PECB *Insights*

EMBRACING THE FUTURE

ISSUE 03 / December **2016**

When Standards Matter

Introduction

With the end of the year approaching, we are delighted to release an exclusive edition of PECB Insights magazine, a year-end gift. The end of this journey marks the beginning of another one, an exciting one. One that will feed your interests with the most leading-edge, relevant, and useful insights which fit to your area of expertise.

We want to give you a sneak peek and reassure you that in this journey we will not only continue to evolve in the modern world together with our customers, partners, and stakeholders; but also will supplement your professional opinions and make it possible for you to become indispensable to the society. When we say that novelties' are our specialty, we mean it, and surely, 2017 will bring lots of them.

Tim Rama
Commercial Director at PECB

PECB *Insights*

ISSUE 03 / DECEMBER **2016**

CONTENT

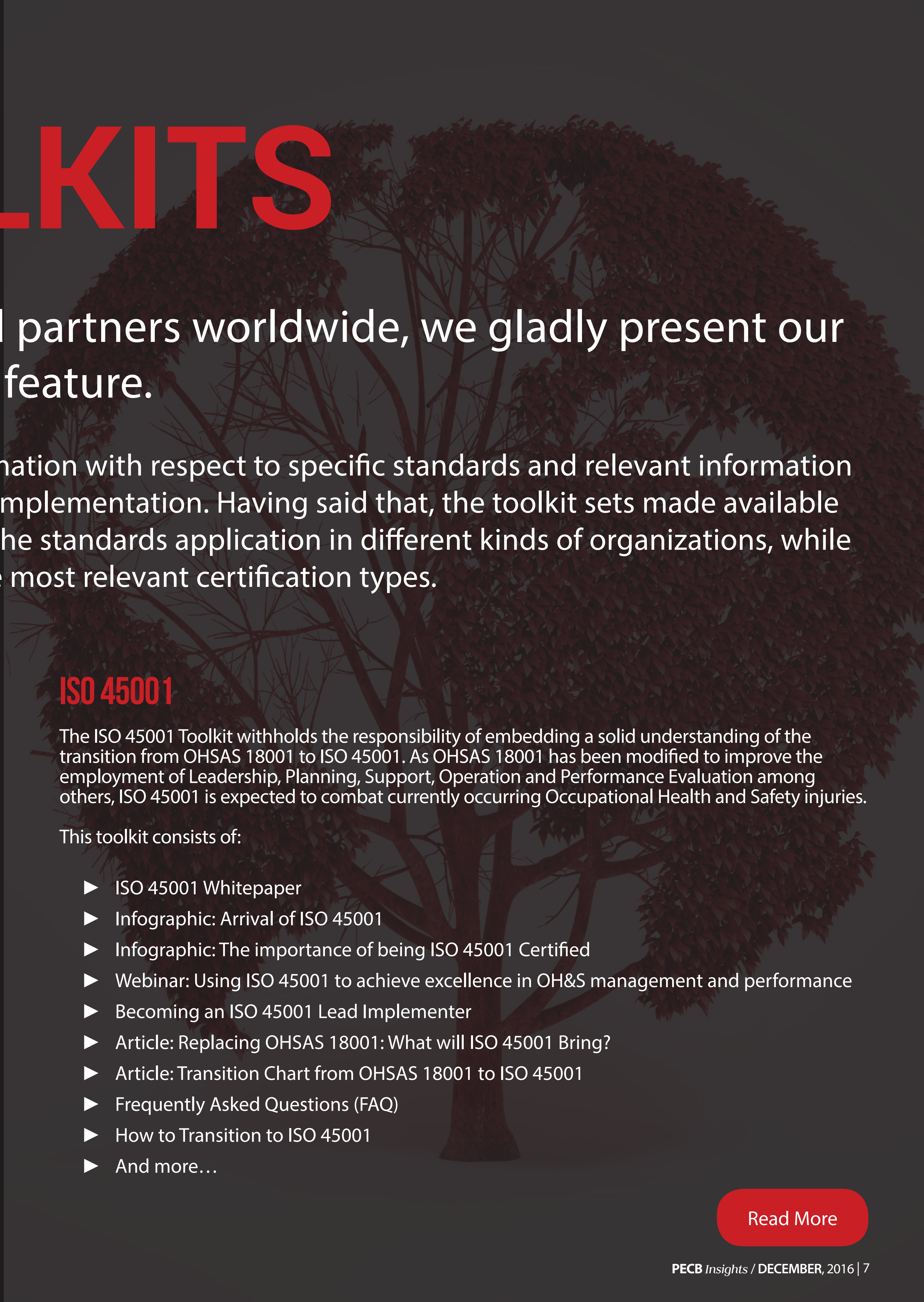
EMBRACING THE FUTURE

Emphasizing upon the mission of PECB Insights, our team is bound to simplifying the complexity of management systems while increasing effectivity to your own organization. With each issue specializing in one operational philosophy, PECB Insights will deliver complete and accurate information based on trending concerns of various industries.

The scope of PECB Insights will continue to be consisting of Quality Management, Health and Safety, Environment, Business Continuity, Resilience, Service Management, Information Security, Cyber Security, and Risk and Management Systems. Striving to keep you constantly updated with the latest developments regarding the industries concerning the above, we have been engaged in the development of delivering valuable information through other credible sources.

Therefore, marking our accountability to ascertain our readers on complete information provision and relevancy we hereby officially announce the development of our online version of PECB Insights. The new version will be launched in January 2017 with a new website, a unique mobile app (IOS & Android), and a fresh new look on the printed edition, exclusive for PECB Certified Members. From next year, PECB Insights will be released on a monthly basis, each of the issues elaborating a promising topic in a variety of industries. Apart from the PDF version, you will be able, from hereinafter, to keep your-self constantly updated and prepared through the website (insights.pecb.com) that will be accessible to everyone.

Additionally, by giving you access to remarkable content, we encourage you to take part in moving together towards succeeding our mission. Our mission is to provide our readers comprehensive and exclusive articles that inspire trust, continual improvement, demonstrate recognition, promote best practices, and benefit society as a whole. We are not satisfied until we hear that you, our readers and supporters, sitting in your favorite coffee shop, are whiling away the afternoon reading stories from our magazine that make you think about how easily you can improve your day-to-day operations, increase productivity, and achieve excellence.



TOOLKITS

Increasing convenience to our readers and partners worldwide, we gladly present our toolkit feature.

The toolkit's aim is to provide you with useful and concise information with respect to specific standards and relevant information needed to increment value of various management standards implementation. Having said that, the toolkit sets made available to you, will give all the essential information needed regarding the standards application in different kinds of organizations, while supporting your selection of the most relevant certification types.

ISO 37001

The ISO 37001 Toolkit will simplify the understanding of Anti-bribery Management System in particular. Emphasizing upon the importance of training and certifying against ISO 37001 will simultaneously accentuate upon benefits; thereby, presenting an implementation framework based on different organizations globally.

This toolkit consists of:

- Whitepaper
- Article : Benefits of implementing ISO 37001 in an Organization
- Article: Integrating ISO 37001 with other Management System Standards
- Implementation Guide
- Frequently Asked Questions (FAQ)
- Infographic: How to raise Anti-Bribery awareness
- Infographic: ISO 37001 application across the world
- Webinar: Key elements of an effective Anti-Bribery Management System
- ISO 37001 Lead Auditor Designation
- ISO 37001 Lead Implementer Designation

Read More

ISO 45001

The ISO 45001 Toolkit withholds the responsibility of embedding a solid understanding of the transition from OHSAS 18001 to ISO 45001. As OHSAS 18001 has been modified to improve the employment of Leadership, Planning, Support, Operation and Performance Evaluation among others, ISO 45001 is expected to combat currently occurring Occupational Health and Safety injuries.

This toolkit consists of:

- ISO 45001 Whitepaper
- Infographic: Arrival of ISO 45001
- Infographic: The importance of being ISO 45001 Certified
- Webinar: Using ISO 45001 to achieve excellence in OH&S management and performance
- Becoming an ISO 45001 Lead Implementer
- Article: Replacing OHSAS 18001: What will ISO 45001 Bring?
- Article: Transition Chart from OHSAS 18001 to ISO 45001
- Frequently Asked Questions (FAQ)
- How to Transition to ISO 45001
- And more…

