PECB

When Recognition Matters

WHITEPAPER

ISO 28000

SUPPLY CHAIN SECURITY MANAGEMENT SYSTEMS

CONTENT

PRINCIPAL AUTHORS
Eric LACHAPELLE, PECB
Mustafe BISLIMI, PECB
Bardha AJVAZI, PECB

INTRODUCTION

The ISO 28000, Supply Chain Security Management System International Standard, has been developed in response to the high demand from industries.
Increasingly, organizations are discovering that they must depend on effective supply chains to compete in the global market. Recent threats and incidents relating supply chains and their level of security have demonstrated that it is crucial for organizations to secure their supply chains to prevent risks.

Organizations of all sizes and types that are involved in production and services, storage or transportation at any stage of the product, should consider implementing or improving their Supply Chain Security Management System to determine adequate security measures and comply with regulatory requirements. If security needs are identified by this process, the organization should implement mechanisms and processes to meet these needs.

Considering the dynamic nature of supply chains, some organizations managing multiple supply chains may look to their service providers to meet related governmental or ISO supply chain security standards as a condition of being included in that supply chain in order to simplify security management.
A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This International Standard is based on the ISO format adopted by ISO 14000:2004 because of its risk based approach to management systems. However, organizations that have adopted a process approach to management systems (e.g. ISO 9001:2000) may be able to use their existing management system as a foundation for a security management system as prescribed in this International Standard.

What is a Supply Chain?
A supply chain is an associated set of resources and processes that begin with the sourcing of raw materials and extend through the delivery of products or services to the end user across modes of transport.
A supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

The ISO 28000:2007 is based on the methodology known as Plan-Do-Check-Act (PDCA), which can be described as follows.

- Plan: establish the objectives and processes necessary to deliver results in accordance with the organization's security policy.
- Do: implement the processes.
- Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- Act: take actions to continually improve performance of the security management system.

An overview of ISO 28000:2007

ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.

ISO 28000 was prepared by Technical Committee ISO/TC 8, (Ships and marine technology) in collaboration with other relevant technical committees responsible for specific nodes of the supply chain.
This first edition of ISO 28000 cancels and replaces ISO/PAS 28000:2005, which has been technically revised.

ISO is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

1. establish, implement, maintain and improve a security management system;
2. assure conformance with stated security management policy;
3. demonstrate such conformance to others;
4. seek certification/registration of its security management system by an accredited third party certification body;
5. make a self-determination and self-declaration of conformance with ISO 28000:2007.

Key clauses of ISO 28000:2007

The ISO 28000 is organized into the following main clauses:

Clause 4.2: Security management policy
Clause 4.3: Security risk assessment and planning
Clause 4.4: Implementation and operation
Clause 4.5: Checking and corrective action
Clause 4.6: Management review and continual improvement

II Clause 4.2: Security management policy

Top management shall authorize an overall security management policy that will:

- be consistent with other organizational policies;
- provide a framework that enables the specific security management objectives, targets and programmes to be produced;
- be consistent with the organization's overall security threat and risk management framework;
- be appropriate to the threats of the organization and the nature and scale of its operations;
- clearly state the overall security management objectives;
- include a commitment to continual improvement of the security management process;
- include a commitment to comply with current applicable legislation, regulatory and statutory requirements and with other requirements to which the organization subscribes;
- be visibly endorsed by top management;
- be documented, implemented and maintained;
- be communicated to all relevant employees and third parties;
- be available to stakeholders where appropriate;
- and provide for its review.

What is a Security Management Policy?
A security management policy includes overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

II Clause 4.3 Security risk assessment and planning

Furthermore, the organization shall prepare the security risk assessment and planning for the supply chain security management system.

Security risk assessment - This assessment shall consider the likelihood of an event and all of its consequences which shall include:

- physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action;
- operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety;
- natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective;
- factors outside of the organization's control, such as failures in externally supplied equipment and services;
- stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;
- design and installation of security equipment including replacement, maintenance, etc.
- information and data management and communications;
- a threat to continuity of operations.

Legal, statutory and other security regulatory requirements – A procedure should be established, implemented and maintained to identify and have access to the applicable legal requirements and other requirements to which the organization subscribes related to its security threat and risks, and to determine how these requirements apply to its security threats and risks.

Security management objectives – A procedure should be established, implemented and maintained to document security management objectives at relevant functions and levels within the organization, which shall be consistent with the policy.

