PECB

When Recognition Matters

APPLICATION SECURITY MANAGEMENT WITH ISO/IEC 27034

Companies are dealing with many security efforts to protect their information. One of their biggest challenges is to have a security system that is operational, simple, organized, efficient and timely effective. Along with an information security management system (ISMS), companies should implement other processes and controls or comply with guidance guidelines that will ensure a secure information flow on their information systems and applications. Companies implementing ISO/IEC 27001, and companies who don't because of not seeing it as the priority on their agenda, ultimately still have to protect sensitive information, such as information collected, computed, stored and communicated by their applications. As a result of any breach or lost concerning organization's sensitive information, it can produce an unacceptable impact and make a difference between profitability and loss. Organizations' should make an investment to train their staff on standards such as ISO/IEC 27034 which specifically deals with application security. Furthermore, application security is not only about protecting an application, but rather about protecting sensitive information involved by the use of an application. Yet, not all applications have to be protected except those for manipulating sensitive information. Significantly, ISO/IEC 27034 provides clear guidance on why and how companies can identify, define and verify the security on a sensitive application. It also shows their conformance towards a measurable level of trust defined by ISO/IEC 27034.

WHAT ARE THE BENEFITS OF APPLICATION SECURITY?

ISO/IEC 27034 Application Security provides a framework that helps organizations to identify and protect specific application's sensitive information. Nonetheless, it is difficult and costly to try to protect all organization's applications.

Likewise, using a risk management approach, the ISO/IEC 27034 framework proposed components such as Application Security Controls (ASC) and processes to ensure that sensitive applications meet the Targeted Level of Trust (i.e. the required security level). This is done so that no sensitive information can be accessed, modified or lost by neither any unexpected event nor unauthorized person, internally or externally. Therefore, when ISO/IEC 27034 is well implemented and managed by an organization, it will not only help to provide expected and verifiable evidence to demonstrate that adequate protection of sensitive applications is in place, but it will also help to support the organization's ISMS and the ICT security. However, while trying to implement application security at a large organization, it might seem expensive and time-consuming. Still, using the ISO/IEC 27034 framework to implement Application Security will be an assurance for optimizing security implementation and the benefits are irreplaceable. Importantly, a well-managed application security process will provide you required evidence that you can trust your applications as adequately protected to face any incident (accepted risks) that may happen at that time.

The ISO/IEC 27034 framework will provide you clear guidance on how to handle the application security issues, taking in account your specific Business, Regulatory and Technological contexts.
Moreover, implementing ASCs identified by your Level of Trust is a set of processes that are not only well integrated on the System Development Life Cycle (SDLC), but also to your day-to-day operational processes.

Required ASCs can be implemented internally by the company employees or externally by outsourcing the companies that deal directly with the specified security matters. In both situations, these ASCs are verifiable and expected results can be provided to prove their adequate implementation. Without these evidence, a company cannot verify any successful security implementation.

Managing application security is not trivial. It's not only a code review process and vulnerability testing anymore. Application security is not only for organizations' developing application but for organizations that need to use and operate applications to make a successful business. Application security has to be planned, defined and managed in respect of organization's priorities and resources. Too much security is a waste of money, but not enough security can be a threat to the organization survival. Looking in that way, it's maybe better to invest in the necessary training and certification to make sure application security will be understood and well managed by your experts.

ISO/IEC 27034 AS GUIDANCE FOR APPLICATION SECURITY

Thinking of deeper security implementation implies that more procedures and standards should be considered. The proper implementation of ISO/IEC 27001 and its ISMS provide good assurance for information security matters on the company. But, ISMS' limitation is to identify what applications should be protected, and will not tell you what to do and that's where ISO/IEC 27034 gains all its value.

ISO/IEC 27034 Application Security standard content

PART 1 - Application Security: Overview and concepts (published)

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

PART 2 - Application Security: Organization Normative Framework (published)

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

This part explains the relationships among these processes, the activities associated with them, and the means by which they support the Application Security Management Process. It presents how an organization should implement the standard and integrate it into its existing processes.

PART 3 - Application Security Management Process (expected for 2017)

Part 3 presents an in-depth discussion of the processes involved in an application project: 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.

This part explains the relationships among these processes, their activities and interdependencies, and how they introduce security into an application project. It presents how an organization should implement the standard on an application project-level and integrate it into its existing processes.

PART 4 - Application Security Validation (work in progress)

Part 4 presents an in-depth discussion of the application security validation, audit and certification process for organizations, applications, and people.

It presents what and how the implementation of this IS should be verified and audited on three (3) levels, as:

1) Organization level – where it will frame and guide auditors to validate the organization's AS objectives and audit/verify how an organization complies with its AS objectives and criteria.
2) Application level – where it will frame and guide auditors to measure the application's Actual Level of Trust and compare it with the application's Targeted Level of Trust previously selected by the organization, to certify this application as secure as expected.
3) Peoples level – where it will frame and guide the development and the implementation of an ISO/IEC 27034 AS professional certification.

PART 5 - Protocols and application security control data structure (expected for 2017)

Part 5 presents the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model, in order to facilitate the implementation of the 27034 AS framework and the communication and exchange of ASCs.

PART 5.1 - Protocols and application security control data structure – XML Schemas (expected for 2017)

Part 5 presents and explains an XML Schemas example, describing the Application Security Control (ASC) and the Application Security Life Cycle Reference Model (ASLCRM) components.

PART 6 - Case studies (expected for 2017)

Part 6 provides case studies and examples of ASCs tailored for specific application security requirements.

PART 7 - Application Security Assurance Prediction Model (expected for 2017)

Part 7 codifies the requirements and framework for making predictive security claim statements to replace ASC in an AS project when allowed.

Each part is entitled to bring explanations on how to treat every aspect on Application Security. Organization security plans should be in accordance with the application security.

NOTE: Because of the ISO/IEC 27034 project still a work in progress, this list of parts is not definitive. Documents can be added or removed and document's name can be changed as the project will evolve.

PECB is a certification body for persons, management systems, and products for a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise in multiple fields, including ISO/IEC 27000 Information Security courses.

For further information, please visit: Information Security Management Courses or IT Security Courses

ABOUT THE AUTHORS

Gezim Zeneli is an Account Manager for Information Security at PECB. He is in charge of conducting market research while developing and providing information related to Information Security Standards. If you have any questions, please do not hesitate to contact: marketing.sec@pecb.com.

Mr. Luc Poulin has more than thirty years' experience in computer science, during which he acquired a solid expertise in IT systems and software engineering. He has specialized in managing, implementing and evaluating the overall security of information systems within development and operation environments.

He has a Ph.D CISSP-ISSMP CSSLP CISM CISA CASLI , CASLA and currently working as CEO- Information / Application Security Senior Advisor at Cogentas Inc. You can contact Luc via email Luc.Poulin@Cogentas.ca