Read More

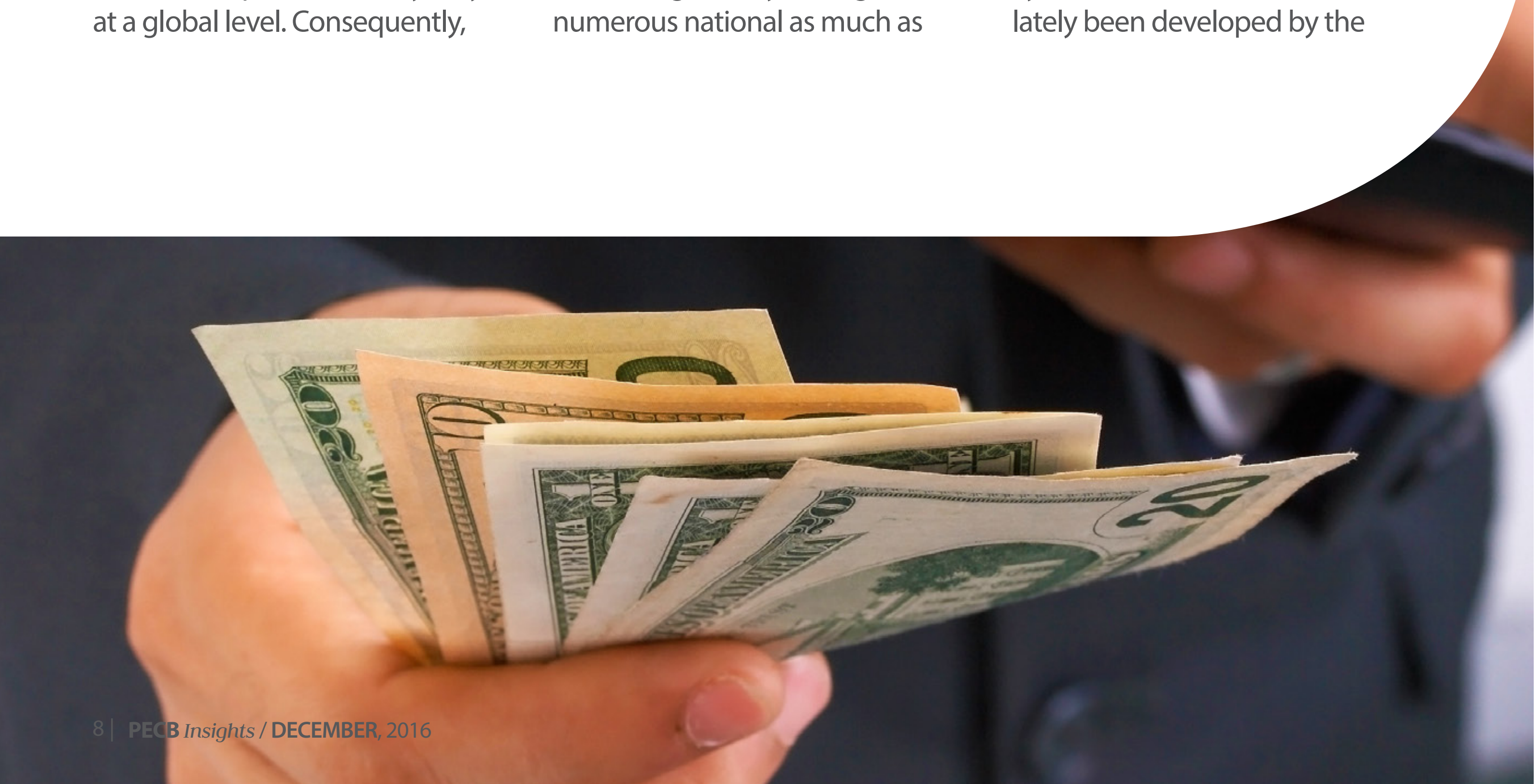
ANTI-BRIBERY MANAGEMENT SYSTEMS: ABOLISHING CORRUPTION

Fundamentally, we may address Bribery as one of the most harmful phenomena to the development of societies, economies, and commercial activities among others. Its spread has led to the formation of many legal frameworks, designated to prevent and tackle its practice in all types of organizations. As such, bribery refers to any offering, accepting, or promising of any sort of value in order to influence the decision, action or even judgment of persons in charge of a duty.

Further, bribery is becoming significantly concerning among individuals and various businesses. According to the World Bank, over $ 1 trillion is paid in bribes yearly, at a global level. Consequently, this is leading to decreasing levels of confidence, trust, and transparency in both public and private sectors. Thus, International Organization for Standardization initiated the establishment of an Anti-bribery Management System; dealing specifically with the elimination and control of bribery risks while aiming to raise integrity in all organizational activities. Both public and private organizations are majorly infected by this degrading political and social phenomenon and shall, therefore, assess this problem with seriousness rather than neglecting its way to success. Though, at the governmental level, some progress has been made towards combating bribery through numerous national as much as international legal frameworks and conventions.

Yet, putting a stop to bribery is not a process or even a procedure with the intent of being abolished by the government alone. Instead, it requires immense effort and unification of organizations as much as members of the society. Integrating a culture of transparency, openness, integrity, and compliance would certainly contribute to strengthening policies and practices associated with the implementation of Anti-bribery laws and Management Systems.

As an Anti-bribery Management System, ISO 37001 standard has lately been developed by the International Organization for Standardization. The purpose of developing and implementing this standard is to establish, implement, maintain and enhance an Anti-bribery program that prevents, detects and addresses bribery risks in an organization or institution. Moreover, ISO 37001 is designed to help organizations comply with anti-bribery laws. This international standard is only applicable to bribery, as it sets requirements and guidance for the establishment of an anti-bribery management system in compliance with anti-bribery laws. Furthermore, an Anti-bribery management system can stand-alone or can be integrated with other Management Systems already implemented within the organization.



Nevertheless, ISO 37001 is witnessed to positively impact businesses in terms of revenues and costs, more than it could affect their social responsibility. This is occurring due to the gray areas companies identify and therefore can ditch various litigations. However, large companies are indirectly obliging organizations in their value chains to possess an Anti-bribery Management System certification. As a result, organizations have managed to put controls on their supply chain, ultimately lowering personal gains of individuals while increasing revenue levels for value chain members. Correspondingly, costs are affected when eliminating inappropriate behavior; organizations are not only driven to have and/or deal with relevant regulatory measures in place to prevent and tackle bribery, but also lower the risk of jeopardizing the company's credibility and reputation. Certainly, any type of unjust behavior would bring unease among all stakeholders, exposing the company to vulnerabilities or threats and bringing back the company to its original state takes much effort, and effort, costs.

Nowadays, nearly every company or business is visible to some amount of bribery risk. To assist you in effectively implementing an Anti-Bribery Management System, we are offering the PECB Certified ISO 37001 Lead Implementer training and certification.

ISO 14001 CERTIFICATION

GUIDANCE TO PROTECTING THE ENVIRONMENT

INDUSTRIALIZATION AND ITS IMPACT ON THE ENVIRONMENT

The Industrial Revolution marked a major turning point for the economic growth and development of a society. This process began in the 18th century in Great Britain, and increased tremendously, bringing wealth and power to several other countries. Replacing agrarian, handicraft economy with machinery manufacturing has changed production capabilities and labor patterns. As a result of mass production, use of energy increased and led to depletion of natural resources, such as deforestation. This inevitably brought carbon emissions, pollution of the water and soil, the primary issue 'global warming'.

The global economy has learned its lesson and is aware that economic impact of global warming is highly important since it is costing the world more than $ 1.2 trillion a year. All businesses have a legal and moral obligation to follow all environmental laws.

Yet the problem is that this issue is usually the last thing to be considered, especially for the companies which are in the growth process. Certainly, this is not a smart move, since the reason why most of the startups fail is because of their negligence towards environmental protection.

Nowadays, organizations are acting more quickly on going beyond environmental compliance, by implementing laws, regulations and environmental management systems, such as ISO 14001.

WHY SHOULD YOU IMPLEMENT ISO 14001?

ISO 14001:2015 is the world's most recognized framework for environmental management system. Governments around the world encourage the implementation of ISO 14001 and it has been adopted as a national standard by many countries. Moreover, it is part of ISO 14000 family of standards that are designed to be mutually supportive, but also used independently. Organizations implement this structured system in order to have a better control of the environmental impacts and performance caused by the environmental aspects of various activities, services and products. In addition, the ISO 14001:2015 standard emphasizes the importance of aspects and impact of product "life cycle". However, the main driver for environmental improvement is the pressure received from the supply chain; surely, most suppliers understand that the dedication to improve the environmental performance will ensure their presence on suppliers' lists.

Before the implementation, an organization needs to complete several steps such as:

- Establishing environmental policy that reveals its responsibilities;
- Identifying current and potential environmental impacts;
- Determining the environmental risks that are associated with the organization's activities and processes;
- Establishing objectives and programs to achieve the required targets;
- Ensuring compliance with regulatory requirements;
- Continuously improving the environmental performance by reducing pollution and waste.
- Initiate actions to prevent or at least mitigate the environmental risks.

Another important matter is training and awareness of employees about their responsibilities, at all levels. The higher understanding of what an EMS offers and why it is crucial for the company to implement, the easier it will be to apply. Further, employees must be trained accordingly to their roles in the company and the environmental team should be aware of energy efficiency and waste management in order to create opportunities for improvement and cost savings. Also, alternative materials and production processes play a major role in environmental practices.

ISO 14001 CERTIFICATION

Once the standard is successfully implemented, the organization can apply for its EMS Certification. Organizations seek certification due to supply chain pressures; they need to prove that their EMS meets the requirements of ISO 14001. In order to obtain the certification, an organization goes through 2 Stages of assessment processes, where internal policies and other procedures are being verified if they are in compliance with ISO 14001 requirements. Once these are completed, the client receives the ISO 14001 Certification, which proves the compliance with the relevant standard.

Companies are aware of many benefits that the certification brings along, few of many are:

- Reduced waste;
- Fulfill their legal obligations;
- Safeguarding the environment as part of their social responsibility;
- New clients and increased market share;
- Creation of a corporate image and credibility;
- Increased stakeholder (interested parties) confidence;
- Access to a new market;
- Lower operational costs;
- Cost savings and much more.

SELECTING AN ACCREDITED CERTIFICATION BODY

Choosing the right accredited certification body is a specified requirement to operate in the global marketplace. PECB offers ISO 14001 EMS Training and Certification services, with the support of highly qualified competent people that have relevant sector expertise, who will guide you through each step and help you overcome any obstacle you might encounter. A worldwide recognition of the certification proves its credibility and great access to a domestic and overseas market, with an independent and impartial approach. ISO 14001 Environmental Management System Certification will improve your business performance and reduce cost while focusing on your impact on the environment.

