PECB

When Recognition Matters

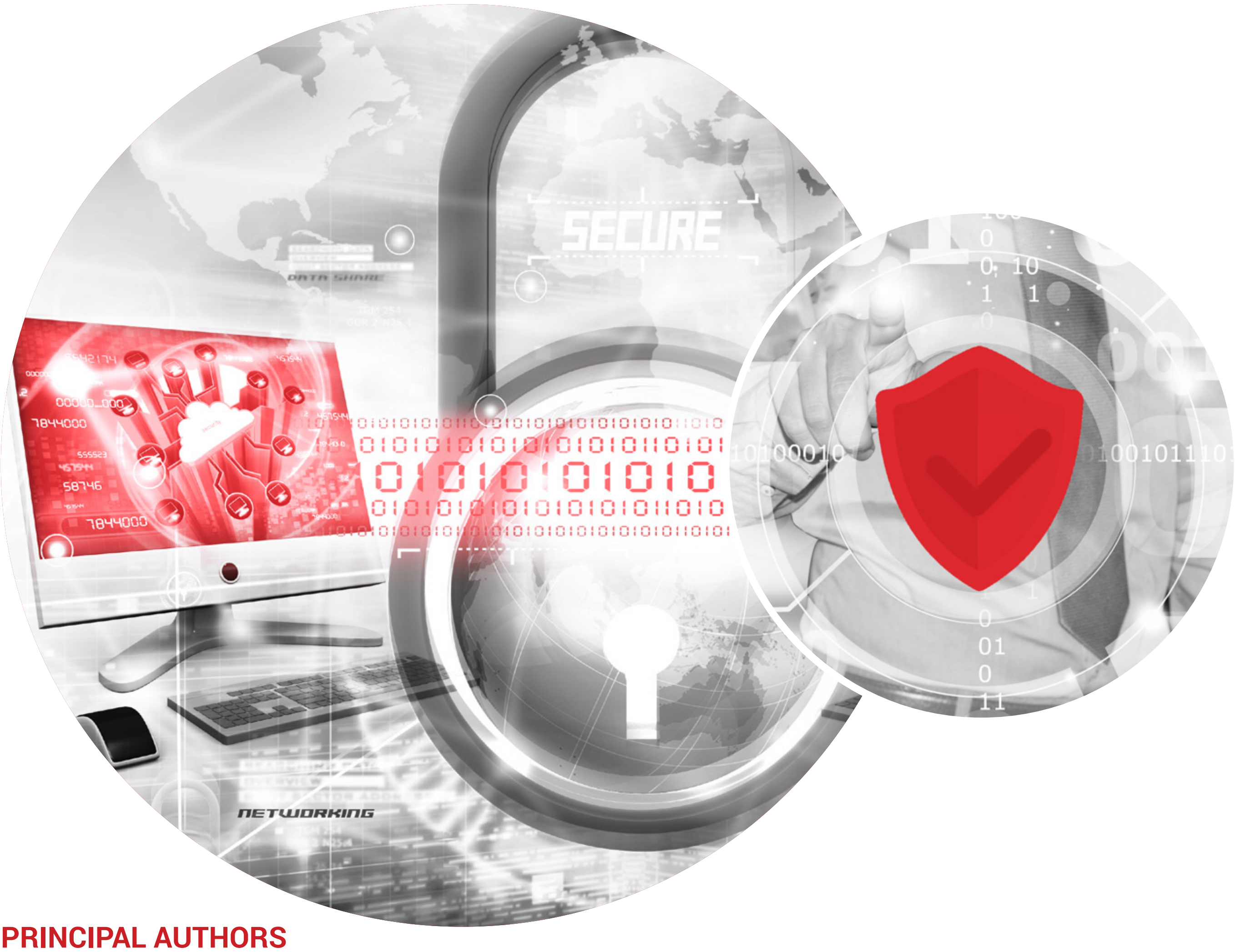
WHITEPAPER

ISO/IEC 27005

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES INFORMATION SECURITY RISK MANAGEMENT

www.pecb.com

CONTENT



PRINCIPAL AUTHORS
Eric LACHAPELLE, PECB
Rrezarta HALILI, PECB

EDITORS:
Anders CARLSTEDT, Carstedt Inc.

