PECB Insights

RISK RESILIENCE

ISSUE 01 / APRIL **2016**

When Standards Matter

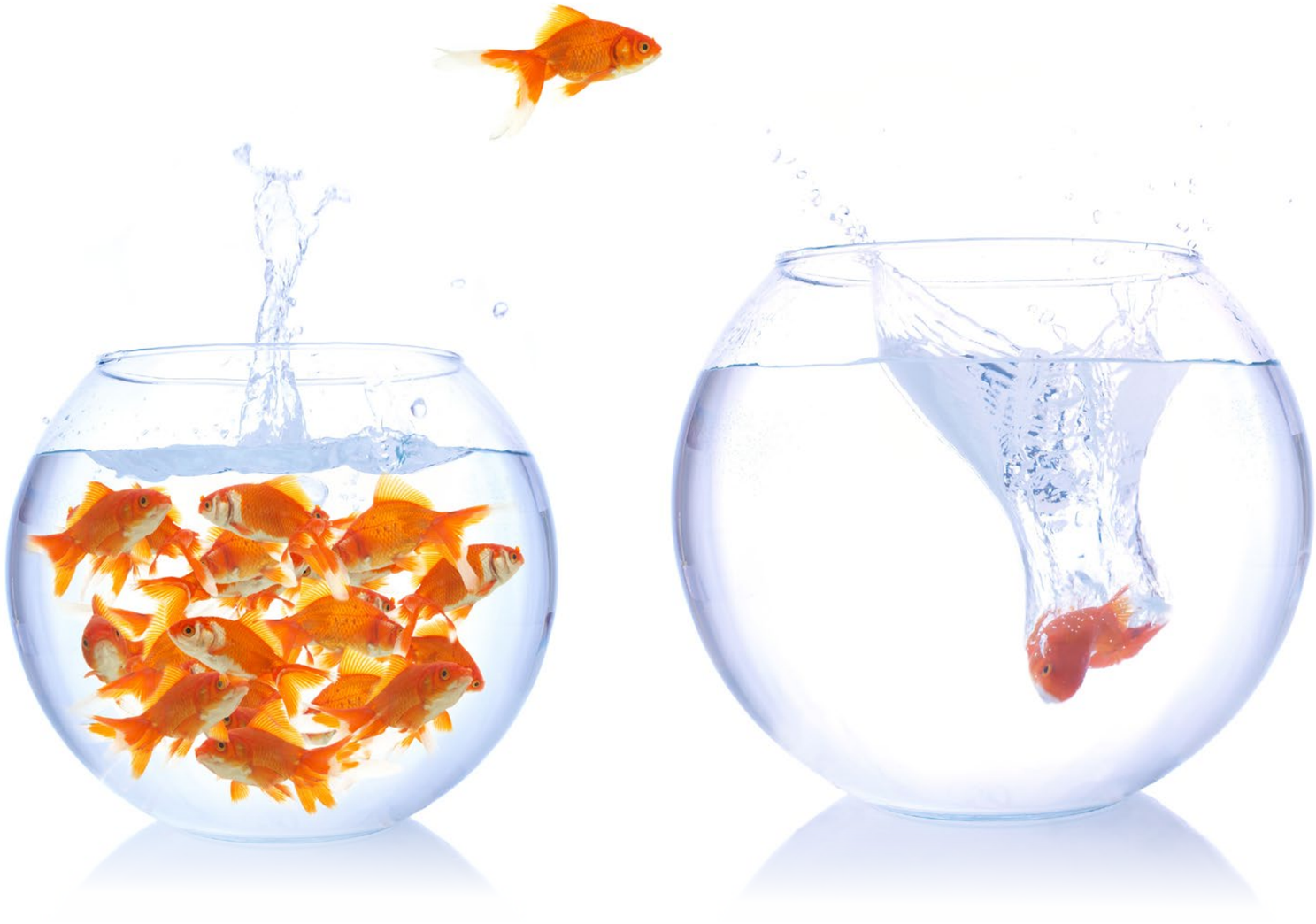
Intro

They say that there is nothing more important than being fully equipped with the right knowledge, expertise, and resources to provide your customers satisfactory products and/ or services. But what is more important is the recognition of the dedication and hard work your organization invests day-in and day-out to not only meet customer expectations, but also exceed them. Everyday PECB is one step closer to our vision of a world where best practices are widely disseminated, accessible, affordable, known and used. Our mission to enhance the accessibility of standards, compliance and education for people and organizations by reducing the certification costs and widening the range for education and certification programs is gradually being accomplished. We will continue our journey to support worldwide professionals that want to differentiate themselves, and follow best practices based on internationally recognized standards.

Eric Lachapelle
CEO at PECB

PECB *Insights*

ISSUE 01 / APRIL **2016**



WHY RISK RESILIENCE?

In recent years, a rapid increase in foreign investment, imports and world trade is occurring. As the economy is becoming more integrated, competitive and complex, organizations find themselves confronting international competitors. In response, many businesses are increasingly looking for new opportunities in international market.

Before entering such market, it is very important to understand the needs, rules and strategies which help you to grow and increase profitability. An effective risk management strategy is a must. It means identification of project's strength, weaknesses, opportunities and threats. These strategies are crucial for upcoming organizations' events and activities; hence to ensure success, the potential problems should be handled or avoided. Achieving such objectives depends on preparation, evaluation and results of your strategic plan and goals.

As an international certification body, PECB recognizes the importance of risk management processes by presenting commitment and knowledge to risk management best practices and regulatory framework. It enables society to make better educated risk decisions through creating a culture of risk awareness. We do this first in our internal processes of every service that we provide, but also by providing professionals updated crucial information, through articles, infographics, whitepapers and webinars to help them increase their professional development entirely for free.

Considering that our company is highly focused on making internationally recognized best practices accessible for everyone, we always involve professionals, webinar participants and readers in our projects such as webinars, articles, and other informative campaigns. The main focus of our projects is to address the essentials of the risk management newest topics and guide professionals when encountering issues related to their field.

RISK ASSESSMENT IN PROJECT MANAGEMENT

ABOUT RISK ASSESSMENT AND PROJECT MANAGEMENT

A project is a set of inter-connected tasks intended to attain a certain goal, with a particular series of resources, within a fixed duration and cost. Given that each project tasks have specific timelines and deliverables, there are always uncertainties considered as risks that are expected to happen and will affect the project's success.

Risk comprises two factors: the probability of its occurrence, and the consequences if it does so.

In order to enable the analysis of risks related with a project, the process of a project risk assessment and management is required. If the processes are undertaken appropriately, it will raise the probability of successful completion of a project to performance, cost and time goals. The overall process of managing uncertainties, which affects the achievement of project objectives, involves two activities: Risk Assessment and Risk Management.

