PECB

When Recognition Matters

AUDITING INFORMATION SECURITY

In everyday environment you can find information everywhere as you can find threats and vulnerabilities toward it. This is why for these environments it has become more than needed to secure information. Methods, tools, software, and entire management systems within organizations are found to ensure and preserve the confidentiality, integrity and availability of information.

To ensure all this, organizations are considering requirements and mandatory steps to implement one of the most important information security standards ISO 27001. ISO 27001 is a specification for an information security management system (ISMS), which has proved to have influence in good governance, conformity, cost reduction and marketing for a company.

Implementing ISO 27001 will result in a group of documents, a lot of resources investments, education and awareness plans, consultancy and control implementation. But nothing is done here; still there is a lot to be done. The organization should consider continuing with the audit process.

This is the part when the stress comes into play, is everything at the right place so the organization will be certified with ISO 27001. In this case the organization will have to pass through Stage 1 and Stage 2 in order to get certified.

Through the Stage 1 the audit will secure auditee's management system documentation, which means that the audit will ask for ISMS scope, policy, objectives and risk management methodology, Risk Assessment Report, Statement of Applicability, Risk Treatment Plan, procedures for document control, corrective and preventive actions, and for the internal audit. Then the audit will evaluate auditee's location and site - specific conditions, determine the preparedness of Stage 2 audit, collection of information for Stage 2 planning, prepare the Stage 2 audit, to evaluate the internal audit and management review if they are performed and planned.

If none of these elements are missing, then in two or more weeks the auditor and his team will proceed with the second stage. Audit objectives of this stage are to verify and evaluate if all standards requirements are in conformity to the organization, if they are effectively implemented within the organization and are able to allow the organization to reach its security objectives. During the Stage 2 of the audit, the audit team will go through observation, documentation, interviewing of employees, technical verification and analysis.

Once this stage is completed, the organization should be prepared to receive a certification or to be informed that there are some parts in information security management system that they have to add or improve. So the organization has to work harder and do more. This cannot be good news for the organization; however there is something that could be done.

If the organization is informed that they have to add or improve something, then the organization would receive some suggestions from the auditor regarding these issues. After getting these suggestions the organization would usually have 90 days to improve and correct the identified nonconformities. Improved system will serve more than anything to your organization, so spending more time in correction actions will just help your organization.

Once you are sure that the improved actions have resulted in the nonconformity correction, you are ready to inform the auditor who will be found in site again. And if the job is done properly, then the auditor will accept corrective action and proceed with the certificate.

It is a known fact that all this has caused your organization to spend more time, resources, stress, extra work and obligations, but at least by the end of this stage you will be ISO 27001 certified, which would be valid for three years, and above all this fact will make difference for your company.

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 toward your company.

PECB International is a certification body for persons 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 www.pecb.com/site/renderPage?param=139.