Published on November 20th, 2015

INTRODUCTION

Information Security Risk Management, as proposed by this standard, goes beyond specific passwords, firewalls, filters and encryption. Its comprehensive approach, for the time being part of a growing family of ISO/IEC 27000 series of standards in the area of information security management systems, helps businesses take a structured approach of managing information security risks. It is a supportive standard which provides guidelines.

However, this standard does not go into details of giving strict specifications and recommendations or, naming any specific risk analysis method, although it specifies rigorous processes which should to be undertaken by organizations in order to create a risk treatment plan.

What is Information Security Risk Management?

Information Security Risk Management is the coordinated activities to direct and control an organization to effectively assess and address information security risks over time.

Organizations of any size and type can benefit from this standard, by engaging in a comprehensive and systematic preventive, protective, preparatory, and mitigation process. Simply drafting a response plan that anticipates and minimizes the consequence of information security incidents is not sufficient anymore, but organizations also need to take adaptive and proactive measures to reduce the probability of such an event.

An effective information security risk management process as recommended by ISO/IEC 27005 is key to a successful ISMS as the ISO/IEC 27000 series are deliberately risk-aligned, where at first, it is important for organizations to assess risks before coming with management and risk treatment plans.

ISO/IEC 27005 is developed on account of helping organizations improve the information security risk management, and minimize the risk of business disruption.

Although it does not mention them, as a matter of the employment of risk treatment, the standard allows methods such as OCTAVE, EBIOS, MEHARI, and NIST 800-30. Nevertheless, when using this standard, the organization would still learn how to implement, conduct and maintain a formal process of risk assessment, risk treatment, risk acceptance, communication, consultation, monitoring and review.

Key clauses of ISO/IEC 27005:2011

ISO/IEC 27005 is organized into the following main clauses:

Clause 5: Background
Clause 6: Overview of the information security risk management process
Clause7: Context establishment
Clause 8: Information security risk assessment
Clause 9: Information security risk treatment
Clause 10: Information security risk acceptance
Clause 11: Information security risk communication and consultation
Clause 12: Information security risk monitoring and review

CLAUSE 5: BACKGROUND

The information security risk management process can be applied to part of an organization (i.e department, physical location, service), or to the organization as a whole, and to any information system. It is necessary that the approach to information security risk management is systematic, so that it can be effective. The approach should also be aligned with the overall objectives of the organization.

CLAUSE 6: OVERVIEW OF THE INFORMATION SECURITY RISK MANAGEMENT PROCESS

ISO/IEC 27005:2011 proposes a risk management process which follows 7 stages shown in the table below:

Risk Management Stages
1.Context establishment
2.Risk identification
3.Risk analysis
4.Risk evaluation
5.Risk treatment
6.Risk acceptance
7.Monitoring and review

These stages can be repeated in a cyclical process, and throughout this process, there should be proper risk communication and consultation in place.

CLAUSE 7: CONTEXT ESTABLISHMENT

This clause gives guidance regarding the information about the organization relevant to the information security risk management context establishment. It defines the basic criteria which needs to be established for the risk management approach, risk evaluation, impact, and risk acceptance.

Basic Criteria

An appropriate risk management approach addressing the basic criteria needs to be selected. Moreover, the organization has to assess the availability of the necessary resources to:

- Perform risk assessment and establish a risk treatment plan
- Define and implement policies and procedures, including implementation of the controls selected
- Monitor controls
- Monitor the information security risk management process.

Afterwards, there are a few issues which need to be considered when developing the risk evaluation criteria, such as:

- The strategic value of the business information process
- The criticality of the information assets involved
- Legal and regulatory requirements, and contractual obligations
- The operational and business importance of availability, confidentiality and integrity
- The expectations and perceptions of stakeholders, and negative consequences for goodwill and reputation

The impact criteria should also be determined, so that it shows how an information security event would have an impact on information assets, operations, business, financial value, plans, deadlines, reputation, and legal, regulatory or contractual requirements.

