PECB Insights

THE IMPORTANCE OF AUDIT

ISSUE 02 / JULY 2016

When Standards Matter

A **Word** from our **President**

On behalf of PECB, it is with great pride that I invite you to read the newest edition of PECB Insights!

At PECB, our best feature is our global team of highly knowledgeable individuals and professional business partners, who, through their hard work, passion and dedication are continually driving our organization forward. Our wide range of products and services, as well as the extensive work accomplished over the last decade, are benefiting thousands of men, women and organizations who are concerned or working with the best practices based on internationally recognized standards.

We have dedicated our collective heart and soul into our success, and we will continue to do everything professionally, ethically, precisely and amazingly to achieve our vision of a world where best practices are widely disseminated, accessible, affordable, known and used.

Faton Aliu
President and COO at PECB

PECB *Insights*

ISSUE 02 / JULY **2016**

CONTENT

WHY CHOOSE A THIRD PARTY CERTIFICATION BODY?

You have probably been wondering if your company is doing things right. Questions which imply insecurities regarding the company's performance in the market have surely been asked many times among the workers such as: Are we keeping proper record of processes within the company? Are we tackling problems efficiently? Is what we do in proportion with what we are supposed to do? Is the company well organized? These might be some of the most frequent topics internally. So, what should be done in order to eliminate these issues? It is highly important and recommended to hire a professional authority which is independent and also able to complete the process based on the experience and certain codes of conduct. That authority is a third party audit certification body. But, before doing so, choose wisely!

There are various third party audit companies in the market, but do they all have the set of values that are right for your organization? Choosing the right certification body to conduct third party audit is essential for your organization's success. It not only provides your company an advantage in the marketplace, but also helps add value to the way processes are conducted. Moreover, quality and success are not only comprised of dedication and perseverance, but also recognition. This recognition is granted by a professional and experienced certification body.

Receiving internationally recognized certificate with globally known certification body establishes your organization as an adaptive and flexible company that is in pace with global best practices and regulatory frameworks. At the same time, embedding trust in your customers' perception of the product and services your organization offers. Placing your organization with a trusted and valuable certificate will have a multifaceted impact on your business, ultimately cascading to an increase in market share and recognition.

Prove your organization's credibility and integrity with PECB certificate because recognition matters!

ISO COMPLIANCE, CERTIFICATION, AND ACCREDITATION EXPLAINED

The International Organization for Standardization (ISO) produces thousands of standards every year covering multiple topics and disciplines. A certain group of those standards known as management system standards are designed to support organizations in delivering products and services which are higher in quality, safer, more secure, more resilient, and environmentally friendly.

These standards are well known such as ISO 9001 (Quality Management), ISO 27001 (Information Security), ISO 14001 (Environmental), ISO 22301 (Business Continuity) and the soon to be launched ISO 45001 (Health and Safety).

Some organizations are required to implement these standards and some others to demonstrate their compliance to them. Within the industry, there is a lot of "noise" about compliance, certification and accreditation, and the difference between these terms. So what do they actually indicate in reality?

COMPLIANCE

Any organization can choose to implement a management system standard and use the standard to drive improvement and manage risk. They can choose to meet the requirements and perform internal audits as part of their overall management system. When an organization implements such standards there are no mandatory requirements (demanded by the standards themselves) to undergo an external audit. Essentially, any organization can implement the standard and claim to be compliant. Customers of such organizations may ask that their suppliers meet certain standards and in some cases suppliers may simply state that they are compliant, however, some customers may go one step further and ask for evidence or choose to audit their supplier. For organizations with multiple customers, this could certainly be a large burden having to handle multiple customer audits through the year. This costs time, resources, and often coinage to produce the same evidence time after time.

CERTIFICATION

Certification to ISO standards for an organization is simply a way of proving that an organization does indeed comply with the relevant standard(s). It does not involve implementing extra requirements or controls, and if an organization has already become truly compliant, certification should be a simple next step.

Certification involves an audit being performed by an independent organization known as a certification body. A certification body will usually perform an audit over two stages. Stage one is a high level review of the management system, whereas stage two is used to look at the management system in much closer details to provide evidence of compliance in various areas.

A good certification body and their auditors will approach the audit from a positive perspective, attempting to find evidence of conformity and are not in the business looking to "catch people out" or to deceive people. In the event that non-conformities are found (by failing to fulfil requirements of the standard), then agreements can be made on how this will be addressed, which in some cases may need a re-visit and in others it may be acceptable to correct the non-conformity over a longer period of time.

If an organization meets the requirements and is recommended for certification, then the certification is awarded for a period of three years. During that time the organization must undergo annual surveillance audits. Surveillance audits are much smaller than the original audit and are designed to check whether the organization is maintaining and improving its management system.

WHAT ARE THE BENEFITS OF BEING CERTIFIED?

If an organization has taken the time to become compliant, then getting certified can have the following benefits:

- The organization can easily prove compliance to customers and interested parties
- The organization is independently recognized for its efforts
- The level of auditing from customers can often be significantly reduced as independent certification can increase assurance
- Many organizations are now demanding that their suppliers are certified to ISO standards

HOW DO WE CHOOSE A GOOD CERTIFICATION BODY?

There are many factors to take into consideration, but first we should describe an important matter. There are no rules or laws preventing anyone from setting up a company and calling it a "certification body" and awarding certificates. So how can we be sure that a certification that has been awarded by a "certification body" is credible and reliable?

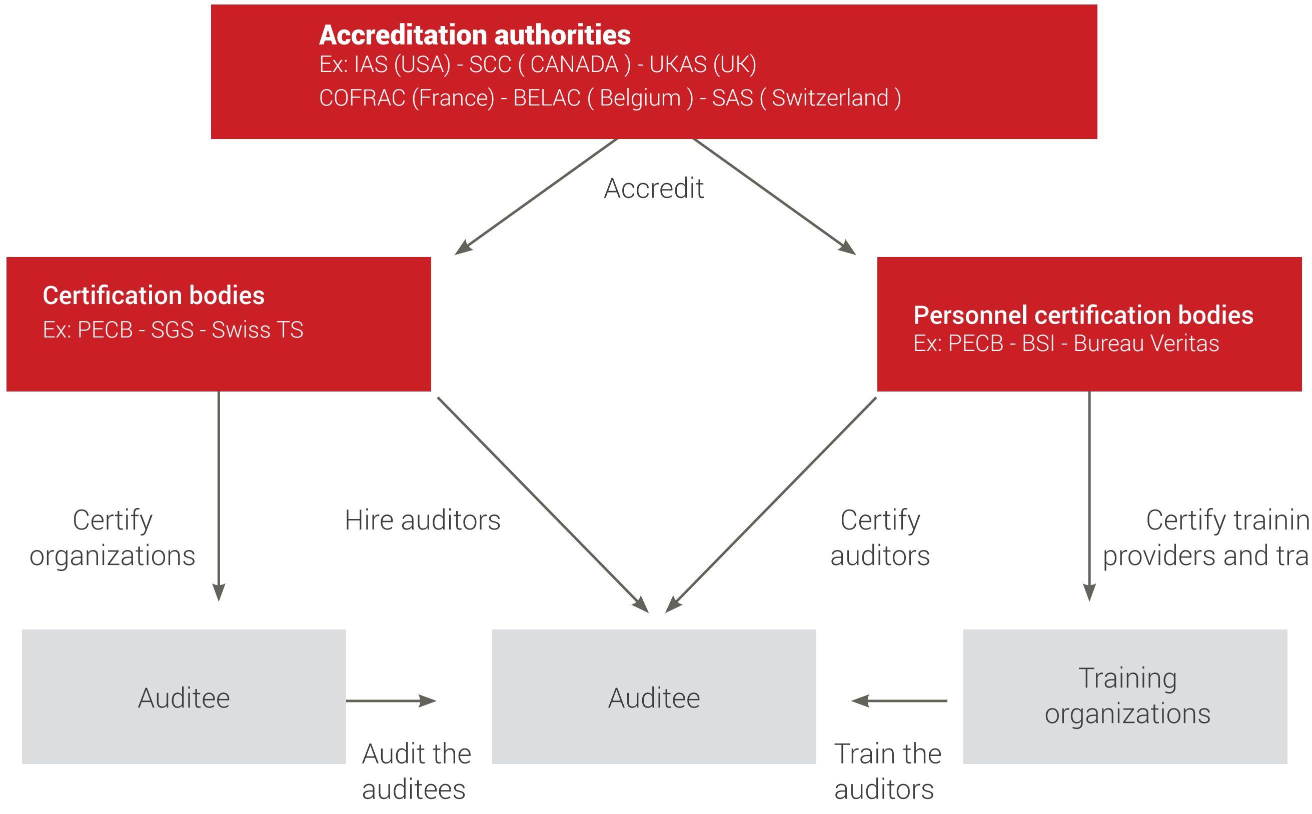
One response is accreditation. In order to demonstrate that their certification processes are fair, credible, and trustworthy, certification bodies should follow a standard known as ISO 17201. ISO 17021 lays out how a certification body should operate in order to provide confidence in the certifications they award.

When a certification body is compliant to ISO 17021, they can be audited and accredited by an accreditation authority. Most countries around the globe have a national accreditation authority (sometimes more than one) which accredits certification bodies. These bodies are all members of the International Accreditation Forum (IAF).

So when selecting a certification body, always check whether they are accredited by a member of the IAF. There are some "certification bodies" which are not accredited or are accredited by organizations which are not members of the IAF. This does not by default mean that their service is poor, however it is much harder to prove creditability without such recognition.

