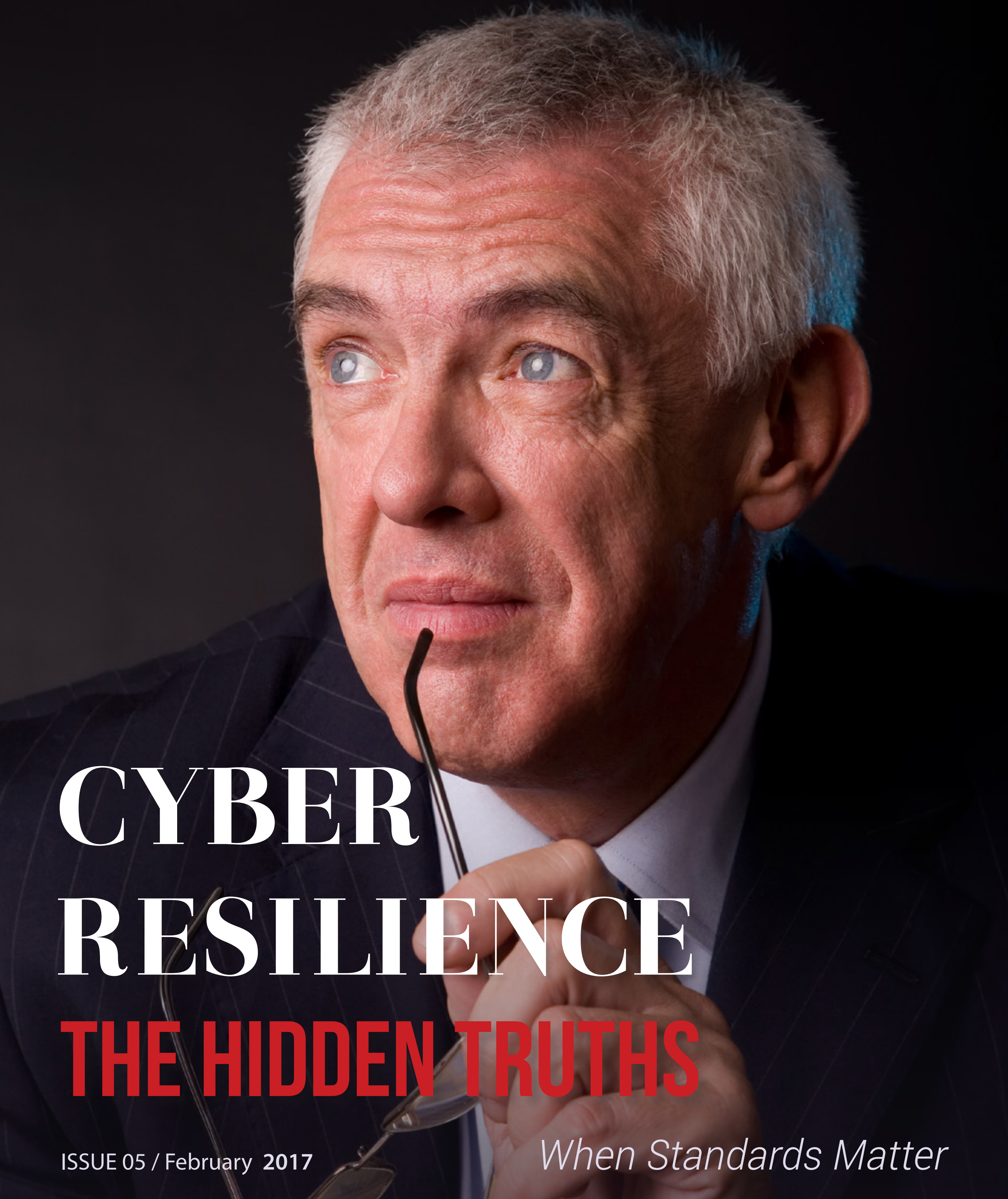
PECB *Insights*

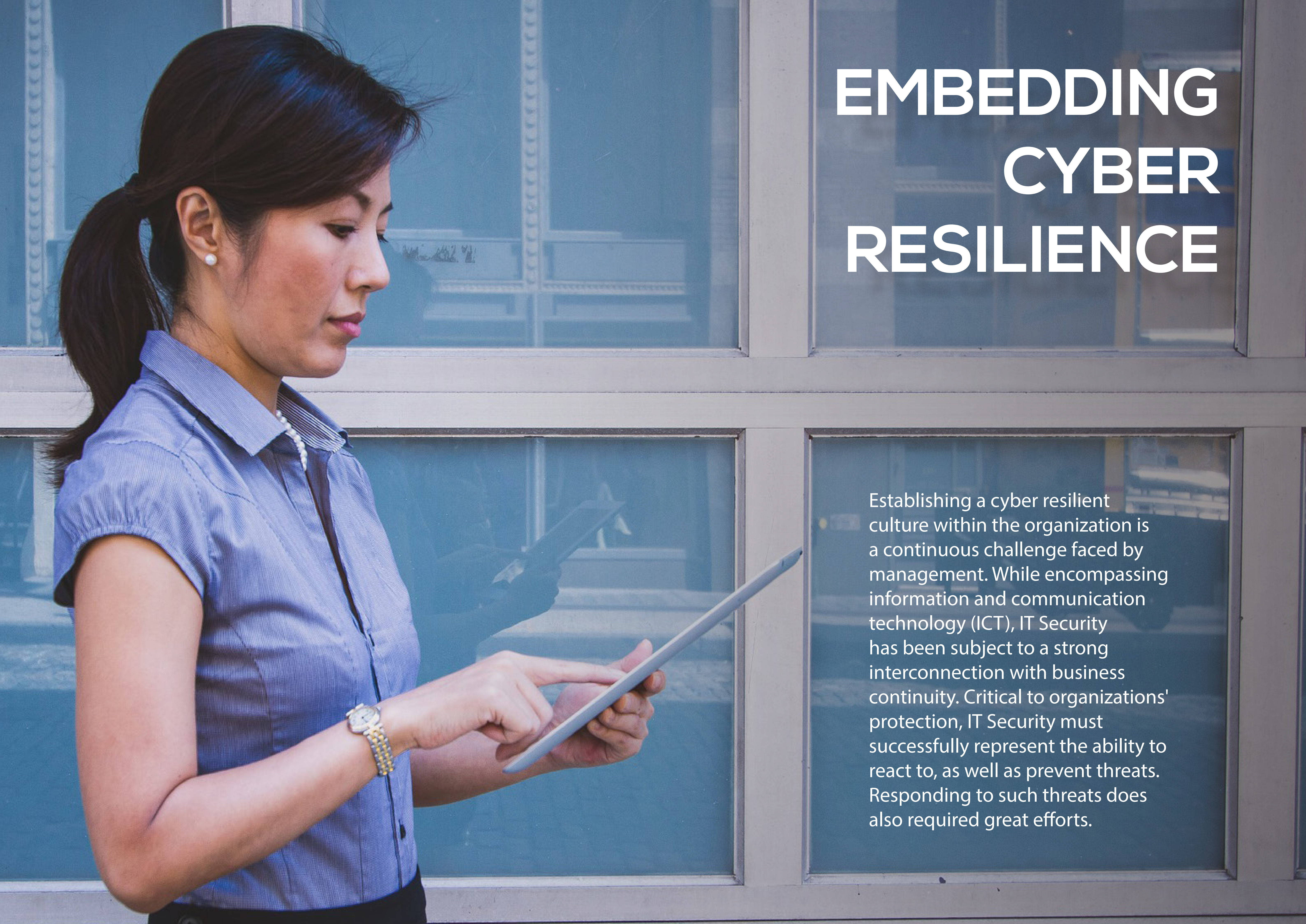


CYBER RESILIENCE

THE HIDDEN TRUTHS

ISSUE 05 / February **2017**

When Standards Matter



EMBEDDING CYBER RESILIENCE

Establishing a cyber resilient culture within the organization is a continuous challenge faced by management. While encompassing information and communication technology (ICT), IT Security has been subject to a strong interconnection with business continuity. Critical to organizations' protection, IT Security must successfully represent the ability to react to, as well as prevent threats. Responding to such threats does also required great efforts.

ARE YOU CYBER RESILIENT ENOUGH?

"THE AVERAGE ANNUAL COSTS RISING FROM CYBERATTACKS SUMS UP TO AN AVARAGE OF $20 MILLION PER ATTACK."

86% SAY THEIR CYBERSECURITY FUNCTION DOES NOT MEET THEIR ORGANIZATION'S NEEDS

57% HAVE HAD A SIGNIFICANT CYBERSECURITY INCIDENT RECENTLY

89% DO NOT EVALUATE THE FINANCIAL IMPACT OF EVERY SIGNIFICANT BREACH

49% HAVE NO IDEA WHAT THE FINANCIAL IMPACT MIGHT BE

46% WILL INCREASE SPENDING TOWARDS IT SECURITY

42% DO NOT HAVE AN AGREED COMMUNICATION STRATEGY IN CASE OF A SIGNIFICANT ATTACK

83%	81%	64%	79%
DO THEIR OWN			
THREAT INTELLIGENCE ANALYSIS	INCIDENT INVESTIGATION	PENETRATION TESTING	SELF-PHISHING

ONLY **24%** HAVE AN INCIDENT RESPONSE PLAN

Source: EY 19th GISS 2016-2017

In this Issue

6 SIGNIFICANT BUSINESS IMPACTS OF CYBER ATTACKS

1

Regulatory compliance

Recently, we have witnessed attacks in the largest organizations of the world. Following such events, there have been many regulations developed to protect customers and individuals from cyber-attacks. Due to a significant number of regulations, your organization is facing fines from 'thousands' to 'hundreds of thousands' of dollars. These fines are issued by the SEC, NFA, CFTC, and FINRA among others.

