain a good relationship between the service provider and the customer based on understanding the customer and their business drives.
2. **Supplier management** - The objective of supplier management is to ensure the provision of consistent quality services.

CLAUSE 8: RESOLUTION PROCESSES

This clause includes incident and service request management, and problem management. It recognizes existing practices in many organizations to process incident reports and service change process through one common process.

The objective of incident management is to restore normal services as soon as possible. On the other hand the objective of problem incident management is to minimize disruptions in the business by identifying and analyzing the cause of incidents and by managing problems to closure.

CLAUSE 9: CONTROL PROCESSES

Configuration Management: This process manages the service assets and Configuration Items (CIs) in order to support other Service Management processes. Configuration records and records of deficiencies are the required documents of configuration management. The objective of configuration management is to define and control the components of the service and maintain accurate configuration information.

Change Management: A change management policy shall be established that defines:

- CIs which are under the control of change management; and
- Criteria to determine changes with potential to have a major impact on services or the customer.

The objective of change management is to ensure that all changes are assessed, approved, implemented and reviewed in a controlled manner.

Release and deployment management: The service provider shall establish and agree with the customer a release policy stating the frequency and type of releases.

The service provider shall plan with the customer and interested parties the deployment of new or changed services and service components into the live environment. Planning shall be coordinated with the change management process and include references to the related requests for change, known errors and problems which are being closed through the release.



The service provider shall document and agree with the customer the definition of an emergency release. Emergency releases shall be managed according to a documented procedure that interfaces to the emergency change procedure.

The success or failure of the releases should be monitored and analyzed and information shall be provided to the change management process, incident and service request management processes.

LINK BETWEEN ISO 20000-1 AND OTHER STANDARDS

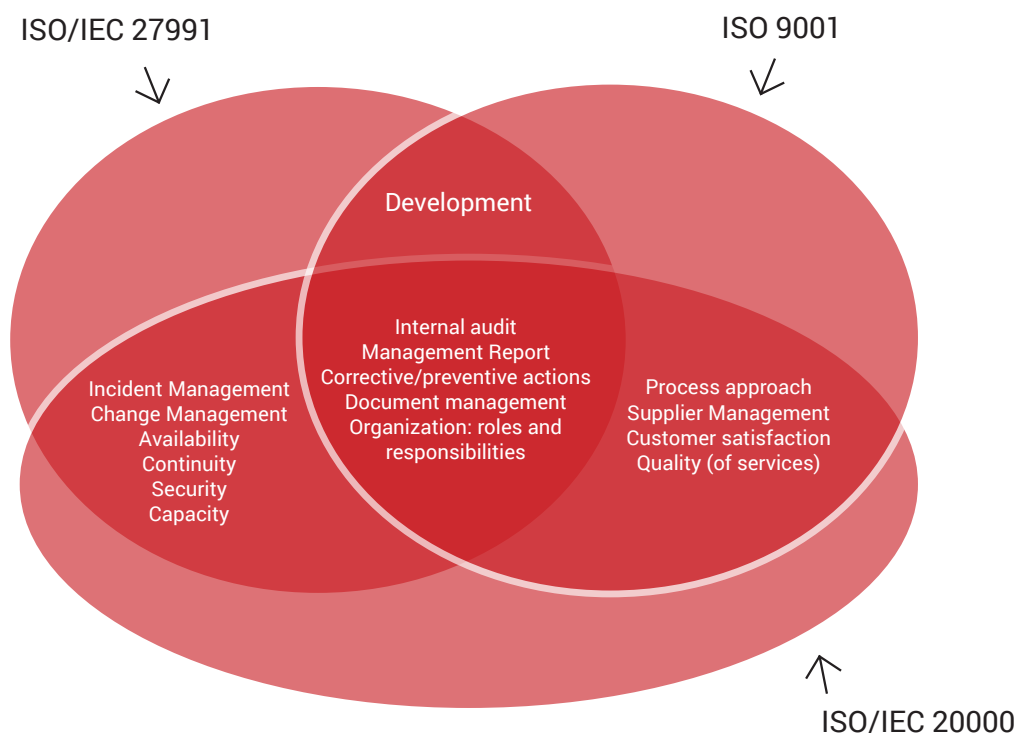
ISO 20000 can be easily linked with ISO 90000 and ISO 27001. All these standards closely follow the principles of quality management system (Plan, Do, Check and Act).

In ISO 20000, the importance of Information Security Management is detailed. The ISO/IEC 27000 family of standards specifies requirements and provides guidance to support the implementation and operation of an information security management system.