The following graphic shows the role of accreditation authorities and certification bodies:

CERTIFICATION SCHEMA



Accreditation authorities
Ex: IAS (USA) - SCC (CANADA) - UKAS (UK)
COFRAC (France) - BELAC (Belgium) - SAS (Switzerland)

Accredit

Certification bodies
Ex: PECB - SGS - Swiss TS

Personnel certification bodies
Ex: PECB - BSI - Bureau Veritas

Certify organizations

Hire auditors

Certify auditors

Certify training providers and trainers

Auditee

Audit the auditees

Auditee

Train the auditors

Training organizations

DOES MY CERTIFICATION BODY HAVE TO BE ACCREDITED BY THE ACCREDITATION AUTHORITY IN MY COUNTRY?

The IAF has a simple motto “one accreditation international recognition”. Some certification bodies such as PECB work globally and undergoing accreditation audits in every single country in which they operate in would not make sense. So all IAF members recognize each other. Indeed, it is a requirement for accreditation authorities to do so “Accreditation body members must declare their common intention to join the IAF Multilateral Recognition Agreement (MLA) recognising the equivalence of other members’ accreditations to their own.”

So as long as your certification body is accredited by a member of the IAF then this is the major point.

WHAT ELSE TO LOOK FOR?

Other factors in selecting a certification body would include, their credibility, their geographic presence, the price (of course) their knowledge of your industry and competence of their auditors. The latter is extremely important. Ensuring the audit team has the right skills, experience, and knowledge is fundamental to have a positive audit experience.

That is why we at PECB are continually involved in educating and certifying individuals and companies against ISO standards, as a way to show their commitment towards excellence, credibility, and international recognition. For more, please visit www.pecb.com.

About the **Author**

Graeme Parker is an experienced professional in Cyber Security, Business Continuity, Risk Management and Governance fields with proven experience in implementing and developing effective management systems against various ISO standards. He is the Managing Director of Parker Solutions Group, the PECB representative in the United Kingdom.

If you have any questions, please contact him at:
graeme@parkersolutionsgroup.co.uk

PECB ACCREDITATION

PECB is accredited by the International Accreditation Service (IAS) under three standards, which proves PECB’s commitment in delivering high-class and recognized services worldwide.

ISO/IEC 17024

PECB is a Personnel Certification Body accredited by the International Accreditation Service (IAS) under ISO/IEC 17024 – Requirements for bodies operating certification of persons

ISO/IEC 17021

PECB is a Management System Certification Body accredited by the International Accreditation Service (IAS) under ISO/IEC 17021 – Requirements for bodies providing audit and certification of management systems

ISO/IEC 17065

PECB is a Product Certification Agency accredited by the International Accreditation Service (IAS) under ISO/IEC 17065 – Requirements for bodies certifying products, processes and services

LEAN SIX SIGMA IS A BUSINESS MUST

Six Sigma is a methodology that can be implemented by all companies and business professionals. You don't have to be a math whiz or an operational genius to be able to implement Six Sigma tools and techniques into your management system processes. Quality is an essential characteristic for industries and organizations to observe, study, and understand. Process improvements frequently begin at an analysis of the level of quality in a system or organization. For organizations that deal with products and services to customers, a system within a company is a procedure that produces, maintains, or chains a product or facility.

The goal of Six Sigma and Lean Six Sigma is to eliminate waste and construct a more efficient system without negatively affecting the quality in the end product. However, lean six sigma methodology believes that the waste produced is created from certain redundant procedures in the process that do not add value to the finished product. Therefore, the main feature that lean six sigma ensures is to deliver value to customers.

An organization is most keen in using a business approach that enables them to satisfy their customers while providing more products or services with fewer resources. The lean approach helps the company understand what important attributes in their operations are key or necessary when producing a product or providing a service. The lean approach focuses on the processes within the operation that only add value and eliminates the processes that do not such as waste, inventory and defects.

Once these unnecessary processes have been defined, then the resources can be allocated to other necessary processes within the operation leading to faster production and delivery, leaving you with a more satisfied customer. Waste is anything that customers don't want to pay for. Lean means that we want to cut out the fat of our processes.

Also, once you embed a lean culture within the company, it automatically leads you to further understand what attributes are required to add value to your finished product, which inevitably lead the organization to ask the question "what" is it that my customer wants and expect from my product or service. This mind set will then allow room for the answer to the problem to arise as to "what" will add value to my product and "why" it hasn't added-value until now.

The "why" is a very important question when applying lean six sigma to the processes because it will lead to understand which redundant processes are being done but not adding value to the finished product. In other words, this proven approach provides you with a framework as to what our customer wants, leaving you with a satisfied customer. Once a customer expectations of a product or service is meet, then that customer is more than likely to become a loyal customer, and retained customer is a benefit of Six Sigma.

NUMBERS MATTER!

According to Aberdeen Group Lean six sigma bench mark report, six sigma essentials produce 40% more savings than those with less rigorous programs, and produce 65% higher project savings. This study states that 95% of all time spent on a process is waste, just 5% of the time you spend on a process is adding value for the customer. Including the time spent on essential tasks that do not add value, including compliance and regulatory requirements.

According to Villanova University, hospitals in the United States perform 48 surgeries each year nationally, smartphone producers sell 487,700,000 smartphones globally and internet cloud service on average operates 99.9% success with six sigma. In addition, Manufacturing Weekly conveys that 70% of companies that manufacture in the U.S. utilize Lean manufacturing practices. Shmula.com goes on saying that process improvement strategies like Lean saved Fortune 500 companies nearly 500 billion dollars in 2009.

METHODOLOGY OF SIX SIGMA

A proven method used by different sort of organization regarding the Six Sigma method is the DMAIC method.

Phase I. Definition - This really helps to interconnect with clientele, workers and shareholders, and other interested parties. The determination of this stage is to:

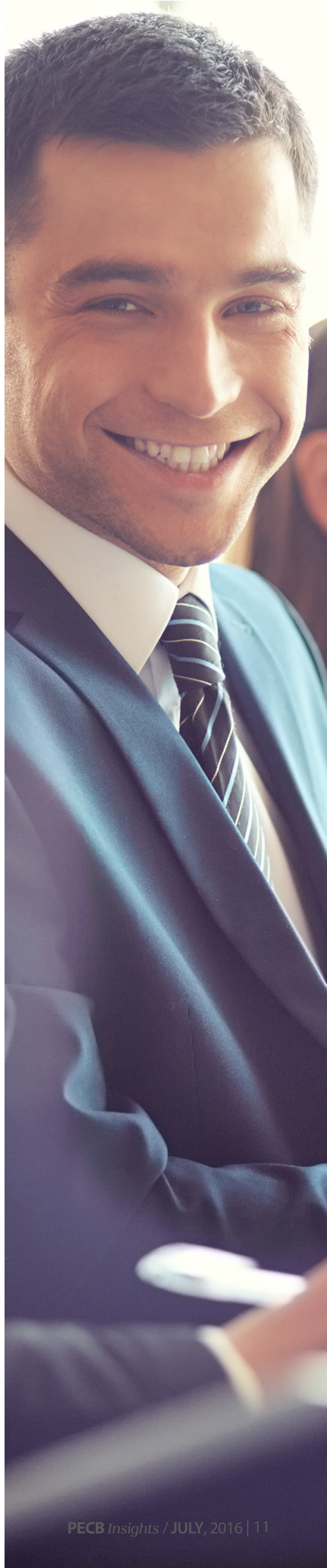
1. take into account the best of the problematic under study work,
2. determine the efforts, and yield and control numerous procedures,
3. responsibilities determination, and the steps of labor and objectives, and milestones for continuation,
4. select team gear,
5. understand the expected benefits of the project (the advantages of the project).

Phase II. Measurement - This stage includes measuring true facts that are dependable to help control the targets that have been formerly clear in the first stage.

Phase III. Analyze - Successful strategy analysis at this stage provides different sorts of statistical methods, and some of the gears that separate important info to clarify the prevailing defects in the services or required domain.

Phase IV. Improve - This stage shelters the design of Six Sigma from start to finish and services for Six Sigma. At this stage, a vital role is the effort to link the crack between the situation of the targeted operations and the current situation.

Phase V. Control - At this stage, it ensures a fruitful plan not to repeat the errors and defects through continuous surveillance, and to lay the fundamentals to confirm the effort by the unification of the new approach.



BENEFITS OF SIX SIGMA TRAINING & IMPLEMENTATION

Decrease cost/increase revenue	Detects processes of over-production leading to waste, inventory and defects. Less rework meaning more time is used efficiently in other areas of the operation to enhance the quality of the end product. I.e. increasing the features and benefits of a product or service with the remaining resources and time.
Effective employees and efficient time management	Employees develop efficient time management skills and understand all current operational process. Use developed skills to identify waste within processes. Employees working together to meet the mission and vision. Sense of belonging brings employee motivation.
Retains customers	Allocate resources to other areas of the operation getting processes done faster, leading to faster delivery time and satisfied customers. Minimizing defects and attaining loyal customers
Develops Strategic planning	Systematic problem solving Detects optimization risks
Enhances supply chain management	Integrates suppliers into the continuous improvement process initiatives. During the ongoing process, suppliers must reduce the waste and variation in their processes to eliminate any extra inventory to defects they may be bringing. Competitive advantage.
Continuous improvement	Embedding a cultural commitment to continuous improvement. Focusing on customer satisfying-not only for short-term but long-term customer focus through the optimization of evidence, material flow and processes.

SIX SIGMA BELTS

Black Belt Proves that your skills are advanced with team leader expert skills, analysist skills, and advanced project manager skills.	**Master Black Belt** Proves that your skills are highly advanced and have been tested with the experience to be a leader in training and coaching.

White Belt For beginners to understand the fundamentals, processes for improvements spoken, but not used in practice yet.	**Yellow Belt** For advanced beginners who have contributed to the Lean Six Sigma projects and management.	**Green Belt** Proves that you are a vital member of the Lean Six Sigma project team.