2

Public relations and Communication crisis

Disclosing the breaches exposes organizations to the media and public, while raising an enormous base of questions. Thus, it is strongly advised for your organization to have an effective strategy of communicating such unexpected events to all the stakeholders. Additionally, with a negative effect to the company's reputation, cyberattacks are a nightmare for Public Relations. Therefore, planning accordingly to crises management requires strong commitment to eliminate this negative impact.

3

Litigation and associated fees

Troubling developments for companies are, truly, the data breach settlements. The volume of lawsuits filed in the previous years has not been lower, though courts have been constantly throwing them out. Currently, we may notice an increase on the effect of customer lawsuits filed towards various organizations regarding IT Security. Simply put, compensating for a base of 1 million customers at a rate of $10 sums up to a $10 million cost for your organization.

4

Operational disruptions or destructions

Undergoing through a cyberattack will also affect your organization and employees in terms of productivity. Theft of information may jeopardize years of effort in one or another project. This is also a factor which directly affects the financial performance of your organization. Additionally, recovering from such incidents will cause loss of focus on daily and mandatory operations, to save the company while recovering the losses.

5

Loss of intellectual property (IP)

If your organization is prone to developing new technologies, this attack will definitely harm the proprietary plans in place. Additionally, information such as trade secrets or licensing agreements will be of extreme harm to the organization. Actually, many cyberattacks are initiated with the cause of intellectual property breaches due to harming the growth and innovation aspects of the organization.

6

Financial Losses

Financial losses arising from the cyberattacks on your organization's network come in both tangible and intangible forms. Regardless of the losses caused, cyber incidents directly affect the organization's performance financially; whether increasing costs, loss of market confidence, reputational damage, demoralization and jeopardy of years of efforts in various projects. As a result, the company may experience high cost of recovery and loss of previously signed project contracts.

TIPS FOR GROWING BUSINESS PARTNERSHIPS

The era we live in is truly amazing

Though, we should be aware of the impossibility for one to pursue this amusement alone. Therefore, establishing partnerships has become an important part of doing business. Seeking for mutual business opportunities, your next business partnership will curl towards innovation and value. The benefits only begin with the access to new talent and resources.

When partnering up with the right peer it is important to be attracted by the good connection and communication you have developed. At times, trusting your gut will be the drive of strategic partnerships established. However, partnering towards further business growth is mandatory to be manifested with focused objectives and a clear vision for development.

Negotiation

The process of negotiating a partner deal will make all the difference. After-all without closing the deal to a win-win situation, there will be no partnerships established. Setting a bottom line of outcomes and the least you are willing to offer, will give you the upper hand on presenting alternatives. Meanwhile, extensive care must be taken towards confidentiality of trade and other organizational secrets you may need to protect.

Networking

Being in business today means it will be unavoidable to ditch on conferences and networking events. In fact, avoiding alike social gatherings is suicidal to your organization. On the contrary, taking advantage of these occurrences will transform to an incredible social capital and open ways of working towards your vision. A great way to get the most of networking events is to attend with a mindset of not shying away of your motivation to craft new partnerships.

Communication

Pre-introduction before any networking event is an incredibly effective communication technique to get a hold of. This way you will be able to get ahead of small group meetings and ensure a one-on-one business meeting with the interested party. Focusing your attention on communicating your organizational values to the right places should be a primary objective. Regular communication is also the basis of establishing effective strategic partnerships for business growth.

PECB STANDARDS INSIGHTS CONFERENCE

Standards, Security, and Auditing

June 29th Montreal, Canada

ESTABLISHING AN EFFECTIVE **INFORMATION SECURITY POLICY**

Securing critical business information has become increasingly important for growing organizations. Information Security Policies are effective tools to communicate management's commitment and expectations from employees and stakeholders regarding security.

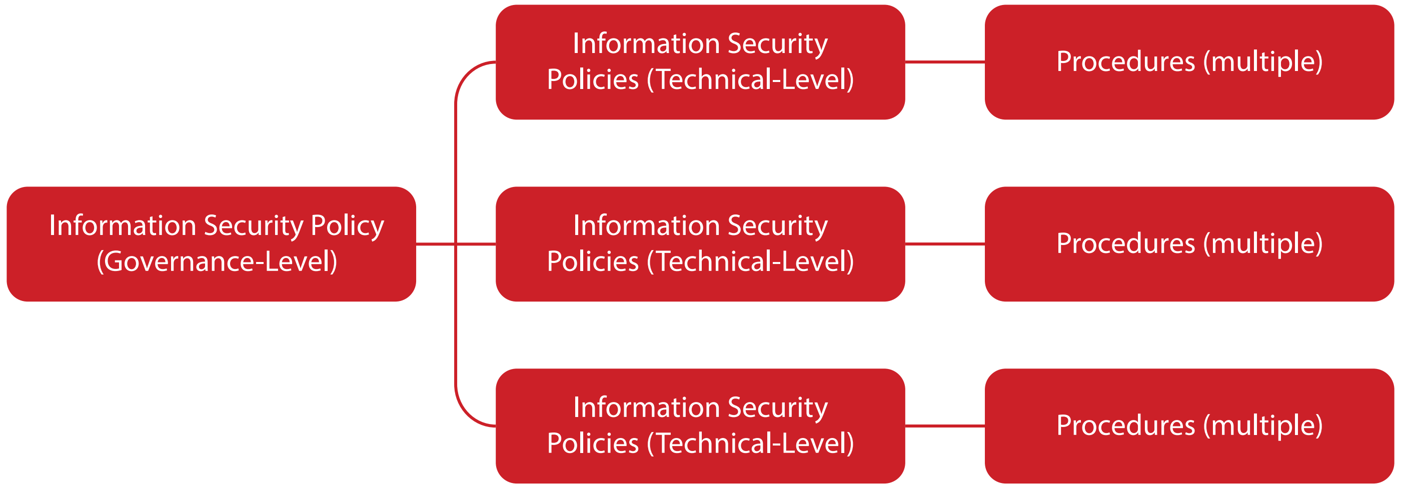
The purpose of this article is to provide an overview of information security policies, including their objective, types, and development lifecycle.

Why do we need Information Security Policies?

Security policies fulfill several purposes such as: a tool to set the rules and expectations required from users, administrators, etc., authorizes the security team to monitor and investigate, defines consequences of violation, minimizes business risks, and helps to comply with laws and regulations.

What are the Types of Policies?

Information Security policies can be classified as Governance-level policy and Technical-level policies. Governance-level policy is the top-most policy, it is a single document, signed and issued by the senior management (e.g. Chairperson or CEO). Technical-level policies complement Governance-level Policy, for example Technical-level Policies are email policy, anti-virus policy, access control policy, etc. and procedures address the "how" part and can be considered as vehicles to effectively execute policies.


Information Security Policy (Governance-Level)

Information Security Policies (Technical-Level)

Procedures (multiple)

Information Security Policies (Technical-Level)

Procedures (multiple)

Information Security Policies (Technical-Level)

Procedures (multiple)

What are the Policy Audiences & Contents?

Content of a policy is based on its audience and governing policy is read by all users. Therefore, it should cover information security concepts at a high level, define these concepts, describe why they are important, and detail what your company's stand is on them. Technical-policies is used by relevant users and should address the "what", "who", "when", and "where" in more detail in terms of the Governance-level policy.

Who Should be Involved?

It is important to determine who is going to be involved in the actual development of policies. Ideally, a policy should be developed by the same group who will later own and enforce it. For example, Governance-level policy can be written by the Information Security team in collaboration with the Senior Management. Depending on the availability of skills and experience, assistance from experienced consultants can be considered. Other roles that may provide input include technical, legal, human resources, and audit and compliance teams, etc.

WHAT ARE THE PHASES OF INFORMATION SECURITY POLICY DEVELOPMENT?

The policy development process starts from securing Senior Management's commitment. Senior Management must be made aware of both the importance and size of the task in advance so that they can allocate resources accordingly. Enforcement and compliance with policies cannot be done without the ownership and support from the Senior Management.

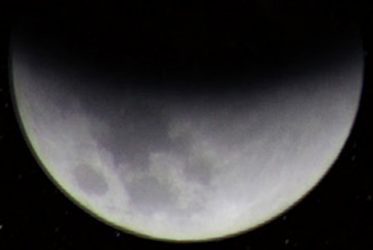
Phase 1 Write

If your company has existing security policies, start with reviewing them to determine company's current stance on a given issue or technology. Talk to subject matter experts and review information material from the internet.

Next, develop an initial draft. Review of right level of balance between rigidity and weakness for implementation. This ensures that the policy is clearly stated and enforced as per the best practices, while at the same time providing a mechanism for dealing with occasional exceptions without weakening the policy.

The Coca-Cola Rule: Replace the name of your organization with Coca-Cola in your Information Security policy. Read the policy again. If the same policy makes sense for Coca-Cola company, you probably need to rewrite the policy. Good policy is always organization specific. Mention why information security is important for your organization. Note: If you have written a policy for Coca- Cola, consider the rules above as the Emirates Airline Rule.

Finally, review with different stakeholders for possible gaps. Such stakeholders include the technical, legal and internal audit departments. Ensure that all identified gaps are closed before publishing policy documents.



Phase 2 Publish

Policy documents should be published so that they are available to all employees. You may put them on the company intranet site, or any other suitable platform. The documents should be accessible and available for download, printing, and saving.