Security management targets – Documented management targets shall be appropriately established, implemented and maintained to the needs of the organization, which shall be consistent with the security management objectives. These targets shall be:

- to an appropriate level of detail;
- specific, measurable, achievable, relevant and time-based (where practicable);
- communicated to all relevant employees and third parties including contractors;
- and reviewed periodically to ensure that they remain relevant and consistent with the security management objectives. Where necessary the targets shall be amended accordingly.

Security management programmes – Management programmes are established, implemented and maintained for achieving objectives and targets, which shall be optimized and then prioritized.

ll Clause 4.4 Implementation and operation

After the risk assessment and planning of the security management system, an organization must consider the following processes for the implementation and operation of the management system:

Structure, authority and responsibilities for security management – An organizational structure of roles, responsibilities and authorities shall be established and maintained consistent with the achievement of its security management policy, objectives, targets and programmes.

Competence, training and awareness – Personnel responsible for the design, operation and management of security equipment and processes shall be suitably qualified in terms of education, training and/or experience.

Communication – Pertinent security management information shall be communicated to and from relevant employees, contractors and other stakeholders.

Documentation – A security management documentation system shall include, but is not limited to:

- the security policy, objectives and targets,
- scope of the security management system,
- main elements of the security management system and their interaction, and reference to related documents,
- documents, including records, required by this International Standard, and
- documents, including records determined by the organization that ensure the effective planning, operation and control of processes that relate to its significant security threats and risks.

Document and data control – All documents, data and information required for this International Standard shall be controlled.

Operational control - Necessary operations and activities shall be identified for achieving:

- the security management policy;
- the control of activities and mitigation of threats identified as having significant risk;
- compliance with legal, statutory and other regulatory security requirements;
- its security management objectives;
- the delivery of its security management programmes;
- and the required level of supply chain security.

Emergency preparedness, response and security recovery – The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them.

ll Clause 4.5 Checking and corrective action

Moreover, after the implementation and operation of the supply chain security management system, the following actions shall be taken to evaluate and correct possible inaccuracies relating the management system:

Security performance measurement and monitoring – The performance of the security management system shall be monitored and measured. Associated security threats and risks shall be considered, including potential deterioration mechanisms and their consequences, when setting the frequency for measuring and monitoring the key performance parameters.

System evaluation – Security management plans, procedures, and capabilities shall be evaluated through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes must immediately be reflected in the procedure(s).

Security-related failures, incidents, non-conformances and corrective and preventive action – Responsibilities and authorities for evaluating and initiating preventive actions, investigating failures/ incidents, initiating and completing corrective actions for these failures/ incidents, and confirming the effectiveness of the corrective actions taken shall be defined.

Control of records - Records shall be established and maintained as necessary to demonstrate conformity to the requirements of its security management system and of this standard, and the results achieved.

Audit – The audits of the security management system shall be carried out at planned intervals.

ll Clause 4.6 Management review and continual improvement

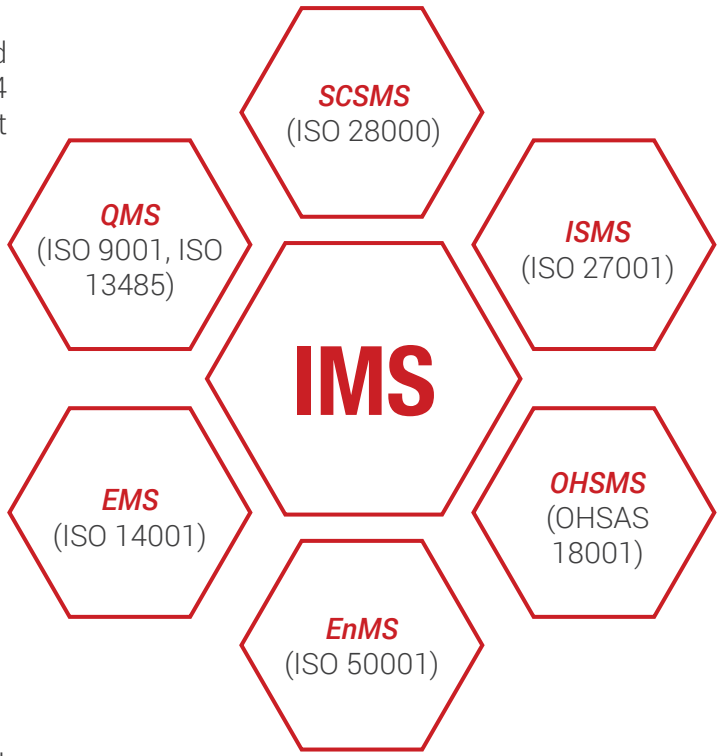
To conclude, top management shall review the organization's security management system at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Management reviews shall include assessing opportunities for improvement or changes to the security management system.