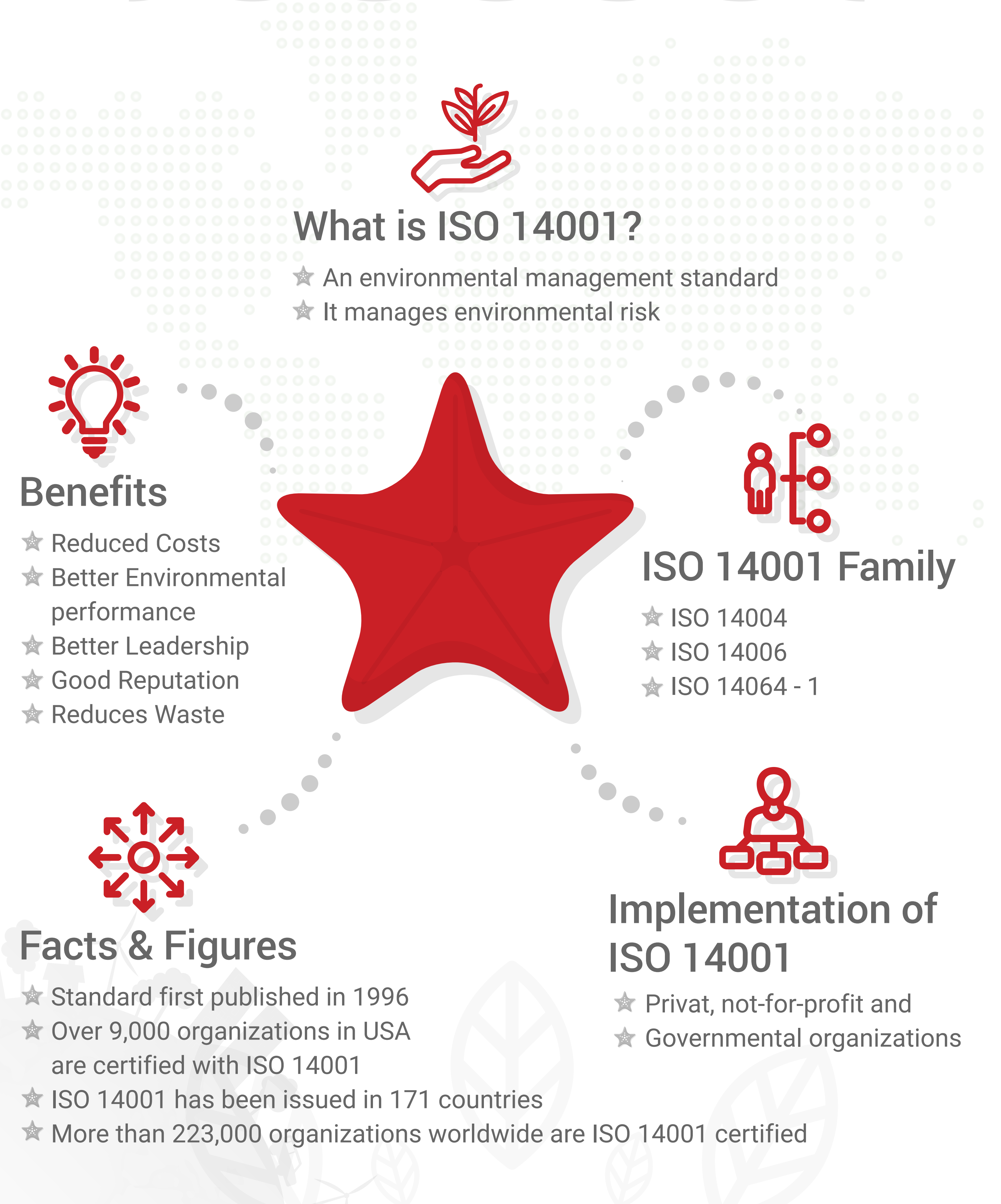
AUTHOR

Suzana Ajeti is a Portfolio Marketing 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 her: marketing.hse@pecb.com.

CONTRIBUTOR

Stephen Lim is PECB Certified Trainer and Managing Director, Principal Consultant & Trainer of JP Power Horizon. If you have any questions, please do not hesitate to contact him: jp.power.stephen@gmail.com

ISO 14001 Standard



What is ISO 14001?

- An environmental management standard
- It manages environmental risk

Benefits

- Reduced Costs
- Better Environmental performance
- Better Leadership
- Good Reputation
- Reduces Waste

ISO 14001 Family

- ISO 14004
- ISO 14006
- ISO 14064 - 1

Facts & Figures

- Standard first published in 1996
- Over 9,000 organizations in USA are certified with ISO 14001
- ISO 14001 has been issued in 171 countries
- More than 223,000 organizations worldwide are ISO 14001 certified

Implementation of ISO 14001

- Privat, not-for-profit and
- Governmental organizations

PECB

Applying ISO/IEC 27001 in the Telecommunications Industry

During the last few years, the Telecom industry has gone through a substantial development period and is aspiring to reach even higher levels of growth by exploring new possibilities in the market. Lastly, this industry has become a quite important piece in the giant puzzle of social interaction.

Along with this significant expansion in the Telecom industry, the need for implementing a Security Management System has had an increase as well. This significant increase is based on the fact that Telecommunication companies are prioritized to protect the huge amount of data that they possess and reduce the number of outages.

Thus, these companies have requirements which include being strict and legal, in terms of their information security management. Consequently, if there is no shield to protect Telecom from various networking threats; it could result in network services becoming unreliable and even losing integrity.

The Telecommunication industry contains a lot of complexity which derives from network elements being owned by different vendors, such as proprietary applications, different operating systems, and procedures that seem unfamiliar for non-Telecom organizations. In fact, this case becomes even more complicated when Telecom operators are supplied with equipment from different manufacturers and when the network management is outsourced, which means that there will be multiple network vendors.

Nevertheless, the Telecom Industry frequently encounters other complex situations that need to be taken into consideration when applying an information security framework in telecommunications, for instance:

- Security incidents
- Complication of operations
- Changing technology
- Strict environment

The biggest security threats to the telecommunication industry

The possibility of information security risks is present in all Telecom organizations, however, the ability to ease and overcome these risks depends on the experience and maturity that operators have.

Threats and results explained in a tabular format

Operators who fail to effectively protect their networks results in:

- Financial costs
- Damaged reputation for Telecom operators in the industry
- Loss of customer reliability
- Legal measures and penalties from governing bodies for failing to deliver secure services

Further, the weaknesses in the network of Telecom can also be used in the worst scenario by criminals and even by terrorist organizations. Evidently, that situation would occur when terrorists would interrupt and use the network communications for their own benefits. By interrupting the communication, a denial of service would occur and this interception can possibly be used to even launch attacks using the network.

Why implementing ISO/IEC 27001 is the most effective way to eliminate these malicious threats?

In order for Telecom industries to protect their networks from various malicious attacks, an effective and strong security system should be implemented. Genuinely, the system being used the most is ISO/IEC 27001 standard. By implementing ISO/IEC 27001, the telecommunications organizations are being led towards having met information security management requirements such as confidentiality, integrity, availability and other matters related to the security property.

Moreover, an Information Security Management System (ISMS) is highly improved when implementing ISO 27001 fundamentals, for the light of the fact that, it provides monitoring, reviewing, and continual maintenance.

Specifically, for the Telecommunication industries, this model is supported by ISO/IEC 27011:2008 and is based and put to practice by ISO/IEC 27002, which delivers clear identification of guidelines needed for maintaining a healthy ISMS in the Telecom industry.

Benefits of implementing ISO/IEC 27001

This standard delivers an application of Information Security Management within the Telecom Industry to ensure the confidentiality, integrity, and readiness of Telecommunication services. The main benefits are:

- Providing Telecom operators with general security control objectives that are based on ISO/IEC 27002, leading to higher and safer levels of information security used inside the organization
- Telecommunication industry will have an increased level of reliance, which will generate higher business profits
- Discretion, reliability, and availability would be assured in Telecom organizations
- Adopting processes and controls that are secure and collaborative, which makes certain that the level of risks is lowered in terms of providing Telecom services
- Increased level of personal alertness as well as public confidence
- Implementing a continual and complete methodology for information technology.

In conclusion, we are aware that Telecom organizations have progressed and developed significantly over the last years. In sync with this growth in the industry, requirements to have information that is secure and reliable is also increasing. That being said, and considering the fact that the information this industry possesses is fragile and confidential, information security is vital.

Customers want their personal information to be accessed by only the authorized personnel. Therefore, the Telecom industries are putting to use various methods to keep their network safe from different malicious attacks, one of which is by applying the ISO/IEC 27001 standard.

Implementing ISMS by utilizing ISO/IEC27002 guidelines, followed by ISO/IEC 27001 certification, results in Telecom organizations ensuring confidentiality, integrity and securing their customer data by maintaining a healthy and consistent ISMS.

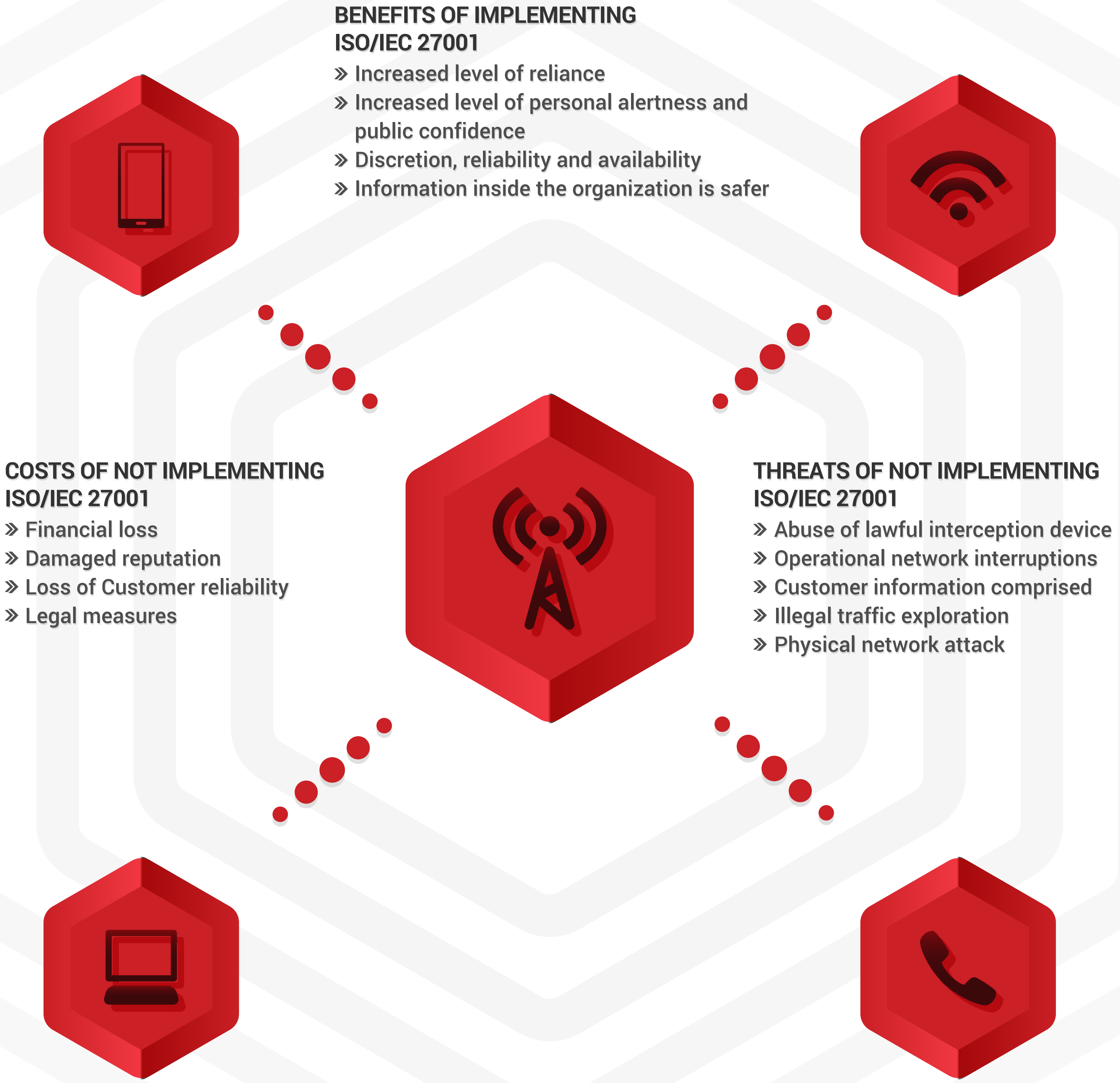
ABOUT

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

CONTRIBUTOR

Mohamed M. Tawfik has 20 years of experience in the telecommunications & Information Technology field, with an excellent career development in competitive multinational environments. Mr. Tawfik is a PECB Certified Trainer and holds several of the market's distinguished information security certificates such as CISM, CISSP, and ISO 27001 Lead Implementer. You can reach Mohamed at mohamed.tawfik1974@gmail.com