Phase 3 Communicate

The most important part of policy development and enforcement is to ensure that relevant employees are aware of them. While email can be an excellent way to inform all personnel about the policy documents, other means of communication should be considered.

An education and awareness development program needs to be designed and implemented. The purpose is to ensure that employees, who are supposed to follow the policies understand the "value" of adhering to them. Patience, awareness, education and policy go hand in hand, each strengthening one other.

Phase 4 Enforce

Newly developed policies and procedures must be given some grace time for compliance. Subsequently, grace period for compliance enhances the effectiveness of enforceability and helps in building employees' confidence and trust. Depending on the size of the company, the grace period can be from a few weeks to few months. Thus, the internal audit department and Senior Management must be taken onboard to decide for the appropriate grace time.

Phase 5 Review & Update

Policies must be reviewed and updated on a regular basis. Ultimately, the purpose is to ensure that the policies are not obsolete due to changing business practices or technology updates. Annual reviews can provide a good balance between agility and stability. However, if required, a need-basis review and update can be conducted after a major change in the business, environment or technology.

Common issues that hurt policy effectiveness

In this section, I will try to identify the top three reasons that contribute in reducing the effectiveness of any policy document:

1. Lack of skills and experience while developing policy documents- Writing a policy document is easy if you want it to end-up as a "shelfware". The right skills and experience are required to engage stakeholders and develop policy that "clicks".

2. Lack of proper education and awareness plan- No matter how well policies are written, they are of no use if the practitioners are not aware of the value of adhering to them. Therefore, more effort and time must be invested in developing and implementing an effective awareness program for all employees and stakeholders to digest.

3. Demonstrable commitment from all levels of management- All levels of management must demonstrate their commitment in adhering to policies, especially because it is very different to follow them after their development. This cultivates confidence and trust among the employees.

ABOUT THE AUTHOR

Ikram A. Khan is the CEO of Business Beam. In his 20+ years of experience, he has successfully completed 40+ consultancy assignments and 200+ training sessions. He is a PECB Certified Trainer for ISO 27001, ISO 20000 and ISO 38500. He is also an accredited trainer for COBIT, ITIL and PRINCE2. He is based in Karachi, Pakistan.

CORPORATE SOCIAL RESPONSIBILITY
AN OVERVIEW OF ITALIAN AND PAKISTANI ORGANIZATIONS

Conducting Corporate Social Responsibility (CSR) audits in Pakistan & Italy on various standards (SA8000, BSCI, ETI based Sedex) and the Code of Conduct (COC) of numerous buyers around the world it can be stated that; CSR is a platform where the whole organization can manage various standards at the same time or effectively integrate standards along with the complete package of human resource management.

Corporate Social Responsibility originates and is created from the developed premier social compliance standard-SA8000 and other standards are developed based on this standard to ensure the basic human rights of workers with additional focus on the industry applied, objectives desired to be reached, required and/or marked areas. Even though, wordings and clauses might be different from one standard/COC to another the requirements remain the same. Essentially, organizations have to develop their system and structure according to the requirements from multiple standards in order to fully fulfill their CSR requirements and develop one system to implement accordingly.

When implementing CSR requirements with other standards the organization, should focus on the following components described below to comply with the CSR framework and shine as an organization that is committed to protect and benefit society as a whole.

Child Labor

Helping children, who want to study but are unable to do so because of their financial limitations, is characterized as a human act from the organizations' side of contributing to their surrounding society. Various organizations can play a major role to assist children facing financial difficulties By helping them attain the most basic right; education. In return, these children are working for a few hours after school with the purpose of getting some experience while contributing to the funding organization.

Forced or Compulsory Labor

The principle of every organization, regardless of its size, should create a secure atmosphere in which workers will not engage in or support any forced or compulsory labor, as well as allow the withhold of any part of the personnel's salary, benefits, property or documents. Employees must have the right to leave the workplace premises after completing their duration of work without any objections, unless they have been offered Over Time. Equally, organizations should not involve in any form of slavery type of contracts with their employees nor support human trafficking.

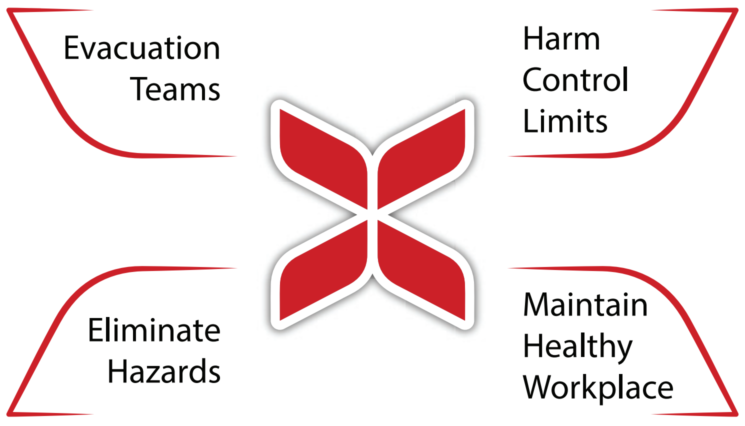
Health & Safety and Environment

Some CSR policies include the application of numerous environmental systems (i.e. EMS), supporting an organization to guide their own control limits of harming the environment. Environmental aspects are normally covered while preparing/managing Health and Safety activities and are considered as the main element of HSE.

Providing a safe and healthy workplace environment to all workers by assessing all the workplace risks is another principle of effectively maintaining CSR. Definitely, by conducting formal and periodic occupational health and safety risk assessments we can identify as well as address potential health, safety and environmental hazards.

Assessing the entirety of the organization's risks will support the evaluation of taking advanced steps in preventing the risks. Some hazards though, still remain after effective minimization of the causes of all hazards in the workplace environment. However, in cases where these hazards do occur organizations must have the resources, process and procedures in place to provide first aid and assist the worker in obtaining follow-up medical treatment.

Main CSR Elements


Evacuation Teams

Harm Control Limits

Eliminate Hazards

Maintain Healthy Workplace

Organizations are also advised to pay more attention to and consider the mothers that are expecting and nursing by providing less hectic tasks during that period and allowing additional breaks if needed; as well as setting up separate rooms for nursing mothers is highly advised.

Upon developing risk assessment methods, organizations need to conduct training on lowering the staff doubts and concerns, increase awareness, and should involve all staff in evacuation drills so they can remove themselves from imminent danger without seeking permission from the organization.
Teams developed by the organization should be trained in Fire Fighting, First Aid and other required trainings identified by the organization.

Freedom of Association & Right to Collective Bargaining

The freedom of employees to join and organize labor union(s) of their choice and to bargain collectively on their behalf with the organization should be provided. Another mandatory requirement is to allow workers to freely elect their representatives; some organizations also engage their own representatives, usually experts from their own industrial area to help with specific discussing matters.

Representatives(s) discuss mostly matters related to discrimination, harassment, intimidation or retaliation and collectively identified issue with the management of the organization(s).

Discrimination

In this section Human Resources (HR) must have developed strategies and policies on preventing any engagement in or support of discrimination in hiring, remuneration, access to training, promotion, termination or retirement based on race, national or territorial or social origin, caste, birth, religion, disability, gender, sexual orientation, family responsibilities, marital status, union membership, political opinions, age or any other condition that could give rise to discrimination. Further, hiring of a woman shouldn't be subject to pregnancy or virginity tests under any circumstances.

Organizational policies must include personnel's rights, practices, and prevent discrimination in terms of race, national or social origin, religion, disability, gender, sexual orientation, family responsibilities, union membership, political opinions or any other condition that could give rise to discrimination. The organization shouldn't allow any behavior that is threatening, abusive, exploitative or sexually coercive, including gestures, language and physical contact, in the workplace and in all residences or property governed from the organization. If at any point such events occur, the acting individuals must be taken to the Disciplinary Committee.

Disciplinary Practices

It has not been witnessed that organizations have incorporated in their policies some sort of corporal punishment, mental or physical coercion, or even verbal abuse of personnel. However, the violation on already developed policies by the organization punishes their members with a deduction in wage.

Working Hours

Country's Law is the primary source used when preparing the working hours' and regulations along with the obligatory (Tea, Lunch & Prayers) breaks. Employees in Pakistan work for 48 hours a week, six consecutive days with an additional 12 hours of overtime weekly limit whereby their seventh day will be off. Temporarily, piece rate and home workers are being observed to help decide when to provide jobs, based on their working hours and skills, this decision will be made. Due to fog, work does not start till the air is clear.

Remuneration

Every country has made their minimum wage's amount according to the food basket with minimum number of family members, as announced by national law.

Most of the organizations are providing pay-slip to the staff with complete information of their duration, leaves, overtime, loans and deductions (if any). Many organizations have their attendance system incorporated with the organizations policies and practices, used for calculating staff's salary. Temporary staff also gets the same treatment in calculating their wages.

Management System

Company policy statement must be available to all staff in local language and also available in English for international customers', suppliers, sub-contractors and sub-suppliers. The company policy is usually followed according to the targeted standard and/or COC, and organizations are fulfilling the requirements accordingly. Other Policies & Procedures are required to be developed which assist in the proper implementation of the system.

Top management and other monitoring (worker/unions) representatives are conducting regularly management reviews and audits of their policy statements and procedures, implementing the Standard and performance results, in order to continually improve.
A major element of the system is Internal Auditing (IA), having the ability to enhance any management system of the organization. The generated information and data will assist in developing a better system of the organization. Furthermore, this will help in their announced and unannounced audits for certification or from the client's end, verifying compliance in shape of COC audits. Certification & COC audits are based on upcoming contracts and/or orders.