RISK ASSESSMENT - IN A NUTSHELL

Risk analysis settles on obtaining a deeper understanding on which project tasks, outputs, or events would influence its success. This requires project managers experience, knowledge of the project, and critical thinking to decide on what strategies should they embark, from where tactics and activities will be based upon.

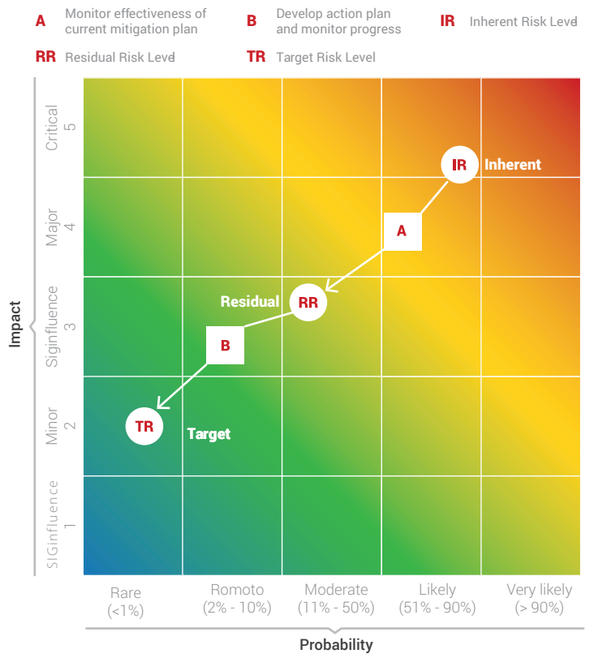
Performing risk analysis features two options a project manager can use depending on the identified risk source and its degree of detail: qualitative and quantitative analysis.

Qualitative analysis uses a descriptive set of attributes to qualify potential consequences and the possible chances that will occur. This approach, by practice, will need further explanation to justify a risk's position in this type of assessment, albeit an easy practice to assert risks.

Quantitative analysis, on the other hand, provides a measurable level of understanding of risk by using a numerical set of attributes to determine its consequence and likelihood. In contrast to qualitative analysis, this may require extensive use of time and resources, which is one of the project constraints across all phases. This follows that the level of detail is dependent on the breadth of data used and the depth of the calculation applied to present either a single number or sets of patterns that will explain the impact and probability of analyzed risks.

Experience has revealed that qualitative analysis typically leads to a primary level of quantitative analysis, as the latter present statistical evidence to the former, given its descriptive nature of detailing risks.

The risk evaluation stage includes both identification and analysis of project risks and assists the project team in making decisions to address the analyzed risks. The illustration shows the relationship between the impact and probability, which is also known as a Risk Map (or heat map). Risk Map analyzes values that are plotted across this chart based on their risk levels, which is the output of risk analysis. With the project's risk criteria featured on the map, the project manager and his/her team are given a good visual on which risks should be given further attention. With mitigation strategies planned, based on evaluated risks, having an effective risk management framework implementation and risk treatment plans may not necessarily indicate the completion of risk treatment. Instead, it effectively minimizes the impact and it allows clear decisions to be made.



The necessity on reacting to risks may be critical and it involves the following:

- Recognizing defensive and proactive actions to avoid risks or to reduce its effects,
- Initiating further analysis to decrease insecurity through monitoring and measurement of key metrics.

The benefits of performing risk assessment in project management include reduction to project risk exposure, precise and clear decision making on key issues within every project phase, and clearer definition of risks related to particular projects with the risk assessment approach.

IDENTIFYING PROJECT RISKS- A CLOSER LOOK

Identifying project risks marks is a challenging start for project managers and his/her team, particularly in the project's planning phase. The Project charter, which marks a formal statement of initiating a certain project, is a good springboard to identify risk sources and factors as the identification stage generally covers three things to identify:

01 The external context (e.g. the project's impact to its external clients and market)

02 The internal context (e.g. the key deliverables and controls at strategic, tactical and operational levels)

03 The needs and expectations of the project stakeholders.

Methodologies such as SWOT analysis, Delphi Techniques, and Stakeholder analysis, to mention a few, may be useful, but should be meaningful and time-efficient to the project in terms of execution, resource allocation and decision making.

Nowadays, one of the major complexities faced by Project Managers is the difficulty of not covering a general risk register to refer to when identifying the project risk. For purposes of managing the execution of the project risk management, all project risks should be recorded in the risk register, which is an exhaustive list of all risks identified, their root causes and consequences, and what were the actions taken to address it. This should be updated constantly throughout the lifecycle of the project.

The process of identifying risks must engage all project team members so they can contribute in adding details and take part in the risk assessment process, while at the same time, manage and align the project's scope, critical tasks, resources and timelines. In addition, when risks are fully assessed, a risk treatment plan is developed and should illustrate the level of risk which can be managed for the project, to achieve its objectives and optimize resource utilization, preferably in costs. Risk can also be identified by competent specialists and professionals as well, which in this case are project managers.

RISK ASSESSMENT AND PROJECT MANAGEMENT MAKING A GOOD PAIR FOR PROJECT SUCCESS

The process of risk assessment updates and enhances the project's risk profile, reflected in its project risk criteria, risk register, and risk treatment plans, done on a scheduled basis within the project timeline.

Similarly as with other projects and management systems on its continuous improvement initiatives, risk management and assessment should be executed continuously since new risks may be identified. A good risk management framework will clarify the overall approach in managing risks for any projects, regardless of size and scale. It will point how much risk is tolerable and who should be implicated in carrying out the qualitative analysis of the known risks. More importantly, the framework ensures there is always a backup plan to address challenges and opportunities to ensure project success, regardless of the number of uncertainties a project may face.

HOW ISO 21500 CAN BE APPLIED AND/OR HELP IN PROJECT MANAGEMENT?

Project management is highly important for organizations worldwide. This clearly indicates that the need for qualified professionals in project management will keep increasing. ISO 21500 Project Management training and certification ensures professionals and organizations have a proper risk control in project management. To help professionals become better project managers, PECB as a certification body on a wide range of professional standards, among other services, it offers training, exam and certification against Project Management with ISO 21500.

ISO 21500 Professional Training courses offered by PECB are:

- ISO 21500 Lead Auditor **(5 days)**
- ISO 21500 Lead Project Manager **(5 days)**
- ISO 21500 Project Manager **(3 days)**
- ISO 21500 Foundation **(2 days)**
- ISO 21500 Introduction **(1 day)**

For further information, please visit:
https://pecb.com/iso-21500-training-courses

About the **Authors**

Alba Keqa is an Account Manager for Risk & Management at PECB. She is in charge of conducting market research while developing and providing information related to Risk and Management standards. If you have any questions, please do not hesitate to contact: marketing.rm@pecb.com.