ISO 28000 and other integrated management system standards

The ISO 28000 International Standard is based on the ISO format adopted by ISO 14001:2004 because of its risk based approach to management systems.

The integration of all management systems into a single centrally managed system is defined as an ***Integrated Management System (IMS)*** and it includes standards such as:

- SCSMS (ISO 28000)
- ISMS (ISO 27001)
- QMS (ISO 9001, ISO 13485)
- EMS (ISO 14001)
- EnMS (ISO 50001)
- OHSMS (OHSAS18001)



Other security management standards

- ISO 31000 - Risk Management
- ISO 27001 - Information Security Management
- ISO 22301 - Business Continuity

ISO 28000 series

The ISO 28000 series of International Standards specifies the requirements for a security management system to ensure safety in the supply chain.

The series consists of the following standards:

- ISO 28000:2007, Specification for security management systems for the supply chain;
- ISO 28001:2007, Security management systems for the supply chain – Best practices for implementing supply chain security – Assessments and plans – Requirements and guidance;
- ISO 28003:2007, Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems;
- ISO 28004:2007, Security management systems for the supply chain – Guidelines for the implementation of ISO 28000.

Integration with other management systems

The general requirements are ordinarily identified in every management system. These requirements assist in:

- determining and applying objectives according to the organization's habits and needs;
- upholding the objectives based on strong management commitment by monitoring and reviewing;
- documenting pertinent management system processes;
- regular 'health-checks' via internal or external audits;
- and gaining benefits through continual improvement as achieved by a regular management review.

In addition, the table below presents the general requirements of several standards, which also serves as a comparing tool between SCSMS and 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 9001:2008	ISO 14001:2004	ISO 8001:2007	ISO 20000:2011	ISO 22301:2012	ISO 27001:2005
Objectives of the management system	5.4.1	4.3.3	4.3.3	4.5.2	6.2	4.2.1
Policy of the management system	5.3	4. 2	4.2	4.1.2	5.3	4.2.1
Management commitment	5.1	4.4.1	4.4.1.a	4.1	5.2	5
Documentation requirements	4.2	4.4	4.4.4	4.3	7.5	4.3
Internal audit	8.2.2	4.5.5	4.5.5	4.5.4.2	9.2	6
Continual improvement	8.5.1	4.5.3	4.6	4.5.5	10	8
Management review	5.6	4.6	4.6	4.5.4.3	9.3	7

Supply Chain Security - The Business Benefits

ISO 28000, although dedicated to supply chain security, is potentially applicable to any organization that wishes to implement self-assessment or become certified to an internationally recognized security management standard.

There are several motives why one might seek this certification. Some of the key benefits include:

- Integrated enterprise resilience
- Systematized management practices
- Enhanced credibility and brand recognition
- Aligned terminology and conceptual usage
- Improved supply chain performance
- Benchmarking against internationally recognizable criteria
- Greater compliance processes

Implementation of SCSMS with IMS2 methodology

Considering the well documented benefits of implementing a Supply Chain Security Management System based on ISO 28000, makes the proposal easier to decide on.

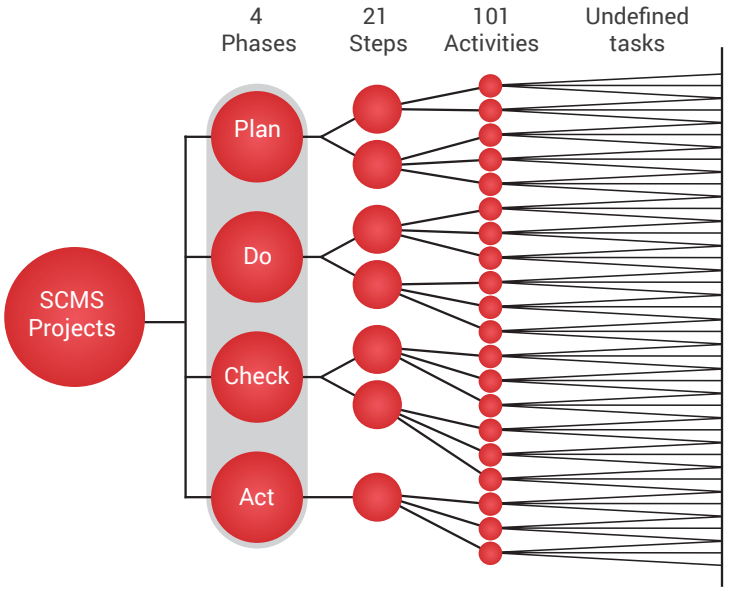
Most companies now realize that it is not sufficient to implement a generic, "one size fits all" social security plan. For an effective response, with respect to maintaining the supply chain, such a plan must be customized to fit to a company. A more difficult task is the compilation of an implementation plan that balances the requirements of the standard, the business needs and the certification deadline.

