PECB

When Recognition Matters

WHITEPAPER

ISO 27034

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – APPLICATION SECURITY

www.pecb.com

CONTENT

PRINCIPAL AUTHORS

Eric LACHAPELLE, PECB

Mustafe BISLIMI, PECB

Bardha AJVAZI, PECB

INTRODUCTION

Software plays a significant role in virtually every aspect of our lives. Many organizations take information security measures and controls to protect their information, information assets and business processes. However, without a formally specified information security management system (ISMS), these controls are inclined towards disorganization and disconnection, since they are mostly implemented as ad hoc temporary solutions to certain situations.

Application Security Survey
In a survey of more than 100 banking/security leaders, 57% of respondents say they are a bit or very confident in their own applications, and 90% say application security is somewhat or a significant part of their overall information security programs.
Still, when it comes to applications developed or managed by third-party service providers, 81% are only somewhat or not at all confident in the security, and this faith erodes even further with large institutions ($2 billion or more in assets under management), where 91% are only somewhat/not at all confident.

Organizations face an ever-growing need to protect their information through the application level. Applications should be protected against exposures which might be inherent to the application itself (e.g. software defects), that appear in the course of the application's life cycle (e.g. through changes to the application), or arise due to the use of the application in a context for which it was not intended.

Application Security serves as guidance on information security to those specifying, designing/programming or procuring, implementing and using application systems, i.e. in business and IT management, developers and auditors and specially the end-users of application systems. The purpose is to guarantee that computer applications deliver the desired/necessary level of security in support of the organization's Information Security Management System.
Using a methodical approach to increase application security provides indication that information being used or stored by an organization's applications is adequately protected.

Applications can be established through internal development, outsourcing or purchasing a commercial product. Applications can also be acquired through a combination of these approaches, which in cases may present new security effects that should be considered and managed.

Some examples of application models are: human resource systems, finance systems, word-processing systems, customer management systems, firewalls, anti-virus systems and intrusion detection systems.

TypedQuery<Person> query = em.createQuery(
parameters.contains("name")){
values[0]
12

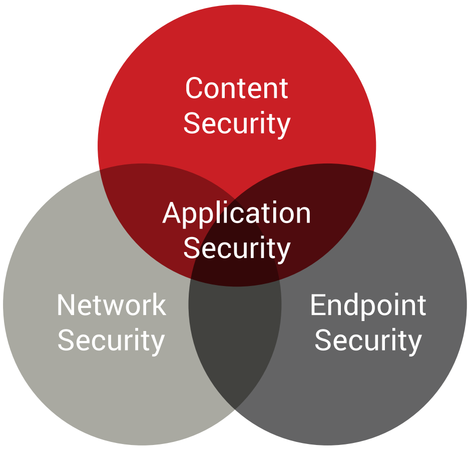
An Overview of ISO/IEC 27034

The ISO/IEC 27034 is a multi-part standard (six documents or parts) that provides guidance on specifying, designing, selecting and implementing information security controls through a set of processes integrated throughout an organization's Systems Development Life Cycle/s (SDLC).

ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

ISO/IEC 27034 is made to assist organizations in integrating security easily throughout the life cycle of their applications, by providing concepts, principles, frameworks, components and processes.

The requirements and processes specified in ISO/IEC 27034 are not planned to be implemented in isolation but rather integrated into an organization's existing processes.



Security requirements should be defined and analyzed for each and every stage of an application's life cycle adequately addressed and managed on a constant basis.

ISO/IEC 27034 - Information technology — Security techniques — Application security is currently developed into one part:

Part 1: Overview and concepts

However, the following parts are under preparation:
Part 2: Organization normative framework
Part 3: Application security management process
Part 4: Application security validation
Part 5: Protocols and application security control data structure

Key Clauses of ISO/IEC 27034

ISO 27034 is organized into the following main clauses:

Clause 5: Structure of ISO/IEC 27034
Clause 6: Introduction to Application Security
Clause 7: ISO/IEC 27034 Overall Processes
Clause 8: Concepts

Each of these key activities is listed and described below.

At the November 2012 Cloud Security Alliance Congress, US Bank gave a financial services view of the importance of software applications. Compromised software is a tremendous risk to the global economy. 93.6% of the total global currency, or $212 trillion, is digital, and exists in software only.

Clause 5: Structure of ISO/IEC 27034

ISO/IEC 27034 consists of six documents or parts:

Part 1 (Overview and concepts) presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

Part 2 (Organization normative framework) presents an in-depth discussion of the Organization Normative Framework, its components and the organization-level processes for managing it.

