TAKING CONTROL OF INFORMATION SECURITY

PECB
When Recognition Matters

www.pecb.com
Everyday information is collected, processed, stored and transmitted in many forms including electronic, physical and verbal, within all types of organizations. All this is reached by using a huge range of devices and systems starting from personal computers, cellular phones, servers, workstations, personal digital assistants, telecommunications networks systems, industrial/process control systems, environmental control systems, etc. So, organizations are trying to achieve their missions, objectives and their business functions in very complex atmosphere.

Information systems, or better say, their latest achievements are giving competitive advantages to organizations, and they are helping organizations to offer the best for their clients. However, now it is a known fact that same achievements have become serious threats of losing of functions, image, or reputation of organization.

As an answer to this, it is very important that leaders and managers at all levels go beyond understanding and thinking about Information system, they have to take responsibilities and are held accountable for ensuring its confidentiality, integrity and availability.

In order to achieve this, these organizations can develop a management system, basis to Information Security Management System. As a practice given by ISO 27001, ISMS presents an integrated process which can be incorporated inside the overall management structure of the organization.

This management system contains the establishment, implementation, maintenance, review and improvements of an information security management system. It contains requirements about policy, roles definitions, responsibilities and authorities of each participant connected with information security. Furthermore it requires processes, procedures and organizational structures that will prevent, detect, and respond different types of threats. And, for all identified threats an organization should identify and implement controls that will mitigate risk and maintain its level in a specific alignment.

In addition to this, ISO 27002 can be useful as a guideline for controls. This information security standard can be used to select information security controls, to improve security practices and to develop security guidelines and
standards. It gives information security responsibilities, precise explanation of controls objectives and detailed guideline how to implement these controls.

So, by using ISO 27001 an organization will have a management system that will plan, implement, monitor, review and improve information security inside the organization, while ISO 27002 can be used to put controls and their objectives for all requirements asked by ISO 27001. For every risk situation identified in ISO 27001, ISO 27002 will give a set of controls how to decrease the risks, and how to maintain it in an accepted level.

Implementation of both of these standards should be in accordance with top management, business management, auditors and IT managers, who will decide within the business context and consider the implementation cost. However, by the fact that information systems have become one of the most important engines in which the whole organization depends on, compliance with international standards will help not just to have risk identified and under control, but to strengthen customer trust and achieve market differentiation for wider range of business opportunities.

Professional Evaluation and Certification Board (PECB) is a personnel certification body on a wide range of professional standards. It offers ISO 27001, ISO 27002, ISO 27005, ISO 20000 and ISO 22301 training and certification services for professionals wanting to support organizations on the implementation of these management systems.

ISO Standards and Professional Trainings offered by PECB:

- Certified Lead Implementer (5 days)
- Certified Lead Auditor (5 days)
- Certified Foundation (2 days)
- ISO Introduction (1 day)

Lead Auditor, Lead Implementer and Master are certification schemes accredited by ANSI ISO/IEC 17024.

Rreze Halili is the Security, Continuity and Recovery (SCR) Product Manager at PECB. She is in charge of developing and maintaining training courses related to SCR. If you have any questions, please do not hesitate to contact: scr@pecb.com.

For further information, please visit http://pecb.com/site/renderPage?param=139