An organization using the Lean Six Sigma techniques have benefited in the long-run as mentioned above, however when acquiring yourself with a black belt reveals the capabilities you carry to be able to conduct projects and implement improvements for the organization. On that note no matter the project undertaken, it needs organizational support to succeed to the fullest potential. With the right individuals, the project is ensured to succeed and add value to align the organizations mission and vision.

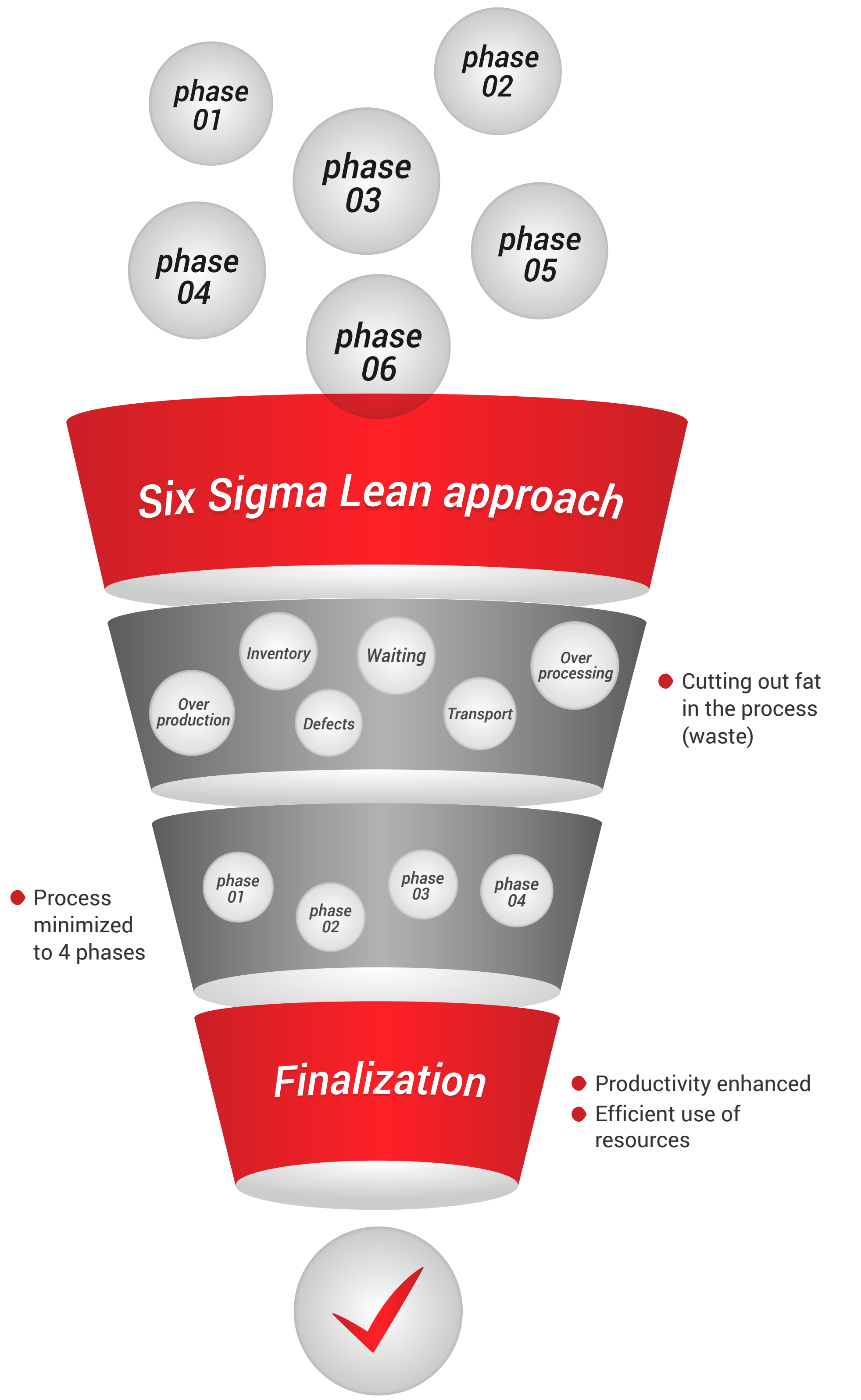
Here at PECB, we are highly focused in process improvement and pay high attention to six sigma methodologies to influence organizations and individuals reduce waste and increase revenue. PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including Six Sigma training courses and other services.

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.

Mohammad Youssef Khan is a PECB Certified Trainer and Executive Consultant & Trainer at Six Sigma Associates - SSA. He is an accomplished expert with over 10 years' experience in the field of project and program management, business process analysis and design, as well as operational and organizational excellence. If you have any questions, please do not hesitate to contact: 6sigmapk@gmail.com.

WHY CONSIDER SIX SIGMA?



- Cutting out fat in the process (waste)
- Process minimized to 4 phases
- Productivity enhanced
- Efficient use of resources

- Six sigma essentials produce **40%** more savings than those with less rigorous programs
- **65%** higher project savings
- **95%** of all time spent on a process is waste
- **5%** of the time you spend on a process is adding value for the customer
- **70%** of companies that manufacture in the U.S. utilize Lean manufacturing practices
- Lean saved Fortune 500 companies nearly **USD 500** billion in 2009

RISK APPETITE
THE CORNERSTONE OF
ENTERPRISE RISK MANAGEMENT

Enterprise risk management has become a crucial component of contemporary corporate governance and is an evolving discipline that has been supported and promoted throughout years.

While an expanding list of companies has become identified with failure to anticipate and manage risks within their organizations, the changing competitive environments push companies to take risk in order to optimize their profit. It is impossible making profit without taking any risk. And yet, taking such risks without being able to manage them can guide towards collapse. While conducting proper oversight, top management along with the board amust tackle the challenge to define how much risk is acceptable in following their objectives. The key enabler is to understand the level of risk they are willing to accept.

Risk appetite is an essential business concept that makes a significant distinction to how organizations are governed. Risk appetite is the amount of risk which the company is willing to accept. It is a key enabling structure and active relation among risk management, strategy and target setting. Every organization follows different aims to add value, and should generally recognize the acceptable level of risk in doing so.
External stakeholders and different divisions of the organization usually have different perceptions. Lot of organizations consider risk appetite as the focus of appealing theoretical discussions regarding risk, but do not successfully incorporate the theory into their daily activities or day-to-day decision making process. Once a board identifies a strategy, it should decide whether it supports the level of risk appetite.

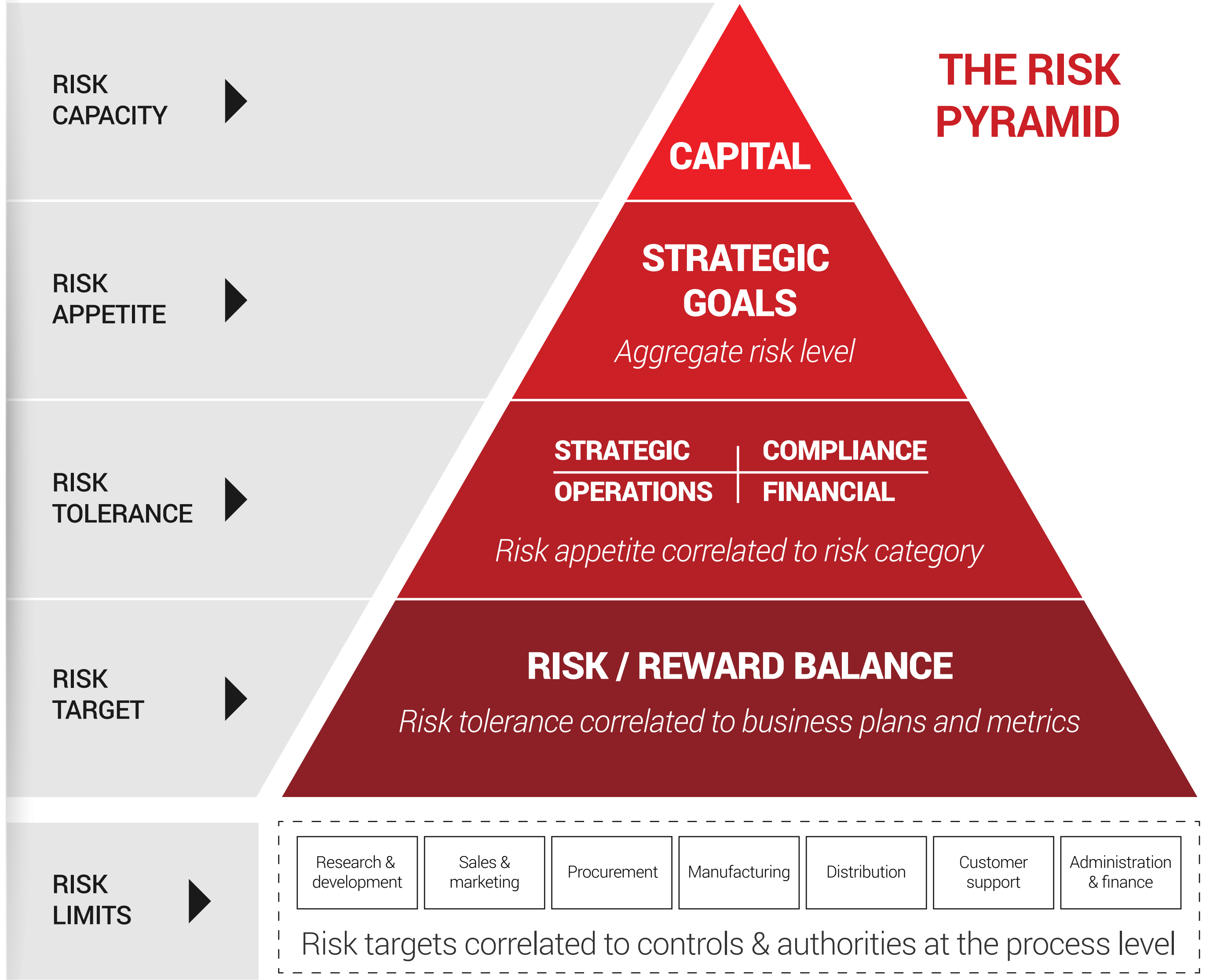
Consequently, an organization must recognize risk appetite along with operational strategies or objectives. Thus, management must pursue three main steps:

1. Develop risk appetite
2. Communicate risk appetite
3. Monitor and update risk appetite

Most importantly, communicating risk appetite correctly leads the organization towards considerable benefits. Those benefits encompass:

1. Transparency over the risks
2. Fundamentals for reliable communication to different stakeholders
3. Reduces cost of capital
4. Competitive advantage

Other benefits include more precise financial reporting, superior marketplace presence, enhancement of both perception of the organization and political and community support. The best approach to initiate risk appetite definition is the top-down approach.