APPLYING ISO/IEC 27001 IN THE TELECOMMUNICATIONS INDUSTRY



BENEFITS OF IMPLEMENTING ISO/IEC 27001

» Increased level of reliance
» Increased level of personal alertness and public confidence
» Discretion, reliability and availability
» Information inside the organization is safer

COSTS OF NOT IMPLEMENTING ISO/IEC 27001

» Financial loss
» Damaged reputation
» Loss of Customer reliability
» Legal measures

THREATS OF NOT IMPLEMENTING ISO/IEC 27001

» Abuse of lawful interception device
» Operational network interruptions
» Customer information comprised
» Illegal traffic exploration
» Physical network attack

REASONS TO INCORPORATE A RISK MANAGEMENT PLAN WITHIN YOUR QUALITY MANAGEMENT SYSTEM

The maximization of profit and efficiency are the main quality objectives for any organization. Developing actions to address risks and opportunities when planning will assist an organization to evaluate the level of risk in an operational context. Risk evaluation and analysis are important aspects of any quality management system. The new ISO 9001:2015 identifies within its introduction the importance of "risk-based thinking" and considers that an "external delivering of goods and service" should not target only core processes, but encompass the organization in a holistic approach. While the ISO 9001:2008 version of the standard has always implicitly been geared towards mitigating and avoiding risk while utilizing the PDCA model, the new 2015 version calls out explicitly "risk-based thinking" in addition to the PDCA model. ISO 9001:2015 often is a pairing risk with an opportunity to provide a wide overview of the prevention of risk and a promotion of opportunities to think of risk prior to a near interaction. This standard expects from an organization to address risk affecting products and/or services provided, in order to improve quality as well as customer satisfaction.

THE IMPORTANCE AND BENEFITS OF A RISK-BASED METHODOLOGY

The purpose of any quality management system is achieving conformity to satisfy applicable statutory and regulatory requirements. If risks are continually considered throughout the organization, the possibility of achieving aimed objectives is enhanced, the output is more consistent and customer expectations will be higher regarding products and/or services.

Why is it important for a company to adapt Risk-Based thinking?

- Improved governance
- Improved customer satisfaction and confidence
- Established proactive culture of prevention and continual improvement
- Boosted strong knowledge base
- Assured consistency of the quality of products and/or services
- Improved customer services
- Other benefits
- High confidence of stakeholders and proper use of risk techniques
- Helps organizations to apply management system controls to identify and analyze risks and minimize losses
- Higher management system performance
- Enables organizations to react and protect their business while increasingly growing, and gives stability

SIX REASONS TO CONSIDER RISK PLANNING WITHIN THE MANAGEMENT SYSTEM

Organizations that are affected by risk can have consequences in terms of professional reputation and financial metrics, including environmental, safety as well as social outcomes. Hence, effectively managing potential risk helps an organization to have a higher performance track record in an environment full of uncertainty.

The risk is always considered to be a part of every business, company, or organization. However, it is very important to know how to deal with negative risk. Incorporating risk evaluations will help companies to determine the levels of risks, in order to decrease and mitigate the potential negative risks and permit a better decision for the future potential risks.

RISK PLANNING, A CORE DECISION TO IDENTIFY RISKS

It is the duty for any organization to identify and curtail potential risks. If an organization is aware of potential risks that are related to their business, avoiding them will be easier in the long run. By being aware of the risk, top management will be able to make a plan to reduce the impacts, even if the risks are recognized, management will have a better decision-making process in place and deal with them.

RISK PLANNING, A FINANCIALLY WISE PROCESS

Organizations that have already planned for risk are more financially prepared when a problem may present itself. Businesses that have risk planning in place will be more likely to have loans and other financial instruments in place to remain operational in times of need.

RISK PLANNING PROTECTS AN ORGANIZATION'S RESOURCES

Risk planning assists the organization to respond to potential risks accordingly and appropriately. These kinds of actions will help an organization to focus more on the working tasks that are related to the day-to-day business operations. It also assists the organization in regards to time, money and overall resources required for a higher level operation or working performance.

IMPROVING ORGANIZATION'S BRAND THROUGH RISK-BASED PLANNING

If an organization has applicable risk planning in place, it demonstrates and shows the overall positive manner about how the organization operates. All of the members of an organization will have more confidence and higher moral when they are working for a respectable and responsible organization. The customer also will then be satisfied that they are doing business with a professional and proactive organization.

RISK PLANNING ASSISTS AN ORGANIZATION TO DISCOVER REUSABLE INFORMATION

To manage risk, an organization needs a collaborative effort and many people involved. Information that may be needed to be learned and communicated through processes of risk planning and mitigation can be applied in the similar situations, which may arise after the plan has been developed. As a result, people that are impacted by the plan do not need to start from the beginning, whenever the problem needs to be resolved, but may need continued training whenever significant changes to the organization do occur.

RISK PLANS AND INSURANCE

Including different types of insurance is one of the key assurances of risk planning. The best way to defray the negative impact of risk is by having proper insurance in place.

PECB is a certification body for persons, management systems, and products for a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise in multiple fields, including ISO 9001 Quality Management System courses

AUTHORS

Sherif Mehmeti is a Portfolio Marketing Manager for Quality Management Systems at PECB. He 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

Jason Teliszczak is the CEO/Founder of an international firm; JT Environmental Consulting. Mr. Teliszczak and his highly qualified and knowledgeable consultants assist clients in implementing best practices, gain, and/or maintain certifications within, but not limited to the: Aerospace, Data Security, Energy, Engineering, Environmental, Food Defense/Safety, Medical Devices, Quality, Safety, Security, and Waste industries. Please feel free to contact JT Environmental Consulting at info@jtenv.com

SIX REASONS TO CONSIDER RISK PLANNING WITHIN THE MANAGEMENT SYSTEM

RISK PLANNING, A CORE DECISION TO IDENTIFY RISKS

RISK PLANNING A FINANCIALLY WISE PROCESS

RISK PLANNING PROTECTS AN ORGANIZATION'S RESOURCE

IMPROVING ORGANIZATION'S BRAND THROUGH RISK BASED PLANNING

RISK PLANNING ASSISTS AN ORGANIZATION TO DISCOVER REUSABLE INFORMATION

RISK PLANS AND INSURANCE

PECB

APPLICATION SECURITY MANAGEMENT WITH ISO/IEC 27034

Companies are dealing with many security efforts to protect their information. One of their biggest challenges is to have a security system that is operational, simple, organized, efficient and timely effective.

Along with an information security management system (ISMS), companies should implement other processes and controls or comply with guidance guidelines that will ensure a secure information flow on their information systems and applications. Companies implementing ISO/IEC 27001, and companies who do not because of not seeing it as the priority on their agenda, ultimately still have to protect sensitive information, such as information collected, computed, stored and communicated by their applications. As a result of any breach or lost concerning organization's sensitive information, it can produce an unacceptable impact and make a difference between profitability and loss. Organizations' should make an investment to train their staff on standards such as ISO/IEC 27034 which specifically deals with application security. Furthermore, application security is not only about protecting an application, but rather about protecting sensitive information involved by the use of an application. Yet, not all applications have to be protected except those for manipulating sensitive information. Significantly, ISO/IEC 27034 provides clear guidance on why and how companies can identify, define and verify the security on a sensitive application. It also shows their conformance towards a measurable level of trust defined by ISO/IEC 27034.

What are the benefits of application security?

ISO/IEC 27034 Application Security provides a framework that helps organizations to identify and protect specific application's sensitive information. Nonetheless, it is difficult and costly to try to protect all organization's applications. Likewise, using a risk management approach, the ISO/IEC 27034 framework proposed components such as Application Security Controls (ASC) and processes to ensure that sensitive applications meet the Targeted Level of Trust (i.e. the required security level). This is done so that no sensitive information can be accessed, modified or lost by neither any unexpected event nor unauthorized person, internally or externally. Therefore, when ISO/IEC 27034 is well implemented and managed by an organization, it will not only help to provide expected and verifiable evidence to demonstrate that adequate protection of sensitive applications is in place, but it will also help to support the organization's ISMS and the ICT security. However, while trying to implement application security at a large organization, it might seem expensive and time-consuming. Still, using the ISO/IEC 27034 framework to implement Application Security will be an assurance for optimizing security implementation and the benefits are irreplaceable. Importantly, a well-managed application security process will provide you required evidence that you can trust your applications as adequately protected to face any incident (accepted risks) that may happen at that time.

The ISO/IEC 27034 framework will provide you clear guidance on how to handle the application security issues, taking in account your specific Business, Regulatory and Technological contexts. Moreover, implementing ASCs identified by your Level of Trust is a set of processes that are not only well integrated on the System Development Life Cycle (SDLC), but also to your day-to-day operational processes.