Joshua Rey Albarina is a Senior Consultant for ISO standards and business best practices at SAS Management, Inc. in the Philippines. He is a PECB certified trainer and an ISO 31000 Risk Manager, Lead Implementer (ISO 9001 and 14001) and Lead Auditor (ISO 22301). If you have any questions, please do not hesitate to contact: joshua.albarina@saservices.com.ph

PROJECT MANAGEMENT

Project Management boosts success rate by **26%**

67% of Project Managers believe that training indicates to better project performance

44%

ONLY **44%** OF PROJECT MANAGERS ARE SATISFIED WITH THE PROCESS OF MANAGING WORK

ISO 21500 PROFESSIONAL TRAINING COURSES OFFERED BY PECB ARE:

- ISO 21500 LEAD AUDITOR (5 DAYS)
- ISO 21500 LEAD PROJECT MANAGER (5 DAYS)
- ISO 21500 PROJECT MANAGER (3 DAYS)
- ISO 21500 FOUNDATION (2 DAYS)
- ISO 21500 INTRODUCTION (1 DAY)

source: www.pmi.org

INFORMATION SECURITY IN BANKS AND FINANCIAL INSTITUTIONS

The importance of information security in our lives is widely understood by now. Investments of organizations into information security keep growing, but also do cybercrime risks and costs of data breaches.

By their very nature, financial institutions are an attractive target for attackers. Also, the data breach costs per capita in financial industry are among the highest. The investments into information security have also become mandatory in order to achieve credibility for the clients and interested parties as well as to achieve regulatory compliance. Thus, a lot of challenges need to be met by banks and financial institutions.

INFORMATION SECURITY THREAT SOURCES

Financial attacks mostly come from outside the institution, where intruders try to gain information or try to counterfeit the transactions. These institutions need to show their commitment toward reaching the highest level of security, and always staying up to date with the newest technique and technology. Many cases have been reported as fraudulent, especially in fall 2012 in U.S., where the depository institutions were subject to denial-of-service (DDoS) attacks by a hacker group from Middle East. Another case was reported in the U.S., in 2014, where a major depository institution suffered data breach. Based on a public statement, the number of affected individuals and small businesses was 83 million. The institution declared that customer funds were not affected by this hacker group; however, the attackers managed to obtain customer information such as e-mail addresses, home addresses and telephone numbers. According to GAO.GOV sources, another technique used to get access to customer funds and information is ATM Skimming, which costs depository institutions hundreds of millions of dollars annually. This technique involves placing an electronic device on an ATM machine to retrieve information from the card's magnetic stripe at the time when a customer uses the machine.

THE IMPACT OF COMPROMISED INFORMATION IN FINANCIAL INSTITUTIONS

In general, data breaches lead to an abnormal high churn rate of the customer base. Additionally, in the financial industry, there will be investigations by the responsible regulatory bodies following a data breach, which could also lead to license termination for the affected organizations. Therefore, data breaches and security incidents require a rapid response to mitigate the impact on these institutions and to demonstrate due care. Banks and financial institutions need to strengthen their incident response teams to make sure appropriate encryption is used with all data, and also train their staff on a regular basis to acquire and maintain their BCM and DR capabilities, just to name the most efficient measures. To alleviate purely the financial impact of security threats, also insurance protection can be bought.
Depending on regulatory and legal obligations, organizational culture, geographic location and size, it might be appropriate to setup an internal or external CSIRT (Computer Security Incident Response Team). While the internal CSIRT is considered the most preferable option, businesses shy of the involved personnel costs could consider outsourcing these tasks to an external provider. On the other hand, a CSIRT is one of the most effective measures to cut data breach costs.

INSTITUTION AND EMPLOYEE RESPONSIBILITY TO ENSURE SECURE INFORMATION FLOW

Having software and tools available within an organization to safeguard information is not enough. Employees need to understand the threat's effect in their working areas, and how crucial are the tools that must be used to defend against these threats. Thus, employee awareness and training is the key to resilience. They should always keep in mind that the information should be kept safe, and need to be vigilant not to become a victim of any counterfeiting actions.

Banks and financial institutions need to show their commitment to provide any necessary resources to ensure employees' awareness. Among many criteria, there should also be a fulfillment of the following:

- The institution should implement a policy on how to govern its information security issues.
- Should have the authority and resources needed to carry out information security duties, including the implementation, maintenance and improvement of the information security management system.
- Institution should provide its staff with training and awareness sessions in order to understand information security policy and processes that are crucial for the institution.
- All employees need to be aware that passwords shall be strictly case sensitive and hard to be gained.
- There should be defined accountability on how to use the institution devices.

ONGOING STRATEGY TO KEEP INFORMATION SECURE

Retail banking and respondents from The Economist and HP survey declared that banks and other financial institutions should pay more attention on securing information, rather than improving information flow.

The information security strategy needs to support the business objectives of the organization. Employing effectiveness and efficiency need to be improved in order to provide a better service for the customers. When performing security operations, a significant attention should be allocated to the necessary information that institution needs to provide to the employees, and this should be done appropriately and timely manner. Banks and financial institutions should be strongly committed on implementing a management system to deal with the security of information by employing people who are experienced and know how to deal with security issues. Implementing ISMS based on ISO Standards is a massive assurance that an organization is meeting its regulatory requirements to apply due care to information security risks and that the ISMS is able to provide the whole organization with the necessary information. The ISO/IEC 27001 Information Security Management System standard ensures that organizations are addressing information security risks in a structured manner. Companies that obtain ISO/IEC 27001 certification validate that the security of financial information, intellectual property, employee details, or information entrusted from third parties is being managed successfully, and is improved continually according to the best practice approaches and framework.

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

For further information, please visit:
https://www.pecb.com/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.

Friedhelm Düsterhöft is a Senior IT Security Consultant and Managing Director of msdd.neT GmbH, offering ISO 27001 implementation, audit and training services. Please contact him at fd@msdd.net to discuss your specific needs and challenges. msdd.neT is an official PECB partner.