The maximum amount of risk in an organization is known as risk capacity. The amount of risk must be taken by the company in order to achieve its financial goals. Unlike risk capacity, risk tolerance is the specific amount of risk an organization is willing to take in regards with a specific category of risks. Categories of risk include strategic, operational, financial, compliance and reputational risks.

Furthermore, a risk target is the most advantageous level of risk that an organization wants to acquire to achieve defined business objectives. And finally, risk limits are used to guarantee the real levels of risk that will settle within the agreed-upon risk tolerances. Breaking risk limits will usually act as a trigger for remedial action at the process level. Enterprise risk management allows management to successfully deal with related risk and uncertainty, boosting the ability to build value. Additionally, ERM can provide practical assurance that management is informed of the degree to which the body is moving toward accomplishment of the goals.

Enterprise risk management consists of eight interconnected

elements: Internal and External Environment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Information, Communication and Monitoring. ERM is not firmly a consecutive process, it is a multidirectional process in which nearly any element can and does influence another.

With all above in place, a useful and proven scheme for effectively managing many risks may be applied to streamline risk management and align it to best practices. Such a solution involves adopting an internationally recognized standard such as ISO 31000, which drives the most relevant best-practice from organizations worldwide and tailored to reduce or eliminate bias. ISO 31000 explains the mechanism of risk management implementation. It provides principles; a framework and a process to implement a risk management suite. Moreover, with due cognizance of its own internal and external contexts, an organization must recognize the applicable and relevant obligations and should put into practice a system of controls to attain compliance. Additionally, ISO 31000 distinguishes the significance of feedback by means of two mechanisms: "communicating and consulting" and the "monitoring and reviewing" of performance. Communicating and consulting ensure the engagement of relevant internal and external stakeholders while monitoring and reviewing guarantee that the organization observes risk performance, thereby gaining knowledge from experience and practices.

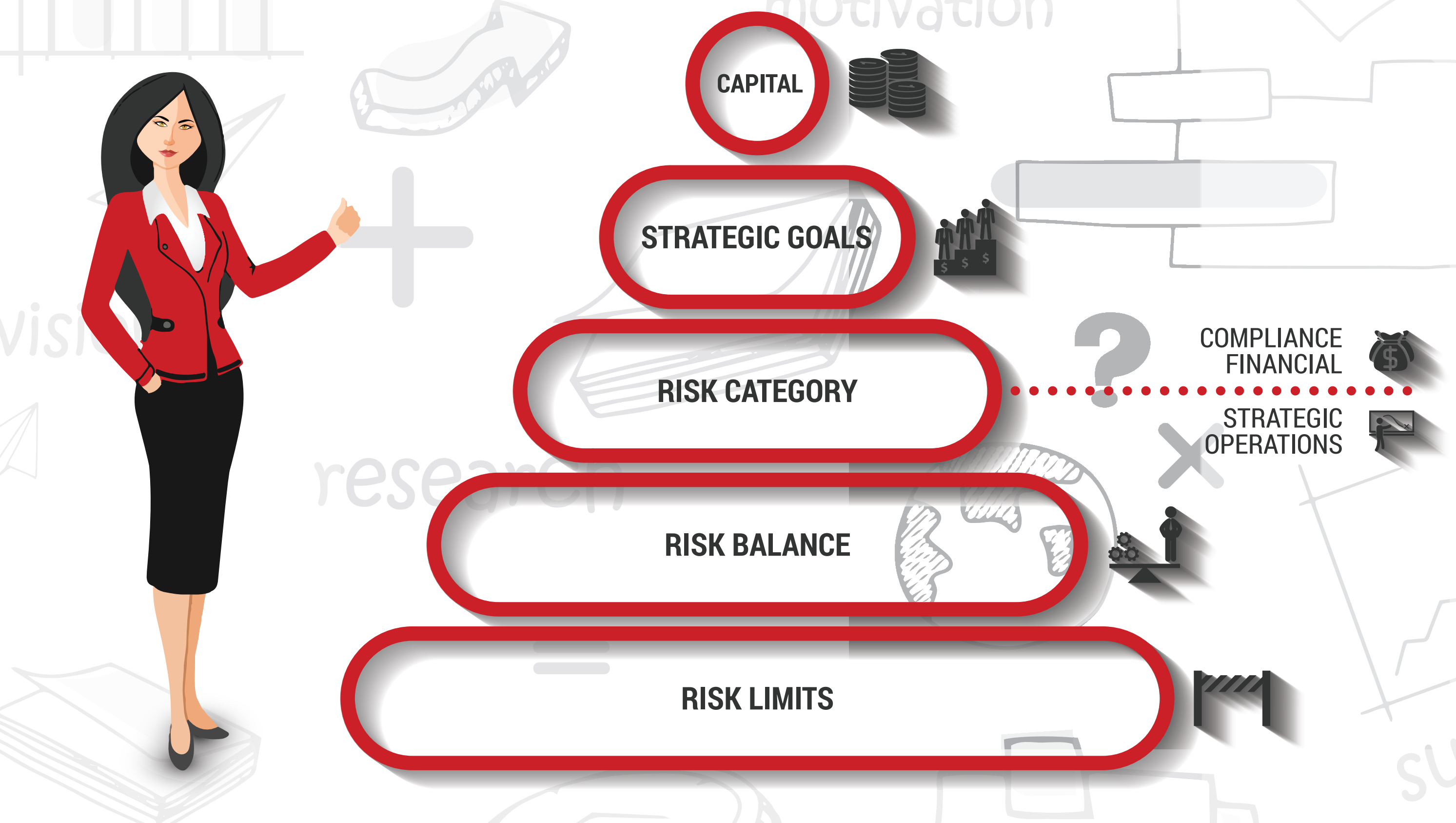
PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO 31000 Lead Risk Manager Course.

About the author:

Alba Keqa is a Portfolio Marketing 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.

Contributor:

David Lannoy is a Senior Enterprise Risk Manager in a global telecommunication company and has vast experience in Risk Management gained over 15 years working in various sectors including transport and finance. He is a regular guest lecturer and master thesis supervisor in well ranked Business Schools. Due to this valuable experience and academic track record, he has been able to join The Institute of Risk Management in London as a Specialist Member and has also become Certified ISO 31000 Risk Professional and Certified PECB Trainer.



DETERMINING RISK PYRAMID IS ALL WE NEED

7 Reasons to Adopt ISO 26000

In recent years, organizations around the world are becoming increasingly aware of a clear need to demonstrate practices of socially responsible behavior. The objective of the 'organizational social responsibility' concept is to contribute to sustainable development, through transparency and ethical performance.

To assist organizations of all types and sizes in addressing their SR, the International Organization for Standardization has published first global standard on Corporate Social Responsibility, ISO 26000.
It is a voluntary guidance document that offers suggestions, advices, proposals, and recommendations of social responsibility. It helps promote credible reporting, company's accountability and it improves market performance.

7 CORES OF ISO 26000

ISO 26000 is based on seven principles, seven core subjects of social responsibility defined in the standards. The organization must identify the significant issues for them to address. It is done in a prioritized manner, through involvement and dialogue with stakeholders.

ISO 26000 seven core subjects are:

- Organizational governance
- Human rights
- Labor practices
- The environment
- Fair operating practices
- Consumer issues
- Community involvement and development

1 **Organizational Governance**
Refers to how your business makes and implements strategic decisions, to achieve its objectives. Your decision-making processes should be structured so that the principles of social responsibility can be applied.

2 **Human Rights**
Human rights are basic rights to which all humans are entitled. Businesses are to respect and support human rights within their own operations and by collaborating with stakeholders.

3 **Labor Practices**
Labor practices in an organization must be in accordance with all policies, and actions related to the working conditions by the organization and developed on its behalf, including subcontracted work. Labor practices include health and safety of workers, hiring, promotion, training and skill development, etc.

4 **The Environment**
Consequences of any decision and action taken by an organization will impact the environment. This is associated with the use of resources, the location of activities, waste, and pollution. Organizations must take a closer look when approaching an environmental direct and indirect impact, in order to minimize any negative outcomes.

5 **Operating Practices**
This core refers to the ethical conduct, practicing accountability and fairness when doing business with others, including organization's stakeholders and suppliers. Addressing issues such as anti-corruption, respecting the law, and promoting social responsibility through the business chain are few of the important ISO 26000 themes.

6 **Consumer Issues**
Organizations must be transparent to their customer about their services and products. Customers must be given the necessary information regarding the product and service provided by any organization. Fair marketing, consumer service, support, data protection and privacy are issues that establish a credible image of the organization.

7 **Community Involvement and Development**
Organizations must acknowledge the value of communities where their business is active in. Community's involvement in the organization's practices will contribute to sustainable development. Supporting skill development programs, employment creation, and social investment will have a positive outcome on both sides.

