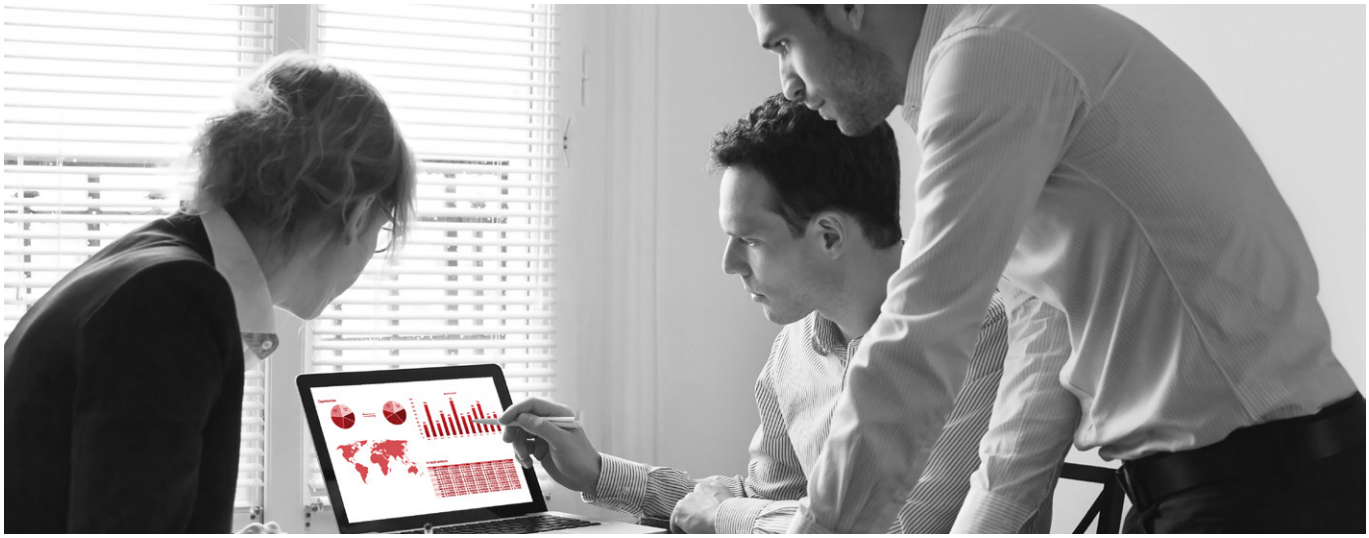
PECB

When Recognition Matters

KEY STEPS FOR AN EFFECTIVE ISO 27001 RISK ASSESSMENT & TREATMENT



In view of the developments that have occurred in the processing, storage and sharing of information; security has become an important aspect of an organization.

It has become more imperative for an organization to understand the various threats and risks facing them as they seek to protect their information. The rapid development of new technologies and communication has led organizations to the realization that implementing Information Security Management System (ISMS) in their organizations is necessary.

WHY IS THE RISK ASSESSMENT SO IMPORTANT FOR COMPANIES?

The risk assessment process is the most complicated, but at the same time the most important step to consider when you want to build your information security system because it sets the security foundations of your organization. After all, organizations want to be assured that they are aware of the risks and threats that could emerge from the processes, the people or the information systems that are in place.

Factually, this assertion is the main viewpoint of ISO 27001 standard implementation too. This information security framework helps to identify risks and threats by assessing them early on and mitigate various incidents that could occur to the organization. Also, it helps to differentiate and direct our concentration to the most important risks rather than the less important ones. That way, we are able to eliminate the bigger threats that may lead to distressing results or consequences which could be catastrophic to the organization.

RISK ASSESSMENT METHODOLOGY, IMPLEMENTATION, AND TREATMENT

Yet, there are a lot of cases when companies perform risk management incorrectly by executing the process differently from each department/part of the organization. Due to this approach, many organizations always have problems in the risk assessment implementation phase.

Thus, in order for an organization to complete the process correctly, firstly they must determine and define the rules or the methodology 'how to' implement risk management and risk assessment within the entire organzation. After defining the method, they need to make sure that the whole organization is implementing the same rule simultaneously. For instance, you should define whether you want the risk assessment to be qualitative or quantitative and what the level of the acceptance for a particular risk type should be, and so on.

Secondly, after you choose the methodology that you want to use to assess risks your organization faces; you need to begin to categorize those risk types. As soon as you identify your risks types, you can commence to list all of your asset's threats and vulnerabilities linked to those threats. Nevertheless, by conducting this process, the organization can possibly reveal problems that they were not aware of and focus on the risks that may have devastating effects in the organization.