The link between ISO 20000 and standards mentioned above is strong; given the fact that almost all of the SMS clauses are similar to these standards, therefore there is likelihood to integrate these ISO's. All these standards can either be individually implemented or with each other.

If your organization is interested in combining management systems such as: a Quality Management System (QMS) with a Service Management System (SMS), or an Information Security Management System (ISMS), it is possible if ISO 9001 (QMS) and ISO 20000 (SMS) or ISO 27001 (ISMS) are implemented simultaneously, or if QMS is implemented before SMS, respectively ISMS.

If an organization already possesses an ISO 9001 certification, there are many common requirements that do not need to be repeated when you combine ISO 9001 with ISO 20000 or ISO 27001. Similarities of clauses between these three standards are described below:





Link with other best practices and standards

In addition to the ISO/IEC 20000 service management standard, apart from 27001, several other well-known standards and practices include:

ITIL® – Is a set of best practices. The main differences between ITIL® and ISO/IEC 20000 are explained in the table below:

ITIL®	ISO/IEC 20000
Practice	Standard
Descriptive	Prescriptive
Processes and control	Management Control
Doesn't show how to manage the processes	Separate sections about management system requirements
Service lifecycle focus	Process control focus

COBIT - Provides a control and management framework with a set of guidelines for IT processes, practices and controls.

Six Sigma - Is a statistical measure of variation and a methodology for improving key processes. Six Sigma uses data and statistical analysis to measure and improve operational performance, by identifying and eliminating "defects" in service management processes.

ISO/IEC 15504 - Is a set of technical standards and documents, for the computer software development process and related business management functions. Its aim is to provide a guide for performing a capability assessment in order to achieve process improvement.

ISO/IEC 17799 - Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.

INTEGRATION WITH OTHER MANAGEMENT SYSTEMS

General requirements presented in the table below are normally stated in any management system. They relate to determining objectives, applying them according to the organization's habits and needs, up-keeping them based on a strong management commitment, monitoring and reviewing, supporting the management system by providing documentation, regular 'health-checks' via internal or external audits and gain benefits through continual improvement as achieved by a regular management review.

The table below shows how an SMS can be considered jointly with other management systems. This will authorize the organization to envision "combined audits" in order to achieve their compliance goals with adequate effort and budget.

Requirements	ISO 001:2008	ISO 4001:2004	ISO 50001:2011	ISO 27001:2005	ISO 22301:2012	ISO 20000:2011
Objectives of the management system	5.4.1	4.3.3	4.4.6	4.2.1	6.2	4.5.2
Policy of the management system	5.3	4.2	4.3	4.2.1	5.3	4.1.2
Management commitment	5.1	4.4.1	4.2	5	5.2	4.1
Documentation requirements	4.2	4.4	4.5.4	4.3	7.5	4.3
Internal audit	8.2.2	4.5.5	4.6.3	5	9.2	4.5.4.2
Continual improvement	8.5.1	4.5.3	4.6.4	8	10	4.5.5
Management review	5.6	4.6	4.7	7	9.3	4.5.4.3



SERVICE MANAGEMENT –THE BUSINESS BENEFITS

As with all major undertakings within an organization, it is essential to gain the backing and sponsorship of executive management. By far the best way to achieve this, rather than through highlighting the negative aspects of not having event sustainability management is to illustrate the positive gains of having an effective event sustainability management process in place.

Today good event sustainability management is not about being forced into taking action to address external pressures. It is about recognizing the positive value of energy use good practice being embedded throughout your organization.

SUPPLIER MANAGEMENT	SERVICE PROVISION CHAIN MANAGEMENT	CUSTOMER REQUIREMENTS ALIGNMENT	BETTER UNDERSTANDING OF THE ORGANIZATION
COST REDUCTION	RESPECT OF THE INTERESTED PARTIES	PROTECTION OF THE REPUTATION AND BRAND	REPUTATION
COMPETITIVE ADVANTAGE	LEAGL COMPLIANCE	EVALUATION, COMPARISON AND IMPROVEMENT OF THE SERVICES	CONTRACT COMPLIANCE

The adoption of an effective event sustainability management process within an organization will have the following benefits:

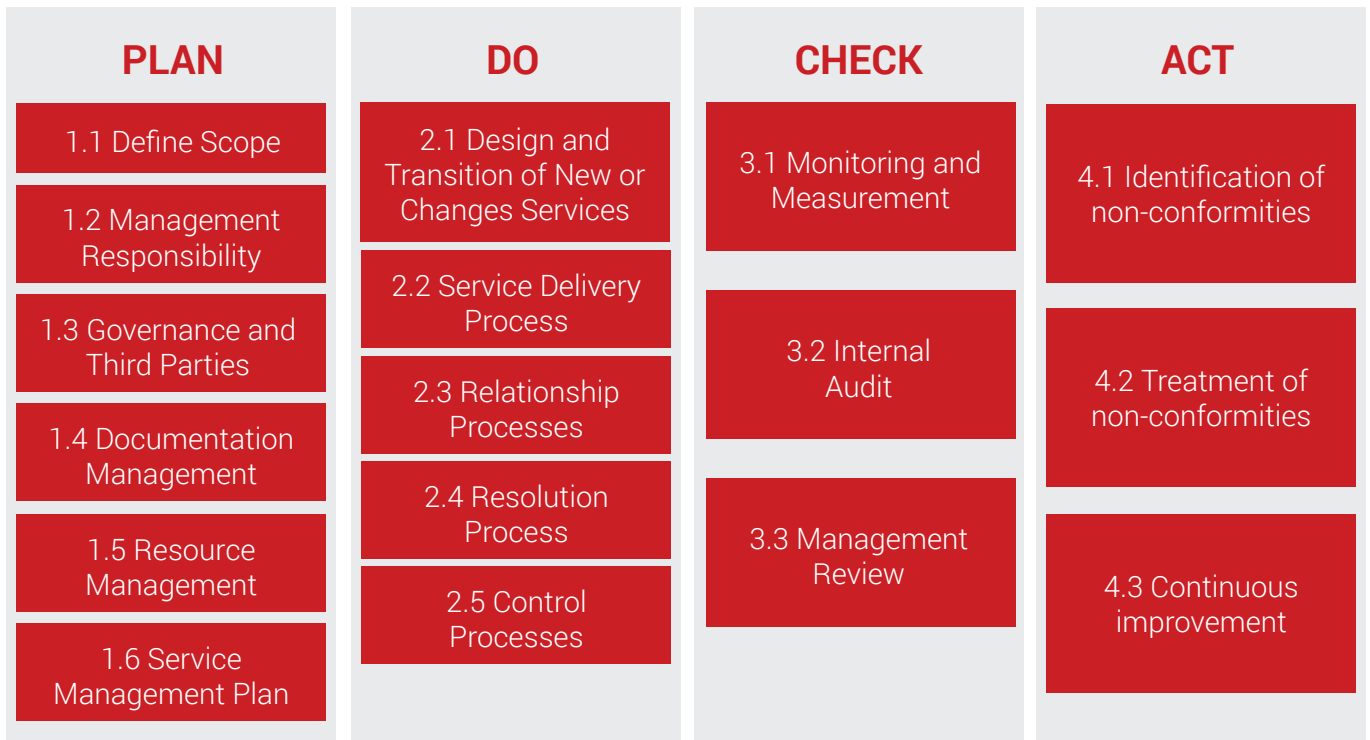
- Provides the ability to manage suppliers effectively;
- Manages the relationship with vendors through notable service level management;
- Gives assurance that IT services meet the needs of the client;
- Awareness and accountability of staff;
- Allows companies to manage their IT through the service supply chain;
- Enables faster and effective transition of IT services;
- Demonstrates service reliability and consistency;
- It boosts reputation and strengthens relationships with key stakeholders;
- Provides a common framework for staff training and career development;
- Reduces the risk, cost and time to market new products and services;
- Increases the confidence of clients, business partners and other stakeholders when working with an organization that possesses ISO/IEC 20000;
- Provides a competitive advantage of differentiation for the organization;
- Enables better automation of IT service management processes;
- Assists satisfaction of requirements of customer and/or other stakeholders;
- Consolidates confidence of customers, suppliers and partners of the organization;
- Complies with national, regional and international laws and regulations.

IMPLEMENTATION OF IT SMS WITH IMS2 METHODOLOGY

Making the decision to implement a service management based on ISO/IEC 20000 is often a very simple one, as the benefits are well documented.

There is no single blueprint for implementing ISO/IEC 20000 that will work for every company, but there are some common steps that will allow you to balance the often conflicting requirements and prepare you for a successful certification audit.