ONLINE BANKING & INFORMATION SECURITY THREATS AND ATTACKS

41% of economic crimes are committed by employees within an organization

60% of firms identify the speed of technological change as a threat to their growth prospects

70% of banking and capital market CEOs identify cyber insecurity as a threat to their growth prospects

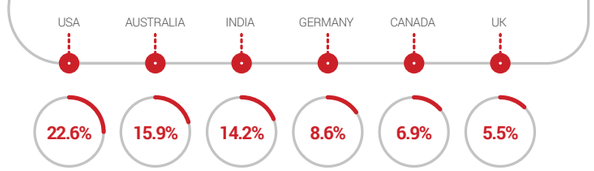
93% of large organizations last year suffered a security breach

£700 m the amount annually spent on cyber security in the UK

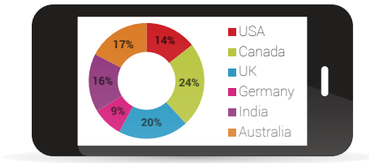
Device spoofing remains the top attack vector with identity spoofing growing rapidly

DESKTOP BANKING

ONLINE PAYMENTS



MOBILE BANKING



ATTACKS BY TRANSACTION TYPE

Mobile based commerce represented 34% of the total transaction 200% increase from 2014 to 2015
Online transaction attacks overall 3.4% by the end of the 2015

Source: www.bba.org.uk | www.threatmetrix.com

REPLACING OHSAS 18001 WHAT WILL ISO 45001 BRING?

A shocking statistic of work-related accidents or diseases that occur daily is recorded worldwide.

According to ILO, every day 6,300 workers die as a result of unfortunate events in the work space or as a result of work related diseases, meaning, one worker loses his life every 15 seconds. In 2014, this added up to 2.34 million, a figure that has raised awareness for the need of a new set of occupational health and safety regulations and requirements.

The measurable loss of world's GDP due to accidents and diseases is 4 %, which is equivalent to about $ 2.8 trillion.

The existing British standard, OHSAS 18001, helps organizations to implement a framework and guidelines for the control and identification of risk, accidents, and the organizations' overall OHS performance. It helps companies to control and/or mitigate risk issues and problems that may arise. At present, there are about 90,000 companies with OH&S certification, in more than 127 countries.

Nevertheless, in the past twenty years the idea of a new International Globalized Standard has been presented. After a few attempts, more than 60 countries have come together to create a global document that will provide a framework for the improvement of OH&S. This document is the new ISO 45001 Occupational Health and Safety management systems requirements that will replace OHSAS 18001.

ISO 45001 is applicable to any organization, regardless of size or the nature of the work. The objective of ISO 45001 has retained that of OHSAS 18001, but with some changes in the standard's requirements, in order to meet the needs of today's business model and to mesh with other recently revised standards.

The main changes are:

The ISO 45001 incorporates Annex SL Framework - the management system format that helps with the creation of Standards and its implementation in organizations. In the future, it is estimated that Annex SL will represent 30-40 % of ISO system standards.

The Annex SL Framework includes 10 Chapters, some of which are already familiar to the public and users of the standards.

High level structure clauses:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

New concepts are included within individual clauses:

- Context of the organization,
- Leadership,
- Documented information.

Context of the organization - Requires a detailed approach in the evaluation of internal and external factors that impact your company. Modification of labor relations, new technology, new materials and services coming from outside might present a risk. ISO 45001 requires you to take into consideration all of the mentioned factors, evaluate them, and decide what measures need to be taken in order to avoid or mitigate risks.

Leadership - There is a strong focus on the top management and leadership. This means that everyone must be included within the decision making process, not only the senior leaders but all levels of the organisation.

Documented Information - A new concept that supports the modern world of processed data, which still incorporates the need for documentation and records.

Terms and Definitions

The terms and definitions section has also been modified in order to make the standard more suitable to any organization regardless the size. 'Hazard Identification' is likely to be replaced by the terms 'Risk Identification' and 'Risk Control'. It has been identified that the term 'Hazard Identification' is rarely used in isolation and forms only a single level of the overall risk process. Preventive action has been removed. As the focus of the management system and its purpose is to control risks, it is considered that a properly implemented management system will become the key preventive tool.

Benefits of the new Standard:

1

Reduce Risk

ISO 45001 has a greater focus on increasing the awareness of occupational health and safety risk. It will provide a framework for organizations of any size and function for the protection of their workers and will provide them with a better system of occupational health and safety. This framework guides and helps a company to correct or mitigate any issues regarding their plant, equipment, facilities and workplace environment.

By fully implementing the standard, a company will see a decrease in the number of incidents and accidents in the workplace and will avoid the possible threat of a costly lawsuit or other statutory penalty.

2

Higher Profits

By incorporating ISO 45001 into the operational system of the company that meets other standards, such as ISO 9001 and ISO 14001, and fully implementing it, the organization will see a reduction in lost and non-productive time as a result of accident and incident. This will lead to the organisation developing a safer workplace environment and greater productivity, with higher employee retention, which will then lead to higher profits.

3

A single internationally-agreed standard

There is a question spread throughout the user's community: why do we need a new standard when the current one is successful?

Nowadays, many organizations are already using ISO management systems standards, so having a matching ISO occupational health and safety system standard makes it easier to integrate it with other systems.

It is recognized that existing British standard OHSAS 18001 helps organisations to implement a framework and guidelines regarding the control and identification of risk, accidents, and overall performance, and the new standard has its base in this. In addition, ISO has also become a benchmark for companies wanting to link their name with success and thus linking OHS to ISO makes good sense.

4

Supply chain and contractor/sub-contractor quality process

There are often many health and safety challenges encountered with goods or services provided by an external supplier, contractor or sub-contractor. By implementing the standard, an organization can then set measures, objectives and targets for their service providers. They can require that their vendors establish and implement a health and safety management system in line with the standards. This will then lead to a significant improvement in the overall supply chain process.