HOW CAN YOU BENEFIT FROM THE ISO 26000?

Persons with ISO 26000 Certification will bring strategic advantage to any organization and increase competitive side of the industry. Social responsibility is a representation of a positive image and guarantee of the employees' satisfaction and customers' trust. Professionals with social responsibility certificates are a great way to attract new investors and sponsor concerned with social responsibility and sustainable development.

PECB is continuously active in assisting organizations worldwide and society as a whole to achieve best practice using standards to provide structure and focus on training and development programs. PECB offers Training and Certification services for ISO 26000:2010-Social Responsibility, which ensures that organizations will not only improve their event organization performance but also have an international impact and independently validate their commitment to their employees through certification.

For further information, please visit ISO 26000 training courses.

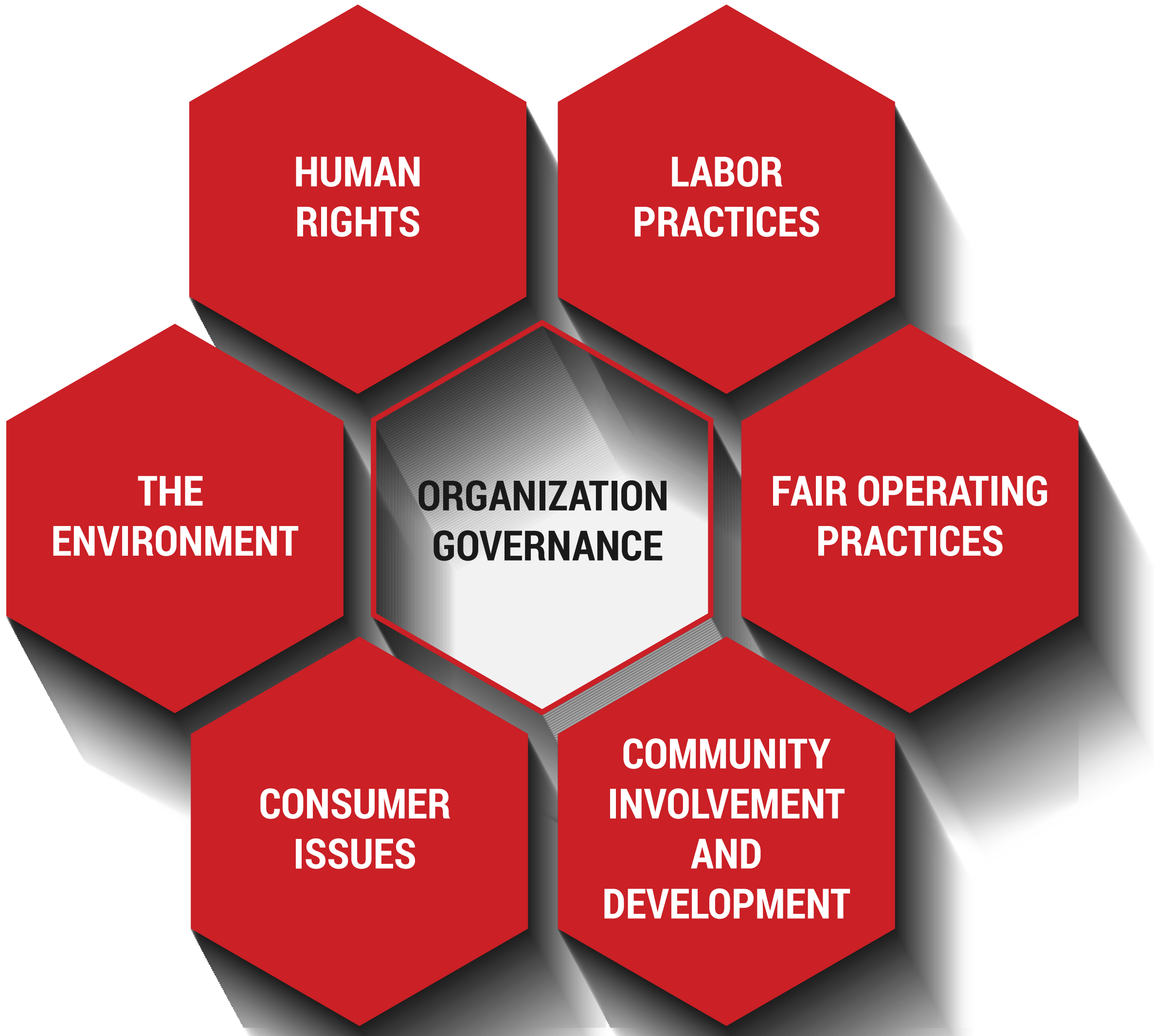
about the author

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

George Ogoti is a MSC (Chemical Engineering) holder, is an International Auditor, Trainer and Consultant on SHEQFS and other systems. He has an excellent knowledge in industry's standards having worked for over 34 years. He is also a certified auditor, trainer and implementer and has extensive coverage in Africa and Middle East. If you have any questions, please do not hesitate to contact him: ogoti@mmcafrica.com.

SEVEN REASONS TO IMPLEMENT ISO 26000



Every Corporate should have at least 10% of employees who are CSR/Sustainability Certified!

- 88% of consumers think companies should try to achieve their business goals while improving society and the environment
- 65% would seriously consider leaving their job if their company harmed the environment
- 32% would seriously consider leaving their job if their company gave no / little money to charity

Adapting ITIL and Implementing ISO/IEC 20000 for a Successful Organization/Business

In this article, you will find out why and how the combination of ISO/IEC 20000 and ITIL after being applied to your business can lead to better organizational accomplishment and set your business up for greater returns.

Nowadays, the main goal of every IT manager and CEO is getting the most effective performance possible and the maximum return on the investments of technology in the global business environment. In the economic environment, technology in business must be focused on the equal dynamics which are necessary for managing and measuring all other enterprise operation phases.

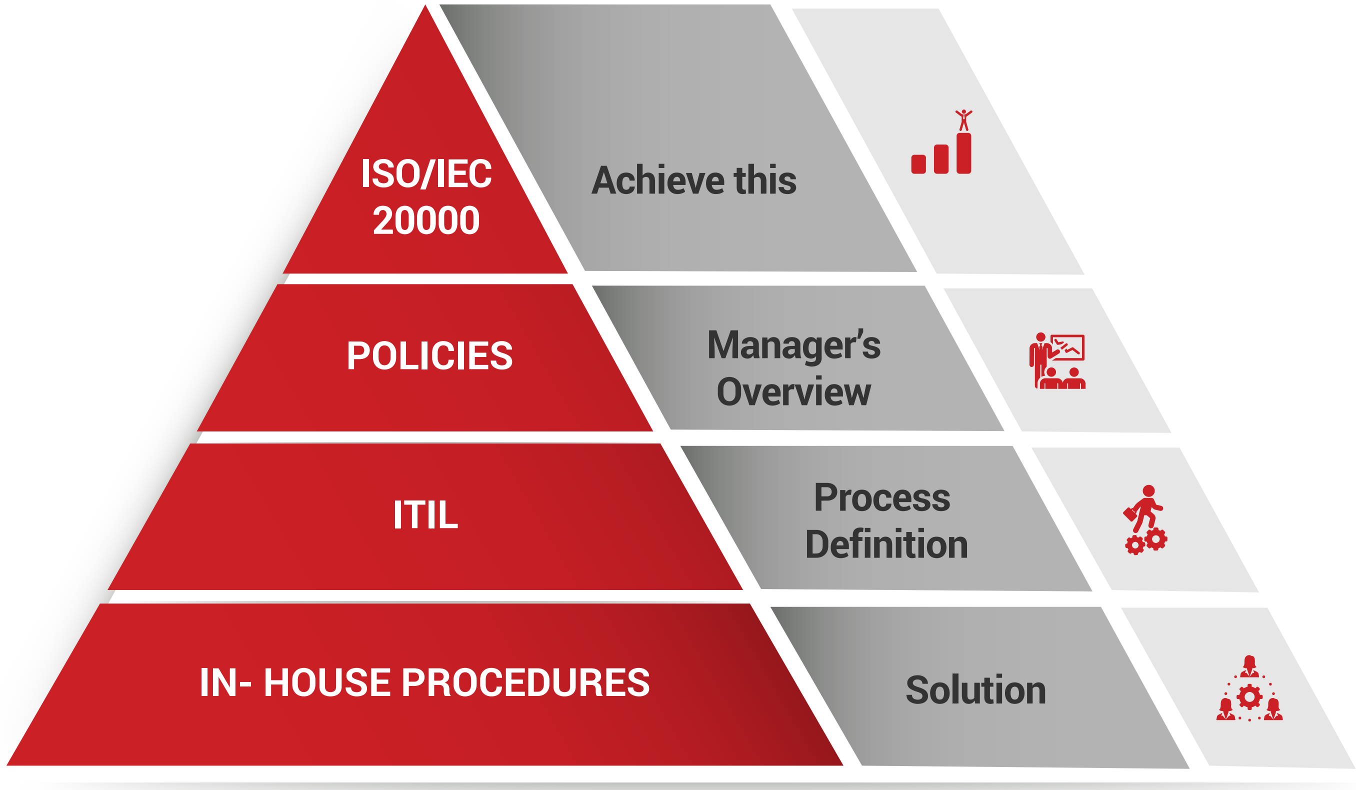
IT management requires risk management, governance, metrics, structure and regular development progress to improve performance and to be effectively combined with greater business objectives. In possible enhancements of the distribution, technology performance and management allow delivery for the business. International standards like ISO/IEC 20000 and the greatest practice frameworks like ITIL have the ability to influence companies, in order to make sure their investments of business technology provide results.