Part 3 (Application security management process) presents an in-depth discussion of the processes involved in an application project, such as: determining the application requirements and environment, assessing the application security risks, creating and maintaining the Application Normative Framework, realizing and operating the application and validating its security throughout its life cycle.

Part 4 (Application security validation) presents an in-depth discussion of the application security validation and certification process that measures the application's Actual Level of Trust and compares it with the application's Targeted Level of Trust previously selected by the organization.

Part 5 (Protocols and application security control data structure) presents the protocols and XML schema for the Application Security Control (ASC) based on the ISO/IEC TS 15000 series: Electronic business eXtensible Markup Language (ebXML).

Part 6 (Security guidance for specific applications) if necessary, could provide examples of ASCs tailored for specific application security requirements.

Clause 6: Introduction to Application Security

Application security protects the critical data computed, used, stored and transferred by an application as required by an organization. This clause includes the application security scope, application security requirements, risk, security costs, target environment, controls and objectives.

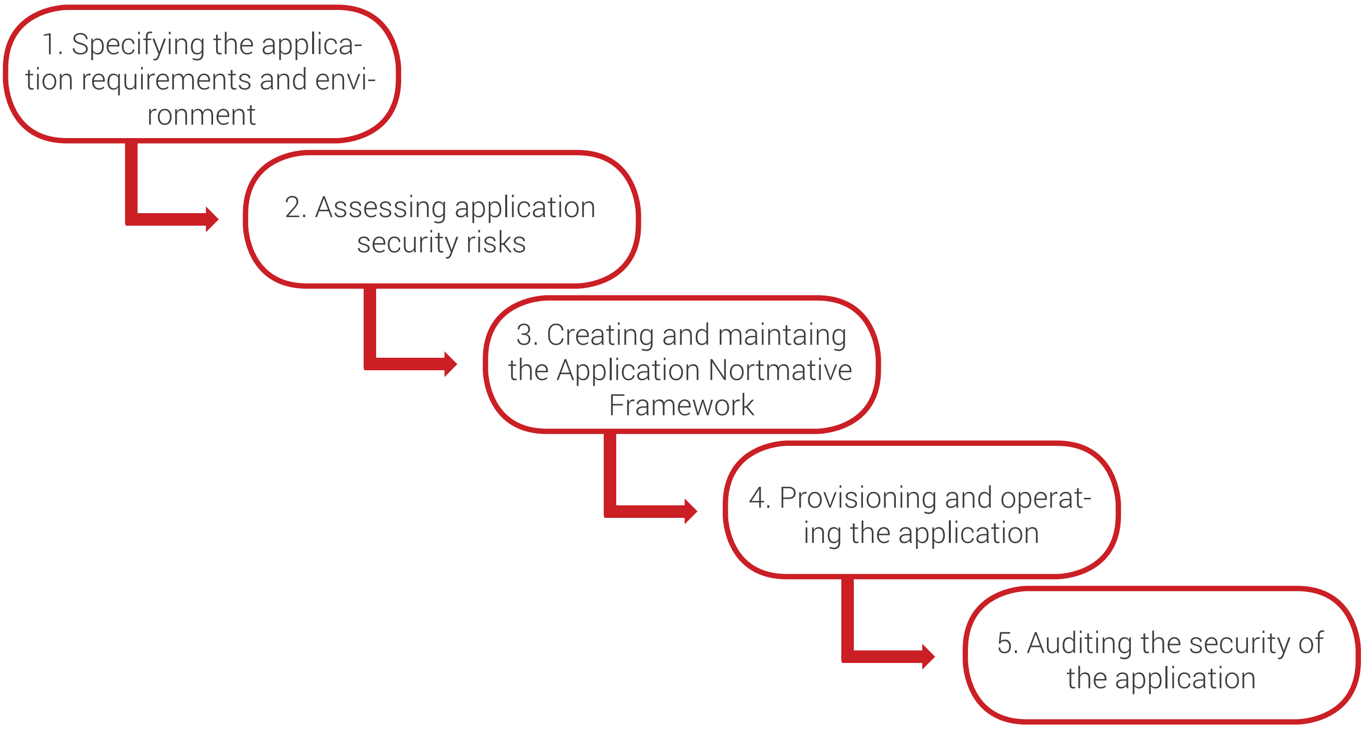
Controls and measurements can be applied to the application itself, to its data, and to all technology, processes and actors involved in the application's life cycle.