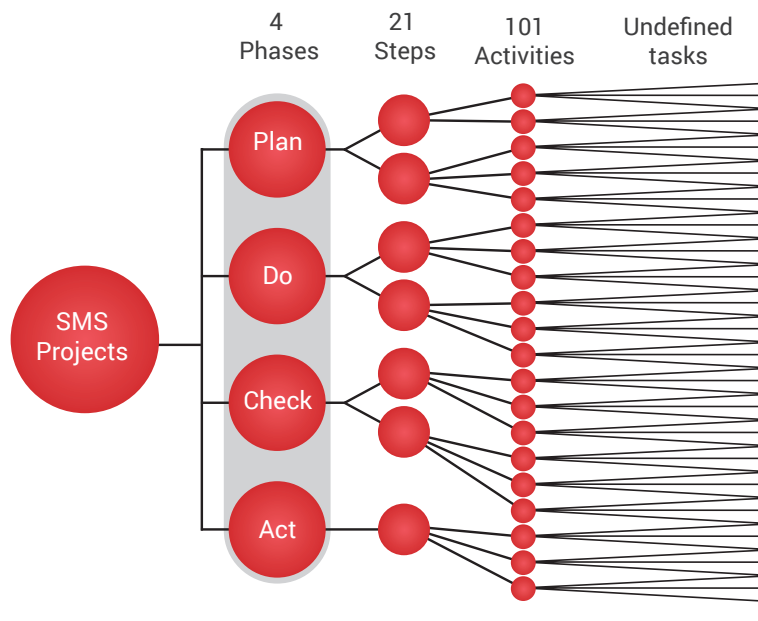
PECB has developed a methodology for implementing a management system. It is called "Integrated Implementation Methodology for Management Systems and Standards (IMS2)" and is based on applicable best practices. This methodology is based on the guidelines of ISO standards and also meets the requirements of ISO/IEC 20000.



IMS2 is based on the PDCA cycle, which is divided into four phases: Plan, Do, Check and Act. Each phase has between 2 and 8 steps for a total of 21 steps. In turn, these steps are divided into 101 activities and tasks. This 'Practical Guide' considers the key phases in your implementation project from start to finish, and suggests the appropriate 'best practice' for each one, while directing you to further helpful resources as you embark on your ISO/IEC 20000 journey.

The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure for documented information can be done before the understanding of the organization. Many processes are iterative because of the need for progressive development throughout the implementation project; for example, communication and training.





By following a structured and effective methodology, an organization can be sure it covers all minimum requirements for the implementation of a management system. Whatever methodology used, the organization must adapt it to its particular context (requirements, size of the organization, scope, objectives, etc...) and not apply it like a cookbook.

CERTIFICATION OF ORGANIZATIONS

The usual path for an organization that wishes to be certified against ISO 20000 is the following:

1. **Implementation of the management system:** Before being audited, a management system must be in operation for some time. Usually, the minimum time required by the certification bodies is 3 months.
2. **Internal audit and review by top management:** Before a management system can be certified, it must have had at least one internal audit report and one management review.
3. **Selection of the certification body (registrar):** Each organization can select the certification body (registrar) of its choice.
4. **Pre-assessment audit (optional):** An organization can choose to do a pre-audit to identify any possible gap between its current management system and the requirements of the standard.
5. **Stage 1 audit:** A conformity review of the design of the management system. The main objective is to verify that the management system is designed to meet the requirements of the standard(s) and the objectives of the organization. It is recommended that at least some portion of the Stage 1 audit is performed on-site at the organization's premises.
6. **Stage 2 audit (On-site visit):** A conformity review of the design of the management system. The main objective is to verify that the management system is designed to meet the requirements of the standard(s) and the objectives of the organization. It is recommended that at least some portion of the Stage 1 audit be performed on-site at the organization's premises.
7. **Follow-up audit (optional):** The Stage 2 audit objective is to evaluate whether the declared management system conforms to all requirements of the standard is actually being implemented in the organization and can support the organization in achieving its objectives. Stage 2 takes place at the site(s) of the organization's sites(s) where the management system is implemented.
8. **Follow-up audit (optional):** If the auditee has non-conformities that require additional audit before being certified, the auditor will perform a follow-up visit to validate only the action plans linked to the non-conformities (usually one day).
9. **Confirmation of registration:** If the organization is compliant with the conditions of the standard, the Registrar confirms the registration and publishes the certificate.
10. **Continual improvement and surveillance audits:** Once an organization is registered, surveillance activities are conducted by the Certification Body to ensure that the management system still complies with the standard. The surveillance activities must include on-site visits (at least 1/year) that allow verifying the conformity of the certified client's management system and can also include: investigations following a complaint, review of a website, a written request for follow-up, etc.