Frameworks and standards are significant tools that allow the Chief Information Officer and other IT managers to have benchmarks, make developments, and check their IT operation performances. In case of using it effectively, ITSM standards and frameworks could provide correct evaluation of what is and what is not working properly, how much IT truly costs and which bottom line price is being provided to the business. In other words, the framework of ITIL contains the best practices for running an Information Technology Service Management System (ITSM). It mainly brings business requirements and IT services into alignment. Briefly, the framework of ITIL plays the role of a guideline for organizations on how to manage their operations in IT, so it can support in a best way the business processes of companies, such as product development, finances management, customer services, research and development, etc. This means, ITIL is making smart developments to management processes of your IT service. It doesn't matter in how big organization or business you are; ITIL can support your institution by providing best practices in IT Service Management System (ITSM).

"What does ISO/IEC 20000 have that ITIL doesn't?" It is our good specification about what the service provider of IT needs to do. It defines requirements for design and transition of new or changed services, service delivery, relationship, resolution and control processes. Also, it provides general requirements for service management system. Moreover, ISO/IEC 20000 is offering improvement of the process or application of new part in a planned and convenient way. While ITIL offers assistance and recommendation that can be adapted to, ISO/IEC 20000 states the standard requirements when the organization is being measured as world class. ITIL is full of guidance on what you should do, what you can do, or what would be the best way to do it, and so on. In general, the requirements are not difficult to understand over what has to be done. Thus ITIL is not completely auditable, but in the other hand, ISO/IEC 20000 is auditable.
Unlike ITIL that is a framework for customers to adopt in their organization, certification of ISO/IEC 20000 is something that must be obtained. It is a certification awarded to organizations that have been able to fulfill the requirements of the standard successfully in their IT departments; and it serves as a standard representation that the business holds for their operations in IT.

Implementing ISO/IEC 20000 /adapting ITIL could provide a great range of benefits to your business, including:

1. Higher quality of IT services
2. Increased productivity
3. Lower costs
4. Better alignment of IT services and the business it supports
5. Globally recognized Certification (ISO/IEC 20000)
6. Competent IT service management organization
7. Better-quality customer satisfaction (more professional service delivery)



RELATIONSHIP BETWEEN ITIL AND ISO/IEC 20000

Why is ISO/IEC 20000

certification so important?

This certification simply can provide a competitive edge to organizations compared to other organizations that don't have this standard. ISO/IEC 20000 is a code which gives a yardstick in order to measure and approve the success of business to adapt the finest practices as stated by ITIL. It also provides an option of measuring how well the business is going in its quest to constantly develop ITSM.

A set of management processes that are designed to assist you in sending more operative IT services is what the standard describes. So, high quality management standards of IT services are very important elements for your accomplishment, and getting the ISO/IEC 20000 certification is a way to guarantee that quality. The most important thing to know about ITIL and ISO/IEC 20000 is that they both need constant development, which may grow the competitiveness and credibility of the business.

It is known that best practices such as ITIL and ISO/IEC 20000 are recognized globally as benchmarks for process development in the department of IT Service Management. ISO/IEC 20000 is a standard with openly stated requirements that have to be met for certification when a minimum of the finest practice standards are matched. ISO/IEC 20000 is ITIL based, but ITIL is created with ISO/IEC 20000 in mind, so they both complement each other very well.

In conclusion, ISO/IEC 20000 explains what we need to do, while ITIL shows us how to do it. ISO/IEC 20000 can be used to measure and implement processes of high level, while ITIL is very useful for the details.

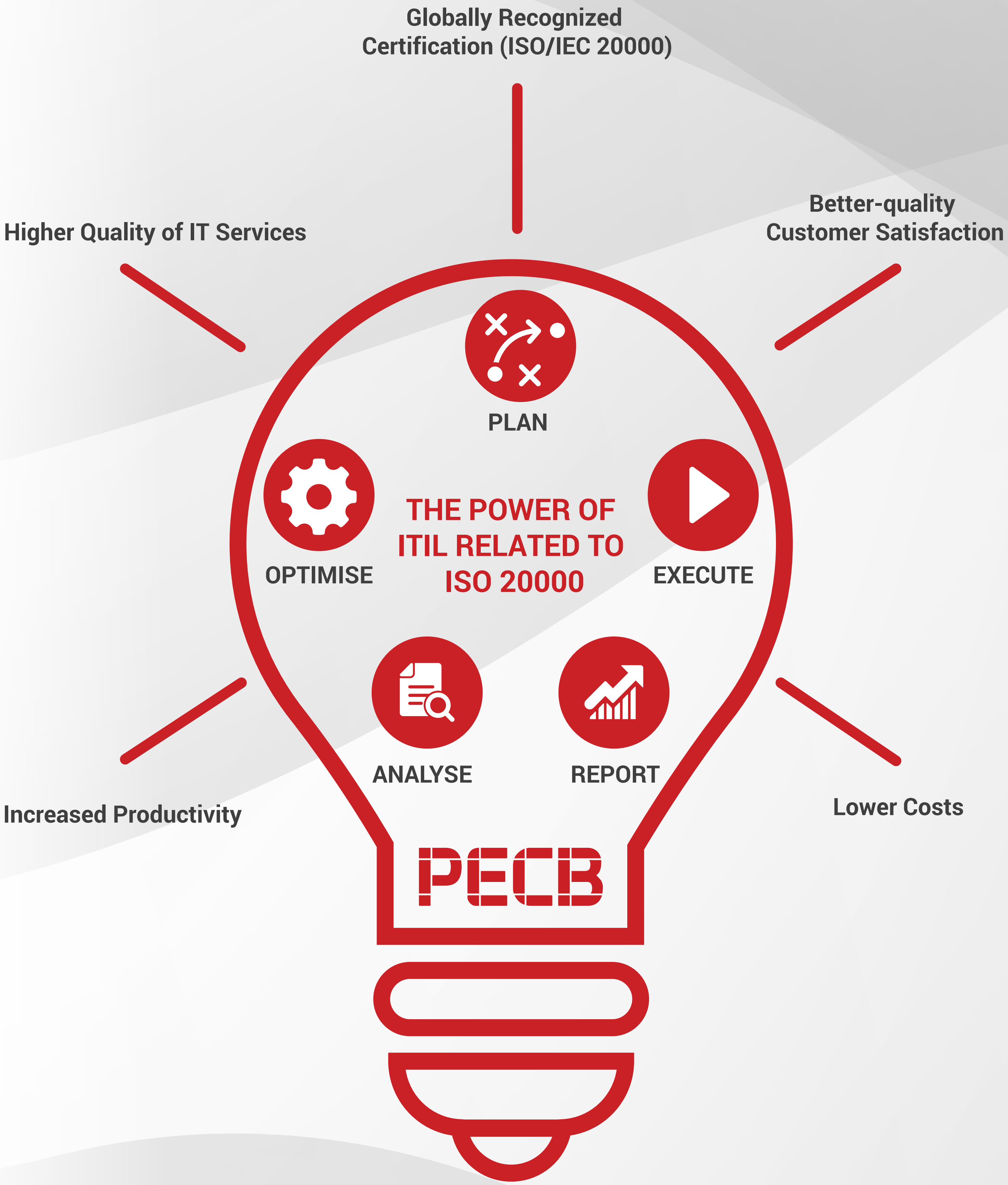
PECB is a certification body for persons on a wide range of professional standards. It offers ISO/IEC 20000 training and certification services for professionals wanting to support organizations on the implementation of these management systems. Design, delivery and improvement of services that fulfill customer requirements have become very important for IT providers.

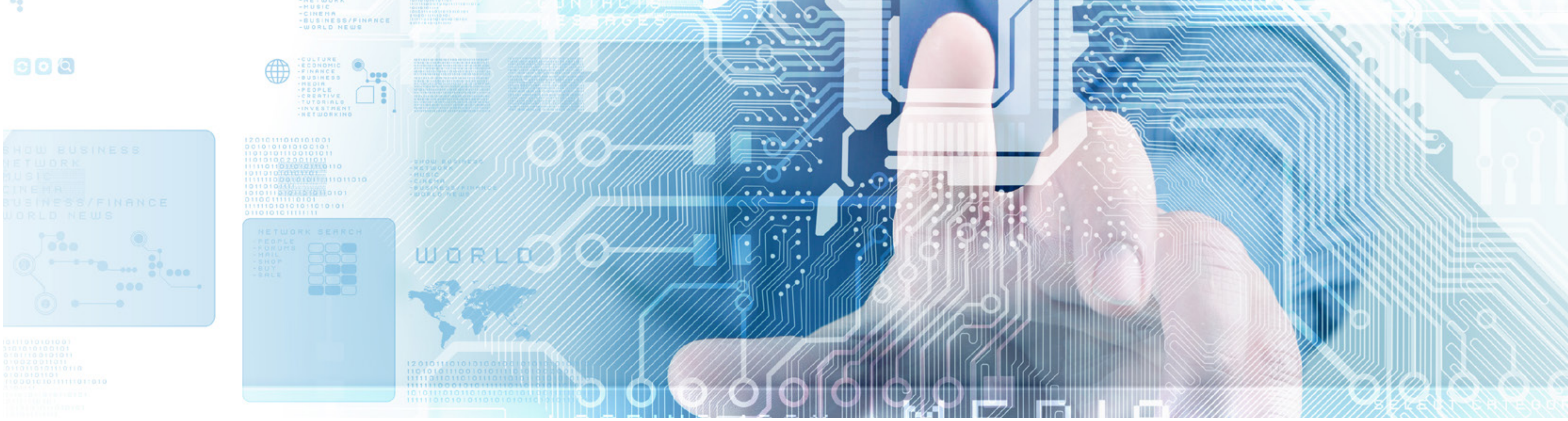
For further information, please visit: https://pecb.com/iso-iec-20000-training-courses

about the authors

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

Silvana Tomić Rotim, A Consultant and Trainer at ZIH. She is also a Certified Quality Lead Auditor, Certified IS Auditor, Certified Information Security Lead Auditor, Certified Management Consultant (CMC), Certified Management Trainer and a Certified TickIT Lead Auditor. If you have any questions, please do not hesitate to contact her: stomic@zih.hr


Globally Recognized Certification (ISO/IEC 20000)
Higher Quality of IT Services
Better-quality Customer Satisfaction
PLAN
OPTIMISE
THE POWER OF ITIL RELATED TO ISO 20000
EXECUTE
ANALYSE
REPORT
Increased Productivity
Lower Costs
PECB



BE CONSCIOUS
OF RANSOMWARE ATTACKS!