The criteria on risk acceptance depends on the organization, and may include e.g. multiple thresholds with a desired target level of risk, under the exceptions approved by top management. These criteria can be expressed as a ratio of estimated profit to the estimated risk.

Scope and boundaries

The scope of information security risk management needs to be defined by the organization. This enables the organization to make sure that relevant assets are considered in the risk assessment. The scope of information security usually consists of the organization's strategic business objectives, functions, legal requirements, contractual requirements, information security policy, overall approach to risk, geographical locations, constraints and interference.

Scope and boundaries

Information security risks should to be managed through an organization which needs to develop the information security risk management processes, the analysis of stakeholders, to define the responsibilities of each internal and external party, and the decision escalation path, and specify records which need to be kept.

CLAUSE 8: INFORMATION SECURITY RISK ASSESSMENT

Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or may exist), the existing controls and their effect on the risk identified, determines the potential consequences, and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.

The following activities are involved in the risk assessment:

- Risk identification
- Risk analysis
- Risk evaluation

Risk identification

The purpose of risk identification is to determine what may happen to cause a potential loss, and to gain an insight into how, where and why the loss might happen. Risk identification includes the following steps:

- Identification of assets – including more than just hardware and software
- Identification of threats – probable to be of natural or human origin, and could be accidental or deliberate.
- Identification of existing controls – a list of controls can be found in ISO/IEC 27001
- Identification of vulnerabilities – probable to exist in the organization, processes and procedures, management routines, personnel, physical environment, information system configuration, hardware, software or communications equipment, dependence on external parties
- Identification of consequences – possible to be manifested as a loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.

Risk analysis

The sub-clause of risk analysis is divided into three important sections:

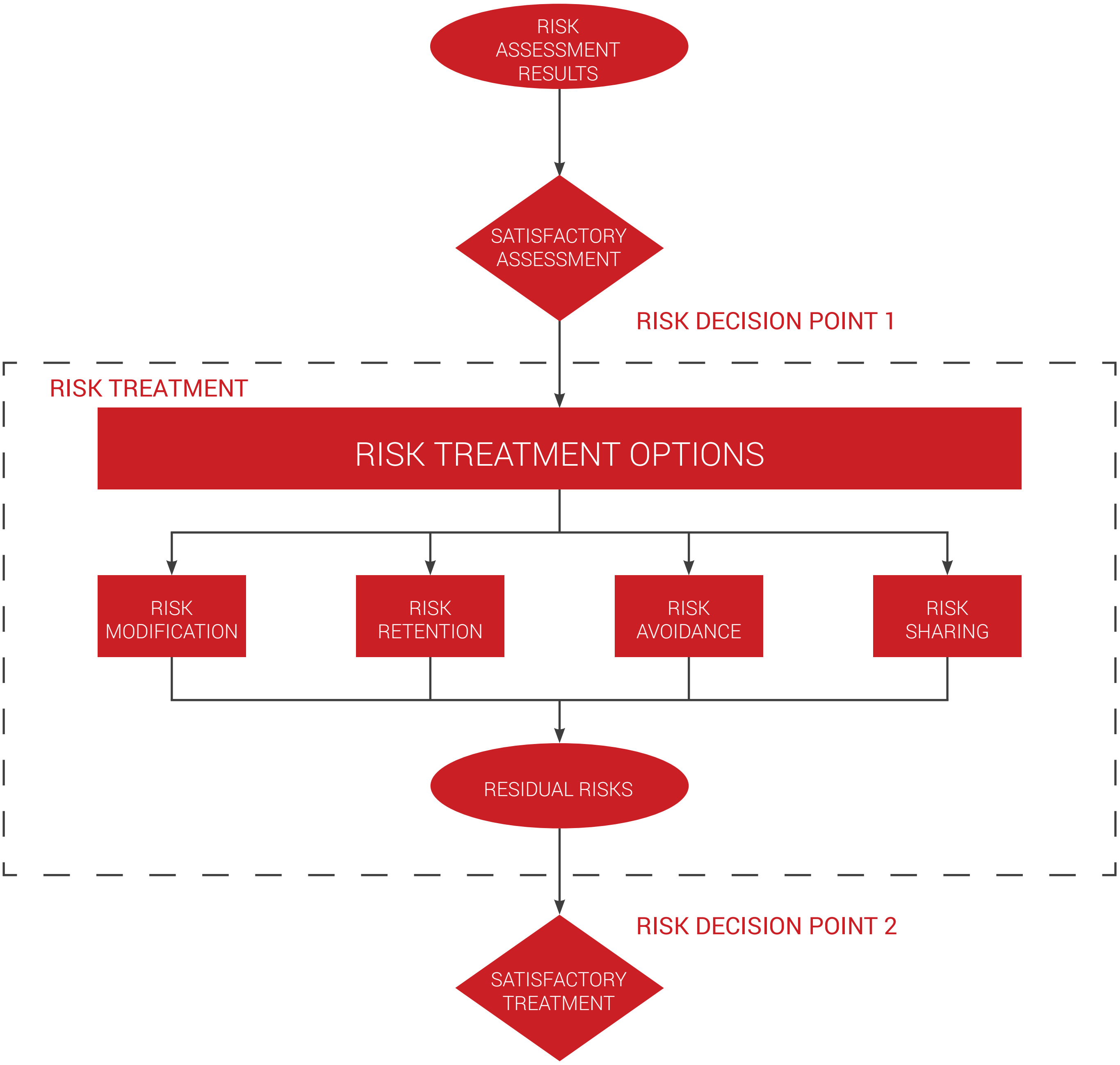
- Risk analysis methodologies – can be divided into qualitative and quantitative.
- Assessment of consequences – heavily reliant on asset valuation.
- Assessment of incident likelihood – takes into account how often the threats occur, and how easily the vulnerabilities may be exploited.
- Level of risk determination – outputs a list of risks with values levels assigned.