Required ASCs can be implemented internally by the company employees or externally by outsourcing the companies that deal directly with the specified security matters. In both situations, these ASCs are verifiable and expected results can be provided to prove their adequate implementation. Without this evidence, a company cannot verify any successful security implementation.

Managing application security is not trivial. It's not only a code review process and vulnerability testing anymore. Application security is not only for organizations' developing application but also for organizations that need to use and operate applications to make a successful business. Application security has to be planned, defined and managed in respect of organization's priorities and resources. Too much security is a waste of money, but not enough security can be a threat to the organization's survival. Looked that way, it's maybe better to invest in the necessary training and certification to make sure application security will be understood and well managed by your experts.

ISO/IEC 27034 as guidance for application security

Thinking of deeper security implementation implies that more procedures and standards should be considered. The proper implementation of ISO/IEC 27001 and its ISMS provide good assurance for information security matters on the company. But, ISMS' limitation is to identify what applications should be protected, and will not tell you what to do and that's where ISO/IEC 27034 gains all its value.

ISO/IEC 27034 Application Security standard content

PART 1

Application Security: Overview and concepts (published)

Part 1 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

PART 2

Application Security: Organization Normative Framework (published)

Part 2 presents an in-depth discussion of the Organization Normative Framework, its components and the organization-level processes for managing it. This part explains the relationships among these processes, the activities associated with them, and the means by which they support the Application Security Management Process. It presents how an organization should implement the standard and integrate it into its existing processes.

PART 3

Application Security Management Process (expected for 2017)

Part 3 presents an in-depth discussion of the processes involved in an application project: determining the application requirements and environment, assessing the application security risks, creating and maintaining the Application Normative Framework, realizing and operating the application, and validating its security throughout its life cycle. This part explains the relationships among these processes, their activities and interdependencies, and how they introduce security into an application project. It presents how an organization should implement the standard on an application project level and integrate it into its existing processes.

PART 4

Application Security Validation (work in progress)

Part 4 presents an in-depth discussion of the application security validation, audit and certification process for organizations, applications, and people. It presents what and how the implementation of this IS should be verified and audited on three (3) levels, as:

1) Organization level – where it will frame and guide auditors to validate the organization's AS objectives and audit/verify how an organization complies with its AS objectives and criteria.

2) Application level – where it will frame and guide auditors to measure the application's Actual Level of Trust and compare it with the application's Targeted Level of Trust previously selected by the organization, to certify this application as secure as expected.

3) Peoples level – where it will frame and guide the development and the implementation of an ISO/IEC 27034 AS professional certification.

PART 5

Protocols and application security control data structure (expected for 2017)

Part 5 presents the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model, in order to facilitate the implementation of the 27034 AS framework and the communication and exchange of ASCs.

PART 5.1 - Protocols and application security control data structure – XML Schemas (expected for 2017)

Part 5 presents and explains an XML Schemas example, describing the Application Security Control (ASC) and the Application Security Life Cycle Reference Model (ASLCRM) components.

PART 6

Case studies (expected for 2017)

Part 6 provides case studies and examples of ASCs tailored for specific application security requirements.

PART 7

Application Security Assurance Prediction Model (expected for 2017)

Part 7 codifies the requirements and framework for making predictive security claims statements to replace ASC in an AS project when allowed. Each part is entitled to bring explanations on how to treat every aspect on Application Security. Organization security plans should be in accordance with the application security.

Note: Because of the ISO/IEC 27034 project still a work in progress, this list of parts is not definitive. Documents can be added or removed and document's name can be changed as the project will evolve.

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

For further information, please visit Information Security Management Courses or IT Security Courses.

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.

Mr. Luc Poulin has more than thirty years' experience in computer science, during which he acquired a solid expertise in IT systems and software engineering. He has specialized in managing, implementing and evaluating the overall security of information systems within development and operation environments. He has a Ph.D. CISSP-ISSMP CSSLP CISM CISA CASLI , CASLA and currently working as CEO- Information / Application Security Senior Advisor at Cogentas Inc. You can contact Luc via email Luc.Poulin@Cogentas.ca.

APPLICATION SECURITY NOWADAYS

1 BUSINESS DISRUPTION ATTEMPTS

*The second quarter of 2015 saw a **132%** increase in DDoS attacks compared to Q2 in 2014, and a **7%** increase compared to Q1 2015.*

2 SECURITY APPS CIRCUMSTANCES

***97%** of apps tested in 2015 contain at least one vulnerability.*

3 MORE LEARNING SESSIONS

***73%** of organization are turning to education and training to make users less susceptible to social engineering; **4%** more than the previous year.*

4 DATA BREACH

*In 2015, at least **60%** of businesses will discover a sensitive data breach.*

5 RISK LEVEL

***10%** of vulnerabilities discovered were rated critical or high risk.*

THE MOST VULNERABILITIES

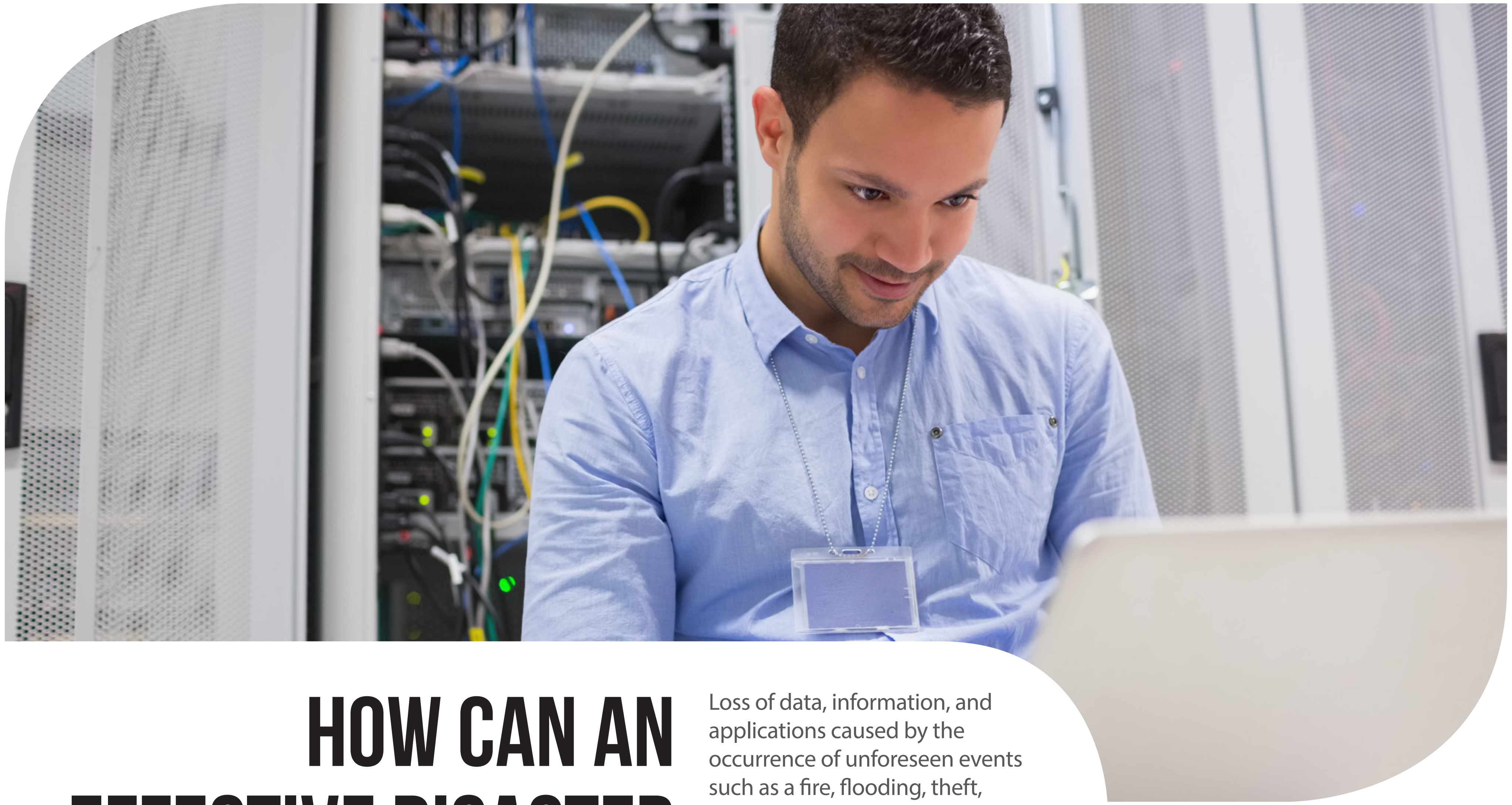
Vulnerable SSL and TLS installations were the most common class of vulnerabilities detected by Trustwave network scanners.

APPLICATIONS WITH HIGH PERCENTAGE OF VULNERABILITIES

Application with the highest vulnerabilities: Session management, Information leakage, Cross site scripting, Authentication and Authorization.

PECB

Source: www.trustwave.com



HOW CAN AN EFFECTIVE DISASTER RECOVERY PLAN HELP YOUR BUSINESS?

Companies have an invaluable asset, the wealth of information, supported every day by the experience gained from its own activities.

Because of some critical issues and the importance of data that the majority of companies have, they invest towards the implementation of techniques and procedures which ensure business continuity and recovery.

Loss of data, information, and applications caused by the occurrence of unforeseen events such as a fire, flooding, theft, virus attack, hardware failure, human error could lead to severe disruptions in organization's operations, productivity or quality of services. Disasters vary in type and level, they are by nature inevitable but mostly unpredictable. It is in a company's best interest to define a disaster recovery plan, in order to return to its normal state in case a disaster happens. For the organizations, a disaster is an unexpected disruption which affects a part or all its business operations, which may have a direct impact on the company's revenue.

Additionally, a disaster can have several negative impacts in cause-and-effect scenarios in every business. One of the most important and greatest challenges for business leaders is making sure that their company has already defined the necessary measures to prevent and/or prepare for any possible disaster and safeguard the business. For instance, when an unforeseen event takes place and brings a process to the end, an organization needs to have a rapid recovery plan in order to continue to provide services or products to their customers. In the event of a catastrophe, it is necessary to have a strategic recovery plan in place, which can address various disruptions from data security breaches to natural disasters. The consequences of a disaster vary, ranging from small interruptions to entire business shutdowns which can take days or months to recover and even cause fatal damage to the business.