Have you ever thought about being prevented from accessing and using your own information?

Recent reports have shown that many companies and institutions pay a ransom in order to regain access to their data. Citizens all around the world could find themselves in the same kind of situation. It is widely known that attacks are not only about gaining access to information for any specific purpose, but also about limiting data usage. This is a quite sophisticated process and intruders are using it wisely.

What is RANSOMWARE?

Ransomware is a type of malware that propagates through networks and infects the computer systems with the intention to restrict data usage by encrypting files of any kind. Once the files are encrypted, it will communicate to the victims that they have to pay a ransom in order to get the password to decrypt their own files.

It is different from other attacking techniques and victims tend to cooperate with the attackers because they think that they can decrypt the files only by paying the ransom. This might make them even bigger victims as it is not guaranteed that they are going to have their data unlocked after paying the ransom. It must be also noted that in many cases, it works out just fine and after paying the ransom you will get the unlock code and you can access your data again. Oddly enough, certain attackers even establish a helpline to assist the victims on how to make the payment and decrypt the files afterwards.

Facts

Ransomware is not a selective attack only targeting corporations that are working with high volume of data. There can be different sorts of attacks. Anyone of us can be a victim of ransomware while we are surfing on the internet or trying to open an email that we did not expect (including hyperlinks or files of any kind). Concerning the latter, phishing email is one of the means to spread onto the victims' computer through malicious content within the email. With the smartphone penetration on the market, the Android devices are becoming more and more targets for such attacks.

The facts are showing that huge profit has been made from malicious activities using ransomware. They target individuals just as well as businesses. The individuals who created the ransomware usually say: 'it was never their intention to release the code and that their intention was not to have financial gains from their usage'.

Kaspersky reported that 36.232 users attacked in 2012 by some sort of ransomware, which number increased to 179.209 in 2015. This is close to a five-fold increase over a course of 4 years.

This financial 'gain' was quite incentive for intruders to try to find more sophisticated variants to reach the intended outcome. In 2013, other ways of advanced Ransomware techniques were introduced. The latest breeds of ransomwares that have been introduced are called "Locky" and "Samas". "Locky" was targeting hospitals and healthcare facilities in the United States, New Zealand and Germany. It spread widely through spam email within attachments. The same was the intention of Samas, another type of Ransomware where the whole network is targeted through scanning for possible entry points to exploit.

The Data Breach Investigation Report (DBIR, one of the largest information security investigation reports worldwide released by Verizon every year) states that ransomware became the 2nd most widespread crimeware and this type of threat is increasing exponentially.

How it can infect your system?

Any malware might seem legitimate. In case a person clicks on a link or on an attachment, a malware can start running in the background without any visible indication to the user. In case of a link, it will take the user to the destination URL that might appear as a legitimate site of one organization, whereas it is a fake site with malicious content. On such sites, the code could activate through exploiting outdated flash versions or getting the user to click on an action button to activate the code. This might not even trigger an alert even when a firewall is actively running, because this action was initiated by the user and it might seem as a legitimate action to the system. In the other case by clicking to open the attachment, the malicious code activates itself.

Either way the malware could infect the machine, even if there is a firewall and virus scanning software running on the PC, and it will start encrypting all the data on the local drives as well as all other resources attached to the same network. Users on the network are not aware that they are infected with such a malware until their access to their files and documents will be denied. They will soon receive a message that says something around: the access to the destination is impossible until you pay a ransom. The victim will be urged to arrange for the payment using bitcoins (purely electronic money), an option that is close to untraceable as a result of anonymity of the currency.

Taking measures to avoid RANSOMWARES!

Looking at the recent facts and incidents, there seems to be a strong commitment to try to find a preventive solution for ransomware threats. One of the most recent cases is the ransom that a Canadian University had to pay in the amount of 20,000$. This university paid it because they couldn`t afford to lose their credibility. At the same time, they took preventive action to avoid this happening again. These actions included user awareness training amongst their students and warn them not to click on links or file attachments that they were not expecting and they have no idea what they contain. But such incidents have also happened in Europe within some public and profit oriented organizations.

FBI and a few security agencies give recommendations on how to be aware of these threats, as follows:

- Pay more attention to security awareness sessions and trainings, relating these security issues.
- Apply security properties on the web browsers and email platform.
- Maintain direct contact with responsible persons and the department when it comes to suspicious cases.
- Implement overall business continuity plan, including scenarios for how to handle such cases.
- Take backups regularly and store it off-line (like on an external drive or USB storage). Not bringing the backup media off-line is crucial, otherwise the backup could also be compromised.

Conclusion

Every security issue is important. It would be ideal to know each fraudulent and malware techniques. Unfortunately, this is impossible as the techniques are always evolving and changing so it becomes more and more difficult to keep abreast of all kinds of threat sources.

A couple of tips beyond the above recommendations (more from individuals' point of view):

Be mindful on what you do while you use any PCs.
Be cautions when clicking on links and opening attachments (allowing macros). When you receive mails with links and files that you were not expecting, it is better to check with the sender over the phone to validate that it was she or he who really sent it.
Always open sites by typing in the link yourself in your browser.

Keep your system up-to-date with security patches (including but not limited to operating system, browsers and flashes, firewall software and office applications).

Some companies say that they have never been compromised and therefore they feel it will not happen to them. They might be wrong, because even if they have good security measures and systems in place and those are configured and operated correctly, one user insufficiently trained can still click and cause the problems with the consequences above described. So after all, unfortunately ransomware is less about the preventive security measures and more about the weakest link, the human factor when awareness gains one of the highest importance to prevent this kind of incidents.

The final piece of advice, make sure that you follow what is happening around the world concerning information security, think about how to avoid those from happening to you and your organisation, and always make sure that you have competent security professionals assisting the operations in your organisation.

PECB is entitled to deliver ISO/IEC 27001 courses and management system audit worldwide. Companies that implement an ISO/IEC 27001 framework show that they can treat better all security issues and efficiently respond to security matters. What is crucial for a company is to provide training and awareness sessions for employees so they can be well-informed regarding ransomware and other malware prevention.

About the authors:

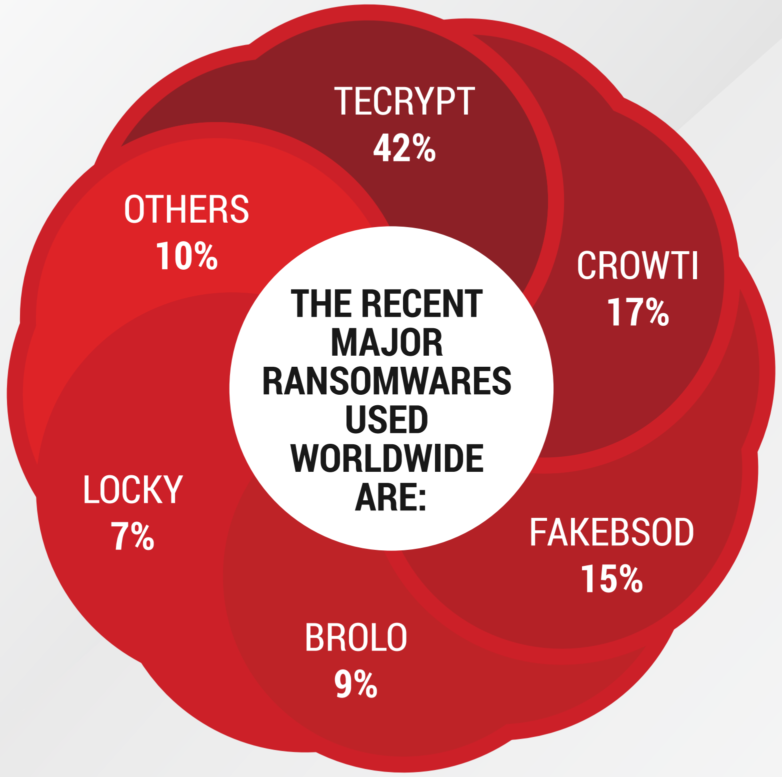
Gezim Zeneli is an Account Manager for Information Security at PECB. He is in charge of conducting market research while developing and providing information related to Information Security Standards. If you have any questions, please do not hesitate to contact: marketing.sec@pecb.com.

Gabor Egei has been working for many years as Information Security consultant, auditor and advisor. Among many certification, he holds also certification on ISO 27001, ISO 27005, CISA and CIRSC. If you have any question, you can contact Mr Egei (zoomzoomge@yahoo.co.uk) at any time.