Risk evaluation

Taking into the consideration the new understandings obtained from the risk analysis, risk evaluation also involves the decisions which need to be taken in cases when an activity should be taken or not, or what are the priorities for risk treatment, considering the estimated levels of risk.

CLAUSE 9: INFORMATION SECURITY RISK TREATMENT

According to this clause, risk can be treated through risk modification, risk retention, risk avoidance and risk sharing, a selection based on risk assessment outcomes and a cost-benefit analysis.



Risk modification: This is achieved through changing the controls which may protect assets through correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness. When changing the controls, it is important to make sure that the solution is sufficient for both performance requirements and information security. Usually, constraints are a hindrance when trying to change the controls to modify the risk such as time, financial and technical constraints, etc.

Risk retention: If according to risk evaluation the results show that the risk is acceptable, it can simply be retained with no need to change any controls.

Risk avoidance: This can be achieved through completely avoiding an activity or risk which gives a rise to the condition. This option is suitable when the costs of treating a risk are too high, or the risk itself is too high.

Risk sharing: This risk treatment option involves other parties such as insurance companies, or sub-contractors who would monitor the information system against an attack. However, this does not mean that the liability is shared, since the responsibility for the consequences still lies with the organization.

CLAUSE 10: INFORMATION SECURITY RISK ACCEPTANCE

Following the risk treatment, an organization needs to make decisions about the risk acceptance of the residual risk which has been reviewed and approved by the responsible managers. As a result, accepted risks are listed by the organization with justification for the risks that do not meet the organization's normal risk acceptance criteria.

CLAUSE 11: INFORMATION SECURITY RISK COMMUNICATION AND CONSULTATION

According to this clause, information security risks need to be communicated between the responsible individuals and the stakeholders. This communication of information security risk should provide assurance of the outcome of the risk management, share the results of the risk assessment, support decision-making, improve awareness, etc. A risk communication plan should be developed by the organization for both, normal operations and emergency situations. The outcome of all this should be a continual understanding of the organization's information security risk management process and results.