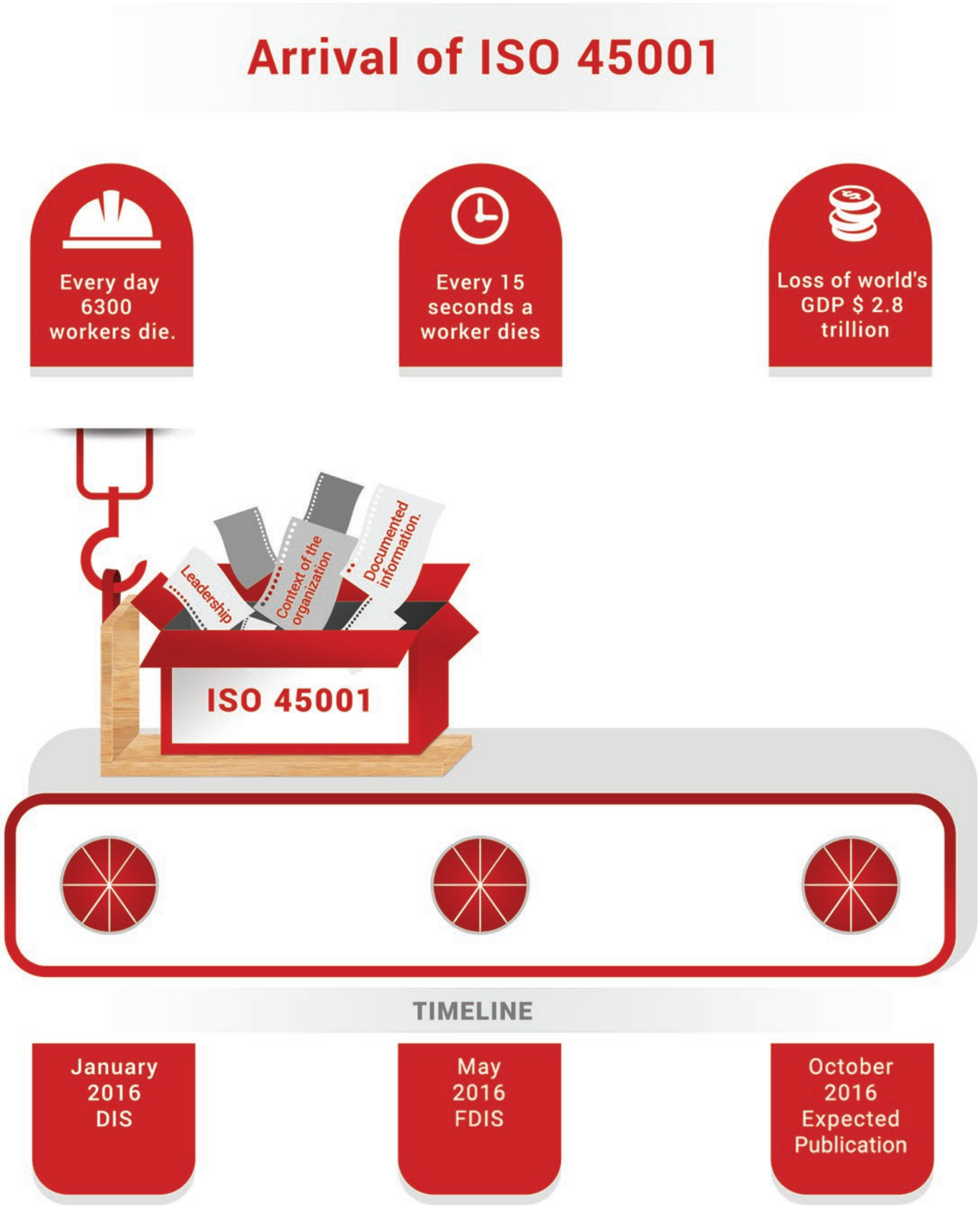
TIMELINE

ISO 45001 is currently under development and subject to acceptance is to be published by the end of 2016.
The transition period from OHSAS 18001 to ISO 45001 is likely to last 2-3 years. For the existing users, it is important to get a draft of the standard, have a detailed look, and plan a transition process towards ISO 45001. For companies that are not using any of the two standards, a good starting point is to use OHSAS 18001 as a guide as to what is coming in 2016.
PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including OHSAS 18001, and soon ISO 45001 courses as well.

For further information, please visit: https://pecb.com/ohsas-18001-training-courses.

About the authors:
Suzana Ajeti is an Account Manager for Health, Safety & Environment at PECB. She is in charge of conducting market research while developing and providing information related to HSE standards. If you have any questions, please do not hesitate to contact: marketing.hse@pecb.com.

Mike Gray is a highly qualified vocational education trainer, assessor and PECB Certified Trainer, delivering training in ISO 9001 Quality Management, ISO 14001 Environment, OHSAS 18001 Health and Safety, ISO 22000 Food Safety and ISO 31000 Risk Management. If you have any questions, please do not hesitate to contact him: mike.gray@mgtdpirii.edu.au



ARE YOU MEETING CUSTOMER EXPECTATIONS?

Nowadays, quality is a word very often heard and spoken by society and industries of all sorts. Almost all organizations- product or service based- have some kind of advertisement signaling towards their company providing quality to the customer.

Apple portrays innovative technology with simplicity and quality design, BMW confirms its high quality manufacturing and Hilton Hotel illustrations its top notch quality service.
Since, the meaning of quality comes down to the how well the features and characteristics of a product or service have the ability to satisfy identified needs, in other words "customer satisfaction".

Customer Satisfaction & Expectations

Customer satisfaction is another strong word in the business world. Satisfying your customer is converting first time clients into loyal ones, growing from positive word-of-mouth advertisement and increased sales coming to fruition for the company. Apple, BMW, and Hilton and other businesses advertise their pursuit of customer satisfaction. Achieving customer satisfaction means meeting customer expectations. If the customer gets what their expecting, then they will be satisfied or vice-versa. Likewise, once their expectations are meet, it is likely to have them return for another great experience with your product or service. Therefore, taking quality into the frontline of business operations, it can really have a chain effect on business efficiently and profits.

According to ASQ Global State of Quality, 82% of organizations in Germany use ISO standards as a quality framework and 70% in the United Kingdom. The Center for Media Research reveals that "poor customer service" costs companies $83 billion annually in the U.S. According to TeleTech Holdings Inc., a positive word-of-mouth has a great influence on consumer decision in using a company; it states that 63% of healthcare customers will consider a company based on positive word-of-mouth. Nonetheless, based on a recent survey done by Accent Marketing services, 80% of customers make additional purchases when they undergo a positive experience with a company and 79% of them tell family and friends.

ISO 9001:2015

Great news, quality experts! ISO 9001:2015 is the new word for quality and confidence today. The implementation of this standard helps organizations be confident in their ability to consistently provide products and services that meet customer expectations and have a built framework for improving customer satisfaction. Revisions have occurred to the standard, but the purpose remains the same.
For organizations to be successful, they must know the customer's expectations, implement the expectations, be confident while having evidence of those expectations being met, and have built monitoring and measuring points in the processes that force examination of the processes to look for ways to improve in meeting expectations. Businesses have to adapt to meet the growing needs of customers. Revisions of the standard occurred to encompass the changes in the field of quality. The standard was revised to meet Annex SL which standardized how standards are written. This makes integration between ISO 9001, ISO 14001 and the other standards more seamless. The second reason for revision was to bring forward the concept of risk management into the standard. Risk Management is the science of studying the activities of an organization, determining potential consequences of these activities, and mitigating the risks to an acceptable or manageable level.

Context of the Organization

The first risk managed in the standard directly links to customer expectations. The revised standard requires determining the influences on the organization and preparing countermeasures within the organization to address these influences. Addressing the "context of the organization" includes determining customer expectations and preparing to meet them. Without understanding customer expectations and ensuring countermeasures are prepared in the organization, one cannot expect customer satisfaction.