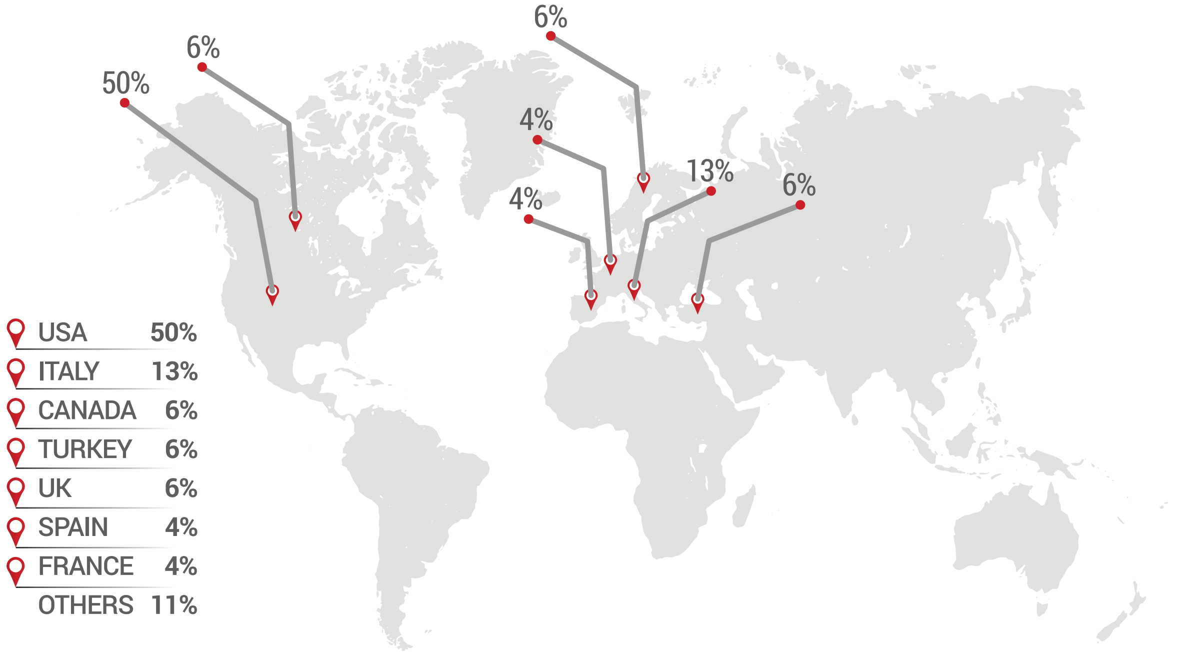
RANSOMWARE AS A VAST THREAT!

Ransomware is a malware that ceases you from accessing the data resources on your system. It holds your PC or files until you pay a ransom. It can be lock screen and encryption Ransomware.

STATISTICS FOR RANSOMWARES WORLDWIDE



MAJOR COUNTRIES THAT MOSTLY DETECTED RANSOMWARES ARE:



USA	50%
ITALY	13%
CANADA	6%
TURKEY	6%
UK	6%
SPAIN	4%
FRANCE	4%
OTHERS	11%

Source: www.microsoft.com

"EXCELLENT FIRMS DON'T BELIEVE IN EXCELLENCE - **ONLY IN CONSTANT IMPROVEMENT AND CONSTANT CHANGE."**

- Tom Peters

ISO Capsule

HOW TO BETTER INTEGRATE MANAGEMENT SYSTEMS TOGETHER FOR BUSINESS BENEFIT?

For the last 30 years, the ISO 9001, as a quality framework, has influenced the market a lot; especially in the field of the governance. It has also increased the maturity of the companies, and this influence has been derivated to other frameworks that we know at the moment, ISO 22301 for business continuity, ISO 27001 for Information Security, Environmental Management, Management of the Supply Chain, Food Safety, and Occupational Safety. Whatever standard you mention, all those are integrated more and more with each other, and this is very important to consider as it helps the industry moving forward.

It helps the industry to better improve by this integration, which means on the other side that this integration needs to get leveraged by someone for somewhat reasons. It is important to take into consideration the market that is increasing time after time; especially for the last ten years speaking about Information Security, or for the last 5 years speaking about Business Continuity. This is something that we really need to take into consideration when speaking about accompanying enterprise respecting the demand, and respecting the requirement for better governance.

Watch the Video

Pierre Dewez

CEO at PECB Europe

WHY ORGANIZATIONS FAIL TO PASS AN AUDIT?

The reasons why companies are failing audits are diverse and the ranking of the top causes might be different depending on the standards the organizations wish to be certified against. However, one of the most frequent non-conformities found across the various standards is the lack of documentation and the lack of organization of the documentation.

Watch the Video

Friedhelm Düsterhöft
Managing Director at msdd.neT

What does fall under the term documentation?

It is suggested by the ISO quality management standard to split documentation into 4 hierarchy levels, which basically differ by the abstraction level or the breadth of scope. On level 1, you will usually have global policy documents affecting the organization as a whole (describing the why); on level 2 will be procedures describing the who/what/when/where of the processes; level 3 are work instruction (the how), and level 4 are records. In ISO terminology, records are logs which contain information about the actual performance of the processes which are generated while running the processes and therefore are valuable evidence for an auditor during stage 2 of an audit to verify that the management system indeed works as designed (level 1 - 3 describe the design).

Which kind of organization might have challenges on documentation process?

Especially larger organizations may find it challenging to keep track of hundreds or even thousands of documents and having the information available promptly when it is needed. They may also think that some documentation required by the standard is superfluous and that their processes are running smoothly without it. However, missing mandatory documentation will always attract the attention of an auditor because it is often an indication that something is going wrong and sometimes even going very wrong. If some documents are deemed as mandatory by a standard, there are very good and understandable reasons why this is the case.

To address these shortcomings and to avoid failing an audit, consequently an organization should describe formal aspects of document handling, the processes and run a document management system which helps to ensure all documents are labeled, versioned and stored consistently. Last but not least, personnel should get trained on the intended way to work with the documentation.

IS TRAINING NEEDED FOR ISMS IMPLEMENTATION AND CERTIFICATION?

Haven taking part of development of international standard for almost a decade or more, I think that the toolbox presented by ISO when it comes to information security and other management systems is stronger than ever. But, however this is something which is continuously evolving, which means that for any individual or organization to make sure that they have the resources they need, with the competence they need.

They need to continuously monitor on what is happening, but also to make sure that their experts internal or external have the knowledge they seek. And one way, for making sure that they get this is to make sure that the person they take on board as consultant or as internal staff have the relevant certification. Also for, let's say internal staff to be on top of the situation, to continuously evolve with the standard is important for them to make sure that they take part of the training at hand. I would say that PECB courses are very..very well aligned with what is happening with ISO for example. I also appreciate the fact as a trainer, as a certified trainer that the courses are rather about the "how" than the "what", so to speak. If you attend the PECB course let's say Lead Auditor course, you get the toolkit you need to go out there and to successfully lead or run audits by yourself. And as for the Lead Implementer courses for example, what I know is widely appreciated by our customers, my customers and organizations.
This is the fact the people get the whole picture, they are able to run the project to set successfully and they know what pitfalls there are, and they also have the opportunity in the classes to discuss with other people in the same position about what to look for and what to avoid, so to speak. So, I think that the whole setup of PECB courses is way of addressing, both individuals, but also the organization for success when it comes both for the implementation and the maintenance of an ISMS. And definitely for organization going for certification, this is something to recommend, because it means that when they are starting out, or later on the process, they know that they have their people on board who can engage with the certification body, in a discussion on the relevant topics.

Anders Carlstedt

Managing Director at PECB Nordics

Watch the Video

PECB UNIVERSITY COMING SOON...

If you aim to advance your career, increase revenues, start your own business, or increase recognition, a graduate certificate or degree is the next step you should consider!

PECB University will soon offer awarding graduate level degrees on the fundamental and prosperous fields of:

- Business Continuity Management
- Information Security Management
- Information Technology Service Management
- Quality Management
- Risk and Management

The enrollment will begin from January 15, 2017.

Stay tuned by visiting: www.pecb.com/university and PECB Social Media

AVAILABLE COURSES

PECB Certified ISO 22301 Introduction – available in French

PECB Certified ISO/TS 16949 Lead Implementer

PECB Certified ISO 39001 Lead Auditor

PECB Certified ISO 9001 Lead Implementer – available in French

PECB Certified ISO 9001 Lead Auditor – available in French

PECB Certified ISO/IEC 27035 Lead Incident Manager – available in French

PECB Certified ISO/IEC 27001 Introduction – available in French

For more information on all PECB courses: https://www.pecb.com/training

NEW MANAGEMENT SYSTEM SCHEMAS

If your company is not yet ready for full ISO 9001, ISO 14001, ISO/IEC 27001, or ISO 22301 certification, you can consider new PECB schemas.

QME – Quality Management Essentials

EME – Environmental Management Essentials

BCE – Business Continuity Essentials

ISE – Information Security Essentials

For more information: https://www.pecb.com/management-systems

WHAT'S *HAPPENING* ON twitter

De Nijs Dirk - @DeNijsDirk

Great @PECB Partner event going on now.

Nelson Melo
@Moz_nelsonmelo

KPMG signs an agreement with @PECB for internationally accredited business courses (ISO certification) in Mozambique

Global Solutions
@GSSGhana

Improve yout riks management and become resilient to risky by attending the @PECB courses below #riskmanagement

twitter.com/pecb

Intex IT - @Intex_IT

Train your team in-house on PECB ISO27001 Lead Implementer we can deliver training at you premises #ISO27001 @PECB

ContinuityLink - @ContinuityLink

Why Choose PECB as Certification Body? Linkedin.com/pulse/why-choo.#infosec #businesscontinuity @PECB @pecb_eu

Advanced Auditing Techniques Event in Stockholm

Debra Hay Hampton

"This course and meeting these people has been life changing. I have learned so much not only from the course but from so many. I am intrigued with the doors that opened just because of being here. The caliper of people present was phenomenal.

I am in awe of "who" they are. It has been worth every penny that I spent! Speaking of spending, I am shocked by what PECB did for us to make sure the students were treated well. PECB went way beyond any expectation I've ever thought of in caring for us as students. I will always remember this."

www.pecb.com

When Standards Matter...