The importance of a disaster recovery plan

A disaster recovery plan incorporates the protection measures taken to reduce the impacts of a disaster so that an organization will be able to preserve or swiftly restart their IT systems. In addition, a disaster recovery plan (DRP), entails an analysis of critical business functions and regular needs and also has an important focus on disaster prevention. Disaster recovery refers to the process of preparing for recovery or continuity of critical technology infrastructure of an organization after a natural or manmade disaster occurs. It is about safeguarding an organization from the negative impacts that events such as natural disasters (earthquakes, fire, storms, etc.) and manmade disasters (terrorism, email virus, infrastructure failure, etc.) generate.

In IT, disaster recovery steps can involve different scenarios such as: restoring servers with backups and re-creating private branch exchanges to meet the business requirements. The disaster recovery plan is a comprehensive plan which provides a roadmap to be followed that allows an organization to recover the affected business functions. The disaster recovery plan is a significant process which can prevent harsh data loss that might result in a serious financial impact, loss of client confidence and harm the reputation of the organization. Thus, being prepared to overcome these disruptive events with minimal operational disruptions and difficulties, recover rapidly is very essential. For that reason, putting into action a recovery plan will make sure that the consequences of a disaster are contained and the organization will recover as quickly as possible.

Nevertheless, we cannot avoid disasters; however, there must be a disaster recovery plan in place, in order to be prepared in the event of a disaster and be able to get back to normal quickly without experiencing damages to vital business functions. On that note, a good disaster recovery plan within an organization can minimize the losses, however; choosing not to have a disaster recovery plan in place can put the organization at risk of significant financial costs, losing its reputation and jeopardizing their customers and stakeholders trust.

The measures that an organization can take to assure that its critical business functions are protected in the event of a disaster:

- Protective measures: the purpose is preventing a disaster from happening. For instance, security controls may help decrease the chances of a terrorist attack and in cases of power disruptions on sensitive equipment, power supply units may help.
- Detective measures: the purpose is noticing some of the disruptive events through the use of observation cameras, fire sensors, and antivirus software etc.
- Corrective measures: the purpose is the re-establishment of the business procedures, systems, and data recovery after disaster hits.

Disaster recovery is suitable for all types of business and industries, regardless of their size. According to London Chamber Commerce and Industry, 90% of businesses that lose data from a disaster are forced to shut down within 2 years of the disaster.

What are the benefits of a Disaster Recovery Plan

Bear in mind that, you cannot foresee all crises regardless if they are natural or man-made or how they will affect your organization. Therefore, the benefits of developing a disaster recovery plan are clear, when implementing a detailed plan the organization could mitigate threats and ensure its critical data and records are secured through proper measures.

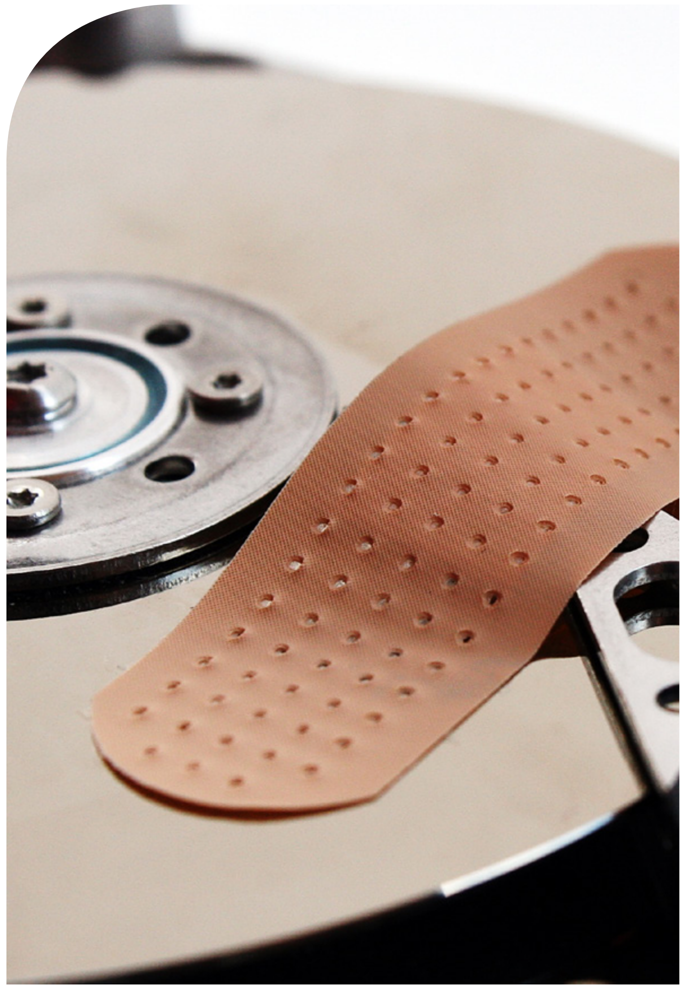
The benefits of having an effective disaster recovery plan within your organization include:

1. Helps an organization to be prepared in the event of a disaster.
2. Secures the records and hardware.
3. Helps to recover the critical data of your organization rapidly and easily.
4. Provides guidelines about the actions that the organization should take after a disruptive event occurs and ensures that the organization continues functioning after the disaster.
5. Established task redundancy, so that, at least two people can perform any of the tasks, keeping the company protected in case of an emergency.
6. Protects the reputation, and increases the confidence of investors.
7. Insurance companies will view your business as more promising when an actual disaster recovery plan is in place.

To ensure that the IT functions can be restored as quickly as possible in a given situation, there must be defined a clear plan in case of a catastrophe. In such cases, it comes down to disaster recovery as a plan that aims to recover data and restore all vital business processes within the required time, and which fills all the gaps in emergency cases.

Any organization wanting to establish, implement, maintain and manage an ongoing Disaster Recovery Plan can refer to PECB training. We are highly committed to Disaster Recovery Planning and continually adding value to this portfolio by developing training and offering certification services.

For further information, please visit Disaster Recovery Training Courses.



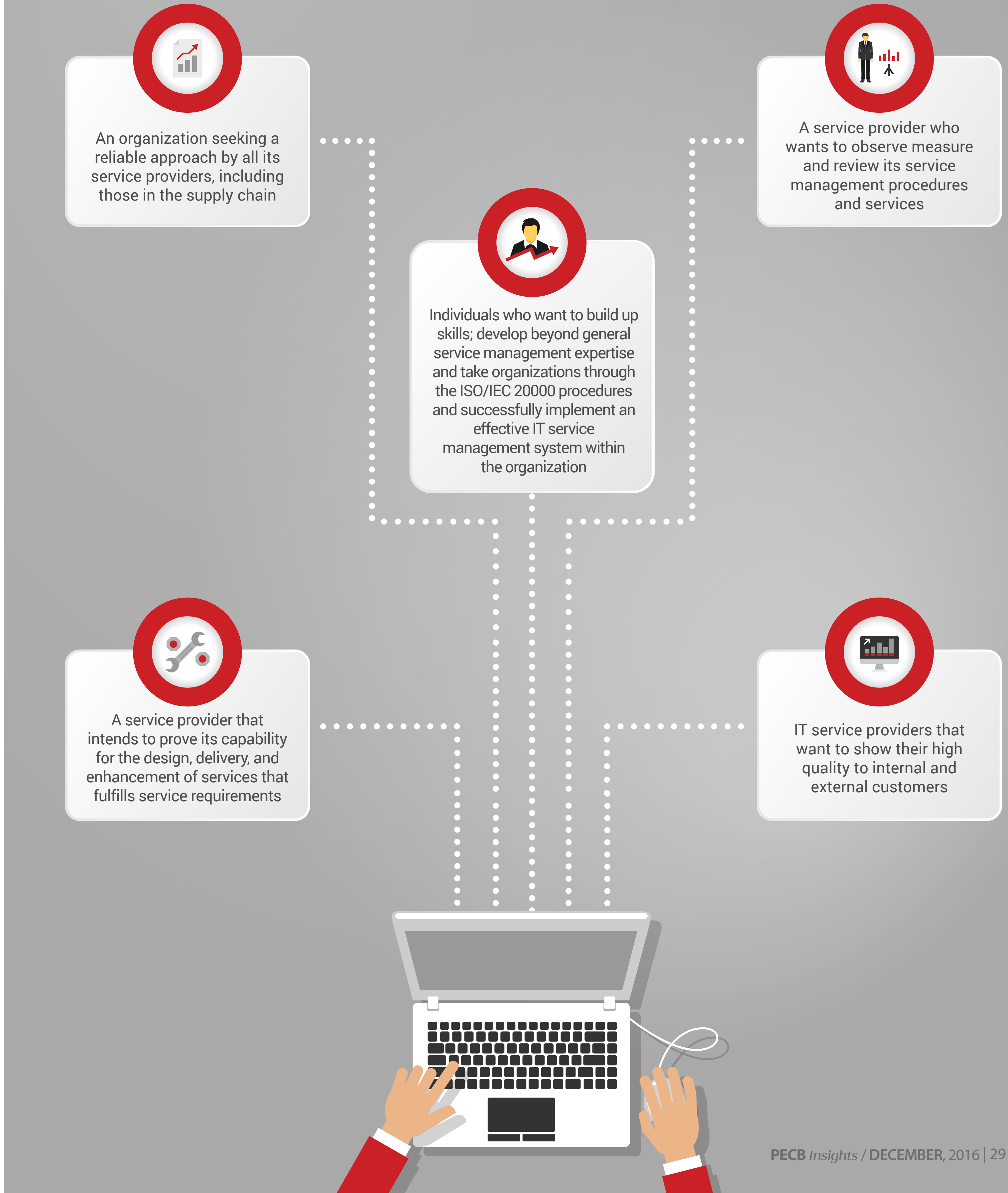
Author

Erita Rexhepi is a Portfolio Marketing Manager for Continuity Resilience and Service Management at PECB. She is in charge of conducting market research while developing and providing information related to CRSM standards. If you have any questions, please do not hesitate to contact her: marketing.crsm@pecb.com.