Corrective and Preventive Actions criteria, procedures take place for any arising discrepancy. Concerned employees need to ensure that these actions are implemented effectively; according to the requirements.

Moreover, training to all working personnel at facilities need to be conducted regardless of the contract type. Those organizations are periodically measuring the effectiveness of training and recording their nature and frequency.

The various types of Suppliers & Contractors, from what has been personally witnessed, are employment agencies, raw material providers, strategic partners and logistics providers. All of these service providers need to evaluate and communicate their policies & procedures when they are providing their services. Likewise, once organizations approve them, they must include in all communications and training programs information about their organization and their strategies to service providers. Also, yearly evaluation should be conducted based on the performance of the supplier(s) and organizations need to decide to continue or discontinue agreements.

PECB

A substantial number of organizations disregard Corporate Social Responsibility's effect in the organization; when in contrary, CSR has continuously witnessed to improve business operations. Additionally, its seriousness has begun ascendance due to societal awareness in terms of Health, Safety, and Environment. Accordingly, PECB's willingness to contribute to your organization while providing certification against ISO 26000 will uplift recognition as much as assurance with respect to social responsibility in not only establishing a healthy working space but also protecting the environment.

ABOUT THE AUTHOR

Tariq Khan is the Founder and CEO of ANM Transformational Solutions. Mr. Khan's expertise specializes on ISO 9001, ISO 14001 and OHSAS 18001 BSCI, SA8000, NEBOSH, HR, C.I.S.A. and Six Sigma. He has also employed his abilities to develop companies like Saudi Arabian Airlines, Dewan Mushtaq Group, and Intertek besides his academic background as a trainer for a variety of management standards.

SURPRISE YOUR CURIOSITY

THE PECB EXPERIENCE

EVENT IN PORTUGAL

JANUARY 2017

PECB

PENHA LONGA
A RITZ-CARLTON RESORT

Quality Management System Effects Cost Decrease

Cost Decrease? Our QMS Costs Us!

These are the typical words heard when the subject is broached about the improvements the quality management system (QMS) makes in decreasing the cost of production of products and services.
Why would this be true? What costs are there in having a quality management system? What are we doing extra that we would not be doing if we didn't have a QMS?

Cost of Having a Quality Management System

The primary cost of having a quality management system is "time". Time to manage the documentation. Time to respond to and address nonconforming material and respond to customers. Time to review orders, choose suppliers, and audit your processes to make sure people are doing what is expected. Time to perform a management review. Time to analyze data.

Without a doubt, all of this is still going to be occurring with or

quality management system is "time". Time to manage the documentation. Time to respond to and address nonconforming material and respond to customers. Time to review orders, choose suppliers, and audit your processes to make sure people are doing what is expected. Time to perform a management review. Time to analyze data.

Without a doubt, all of this is still going to be occurring with or without a formal management system except for the managing of the documents. Even some of this would still be necessary even if there were no formal

without a formal management system except for the managing of the documents. Even some of this would still be necessary even if there were no formal management system.

What about the management review? If a company who doesn't have staff meetings (management reviews); where the company's progress to its goals and its problems are reviewed, where plans are made for the future; then how would the managers of the company communicate and know the expectations for the future? So even without a management system some sort of management review is necessary.

If a company does not address its nonconforming material including analyzing and try to prevent it, they waste money. If customers ask for responses and get none, customers are upset. This costs money.

So really what extra is done? Managing of documentation.

Why Does Managing of Documentation Cost So Much?

Usually because there is too much documentation. Many companies who have been certified with ISO 9001 for many years and many revisions to the standard still have a system that meets the requirements of the 1994 standard!
With the 2000 version and now the 2015 version, documentation should be only what is necessary to control processes and to mitigate risk. This should be less than 50 pages in a large corporation. Note: pages not documents! Fifty pages of documentation. If your management system seems to be costing you, look at the number of documents that add no value and lean the documents. This is a way to decrease the cost of the management system.

How Does Having a Quality Management Save Costs?

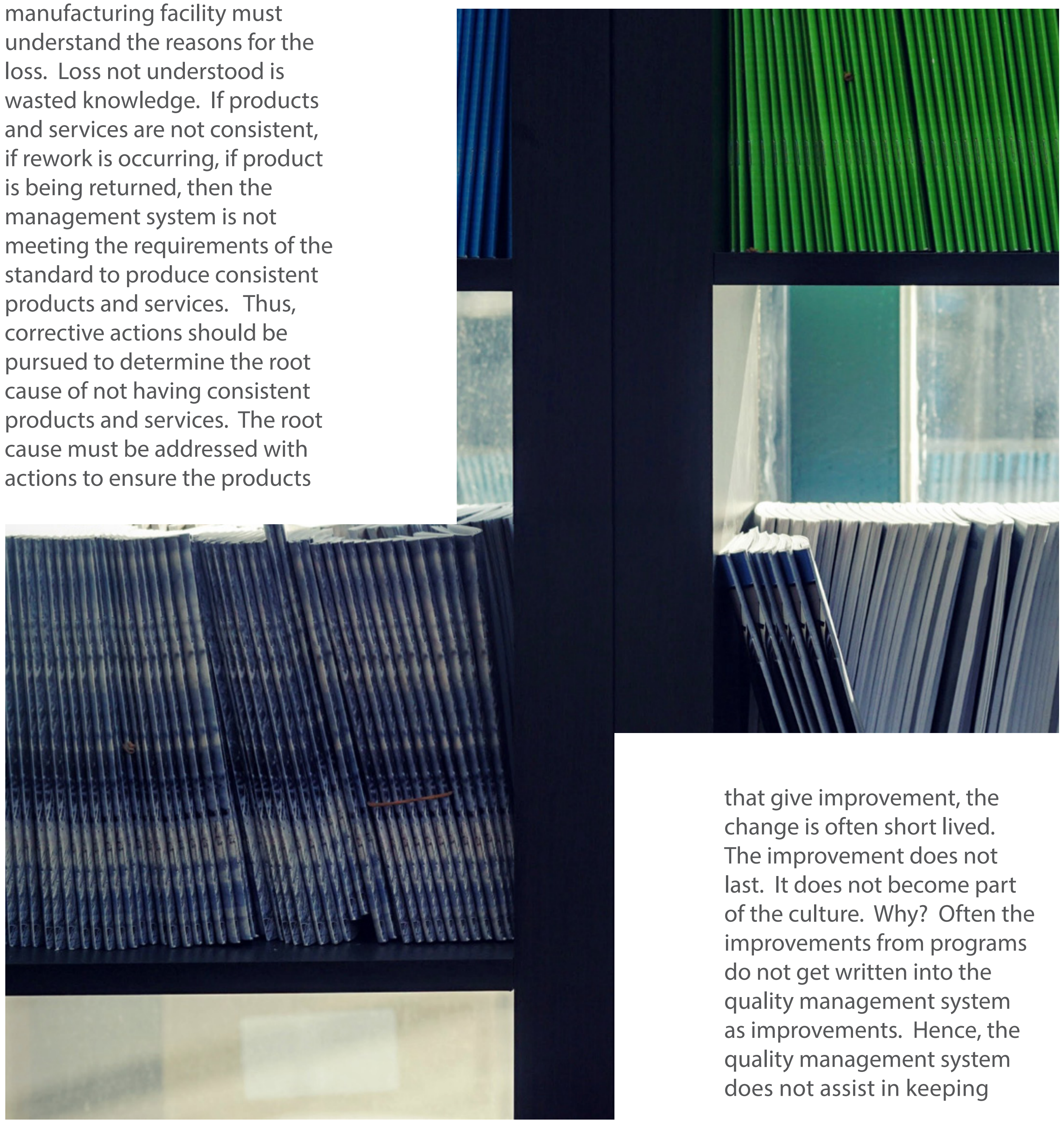
The purpose of the ISO 9001 standard and the other quality management standards such as AS 9100, AS 9120, AS 9110, and TS 16949 are to ensure the production of consistent products and services and to ensure the system is continually improving.

Consistent products and services that meet customer requirements save you and your customers costs. Customers get what they expect. Your processes produce products and services that meet requirements; while, nonconforming products and services do not subtract from profit. Every manufacturing process can experience some loss and still be healthy. Each manufacturing facility must understand the reasons for the loss. Loss not understood is wasted knowledge. If products and services are not consistent, if rework is occurring, if product is being returned, then the management system is not meeting the requirements of the standard to produce consistent products and services. Thus, corrective actions should be pursued to determine the root cause of not having consistent products and services. The root cause must be addressed with actions to ensure the products and services become consistent.