CLAUSE 12: INFORMATION SECURITY RISK MONITORING AND REVIEW

This clause provides monitoring and review for the information security risk factor as well as for the risk management.

Monitoring and review of risk factors:Since risks may change due to changes in vulnerabilities, likelihood or consequences, the organization needs constant monitoring. Especially, the organization needs to make sure to monitor the following:

- New assets within the scope of risk management
- Modified asset values
- New threats
- New vulnerabilities
- Increased impact or consequences which result in unacceptable level of risk
- Information security incidents

Monitoring and review of risk management, and improvement:Ongoing monitoring and review of information security risk management are necessary so that the organization can make sure that the context, the risk assessment outcome, risk treatment and management plans remain relevant and appropriate to the circumstances. Further, the necessary improvements need to be made with the knowledge of appropriate managers. The issues which need to be addressed at this stage are: old criteria verification, legal and environmental context, competition context, risk assessment approach, asset values and categories, total cost of ownership and necessary resources. The result of this monitoring and improvement could be the modification or addition to the approach, methodology, or tools used in the risk management process.

ISO/IEC 27000 family of standards

ISO/IEC 27005 is a supporting and informative standard to other standards, and especially those related to Information Security. For a partial list of those standards, examples in the table below:

Part of the Information Security Management System Family of Standards (27000)			
27000	Overview and vocabulary	27007	Auditing guidelines
27001	Requirements	27008	Guidance for auditors on ISMS controls
27002	Code of practice	27011	Guidelines for telecommunication organizations
27003	Implementation guidance	27013	Integrated ISO 27001 with ISO 20000 guidelines
27004	Measurement	27015	Guidelines for financial services
27005	Information Security Risk Management	27032	Guidelines for cybersecurity
27006	Audit and certification bodies requirements	27035	Security incident management

Link with other information security standards and methods

There are other widely used standards which are related to ISO/IEC 27005, such as:

- ISO 31000
- OCTAVE – Operationally Critical Threat, Asset, and Vulnerability Evaluation
- EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité developed by ANSSI in France
- MEHARI method – Method for Harmonized Analysis of Risk
- NIST 800-30 – National Institute of Standards and Technology
- Harmonized TRA method – (The Right Approach)

Links with ISO/IEC 27001 and ISO 31000

ISO/IEC 27005 is closely linked with the parts of ISO/IEC 27001 which deal with risk management. ISO/IEC 27005's generic framework on risk management applied to information security is actually a detailed elaboration of Clauses 4.2.1c to 4.2.1h, and 4.2.3d of ISO/IEC 27001, also closely linked with the generic framework on the risk management of ISO 31000. ISO/IEC 27005:2011 is aligned to the generic requirements of risk management as presented in ISO 31000.

Information Security Risk Management-The Business Benefits

As with all major undertakings within an organization, it is essential to gain the backing, support and sponsorship of the executive management. Often the best way to achieve this is to illustrate advantage of having an effective information security risk management process in place, rather than highlight the negative aspects of the contrary.