There is no single blueprint for implementing ISO 28000 that will work for every company, but there are some common steps that will allow you to balance the frequent conflicting requirements and prepare you for a successful certification audit.

PECB has developed a methodology (please see example below) for implementing a management system; the "Integrated Implementation Methodology for Management Systems and Standards (IMS2)", and it is based on applicable best practices. This m;ethodology is based on the guidelines of ISO standards and also meets the requirements of ISO 28000.

1. Plan	2. Do	3. Check	4. Act
1.1 Initiating the QMS	2.1 Organizational Structure	3.1 Monitoring, Measurement, Analysis and Evaluation	4.1 Treatment of Non-conformities
1.2 Understanding the Organization	2.2 Document Management	3.2 Internal Audit	4.2 Continuous improvement
1.3 Analyze the Existing System	2.3 Design of Controls and Procedures	3.3 Management Review	
1.4 Leadership and Project Approval	2.4 Communication		
1.5 Scope	2.5 Awareness and Training		
1.6 Security Policy	2.6 Implementation of Controls		
1.7 Risk Assessment	2.7 Incident Management		
1.8 Objectives, Targets and Programmes	2.8 Operations Management		

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 of the implementation project from the starting point to the finishing point and suggests the appropriate 'best practice' for each one, while directing you to further helpful resources as you embark on your ISO 28000 journey.



The sequence of steps can be changed (inversion, merge). For example, the implementation of the management procedure for documented information can be completed 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 following common processes for an organization that wishes to be certified against ISO 28000 are:

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 perform 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 should be performed on-site at the organization's premises.
6. ***Stage 2 audit (On-site visit):*** 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.
7. ***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).
8. ***Confirmation of registration:*** If the organization is compliant with the conditions of the standard, the Registrar confirms the registration and publishes the certificate.
9. ***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 supply chain security systems based on ISO 28000.

Training title	Short description	Who should attend
ISO 28000 Introduction	• One day training • Introduction to concepts • management and implementation of a SCSMS • Do not lead to certification	• Members of an supply chain security team • Supply chain professionals wanting to gain a comprehensive knowledge of the main processes of a Supply Chain Security Management System (SCSMS) • Staff involved in the implementation of the ISO 28000 standard • Employees involved in operations related to a SCSMS • Auditors
ISO 28000 Foundation	• A two days training • Become familiar with best practices for implementation and management of SCSMS • One hour exam	• Members of an supply chain security team • Physical security professionals wanting to gain a comprehensive knowledge of the main processes of a Supply Chain Security Management System (SCSMS) • Staff involved in the implementation of the ISO 28000 standard • Employees involved in operations related to a SCSMSAuditors

ISO 28000 Lead Implementer	• A five days training • Manage the implementation and a management of a BCMS • Three hours exam	• Project managers or consultants wanting to prepare and support an organization in the implementation of a Supply Chain Security Management System (SCSMS) • ISO 28000 auditors who wish to fully understand the Supply Chain Security Management System implementation process • Persons responsible for the supply chain security conformity in an organization • Members of an supply chain security team • Expert advisors in physical security • Technical experts wanting to prepare for an supply chain security function or for a SCSMS project management function
ISO 28000 Lead Auditor	• A five days training • Manage the audit of a SCSMS • Three hours exam	• Internal auditors • Auditors wanting to perform and lead Supply Chain Security Management System (SCSMS) certification audits • Project managers or consultants wanting to master the Supply Chain Security Management System audit process • Persons responsible for the supply chain security or conformity in an organization • Members of a supply chain security team • Expert advisors in supply chain security • Technical experts wanting to prepare for an supply chain security audit function

Choosing the right certifications

The ISO 28000 Foundation certification is a professional certification for professionals needing to have an overall understanding of the ISO 28000 standard and its requirements.

The ISO 28000 Implementer certifications are professional certifications for professionals needing to implement a SCSMS and, in case of the ISO 28000 Lead Implementer Certification, needing to manage an implementation project.

The ISO 28000 Auditor certifications are credentials for professionals needing to audit a SCSMS and, in case of the "ISO 28000 Lead Auditor" Certification, needing to manage a team of auditors.

The ISO 28000 Master certification is a professional certification for professionals needing to implement a SCSMS and to master the audit techniques and manage (or be part of) audit teams and audit program.

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 been performing by the past or which 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 c ertification	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 Implement-er 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