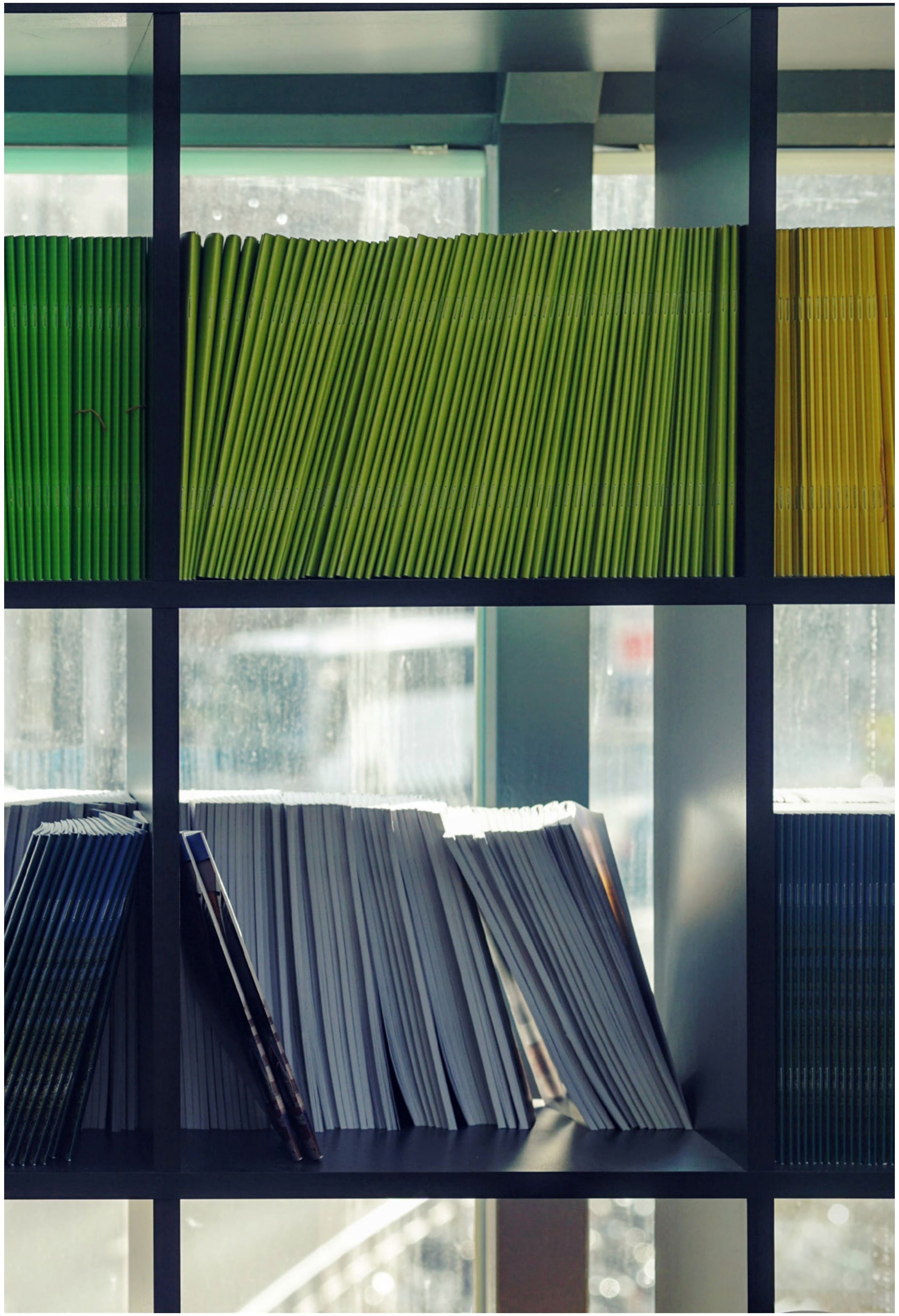
Consistency applies in the office as well as in the plant. What causes inconsistencies in the office? What causes extra work? These inconsistencies cost! Launching pursuit of understanding the sequence and interaction of the office processes (support processes) is essential when looking for those inconsistencies and improving the processes. Having consistent products and services is an essential part of saving manufacturing costs of the products and services.

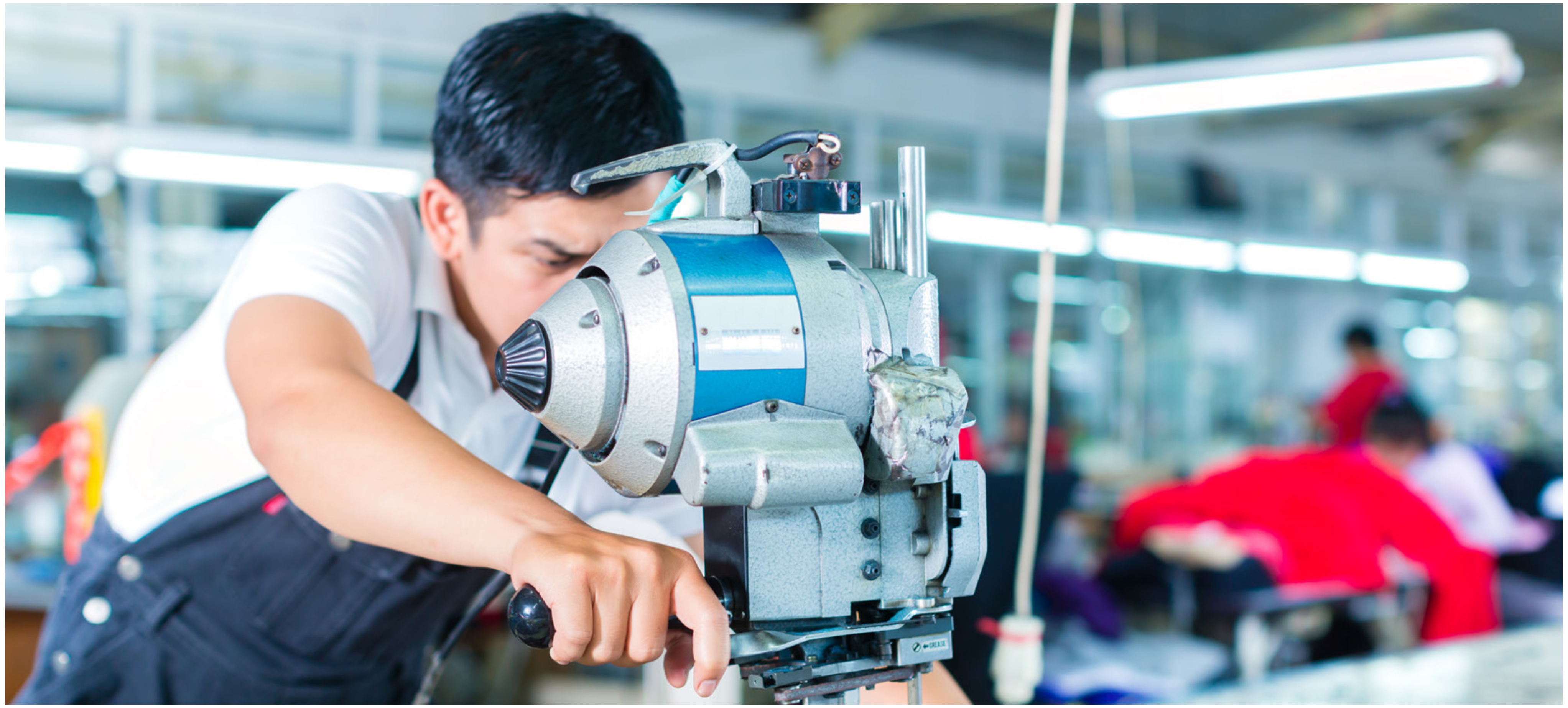
Consistent products and services save money.

Sustaining Improvements Decrease Costs



When companies implement Lean/Six Sigma, Layered Process Auditing, and other programs that give improvement, the change is often short lived. The improvement does not last. It does not become part of the culture. Why? Often the improvements from programs do not get written into the quality management system as improvements. Hence, the quality management system does not assist in keeping





the improvements. Writing the improvements into the processes, result in good investments. Changes become part of the fabric of the way things are done and internal audits ensure the changes are in place per the plan while sustained improvements decrease costs.

Risk Assessments Decrease Costs

When a risk assessment discovers a potential weakness, controls are planned to address the risk, to mitigate the risk. These controls tell us what are the important actions that must be performed to prevent the risk from becoming reality. If a document is not helping mitigate a risk, why does it exist? Risk Assessments can be used to decrease the costs of documentation. Elimination of documents that do not help make more consistent products and services and improve the management system is necessary.

Summary of How a QMS Decreases Costs

Decreased costs come from a more consistent product, service, and by a constant pursuit of improvement. This primarily occurs from two sources: 1. By determining the necessary documentation and eliminating unnecessary documentation. 2. By pursuing of consistent products and services. Both yield improvements in the way products and services are produced and the improvements in the management system.

For more information on minimizing documentation and producing consistent products and services, go to www.CE-Q.com for webinars and free documentation.