Clause 7: ISO/IEC 27034 Overall Processes

ISO/IEC 27034 provides components, processes and frameworks to help organizations acquire, implement and use trustworthy applications, at an acceptable (or tolerable) security cost. More specifically, these components, processes and frameworks provide verifiable evidence that applications have reached and maintained a Targeted Level of Trust

All components, processes and frameworks are part of two overall processes:

1. The Organization Normative Framework Management Process (ONF) – used for managing the application security-related aspects of the ONF.
2. The Application Security Management Process (ASMP) – used for managing security for each application used by an organization. This process is performed in five steps:



1. Specifying the application requirements and environment

2. Assessing application security risks

3. Creating and maintaing the Application Nortmative Framework

4. Provisioning and operating the application

5. Auditing the security of the application

Clause 8: Concepts

- The Organization Normative Framework (ONF) is a framework where all application security best practices recognized by the organization are stored, or from which they will be refined or derived. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself.

- The Application Security Risk Assessment is the second step of the risk management process, which applies the risk assessment process at the application level.

- Application Normative Framework is the third step, which is a subset or modification of the ONF that contains only the detailed information as required for a specific application to reach the Targeted Level of Trust required by the application owner during the final acceptation process element of step 2 of the ASMP.

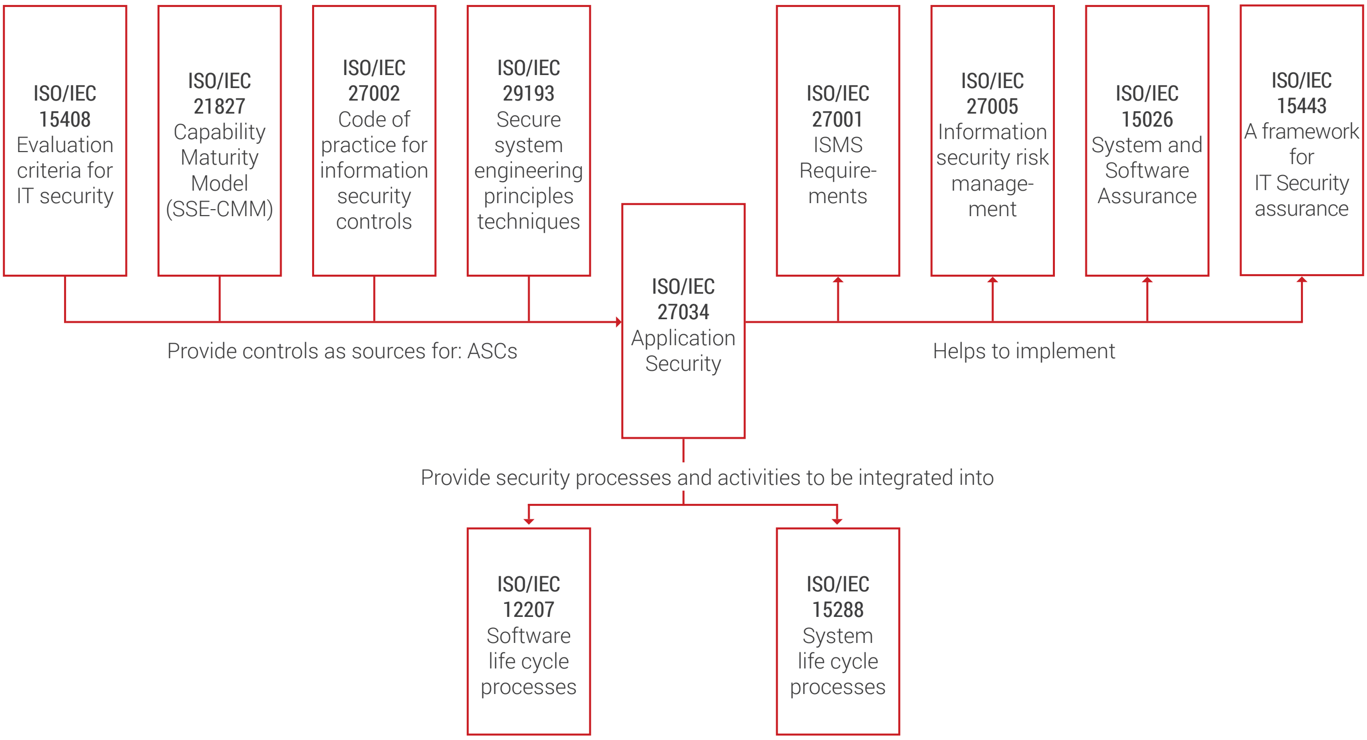
- Provisioning and Operating the Application is the fourth step of the ASMP, which involves the deployment and follow-up within the application project.

According to ISO/IEC 27005,
"Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies 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."