Risk Management

The standard requires organizations to address the risk that products or services will not meet specifications and won't be able to satisfy its customer. The implementation of an ISO 9001:2015 requires a quality management system which is process based and that addresses the risks of those processes not meeting the expectations of the interested parties identified in the "context of the organization" being addressed. It requires built in monitoring and measuring of the processes to ensure they are actively seeking information to improve the process. A successful and thriving business realizes what an effective QMS in an organization can generate.

Benefits of Certification

- Improve customer satisfaction through progressively improving at meeting customer expectations.
- Reputation – Customers know the organization focuses on customer satisfaction and evidence of the quality of what they provide.
- International recognition and proof of quality.
- Incorporating "customers are first" culture by constantly meeting their implied needs.
- Confidence – Management of the organization has planned the processes and can verify the processes are being followed per the plan.

While, the standard never prescribes what to do to achieve quality and satisfaction, it becomes the framework for accomplishment.

"The first step in exceeding your customer's expectations is to know those expectations."
– Roy Hollister Williams

Here at PECB, we are highly focused in customer satisfaction and we strive continuously to provide our clients the best industry services. PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO 9001:2015 courses.

For further information, please visit:
https://www.pecb.com/iso-9001-training-courses

about the authors

Arta Limani is an Account Manager for Quality Management Systems at PECB. She is in charge of conducting market research while developing and providing information related to Quality management systems at PECB. If you have any questions, please do not hesitate to contact: marketing.qms@pecb.com.

Debra Hay Hampton is a certified Lead Auditor of Quality and Environmental Management Systems, a certified Management Consultant by Exemplar Global and a certified Quality Engineer. She has determined the best way to implement ISO 9001. If you have any questions, please do not hesitate to contact: debra@ce-q.com.

Are you meeting customer expectations?

82% of organizations in Germany & **70%** in the United Kingdom use ISO standards as a quality framework

63% of healthcare customers will consider a company based on positive word-of-mouth

80% of customers make additional purchases when they undergo a positive experience with a company

79% of them tell family and friends.

Why Become ISO 9001:2015 Certified?

- Improve customer satisfaction through progressively improving at meeting customer expectations.
- **Reputation** – Customers know the organization focuses on customer satisfaction and evidence of the quality of what they provide.
- International recognition and proof of quality.
- **Confidence** – Management of the organization has planned the processes and can verify the processes are being followed per the plan.

Source: www.prnewswire.com | www.asq.org

SOCIAL ENGINEERING AND RISK FROM CYBER-ATTACKS

Today, many people are facing the risk of losing information and sensitive data. For criminals/hackers, social engineering is one of the most prolific and effective means to induce people to carry out specific actions or to divulge information that can be useful for attackers.

This article will discuss the basics of social engineering by giving a general overview of social engineering.
We will discuss the specific details related to the most common techniques used by attackers to access seemingly secure systems. Also, at the end of this article, we will explain why it is important to be certified against ISO standards and what benefits this can bring in relation to security.

Even though a lot of people use the web and all the services that go with it, general awareness about the cyber world and safe practices to be followed while online is very low. Social engineering is a kind of art; it is the art of manipulating people and one of the most effective means of gaining access to secure system and obtaining sensitive information. In general, social engineering is the process of deceiving people into giving confidential, private or privileged information or access to a hacker. There is really not a lot of difference between the techniques used for social engineering and the techniques used to carry out traditional fraud.
From a technical prospective, social engineering is simple, because it does not require advanced technical knowledge. Instead, social engineering is based on using human psychology such as curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy that in this case are used as weakness.
Attackers use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak). The types of information they seek can vary and the techniques they use range from little sophisticated techniques that can be easily identified such as bulk phishing emails to highly targeted and multi-layered techniques. According to the results of a survey of cyber-security conducted by ISACA and RSA in the first quarter of 2015, it shows that phishing and some other kind of social engineering attacks were the most common attacks within enterprises in 2014. Almost 70% of respondents declared that phishing was exploited in the enterprise, and 50% declared other social engineering attacks, including water-holing attacks, SMS phishing and so on.

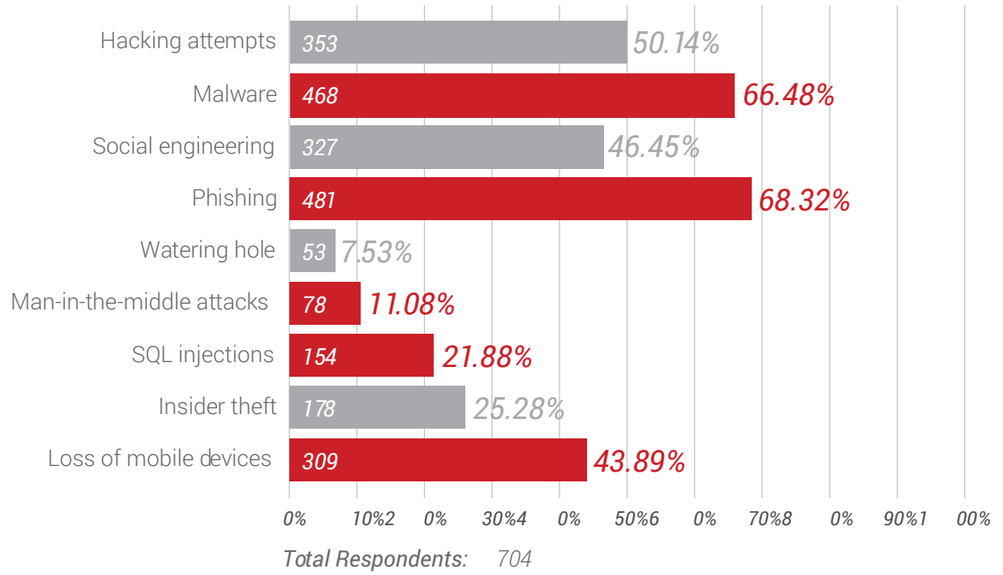


Fig. 1 RSA-ISACA report

What is concerning is that the number of attacks is rising year by year. Based on the "Global State of Information Security Survey 2015" conducted by PricewaterhouseCoopers (PwC), it shows that that the number of detected information security incidents rose 66 percent year-over-year since 2009. On the other side, the survey of 2014 reported that the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013.

As cybersecurity incidents increase and breaches become more significant, they cause an increased financial impact. For more information about financial cost cyber-crime in 2015 read the report that derivates from the study of the Ponemon Institute, sponsored by Hewlett Packard Enterprise.