About the Author

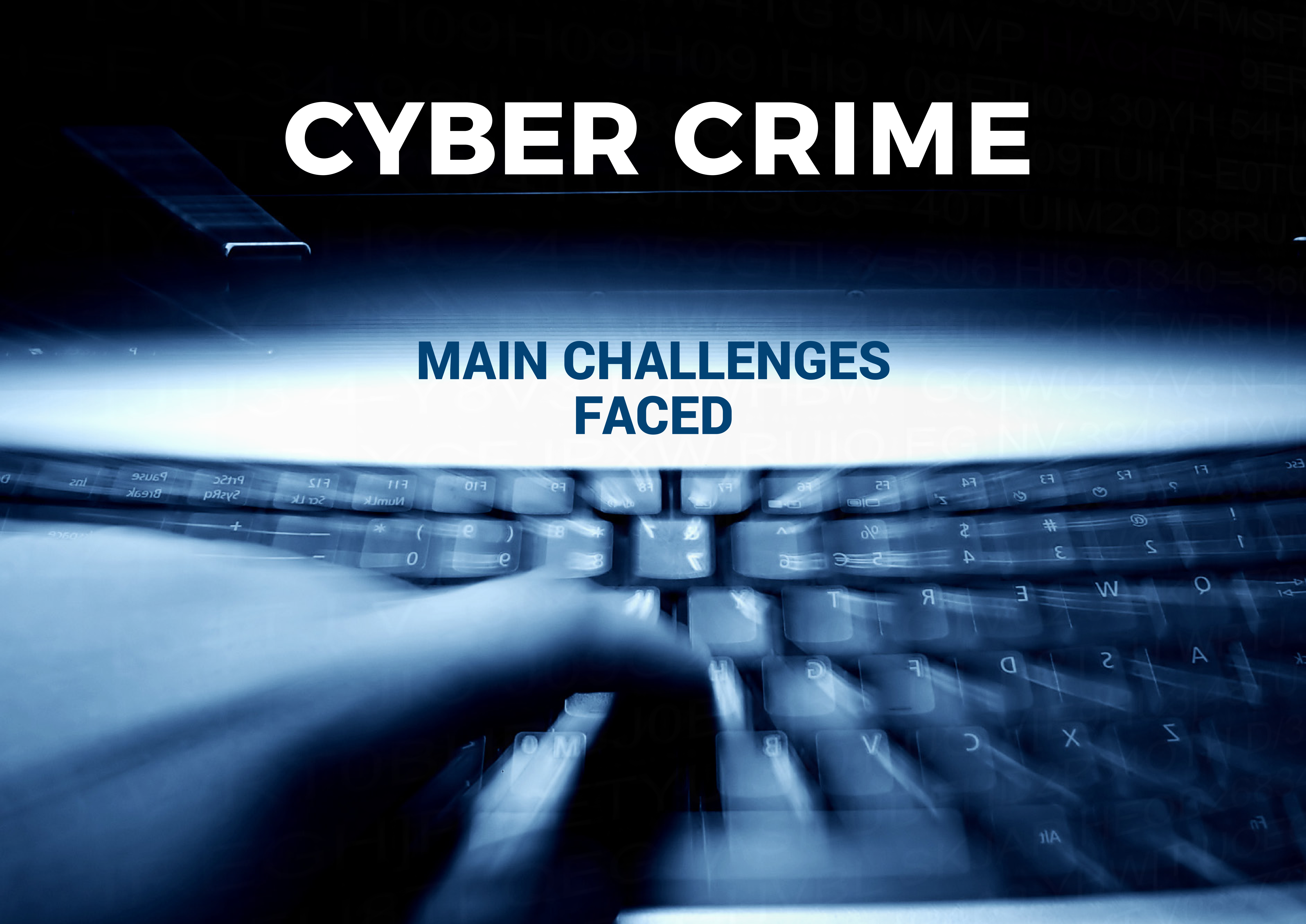
PECB

Certifying against ISO 9001 as a main principle of assuring towards quality management systems has shown to decrease costs, substantially. Further, ISO 9001 implementation did show success of business processes and performance improvements. Suitable to all kinds of organizations, PECB has demonstrated to provide efficient management processes to a large number of organizations through effective training methods of ISO 9001.

Debra Hay Hampton has been a quality engineer since 1979. She is a Certified Quality Engineer, registered as a Professional Engineer in the field of Quality, a Certified Lead Auditor of Quality Management, Environmental, and Occupational Health and Safety Systems. She also audits to ISO 13485, ISO 22000, ISO 50001, and implements AS 9100 and TS 16949.

CYBER CRIME

MAIN CHALLENGES FACED



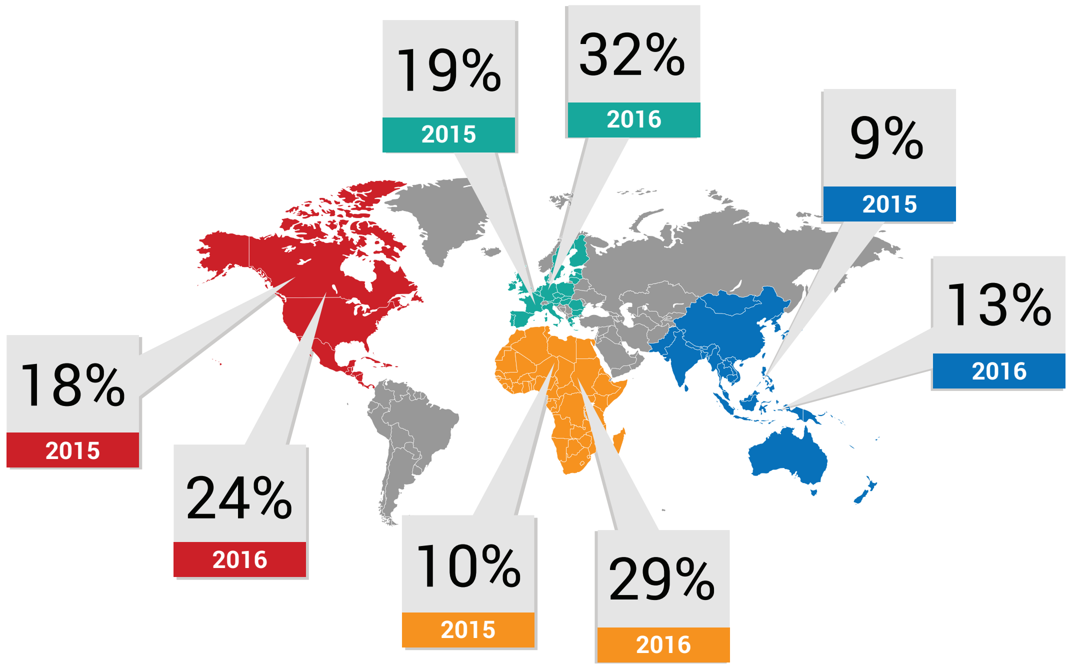
The increasing nature of cybercrime

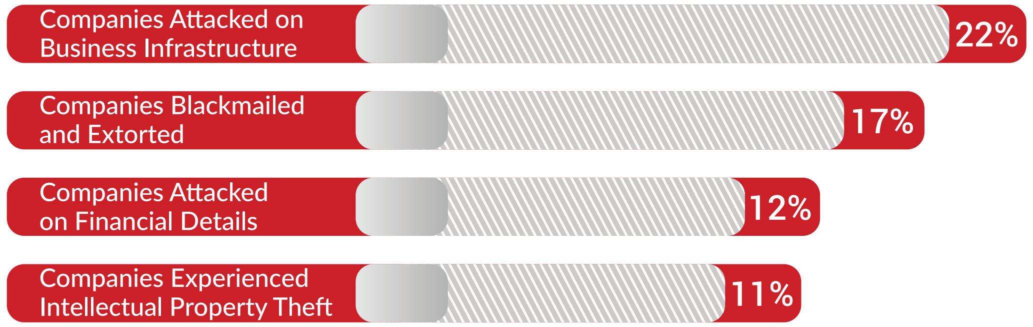
Application services in the cyberspace have gained a huge importance in our lives expanding beyond the business-to-consumers and consumers-to-consumers models to a form of many-to-many interactions and transactions, called the Internet of Everything (IoE), predicting that by 2020 there will be more than 200 billion devices that will join this group.

In some organizations, the system devices have become quite open and are on the way to lose direct control of data security.

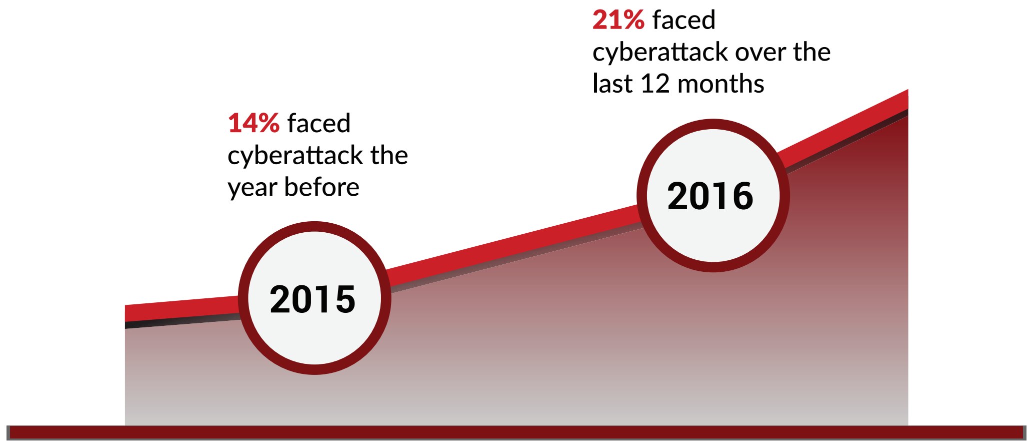
The IoE is causing an increase of threats and vulnerabilities; thus, it is becoming the target of cybercrime in terms of sensitive customer information, intellectual property and even the control of key machinery are increasingly being in risk from cyber attacks. The targeting of electronic assets has the potential to make a material impact on the entire organization and its stakeholders.

Businesses suffering from cyber-attacks





Companies that face cyberattack



Source: Grant Thornton's International Business Report (IBR-2016)

The IBR findings also reveal that globally, of those business leaders who have faced a cyber-attack in the last 12 months, nearly one in eight (13%) only realized that the attack had occurred more than a week after the event. For 4% of them, it took longer than a month.

Cybersecurity is the preservation of confidentiality, integrity, and availability of information in the Cyberspace. In ISO 27032, clause 4.20 specifically, includes the protection of assets from threats mostly related to malicious and other human activity through a risk assessment and controls selection to counter and reduce risk at the acceptable level.

Cybersecurity depends on information security, application security, network security, internet security and CIIP (Critical Information Infrastructure Protection).

There are personal assets (individual consumer's online identity, bank account, medical data, banking and online payment accounts, email accounts, pictures, videos, music records, personal digital devices, PC) and organizational assets (networks, servers, works stations, reputation, business plans, intellectual property, brand) in cyberspace.