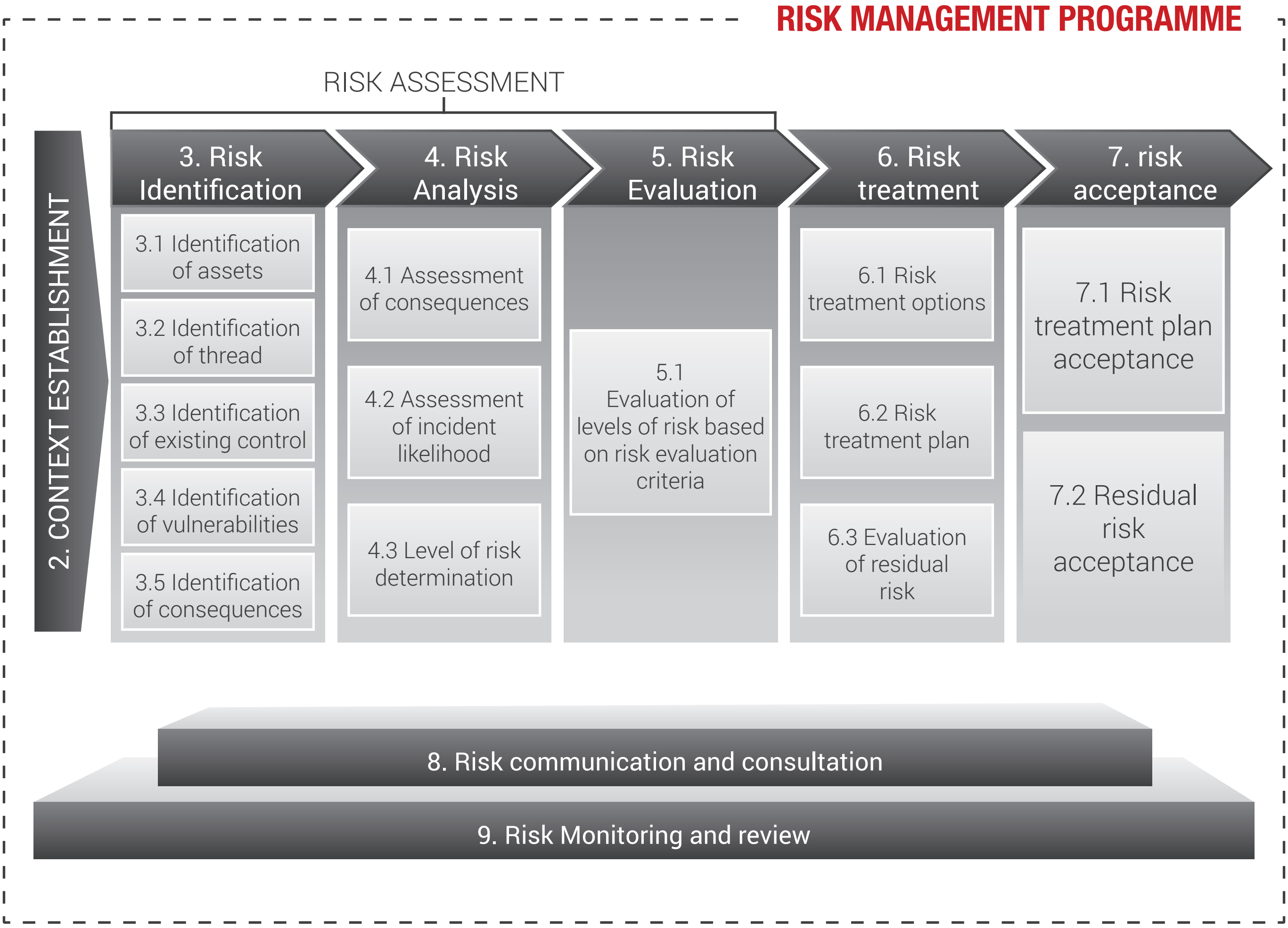
An organization which adopts ISO/IEC 27005 - Information Security Risk Management - will attain a number benefits, including the following:

- Increase the likelihood of achieving information security objectives and the general objectives of the organization
- Encourage proactive information security management
- Be aware of the need to identify and treat information security risk throughout the organization
- Improve the identification of opportunities and threats to the information security
- Comply with relevant legal and regulatory requirements and international norms
- Improve mandatory and voluntary reporting
- Improve governance
- Improve stakeholder confidence and trust
- Establish a reliable basis for decision making and planning
- Improve controls
- Effectively allocate and use resources for information security risk treatment

Implementation of Information Security Risk Management using the PECB Risk Management Framework

Making the decision to implement an information security management system based on ISO/IEC 27005 most of the time, is a very simple one, as the benefits are well documented. Most companies now realize that it is not sufficient to implement a generic, "one size fits all" information security plan.