COMMON SOCIAL ENGINEERING ATTACKS

Phishing attempts. Phishing is one of the most prolific forms of social engineering; it is estimated that 37 million users have reported phishing attacks in 2013. Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate popular company, bank, school, or institution, as well as other methods of communication, including social media, but email phishing is the most common.
Email phishing vary from unsophisticated, which can be easily identified, to very sophisticated, emails appearing legitimate. Phishing emails often ask the user to follow a link to a website, to open an attachment, or require the user to donate money for charity. Despite the fact that email phishing is becoming very sophisticated, there are still some indicators letting the user know the email is false:

- Messages are unsolicited
- Messages are vague, not addressed to the target by name, contain little other specific or accurate information to build trust
- Contain incorrect or poor versions of an organization's logo, and may contain web links to sites that, whilst perhaps similar, are not ones used by that organization.

Baiting is in many ways similar to phishing attacks. Baiting attackers use online adverts and websites and have very unrealistic offers, too good to be true, or send urgent warnings like pop-ups that purport to have detected a problem with the victim's system which by clicking on the pop-up will solve the issue.
But, in fact by clicking the provided link, the user is tricked into giving away personal information, or by clicking the link user's machine may automatically download malware. Another form of baiting is the use of false free Wi-Fi hotspot, where attackers create Wi-Fi that is labeled as free. Although, they provide internet connection, all the data sent over this connection can be captured by attackers.

Watering hole attack is one of the most sophisticated (the most sophisticated form in 2013) social engineering techniques as it requires some more technical knowledge. This attack technique requires the attackers to infiltrate a legitimate site visited by their target, plant malicious code, and then lie in wait.
As with other targeted social engineering attacks, the attacker will research their intended victim(s) and identify one or more trusted websites that they are likely to access. After they identify the suitable website, they look for vulnerabilities within the server that hosts the website and later they insert the code within the server to enable malware to be downloaded.

When a website is compromised, the attackers will be able to monitor almost everything from activity logs (to see who is visiting the website) to the victim's IP.

WHY IS IMPORTANT

TO BE CERTIFIED AGAINST ISO STANDARDS AND HOW CAN ORGANIZATIONS BENEFIT?

Bill Gates once said: "There will be 2 types of business in the 21st century: those that are on the Internet and those that no longer exist." He was not wrong, because currently the vast majority of the businesses are carried out online or at very least organizations have an online presence. Being on the Internet means that the risk from cyber-attack is always permanent, and as explained, social engineering works by manipulating normal human behavioral traits. So, a good way to be protected and ready to handle such attacks (technical and non technical) is to implement fundamental processes and controls based on ISO/IEC 27001.
A key part of this is about raising awareness as how both humans and computer systems can be manipulated. ISO/IEC 27001 determines requirements for an information security management system (ISMS). ISO/IEC 27001, Annex A has 114 controls that help organizations keep information assets secure, even though not all of which are related to technologies, but indirectly, all of them are related to information security. Since ISO/IEC 27001 only contains a brief description of each control, more information about cybersecurity can be found in ISO 27032, which is guidance for cybersecurity inside the ISO 2700 family of standards. ISO 27032 provides a framework for coordination and exchange of information, which is important while managing cybersecurity-related incidents that can occur.
Further, other ISO 27001 series standards can provide greater help such as ISO 27034 which covers the processes for developing secure software, and ISO 27035 which gives guidance on how to detect and react to security (including social engineering) incidents.
The Ponemon Institute's study implies that certification against industry-leading standards can save companies up to US$549,620, while other activities that are promoted by ISO/IEC 27001 can result in even further savings such as:

- employing expert personnel (US$1,458,736)
- appointing a high-level security leader (US$1,291,810)
- training and awareness activities (US$1,150,951)

Finally, it can be concluded that having a certified ISO/IEC 27001 ISMS supported by other key ISO standards such as ISO 27032, ISO 27034 and ISO 27035 organisations can benefit by improving resilience, seizing opportunities to use technology well, keeping risks under controls and actually decreasing security costs.

about the **authors**

Vlerar Shala is an Account Manager for Information Technology and Service Management at PECB. He is in charge of conducting market research while developing and providing information related to the Information Technology and Service Management systems at PECB. If you have any questions, please do not hesitate to contact: marketing.itsm@pecb.com.

Graeme Parker is an experienced professional in Cyber Security, Risk Management and governance fields with proven experience in implementing and developing effective management systems, and also performing various kinds of security testing for small and large organizations. He is the Managing Director of Parker Solutions Group, the PECB representative in the United Kingdom.

“IF YOU DON’T INVEST IN RISK MANAGEMENT, IT DOESN’T MATTER WHAT BUSINESS YOU’RE IN, IT’S A RISKY BUSINESS.”

ISO Capsule

RISK ASSESSMENT IMPORTANCE IN DIFFERENT DISCIPLINES

Jacob A. McLean
Managing Director, KTMC Limited

A risk management is a subject that is very much invoked in our modern world. At the heart of risk management is the macro of risk assessment.

For us to understand the risk assessment process, we need to have a working definition of risk. Risk is defined by ISO 31000 as an effect of uncertainty on objectives. The effect can be positive, upside, or downside negative. We have a broad definition. This broad definition enables us to look at risk from a broad perspective. Risk constitutes opportunities, possibilities of gain or downside risks, negatives, which suggest losses. To get to the real purpose of risk assessment, we must understand that organizations of all types face risks. These risks can affect the achievement of their objectives.

The objectives may range from the organizations activities at the strategic level, so strategic initiatives, its operations, processes, as well as projects. Risks are reflected in society on terms of environmental, technological, safety and security, commercial, financial, economic measures, as well as social, cultural, political and reputational related risks.

How do we classify risks?

When we talk about risks, we generally speak about reputational risks, risk to stakeholders, health safety environmental risks, financial risks, technological risks, risk related to asset integrity, commercial risks, security risks, legal risks, and of course natural and manmade events, which is a wide range indeed.

How do we get our hands around these risks, how do we grasp them and get an understanding of risks?

Well, at the heart of the risk management process is a sub process called risk assessment. Risk assessment consists of identification of risks, analysis of risks, evaluation of risks, as well as determining what method to use in treating the risks. All of these take place within a context, and it is very important to establish a context to communicate and consult internally as well as externally, and of course the monitoring and reviewing is essential.

Let us consider the process of risk assessment. When identifying risks, we need to consider what can go wrong, so what can happen and why. This way we identify the risks.

What are the consequences? What is the probability of future occurrence? Are the factors in place, which can mitigate the existing risks? This is looking at the risk assessment process from a broader perspective.

How should identification aspects be considered?