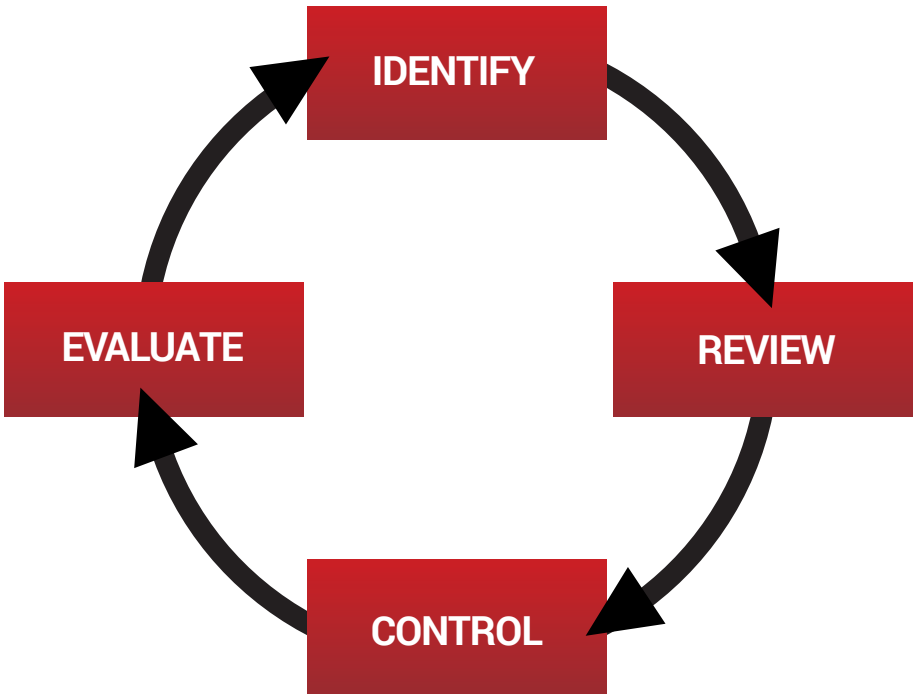
WHAT ARE THE MOST EFFECTIVE WAYS TO ALLEVIATE RISKS?

If an organization wants to manage the risks and threats that their company is facing, there are various solutions that can be helpful. The table below explains some of the solutions and their respective detailed explanations.

Solution	Explanation
Security Controls	In order to treat organizations risks, we may apply the security controls that are found in ISO 27001:2013 Annex A.
Transfer Risks	There is also the possibility of transferring the risk to another party, for instance, putting the responsibility on an insurance company by buying the insurance policy.
Avoid Risks	If an organization finds out that they are conducting an activity that is risky, they need to either stop it or find another alternative method, which would not harm the organization.
Accept Risks	You can also find the most concrete way to accept a particular risk without damaging the organization. One way would be by making a small investment which would ease the threat by improving the situation.

RISK ASSESSMENT REPORT AND THE STATEMENT OF APPLICABILITY

This step requires you to document all the detailed steps, requirements, and controls that you performed so far. Why do we need to document this complete process? The answer is simple, you want to be able to check the results and the progress that your organization has made during a year or two since your risk assessment implementation and you also want to be prepared when auditors knock on your door.



Another essential document that you must possess is the Statement of Applicability (SOA). Besides being used by the auditors as a guideline for the audit process, this statement is also significant to have, for the light of the fact, that it shows the security profile of your company. This document contains or should contain a detailed explanation regarding all the security controls that you have implemented in your organization throughout the whole process; including a justification for the inclusion of the specific controls. The SOA also lists the rest of the controls listed in the ISO 27001:2013 Annex A that the organization has chosen not to implement, including a justification for the exclusion.

HOW DO WE PUT THE THEORY INTO PRACTICE?

The whole purpose of risk treatment and assessment is to put all the processes and steps above into practice and convey some results about the effectiveness and efficiency of their implementation as well as their progress. This process of putting theory into practice is called 'Risk Treatment Plan'. This plan should define the following:

- What is the amount of budget that will be used?
- Who is going to implement each control?
- What timeframe will be used?

The last step of the process after you prepare the statement of applicability is that you need to get the management's consent regarding the whole process. The procedure of implementation will take a substantial amount of time, effort, and money and as we know the managements team approval is crucial because you can't conduct any process without their help and effort.

To conclude, risk assessment and treatment is one of the most fundamental steps that an organization should conduct in order to secure their organization's system by identifying threats that may have disastrous results for them. This process of preventing risks and securing information has now become one of the top trends for organizations throughout the world. PECB provides training and certification services for organizations who want to secure their information assets by implementing ISO 27001. This standard will guide them towards assessing and treating threats that may damage their information system. For more information please visit our website: www.pecb.com/training

About the author

Ardian Berisha is a Junior Portfolio Marketing Manager for Information Security Management at PECB. He is in charge of conducting market research while developing and providing information related to ISM standards. If you have any questions, please do not hesitate to contact him: marketing.ism@pecb.com.

About the contributor

Musa Wesutsa is an Information Security expert with years of experience in IT and Networks Security and ISO 27001 Implementations ranging from Manufacturing to Telecommunications and Mobile Money. Musa is a Certified PECB Trainer and trains mainly ISO 27001 Lead Implementer and Auditor. He is currently the Managing Consultant at Sentinel Africa Consulting. If you have any questions, please do not hesitate to contact him: musa.wesutsa@sentinelafrica.co.ke