Some threats to personal assets are:

- Person's online identity is stolen or masqueraded;
- Unauthorized access to persona's financial information-theft of the person's money and fraud;
- Endpoint being made a zombie or bot virtual theft and virtual mugging

Threats to organizational assets are:

- Website defacement;
- URL stolen by cyber-squatters;
- Information of employees, clients, partners or suppliers disclosed;
- Financial reports breached;
- Unauthorized access to important information on governments

In the assessment of vulnerabilities process the possible reasons that stay behind threat agent activities should be identified:

- Motives (religious, political, economic, etc.)
- Capabilities (knowledge, funding, size, etc.)
- Intentions (fun, crime, espionage, etc.)

The roles of individuals in the Cyberspace may assume different roles in different context and applications and can include the following:

- General cyberspace application users, such as online gamer player, instant messenger user, or web surfer;
- Buyer/seller, involved in placing goods and services on online auction and marketplace sites for interested buyers, and vice versa;
- Blogger and other contents contributor;
- Independent Application Provider (IAP) within an application context;
- Member of an organization;
- Other roles, that a user can be assigned a role unintentionally or without his or her consent.

The government, primarily law enforcement agencies and regulators, may have the following important engagements to play with:

- Advise organizations of their roles and responsibilities in the Cyberspace;
- Share information with other stakeholders on the latest trends and developments in the technology;
- Share information with other stakeholders on the current prevalent security risks;
- Be a conduit for receiving any information, whether close or open, with regard to security risks to the Cyberspace; and
- Prepare the primary coordinator for information dissemination and orchestrating any required resources, both at national-level or corporate level, in times of crisis arising from a massive cyber-attack.

Cybersecurity framework

To address cybercrime and social changes, many governments and institutions launched cybersecurity initiatives, ranging from guidance, through standardization, to comprehensive legislation and regulation.

There are several cybersecurity frameworks available, where the most known are:

- **ISO/IEC 27032:2012 - Guidelines for cybersecurity**
- **NIST Cybersecurity Framework**

ISO/IEC 27032:2012, is an international standard published by ISO, which presents a guideline for cyber security implementation and security practices for Stakeholders in the Cyberspace. It provides an explanation of the relationship between other types of security and also presents a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

This International Standard gives focus to three main themes of cybersecurity that intelligence agencies and national bodies concerned with the protection of critical national infrastructure and with the in-depth research necessary to take place, in order to provide practical solutions that organizations can implement to help mitigate these threats:

- Roles;
- Policies;
- Methods;
- Processes; and
- Applicable technical controls.

This International Standard gives focus to three main themes of cybersecurity that intelligence agencies and national bodies concerned with protection of critical national infrastructure and dedicating research time in understanding in order to provide practical solutions that organizations can implement to help mitigate these threats:

- Dark Net Monitoring – Attack Detection;
- Trace back – Attack Investigation;
- Sinkhole operation – Attack Response

NIST Cybersecurity Framework, published by the Commerce Department's National Institute of Standards and Technology, focuses on using business drivers to guide Cybersecurity activities and considering Cybersecurity risks as part of the organization's risk management process. It includes:

- Framework Core (a set of Cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It consists of five concurrent and continuous functions; Identify, Protect, Detect,

The standard is divided into framework domains and capabilities:	Government guidelines – adopted from the ISO/IEC 27001	Cybersecurity technical controls – set of technical controls for addressing common cybersecurity risks to the critical assets identified	Incident information sharing and handling framework guidelines	Emerging themes – consideration for cybersecurity readiness	
These standards provide guidance for addressing common Cybersecurity risks, including:	Social engineering attacks	Hacking	The proliferation of malicious software ("malware")	Spyware	Other potentially unwanted software
The technical guidance provides controls for addressing these risks, including controls for:	Preparing for attacks	Detecting and monitoring attacks	Responding to attacks		
The technical controls include:	Secure coding	Network monitoring and response	Server level controls	Application level controls	End user workstatior controls
This International Standard also provides a framework for:	Information sharing	Coordination	Incident handling		

Respond and Recover, identifies underlying key Categories and Subcategories for each function and matches them with example Informative References),

- Framework Implementation Tiers (provide context on how an organization views Cybersecurity risk and the processes in place to manage that risk, and
- Framework Profile (identify opportunities for improving Cybersecurity posture by comparing a "Current Profile" with a "Target Profile").

European Strategy for Cybersecurity

The European Union (EU) and its member states have launched wide-ranging programmes and initiatives to strength cybersecurity, responding to the challenges with a defense of cybersecurity initiatives, including the following:

- The European Network and Information Security Agency (ENISA) was formed in 2004 to provide guidance and recommendations for information security;
- The European Commission issued a Cybersecurity Strategy that has been mirrored by a number of national strategies;
- A wide range of cybersecurity-related activities in research and development, regulation and governance are occurring in the EU and member states.
- The EU cybersecurity strategy addresses the perspective that cybersecurity requires common definitions, frameworks and a sense of direction throughout all member states and associated states.
- To adequately address the risk and threats of cybercrime, enterprises need to embed cybersecurity, as an integral part, into their overall governance, risk management and compliance (GRC) frameworks.

Embedding cybersecurity into GRC frameworks includes the following:

- **Good governance** that is in line with existing principles of corporate governance;
- Comprehensive management of **cybercrime risk and threats** that is aligned with existing enterprise risk management (ERM) systems;
- **Compliance** with existing or planned EU-level and national laws and regulations;
- **Resilience** for organizational infrastructures and personnel;
- **Assurance** for information, processes and related controls.

Cybersecurity should also define and maintain appropriate interfaces with related disciplines, such as:

- Critical infrastructure protection
- National emergency management
- Public incident management and disaster management.

NIS Directive and national CSIRTs

In December 2015, the Commission, the Parliament of the EU, and the Council of Ministers reached an agreement on the Network and Information Security (NIS) Directive. Chapter 3 describes the cooperation between competent authorities.

The five Framework Core Functions are not intended to form a serial path, they can be performed concurrently and continuously to form an operational culture that address the dynamic Cybersecurity risk.

IDENTIFY

develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.

PROTECT

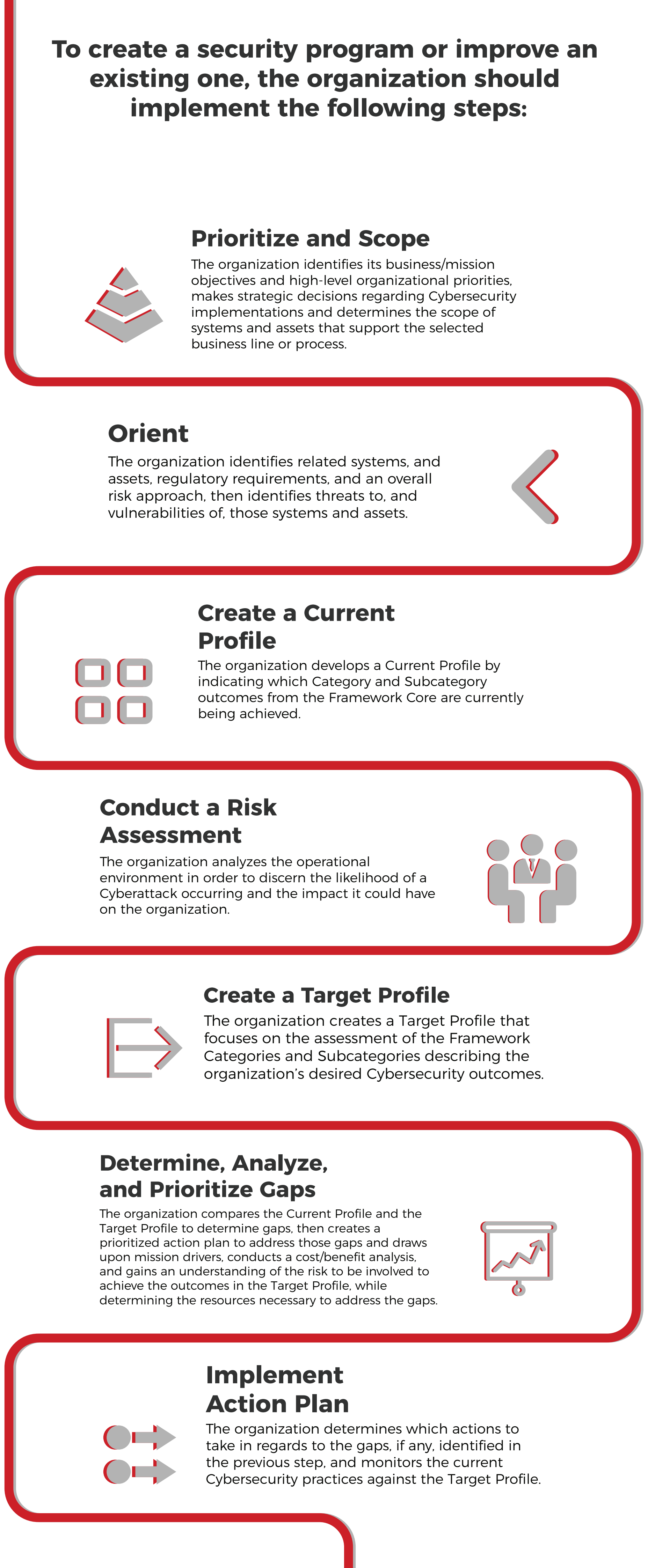
develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

DETECT

develop and implement the appropriate activities to identify the occurrence of a Cybersecurity event.