- Application Security Audit is the fifth step of the ASMP, which deals with the verification and recording of the supporting evidence of whether or not a specific application has attained its Targeted Level of Trust.

Link of ISO/IEC 27034 with other Information Security Standards and Guidelines

Apart from the ISO 27034, other well-known standards which relate to information security are shown in the graph below:


ISO/IEC 15408 Evaluation criteria for IT security
ISO/IEC 21827 Capability Maturity Model (SSE-CMM)
ISO/IEC 27002 Code of practice for information security controls
ISO/IEC 29193 Secure system engineering principles techniques
ISO/IEC 27001 ISMS Require-ments
ISO/IEC 27005 Information security risk manage-ment
ISO/IEC 15026 System and Software Assurance
ISO/IEC 15443 A framework for IT Security assurance
ISO/IEC 27034 Application Security
Provide controls as sources for: ASCs
Helps to implement
Provide security processes and activities to be integrated into
ISO/IEC 12207 Software life cycle processes
ISO/IEC 15288 System life cycle processes

How does ISO/IEC 27034 oppose to ISO 27001 and other International Standards and Frameworks?

Apart from the ISO 27034, other well-known standards which relate to information security are shown in the graph below:

While ISO/IEC 27034 does not depend on ISO/IEC 27001 and is used independently, it is well aligned with ISO/IEC 27001.

ISO/IEC 27034 is similar to ISO/IEC 27001 for the reason that they both provide an application security code of practice that can use the systematic "Plan-Do-Check-Act" methodology.

It is expected that ISO/IEC 27034 will become a key tool to be used to assess any software development company looking for an ISO/IEC 27001 certification; that is if the software development lifecycle is in the scope of the certification.

Other information security standards that reference application security are:

- PCI-DSS - Payment Card Industry Data Security Standard (2004)
- COBIT – Control Objectives for Business and related Technology (1994+)
- NISTIR 7628. - NIST Guidelines for Smart Grid Cyber Security. (2010)
- SAFEcode – promotes the advancement of effective software assurance methods. (2007)
- Cloud Security Alliance Cloud Controls Matrix – Security controls for cloud computing (2008)

What are the Benefits of Application Security?

As with all the major undertakings within an organization, it is essential to gain the backing and sponsorship of the executive management. By far, the best way to achieve this is to illustrate the positive gains of having an effective application security management process in place, rather than highlight the negative aspects of the contrary.

Today an effective application security management system is not about being forced into taking action to address external pressures, but its importance relies on recognizing the positive value of application security management when good practice is embedded throughout your organization.

Predictable and effective response to application security incidents	Protection of people	Maintenance of vital activities of the organization	Better understanding of the organization
Cost reduction	Respect of the interested parties	Protection of the reputation and brand	Confidence of clients
Competitive advantage	Legal compliance	Regulatory compliance	Contract compliance

The adoption of an effective application security management process within an organization will have benefits in a number of areas, examples of which include:

1. Protection of shareholder value;
2. Increase of confidence in the organization from interested parties;
3. Good governance;
4. Conformity;

5. Strong consideration of the implications for application security legislation and duties of care;
6. Avoidance of liability actions;
7. Cost reduction;
8. Improved overall security; and
9. Marketing.

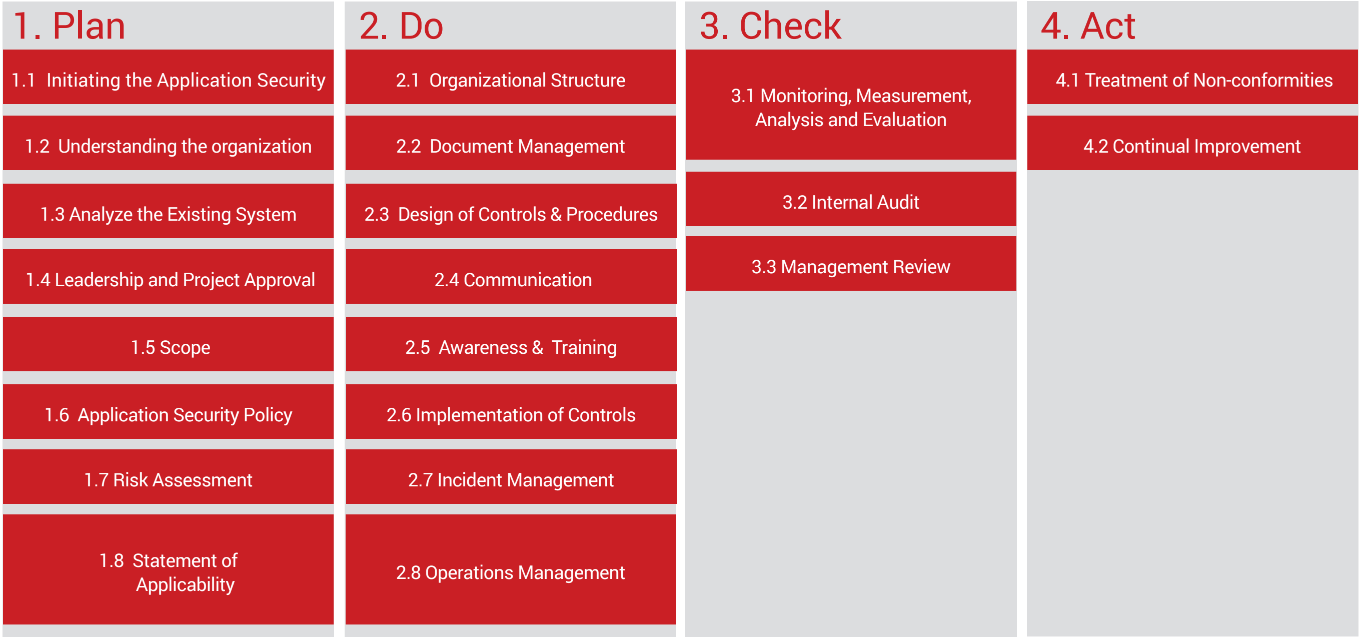
Why is PECB a Worthy Choice?