A framework has been developed by PECB for information security risk management as shown below:


RISK MANAGEMENT PROGRAMME
RISK ASSESSMENT
2. CONTEXT ESTABLISHMENT
3. Risk Identification
3.1 Identification of assets
3.2 Identification of thread
3.3 Identification of existing control
3.4 Identification of vulnerabilities
3.5 Identification of consequences
4. Risk Analysis
4.1 Assessment of consequences
4.2 Assessment of incident likelihood
4.3 Level of risk determination
5. Risk Evaluation
5.1 Evaluation of levels of risk based on risk evaluation criteria
6. Risk treatment
6.1 Risk treatment options
6.2 Risk treatment plan
6.3 Evaluation of residual risk
7. risk acceptance
7.1 Risk treatment plan acceptance
7.2 Residual risk acceptance
8. Risk communication and consultation
9. Risk Monitoring and review

Certification of organizations

The usual path for an organization wishing to be certified against ISO/IEC 27001 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 should previously have produced one internal audit report and one management review at least.

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 for identifying any possible gap between its current management system and the applicable standard requirements.

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): The Stage 2 audit objective is to evaluate whether the declared management system conforms to all the requirements of the standard, has been subject to an actual implementation in the organization, and can support the organization in achieving its established objectives. This stage 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 the action plans linked to the non-conformities only.

8. Confirmation of registration: If the organization is compliant with the requirements 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 for verifying the conformity of the certified client's management system and can also include investigations e.g.: following a complaint, the review of a website, or a written request for follow-up, etc.

Training and certifications of professionals

PECB has created a recommended training roadmap and a number of personnel certification schemes for implementers and auditors of an organization wishing to get certified against ISO/IEC 27001. Whereas, certification of organizations is a vital component in the information security field as it provides the evidence that organizations developed standardized processes based on best practices; certification of individuals also serves as documented evidence of professional competencies and experience for/of those individuals that have previously attended one of the related courses and exams.

It serves to demonstrate that the certified professional holds defined competencies based on best practices. It also allows organizations to make an informed selection of employees or services based on the competencies 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 the training and awareness have been effective.

PECB training courses are offered globally through a network of authorized training providers and they are available in several languages and include different levels such as introduction, foundation, implementer and auditor courses. The table below gives a short description on PECB's official training courses for Information Security Risk Management based on ISO/IEC 27005.

Training title	Who should attend
• Introduction to ISO/IEC 27005 • ISO/IEC 27005 Risk Manager • ISO/IEC 27005/31000 Risk Manager with OCTAVE • ISO/IEC 27005/31000 Risk Manager EBIOS • ISO/IEC 27005/31000 Risk Manager with MEHARI • ISO/IEC 27005/31000 Risk Manager with introduction to methodologies	• Risk managers • Persons responsible for information security or conformity within an organization • Members of the information security team • IT consultants • IT professionals wishing to obtain a comprehensive understanding of risk management within an organization • Staff implementing or seeking to comply with ISO/IEC 27001 or involved in a risk management program, also including those based on OCTAVE, EBIOS, and MEHARI.

Although a specified set of courses or curriculum of study is not required as part of 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. You can verify the list of approved organization that offers PECB official training sessions on our website at www.pecb.com

CHOOSING THE RIGHT CERTIFCATION

The "Certified ISO/IEC 27005 Lead Risk Manager" credential is a professional certification for professionals needing to demonstrate the competence to implement, maintain and manage an ongoing information security risk management program according to ISO/IEC 27005, while the Provisional Risk Manager is granted to those who do not have sufficient professional experience, but have finished the training and passed the exam.

Based on your overall professional experience and acquired qualifications, you will get granted one of these certifications.

Certification	Exam	Professional experience	Risk assessment experience	Other requirements
Certified ISO/IEC 27005 Provisional Risk Manager	Certified ISO/IEC 27005 Risk Manager Exam	None	None	Signing the PECB code of ethics
Certified ISO/IEC 27005 Risk Manager	Certified ISO/IEC 27005 Risk Manager Exam	**Two years** One year of risk management related work experience	Risk management activities totaling 200 hours	Signing the PECB code of ethics

PECB

+1-844-426-7322

customer@pecb.com

Customer Service

www.pecb.com