Co-Author

Artan Mustafa is the Course Development Manager for IT Security at PECB. He is in charge of developing and maintaining training courses related to IT Security. If you have any questions, please do not hesitate to contact him: itsec@pecb.com.

WHO CAN APPLY ISO/IEC 20000?



An organization seeking a reliable approach by all its service providers, including those in the supply chain

A service provider who wants to observe measure and review its service management procedures and services

Individuals who want to build up skills; develop beyond general service management expertise and take organizations through the ISO/IEC 20000 procedures and successfully implement an effective IT service management system within the organization

A service provider that intends to prove its capability for the design, delivery, and enhancement of services that fulfills service requirements

IT service providers that want to show their high quality to internal and external customers

BENEFITS OF IMPLEMENTING ISO 37001 IN AN ORGANIZATION

Bribery refers to any offering, giving, accepting or promising advantage with any value or bribe in order to influence the decision, action, or judgment of persons in charge of a duty.

Any individual or organization that is involved in bribery means that they have accepted or gave something with the intention of influencing the recipient in some way favorable to the party providing the bribe. Until now, many acts, laws, legislations and policies have been established and implemented in order to prevent corruption and bribery around the world; nonetheless, some of them were successfully implemented and many others not. Bribery is becoming a significant concern among individuals and different businesses. Consequently, this is leading to the lack of confidence, trust, and transparency in both public and private sectors. Thus, International Organization for Standardization initiated the establishment of an Anti-bribery Management System that deals specifically with bribery risks.

The purpose of developing this standard is to establish, implement, maintain and enhance an anti-bribery program that prevents, detects and

addresses bribery risks in an organization or institution. Moreover, ISO 37001 is designed to help organizations comply with anti-bribery laws. This international standard is only applicable to bribery, as it sets requirements and guidance for the establishment of an anti-bribery management system in compliance with anti-bribery laws. Furthermore, an Anti-bribery management system can stand alone or can be integrated with other management systems that are already implemented in the organization.

In fact, an Anti-bribery Management System program is suitable to be implemented in any organization. Considering that the nature of an organization differs from one another, the International Organization for Standardization established the standard in such a system that it can be appropriate to different organizations and can be integrated with different management systems. Since ISO 37001 addresses to bribery in the private or public sector, bribery by the organization, within the organization, and by the personnel, it is reasonable to think that the standard is applicable to all types and sizes of the organizations.

Substantially, there are different reasons why an organization should establish, implement, maintain and improve an Anti-bribery Management System. Organizations that wish to implement such a system will have the opportunity to:

- Promote trust and confidence - organizations that implement an anti-bribery management system are more likely to be reliable when it comes to cooperating with potential partners because the risk of bribery is lower. Organizations that have anti-bribery policies in place promote trust and are more likely to sign agreements with other organizations, rather than with organizations that do not have anti-bribery policies in place. Moreover, individuals who are certified ISO 37001 Lead Implementers or ISO 37001 Lead Auditors are more reliable when it comes to helping organizations implement an ABMS or perform audits on an ABMS

- Implement the necessary measures designed to prevent, detect and address bribery - organizations that implement an ABMS according to ISO 37001 requirements will be able to implement the necessary measures to reduce bribery risk by preventing or detecting the risk before it negatively impacts the organization. Moreover, ISO 37001 standard, guides and provides requirements for taking these measures based on the nature of the bribery risk that the organization might face

- Avoid cost - organizations that implement an anti-bribery management system will save money by refusing to pay bribes and by not having to implement costly procedures

Indeed, when taking the appropriate measures designed to help the implementation of ISO 37001, the implementation of Anti-bribery policies will be much easier. Any organization that wants to get certified against ISO 37001 shall follow the requirements and guidelines in order to implement policies that are applicable to them. These policies shall comply with Anti-bribery laws, prohibit bribery, comply with ABMS requirements, commit to continual improvement of ABMS, be documented and communicated within the organization. If the organization implements the necessary measures of ISO 37001 as guided, it will be easier to effectively manage bribery risks, prevent bribery risks and detect potential bribery risks.

Considering that bribery is harming many organizations and leading them to costly litigations, lawsuits, and losses, PECB (Professional Evaluation and Certification Board) has established training curriculums and certification schemes for professionals, consultants or experts who want to gain a comprehensive knowledge of the anti-bribery management system and its principles. Therefore, any organization wanting to establish, implement, maintain and improve ISO 37001 can refer to PECB training. This also stands for organizations wanting to integrate ISO 37001 with any existing management system within the organization.

The Anti-bribery Management System Trainings provided by PECB are listed below:
ISO 37001 Introduction (1 Day)
ISO 37001 Foundation (2 Days)
ISO 37001 Lead Implementer (5 Days)
ISO 37001 Lead Auditor (5 Days)

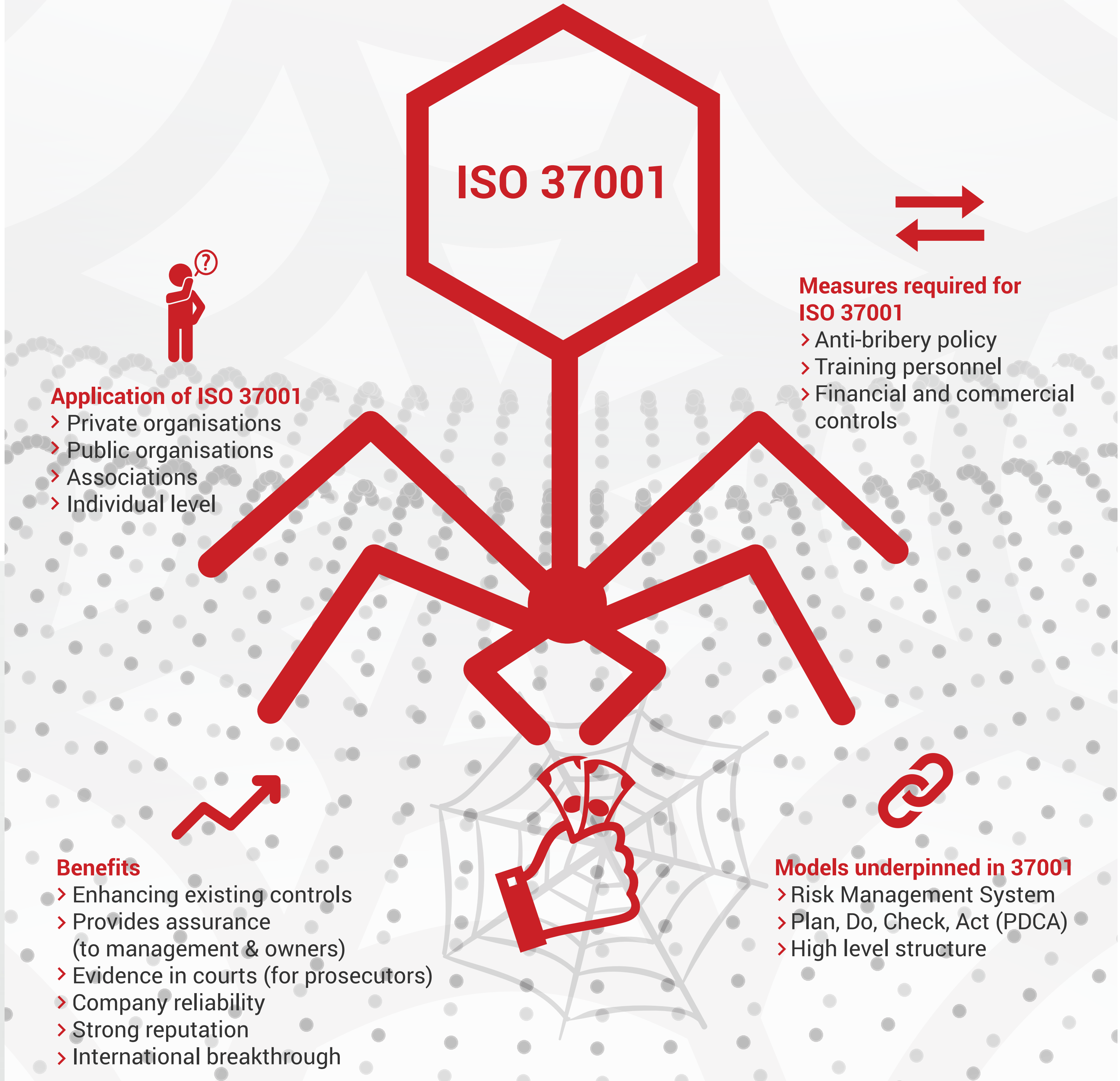
AUTHOR

Donika Muçolli is the Course Development Manager for Risk and Management at PECB. She is in charge of developing and maintaining training courses related to RM. If you have any questions, please do not hesitate to contact her at rm@pecb.com.

CONTRIBUTOR

Mohamad Khachab is a PECB Partner and Trainer, who has 30 years of professional experience in management consultancy, project management, teaching/training, IT Procurement, preparing proposals, information risk management, research, developing bidding documents, and business development activities. If you have any questions, please do not hesitate to contact him at khachabmy@gmail.com.