The identification aspects require that we pinpoint the hazard, the event; in terms of the event, we consider the occurrence as well as the non-occurrence; natural or manmade disasters, upsides and downsides possibilities. For example in the food safety, we all know that there are three basic hazards: physical, chemical and microbiological; all these need to be considered. Then, there is the quality risk; we could consider factors that could decrease the customer satisfaction, and we need to look at the health, safety and environment, which is another broad area. So, we consider here risks of injury to people, or negative impacts on the environment.

How do you define risk analysis?

Why this? Here we determine the likelihood and consequences of the risk. What we need to consider here is the confidence levels, where these are practical. We need to separate minor risks from major, and risk analysis provides data that fits right to the next stage which is risk evaluation. Here we consider the needs for treatment; we decide whether the risk can be tolerated, is it in keeping with the risk tolerance of the organization or entity. We decide whether the activity should be undertaken. We look at priorities for treatment, what are we gonna tackle first. Then we compare the level of risks found in the analysis, with previously establish criteria. So, these are the basic segments, the fundamentals of risk assessment. First identification, then analysis followed by risk evaluation, and then we consider options for treatment.

Risk management, the key to success in the modern world and the heart of risk management is the process of risk assessment. Consider well as you engage in this process.

ISO Capsule

BUSINESS CONTINUITY WITH CYBERSECURITY

Business continuity and cybersecurity have very much in common.
There is preparation you have to prepare for it. You need to have the management commitment in place and the common goals how to protect the enterprise and reduce the impact on the enterprise.

Wolfgang Mahr, PhD
Managing Director at governance & continuuuity gmbh

How can we get the top management commitment?

That's a tricky question. A million dollar question! There are two ways. First of all we can say that the regulations need to be observed. Maybe we can also motivate the management to show proactive governance, being a proactive company management and not just reacting when something happens. I keep saying it's not just following policies, but we need captains who can weather the storm.

In your experience while implementing Business Continuity, where do you find the link between cybersecurity and business continuity?

I think it's with the impacts. If cyber threats can bring down a company for an unlimited length of time and create an impact of thousands or hundred thousands of dollars of euros, then we think of business continuity It's a similar impact as when you think about a fire or explosion. Today the same impact is achieved with cyber-attacks as well, but nobody hears, nobody notices anything, but the damage happens. So, it's completely new dimension of threats. Normally, we have three dimensions that we operate, but now we also have the information domain, and there is also a war out in the frequency domain so we have a total of five threats and we have invented two new dimension of threats.

How can threats be prevented by implementing ISO 27032?

Standards are a good way to attack complex situations. As we've heard during ISO 27032 training, it's the complexity that should be taken into account. You need human resources, you need commitment, and you need technical equipment. You have to correctly set it up, and the standard gives guidelines how to handle these complex situations. Otherwise you get lost and don't know where to start. As you get the standard, attend a training course, raise awareness and knowledge, you are much better prepared to know where to start and who the players are. That's important in maintaining such an approach, as this is really a complex undertaking. It's a project it has a start, but in business continuity we say it's not a project because it never ends. It has to follow the evolution and the development of the organization. Maybe even also in cyber security, because the thigs are much more dynamic. In business continuity with conventional threats, we can make a list of problems we may encounter that might be subjective as well, but with cyber security threats there are people out there who think about new threats 24 hours a day.

THE WEAKEST LINK IN INFORMATION SECURITY

Evanson Ikua
Lead Consultant at
LANet Consulting Group

In IT Security we say that using the weakest link and a program that works towards increasing the issue in training and awareness to users. This is immediate requirement to ISO standards and achievement of these ensures organization will have a very robust IT security and risk management procedure.

What are the biggest challenges companies face in information security?

The biggest challenge with companies is that they do not implement a well rounded information security program. This is normally demonstrated by the fact that most users in the organization do not understand the issues around protecting the protecting information and protecting corporate information. So, our programs try to bring that gap by assuring that all users and all people in the organization from the executives to the line managers and end users to understand the role they need to play in protecting information that belongs to the company and the password information.

What challenges do you face while implementing ISO 27001?

The biggest challenge that we face with ISO 27001 is the lack of understanding from many clients. Many clients do not understand the need, why they need to implement the program to lead them towards conformance with ISO 27001. In some jurisdiction you find that compliance to ISO 27001 is mandatory. All organization that deal with public information for instance are required to comply to that standard and get certified. But in starting jurisdiction outside of their country they find out that the law does not exist for organization to comply and to be certified with ISO 27001. So that brings out very big challenge in terms of organization understanding why do they need to be certified or why do they need to comply to that particular certified or implement the best practices for information security management(2.12)

How should companies convince top management to implement ISO 27001?

The best way to achieving that is to create a very elaborative business cases for the champions in the organization who want to implement ISO 27001 or information security management system the biggest static point to develop a business case(2.46). So, that can be taken to the top management for them to buy a tool- the program of implementing information security according to ISO 27001. Then the moment we have the info for the top management, then everything else becomes easy to provide resources and everything that is needed for the implementation.

NEWS FLASH!

AVAILABLE COURSES

- The PECB Certified ISO 14001:2015 Foundation
- The PECB Certified ISO 9001:2015 Foundation - available in French
- The PECB Certified ISO 9001:2015 Lead Implementer - available in Spanish
- The PECB Certified ISO 26000 Social Responsibility Foundation - available in French
- The PECB Certified ISO 20121 Lead Auditor
- The PECB Certified ISO 17025 Lead Assessor
- The PECB Certified ISO 31000 Lead Risk Manager
- The PECB Certified ISO 45001 Transition
- The PECB Certified ISO 27032 Lead Cyber Security Manager
- The PECB Certified ISO 39001 Lead Implementer
- The PECB Certified ISO 13485:2015 Foundation updated

WHAT'S *HAPPENING* ON twitter

Protiviti Oman (ME) - @protivitiOman

Congrats to our Head of IT Consulting. Now a @PECB trainer - anything to earn confidence & trus from our clients!

Global Standards - @gspakistan

@PECB Authorized Training Partner in Pakistan...
Training will be announced soon

Eric Fourn - @Efourn

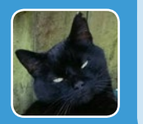
Now @PECB #iso27032 lead cybersecurity manager certified :)

twitter.com/pecb

Iconne Verkes - @IvonneVerkes

Yesterday I had a strange day in a hospital. But the day was ending very good by the message @PECB that I passed the ISO22301 exam.

Jon Winterburn - @jonwinterburn



Got my exam result from @PECB for ISO 27001 Lead Implementer today - I Passed! Thanks to a great coruse from @BeAFirebrand

Dr. Wolfgang H. Mahr - @continuuuity

Thanks @PECB for highlighting the common challenges and solutions: BCM and cyber security youtube.com/watch?v=Whvs3Q...

When Standards Matter...

www.pecb.com