TRAINING AND CERTIFICATIONS OF PROFESSIONALS

PECB has created a training roadmap and personnel certification schemes which is strongly recommended for implementers and auditors of an organization that wish to get certified against ISO 28000. Whereas certification of organizations is a vital component of the supply chain security field as it provides evidence that organizations have developed standardized processes based on best practices. Certifications of individuals serve as documented evidence of professional competencies and experience for/of those individuals that have attended one of the related courses and exams.

It serves to demonstrate that a certified professional holds defined competencies based on best practices. It also allows organizations to make intelligent choices of employee selection or services based on the competencies that are represented by the certification designation. Finally, it provides incentives to the professional to constantly improve his/her skills and knowledge and serves as a tool for employers to ensure that training and awareness have been effective.

PECB training courses are offered globally through a network of authorized training providers. They are available in several languages and include introduction, foundation, implementer and auditor courses.

The table below gives a short description relating PECB's official training courses for Event Sustainability Management System based on ISO/IEC 20000.

Training title	Short description	Who should attend
ISO/IEC 20000 Introduction	<ul style="list-style-type: none"> • One day training • Introduction to concepts management and implementation of a SMS • Do not lead to certification 	<ul style="list-style-type: none"> • IT professionals • Staff involved in the implementation of SMS • Expert advisors in IT • Managers responsible for implementing a SMS • Auditors
ISO/IEC 20000 Foundation	<ul style="list-style-type: none"> • A two days training • Become familiar with best practices for implementation and management of SMS • One hour exam 	<ul style="list-style-type: none"> • Members of an Information Technology Service team • IT professionals • Staff involved in SMS • Technicians involved in operations related to a SMS • Auditors
ISO/IEC 20000 Lead Implementer	<ul style="list-style-type: none"> • A five days training • Manage the implementation and a management of a SMS • Three hours exam 	<ul style="list-style-type: none"> • Project managers and/or consultants • ISO/IEC 20000 auditors • Members of an IT service team • Technical experts
ISO/IEC 20000 Lead Auditor	<ul style="list-style-type: none"> • A five days training • Manage the audit of a SMS • Three hours exam 	<ul style="list-style-type: none"> • Internal auditors • Auditors • Project managers and/or consultants • Members of an IT service team • Expert advisors in information technology • Technical experts

Although no specified set of courses or curriculum of study is required for the certification process, the completion of a recognized PECB course or program of study will significantly enhance your chance of passing a PECB certification examination. The list of approved organizations that offer PECB official training sessions are listed on our website: http://www.pecb.com/partnerEvent/event_schedule_list

Choosing the right certifications

The ISO/IEC 20000 Foundation certification is a professional certification for professionals needing to have an overall understanding of the ISO 20000 standard and its requirements.

The ISO/IEC 20000 Implementer certifications are professional certifications for professionals needing to implement an SMS and, in case of the ISO/IEC 20000 Lead Implementer Certification, needing to manage an implementation project.

The ISO/IEC 20000 Auditor certifications are credentials for professionals needing to audit an SMS and, in case of the "ISO/IEC 20000 Lead Auditor" Certification, needing to manage a team of auditors.

The ISO/IEC 20000 Master certification is a professional certification for professionals needing to implement an SMS, to master the audit techniques and manage (or be part of) audit teams and audit programs.

Based on your overall professional experience and your acquired qualifications, you will be granted one or more of these certifications based on projects or audits activities you have performed in the past or you are currently working on.

Certification	Exam	Professional experience	Audit experience	Project experience
Foundation	Foundation Exam	None	None	None
Provisional Implementer	Lead Implementer Exam	None	None	None
Implementer	Lead Implementer Exam	Two years One year of work experience in the field of certification	None	Project activities totaling 200 hours
Lead Implementer	Lead Implementer Exam	Five years Two years of work experience in the field of certification	None	Project activities totaling 300 hours
Provisional Auditor	Lead Auditor Exam	None	None	None
Auditor	Lead Auditor Exam	Two years One year of work experience in the field of certification	Audit activities totaling 200 hours	None
Lead Auditor	Lead Auditor Exam	Five years Two years of work experience in the field of certification	Audit activities totaling 300 hours	None
Master	Lead Auditor Exam Lead Implementer Exam	Ten years Two years of work experience in the field of certification	Audit activities totaling 500 hours	Project activities totaling 500 hours

PECB



+1-844-426-7322



customer@pecb.com



Customer Service

www.pecb.com