ISO 37001
Anti-Bribery Management System

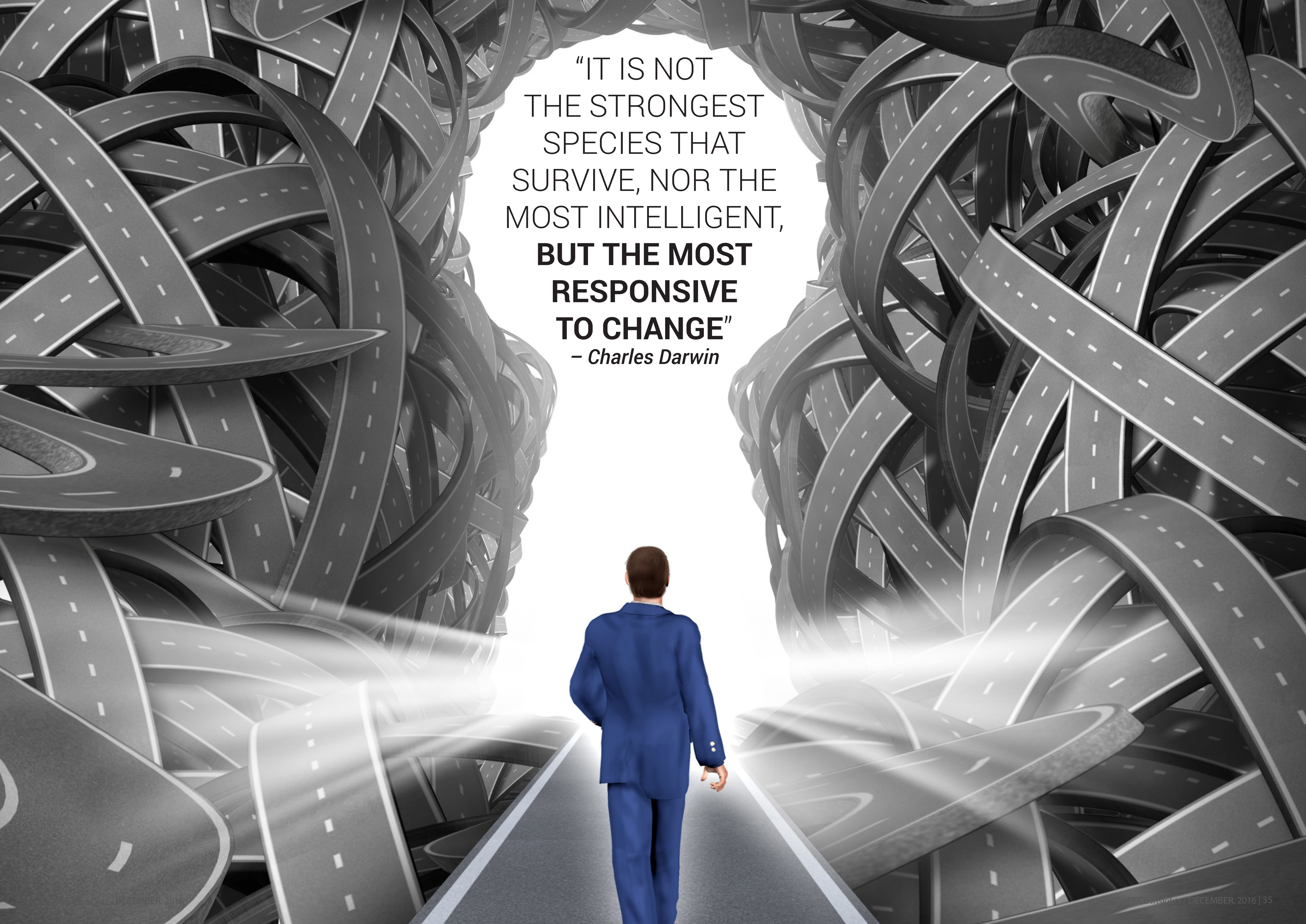


Application of ISO 37001
- Private organisations
- Public organisations
- Associations
- Individual level

Measures required for ISO 37001
- Anti-bribery policy
- Training personnel
- Financial and commercial controls

Benefits
- Enhancing existing controls
- Provides assurance (to management & owners)
- Evidence in courts (for prosecutors)
- Company reliability
- Strong reputation
- International breakthrough

Models underpinned in 37001
- Risk Management System
- Plan, Do, Check, Act (PDCA)
- High level structure



> “IT IS NOT THE STRONGEST SPECIES THAT SURVIVE, NOR THE MOST INTELLIGENT, **BUT THE MOST RESPONSIVE TO CHANGE**”
>
> *– Charles Darwin*

UNDERSTANDING THE COMPLEXITY OF THE CYNEFIN FRAMEWORK

As intriguing as it is, the Cynefin framework distinguishes between four quadrants of organizational decision making, serving as a very effective tool to risk-based thinking. Allowing executives to address complex concepts, this framework holds the purpose of enabling the view of various problems from numerous points of view. The first quadrant, "Obvious", refers to cause and effect solutions to such problems and implies that alike problems can be eliminated through simple logical thinking. However, categorizing problems is a very useful method to address problems in large numbers. The second quadrant of this framework, "Complicated", regards best practices as having the tendency of being unable to be applied from everyone; letting us understand there is a level of expertise needed to address problems falling under this quadrant. "Complex Contexts", refers to the unknown and unpredictable problems which should reveal itself rather than pose a course of action to decision making. Lastly, in a "Chaotic" context relationships between cause and effect become very difficult to know and are rather surprising and with a great impact. This quadrant emphasizes on the necessity of a good crises management strategy.

Peter Davis is PECB Certified Partner and Trainer. He is also the Principal of Peter Davis + Associates, which provides governance, audit and security services to financial, education, government, insurance, and manufacturing clients. Mr. Davis is certified with several certifications such as CISA, CMA, CISSP, PMP etc.

Watch the Video

Peter T. Davis

PRINCIPAL AT PETER DAVIS + ASSOCIATES

KEY SUCCESS FACTORS FOR BCM PROGRAM

The following video reveals the key success factors of implementing and monitoring a Business Continuity Program. In addition, while emphasizing upon the importance of Business Impact Analysis (BIA), it guides towards creating and effective Business Continuity Plan.

According to Raymond Ee, the following factors are considered as mandatory for a successful BCM Program;

Top management engagement will certainly increase the visibility of your BCM program while getting more vulnerable participation and support from the various departments in your organization.

Providing effective training is strongly recommended to organizations considering embarking on a BCM Program; whereby increasing the general awareness and support to the program.

Choosing the right tools to manage your BCM Program, should account growth and therefore implement specialized BCM software for better convenience based on the size of the organization.

As a certified professional in Business Continuity Management (BCM) and certified ISO 22301 Lead Auditor, **Raymond** has provided advisory to more than 30 organizations guiding them to achieve BCM certifications or to improve their current BCMS through gap analysis work. Raymond holds a degree in Computer Science & Information Systems from the National University of Singapore and an MBA from San Francisco State University.

Raymond Ee

BCM Consultant

Watch the Video

PECB

When Recognition Matters

ON YOUR WAY!
PECB EVENT IN SINTRA, PORTUGAL

PECB warmly invites you to the forthcoming prestigious event, hosted in Sintra Portugal from 4th to 7th of January. Notably this prestigious event will drive us through the beginning of 2017, by marking the launch of our newest courses.

January 4-5 Organizational Resilience

PECB ISO 22316 Foundation course will, on one hand, forestall the ability of fast response to various threats and opportunities in both the internal and external business environments. Interpreting resilience, this course will exploit its importance as both a strategic organizational goal and as a dynamic concept. Furthermore, during this two-day course participants will absorb the skills to identify vulnerabilities, address potential threats, and be guided to the effective implementation of resilience planning.

January 6-7 Emergency Management

PECB ISO 22320 Foundation course, on the other hand, is going to target both public and private sectors inevitability to effective emergency response. Minimizing the consequences effect of natural disasters, uncontrolled, and intentional incidents will be precisely addressed as an issue with significant impact on our society and affected the population. Highlighting its importance, this course will enable participants to expand their knowledge headed for managing, controlling, tracking information and adapt to various emergency situations.

Contact us at: events@pecb.com   Details

www.pecb.com/conferences

29th to 30th of June, 2017

Palais des congrès de Montréal

THE PECB STANDARDS INSIGHTS CONFERENCE

The Standards Insights Conference will bring together experts, practitioners, and influencers to continue elevating our professional competencies. A unique event organized by PECB, the Standards Insights Conference will be the first and largest event, specializing in Information Security, Governance Risk and Compliance, and Information Security.

Intending to multiply the opportunity for professionals and luminaries to meet, the PECB Standards Insights Conference will be hosted at "Palais des congrès de Montréal" from 29th to 30th of June, 2017. Harmoniously, sharing knowledge in a different environment would not only create boundless business opportunities among participants but would also extend to the mind-blowing lineup of guest speakers.

With a variety of activities around the astounding city of Montreal, attending this conference will add up to the pre-conference training opportunity on Appréciation du Risque avec la Méthode Mehari course, and ISO 27008 Foundations – Auditing Information Security Technical Controls course.

TRENDING ON twitter

PECB Europe - @pecb_eu

Today at #WCS2016 in Madrid, talking about #Legal #Compliance with @audisec_es ... sounds promising! #CompliancePenal #ISO19600 #ISO37001

Cedric Van B. - @neox_

Featuring @DeNijsDirk, n sharing knowledge. If you're concerned about #privacy take a look!

PECB - @PECB

https://youtu.be/aPFMWQE9RK0 - #Cybersecurity and #Privacy as major issues that many organizations face.

AB Consulting CI - @abconsultingci

@PECB ISO 27001 Certified Lead Implementer - Formation et Certification #ABIDJAN www.eventbrite.fr/e/billets-pecb-iso-27001 @Eventbrite

PECB - @PECB

PECB Retweeted PECB Insights
Follow @PECBInsights! New online #magazine coming soon...Stay tuned! #WhenStandardsMatter

twitter.com/pecb

LIST OF ALL AVAILABLE COURSES

PUBLISHED COURSES

- PECB Certified ISO 37001 Lead Implementer
- PECB Certified ISO 37001 Lead Auditor
- PECB Certified ISO 37001 Foundation
- PECB Certified ISO 37001 Introduction
- PECB Certified Lead Disaster Recovery Manager

TRANSLATED COURSES

- PECB Certified ISO 31000 Lead Risk Manager (French)
- PECB Certified ISO 22000 Lead Auditor (French)
- PECB Certified ISO 29100 Lead Privacy Implementer (Spanish)
- PECB Certified ISO 31000 Risk Manager (Polish)
- Advanced Auditing Techniques (Spanish)
- PECB Certified 22301 Lead Implementer (German)
- PECB Certified ISO 27001 Lead Implementer (Brazilian Portuguese)
- PECB Certified ISO 31000 Risk Manager (Brazilian Portuguese)

UPDATED COURSES

- PECB Certified Lead SCADA Security Manager (English)
- Advanced Auditing Techniques (English)
- PECB Certified ISO 27001 Lead Implementer Course (English)
- PECB Certified ISO 27001 Lead Auditor Course (English)
- PECB Certified ISO 22301 Lead Implementer Course (English and French)
- PECB Certified ISO 27035 Lead Incident Manager Course (French)
- PECB Certified ISO 22301 Lead Auditor (English)
- PECB Certified ISO 13485 Lead Auditor (English)

www.pecb.com

When Standards Matter...