How to Apply Proper Risk Management Methodology on Information Security?
HOW TO APPLY PROPER RISK MANAGEMENT METHODOLOGY ON INFORMATION SECURITY?

Risk in its negative way might be defined as one undesired consequence that may or may not occur, as a result of specific outcome we want to achieve. Shortly, it is the effect of uncertainty on objectives, as defined in ISO 31000.

Many organizations are exposed to different types of risks. High profile risks should be handled in a professional way as part of the corporate governance framework adopted and adapted by these organizations. It goes without saying that the organizations’ success in managing its risks profile properly will be reflected positively on its market share, their prospective revenues, hence their long-haul continuity in business.

Risks related to Information Security are on top of the list to deal with, as Information Systems are becoming more than business enablers for diverse businesses. Organizations need to clearly define its Information Security posture to be able to establish the suitable framework to manage the risks associated with their Information Systems in a right way.

WHAT IS RISK MANAGEMENT ALL ABOUT?

Risk management describes the decision an organization makes, and the steps it takes in response to risks that have been identified. Risk management’s objective is to assure uncertainty does not deflect the organization's endeavor from the business goals.

In many organizations, governance of enterprise IT is a subset of the corporate governance. In the meantime, risk management is considered part of the governance framework, as one of the governance’s paramount objectives is to optimize risks. Hence, Information Security Risk Management can be thought of as an integral part of a holistic Enterprise Risk Management framework that is in turn part of the corporate governance.

The successful strategy to effectively manage Information Security risks would start by top management commitment down to communicating the importance of Information Security to each employee including of course implementing the right Information Security technical products.

Risk management domain includes two subdomains; Risk Assessment and Risk Treatment. The general methodology of risk assessment includes identifying, analyzing and evaluating risks, while risk treatment includes techniques like mitigate/enhance, avoid/exploit, retain/accept and transfer/share risks.
SELECTING THE RIGHT RISK ASSESSMENT METHODOLOGY

It all depends on the security posture of the organization, the complexity of its business and the supporting Information Systems. Anyhow, here is a simple risk management process that might include the following:

1. Risk Classification according to the risk impact factors; i.e. the effect and the frequency
2. Risk Identification based on both the baseline and target states or a gap analysis
3. Initial Risk Assessment by developing a risk impact matrix
4. Risk Mitigation by applying the proper controls
5. Risk Monitoring to continually assess the residual risks’ impact

Risk Analysis as part of Risk Assessment sub-process

1. Define scope
2. Identify related processes
3. Identify assets in those processes
4. Identify threats
5. Identify vulnerabilities
6. Develop metrics to measure the impact severity
7. Evaluate top risks
8. Define countermeasures

Risk Treatment Techniques

1. Risk mitigation by applying the proper controls
2. Risk transfer, using 3rd party services like insurance companies
3. Risk avoidance by eliminating the activities that are associated with the concerned risk
4. Risk retention by formally keeping or retaining the associated risk

Of course, organizations can refer to many useful ISO standards that can help to develop more rigor Information Security Risk Management process; i.e. ISO 31000 and ISO 27005, etc.

Methods used to perform a risk assessment can be either quantitative or qualitative; also, it can be a mix of both methods, a hybrid method.

Additional effective methods that organizations can adopt in order to show conformance on risk assessment (analysis, evaluation and actions that they should take to avoid them) are:

- EBIOS
- MEHARI
- OCTAVE
CONDUCTING BUSINESS CONTEXT ANALYSIS

Risk acceptance is one of the most important activities of any business. Based on the risk the organizations accept to take, the organizations will be able to create opportunities. By creating opportunities and seizing them, the organizations will be able to reach their objectives.

To ensure that the organization is working toward reaching its objectives, the responsible authority (BOD, Board of Directors) should analyze the risk and security posture of the organization. Some of the major points that the BOD need to analyze are:

• What are the business goals?
• Which processes and assets of the organization are involved in achieving these goals?
• What are the risk treatment techniques the organization would undertake?
• What is the outsourcing policy in place?
• What are the legal and regulatory requirements that the organization need to comply with?

RISK THREATS, VULNERABILITIES AND IMPACT

Threat is anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Vulnerability refers to the inability (of a system or a unit) to withstand the effects of a hostile environment.

Risk impact is the consequence of risk events if they are realized.

Organizations should apply information security risk management strategy, and this should lead them toward their lifecycle. It cannot be taken just as the passing phase in order to show conformance. It is rather a need for organization to ensure their way toward achieving business objectives and also to have a healthy business environment.

Continual training and awareness session are one of the factors that organizations should be aiming at, because this will keep up the importance of information security overall. Here at PECB, we are highly committed to Information Security Risk Management and continually adding value to this portfolio by developing training and offering certification services. PECB is accredited body providing individuals with training and certification, as well as companies on management system certification. Among others, we offer ISO/IEC 27005 training, exam and certification services for individuals.

Mohamed Gohar has more than 10 years of experience in ISM/ITSM Training and Consultation. He is one of the expert reviewers of CISA RM 26th edition (2016), and the upcoming edition of CISM RM (2017). Gohar is a Senior ISM Trainer/Consultant at EGYBYTE (www.egybyte.net). You can reach Gohar at mohamed.gohar@egybyte.net and eg.linkedin.com/in/mohamed-gohar-89253840.

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.