Implementation of an ISMS with IMS2 Methodology

Making the decision to implement an Application Security based on ISO 27034 is often 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. For an effective response, with respect to maintaining application security, such a plan must be customized to specific risks, and application security factors. A more difficult task is the compilation of an implementation plan that balances the requirements of the standard, the business needs and the deadline to become certified.

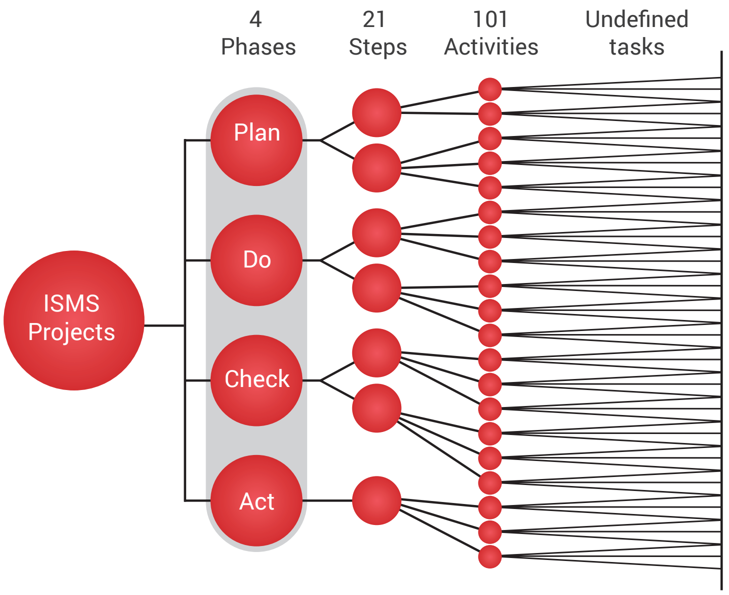
There is no single blueprint for implementing ISO 27034 that will work for every company, but there are some common steps that will allow you to balance the often conflicting requirements and prepare you for a successful certification audit.

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 27034.



1. Plan	2. Do	3. Check	4. Act
1.1 Initiating the Application Security	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 Continual Improvement
1.3 Analyze the Existing System	2.3 Design of Controls & Procedures	3.3 Management Review	
1.4 Leadership and Project Approval	2.4 Communication		
1.5 Scope	2.5 Awareness & Training		
1.6 Application Security Policy	2.6 Implementation of Controls		
1.7 Risk Assessment	2.7 Incident Management		
1.8 Statement of Applicability	2.8 Operations Management		

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.



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.

Steps for Obtaining a PECB Certification

For organizations:	For individuals:
1. Implement the management system	1. Participate in the training course
2. Perform internal audit and reviews	2. Register for the certification exam
3. Select preferred certification body	3. Sit for the certification exam
4. Perform a pre-assessment audit (optional)	4. Apply for the certification scheme upon successful completion
5. Perform the stage 1 audit	5. Obtain certification
6. Perform the stage 2 audit (on-site)	
7. Perform a follow-up audit (optional)	
8. Register the certification	
9. Assure continual improvement by conducting surveillance audits	

PECB

+1-844-426-7322

customer@pecb.com

Customer Service