RESPOND

develop and implement the appropriate activities to take action regarding a detected Cybersecurity event.



To create a security program or improve an existing one, the organization should implement the following steps:

Prioritize and Scope

The organization identifies its business/mission objectives and high-level organizational priorities, makes strategic decisions regarding Cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process.

Orient

The organization identifies related systems and assets, regulatory requirements, and an overall risk approach, then identifies threats to, and vulnerabilities of, those systems and assets.

Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Conduct a Risk Assessment

The organization analyzes the operational environment in order to discern the likelihood of a Cyberattack occurring and the impact it could have on the organization.

Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired Cybersecurity outcomes.

Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps, then creates a prioritized action plan to address those gaps and draws upon mission drivers, conducts a cost/benefit analysis, and gains an understanding of the risk to be involved to achieve the outcomes in the Target Profile, while determining the resources necessary to address the gaps.

Implement Action Plan

The organization determines which actions to take in regards to the gaps, if any, identified in the previous step, and monitors the current Cybersecurity practices against the Target Profile.

The Chapter defines two groups meant to improve NIS-related cooperation between MS. The first is the Cooperation Network, composed of representatives of MS, the Commission, and ENISA. This group is meant to focus on strategic issues. The second group is the CSIRT Network, composed of representatives of MS' CSIRT and CERT-EU, with the Commission as observer and ENISA as Secretary and as an active supporter.

The Security of the NIS of operators of essential services is described in chapter 4, defining security requirements for and duties of operators of essential services.

The Security of the NIS of digital service providers is presented in chapter 4a, defining, security requirements for and duties of digital service providers.

Conclusions

Cybercrime is increasing as a cost to businesses due to cyber-attacks in the past 12 months. At the same time, the increment of the Internet of Everything (IoE) is resulting in new vulnerabilities to the business and citizens. To respond, governments launched several initiates to mitigate the cybersecurity risks, including:

- Establishment of cyber defense strategies
- the development of cyber frameworks such as NIST Cybersecurity Framework;
- the development of the CSIRT Network, composed of representatives of EU MS' CSIRT and CERT-EU;
- the development of training and awareness programs;
- the enforcement of legislation

However, those initiates are not sufficient to combat the cybercrime nor to reduce the cybercrime trend. In addition, the ISO 27001 certification scheme does not assure that the controls and guidance established in ISO/IEC 27032 are implemented and managed. Consequently, the UK Government has developed an industry support certification scheme (Cyber Essentials) providing criteria for organizations to measure their cybersecurity systems aligned with current cybersecurity best practices. Since October 2014 Cyber Essentials certification is mandatory for organizations looking to acquire certain government contracts that involve the handling of sensitive information and delivering particular ICT products and services.

- It is necessary to establish an International certification scheme for cybersecurity management systems and the correspondent personnel certification for Implementers, Auditors and Managers based on ISO 27032 and other cybersecurity best practices. Importantly, public organizations should require all their suppliers and sub-suppliers to be conform to the cybersecurity certification, as well as the operators of essential services and digital service providers. Likewise, governmental authorities should launch an awareness program regarding the combat and prevention of the cybercrime.

ABOUT THE AUTHOR

PECB

Certifying against ISO/IEC 27034 proves that the used applications within your organization pursue a framework of security. Additionally, competence would be increased to implementing the above mentioned policies on cybersecurity through ISO/IEC 27032 Lead Cybersecurity Manager certification

Author

This article has been authored by Mario Lavado, Author of the Month.

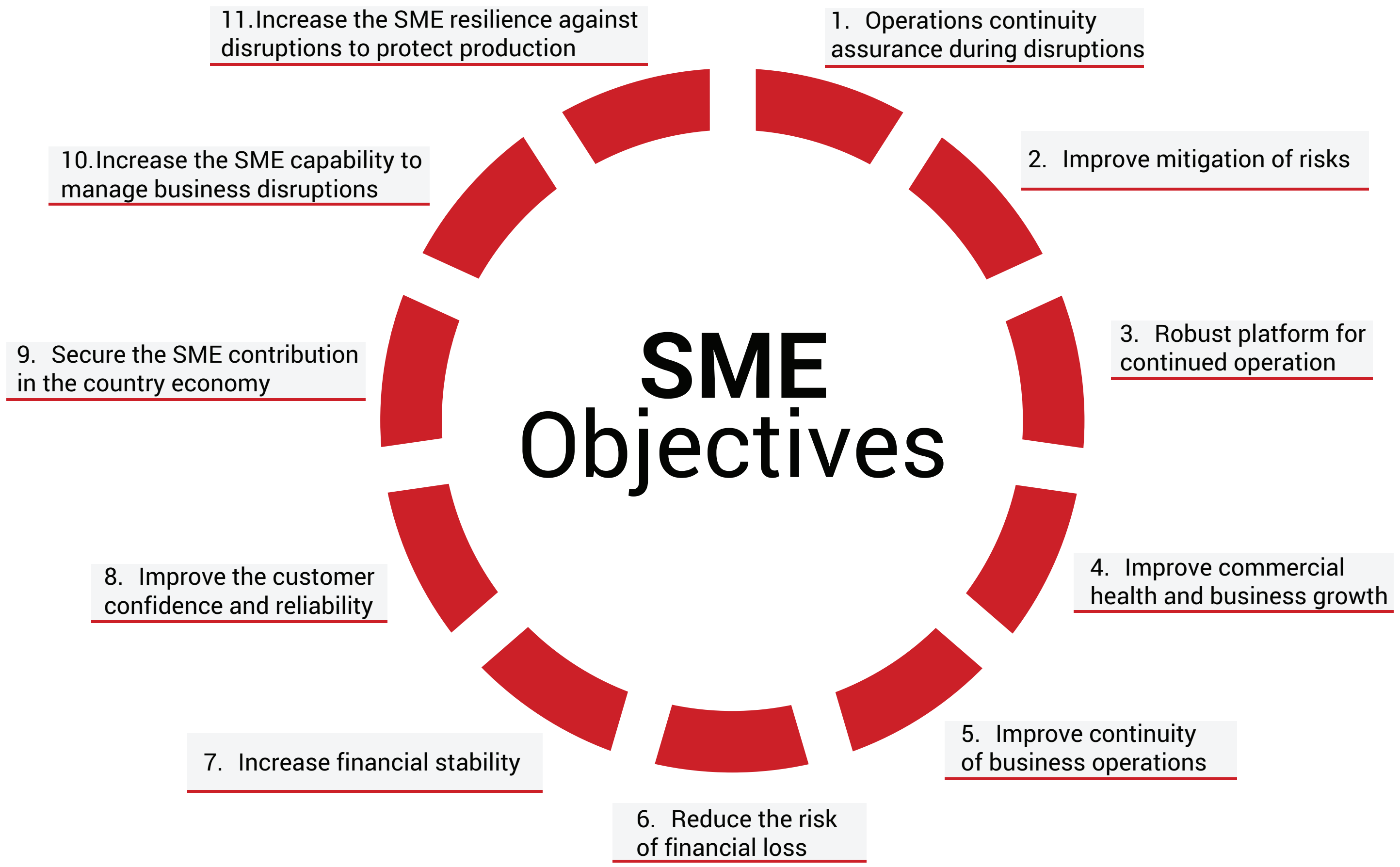
AUTHOR OF THE MONTH

Mário Lavado is a trainer and consultant in Lean Six Sigma, IT Governance, COBIT, ITIL and Lead Auditor for ISO 9001, ISO 27001 and ISO 20000. As a Graduate in Materials and Physics Engineering and a Post-Graduate in Quality Engineering, he has more than 20 years of experience in consulting, training and auditing. Besides his responsibilities in public and private organizations, Mr. Lavado is also involved in the design, implementation and improvement of management systems in the Information Technology area. The expertise of Mr. Lavado has had an impact on organizations such as: INOSERV-Innovation in Services, APCER, Banco de Poupança e Crédito, Vantiv, OnlyConcept, itSMF Portugal, InoCrowd, Instituto de Informática, ASI Consuloting, Link Consulting, Partex, Sommer Allibert, Valmet, and Seagate.

BUSINESS CONTINUITY PLANNING

YOUR BUSINESS OBJECTIVES

Continuity of business operations in the event of a disruption is not only a concern for big corporations but also for every organization irrespective of its size or nature. For far too long, big corporations have invested in the implementation of continuity capability measures to ensure that they are prepared for, can respond to and recovery from, any disruption. Indeed, this initiative has proven to be successful for such corporations even in the midst of disruptions. Implementation of a continuity management program by SME's can, just like big corporations, yield similar results though SME's stand to accrue even more benefits from its implementation. The following are amongst other the benefits that the SME's stand to benefit:



SME Objectives

1. Operations continuity assurance during disruptions
2. Improve mitigation of risks
3. Robust platform for continued operation
4. Improve commercial health and business growth
5. Improve continuity of business operations
6. Reduce the risk of financial loss
7. Increase financial stability
8. Improve the customer confidence and reliability
9. Secure the SME contribution in the country economy
10. Increase the SME capability to manage business disruptions
11. Increase the SME resilience against disruptions to protect production

Continuity Program implementation challenges for SMEs in the developing world

Whilst there are benefits of implementing continuity frameworks, such comes with challenges that the SME's should convert to opportunities. It must be argued that these challenges are driven by varying differing factors that are not necessarily the same as the diversity from continent to continent, country-to-country etc. For most of the developing countries in general and Africa in particular, these challenges are shaped amongst others by factors such as, but not limited to:

1 High cost of securing continuity skills to drive the implementation;

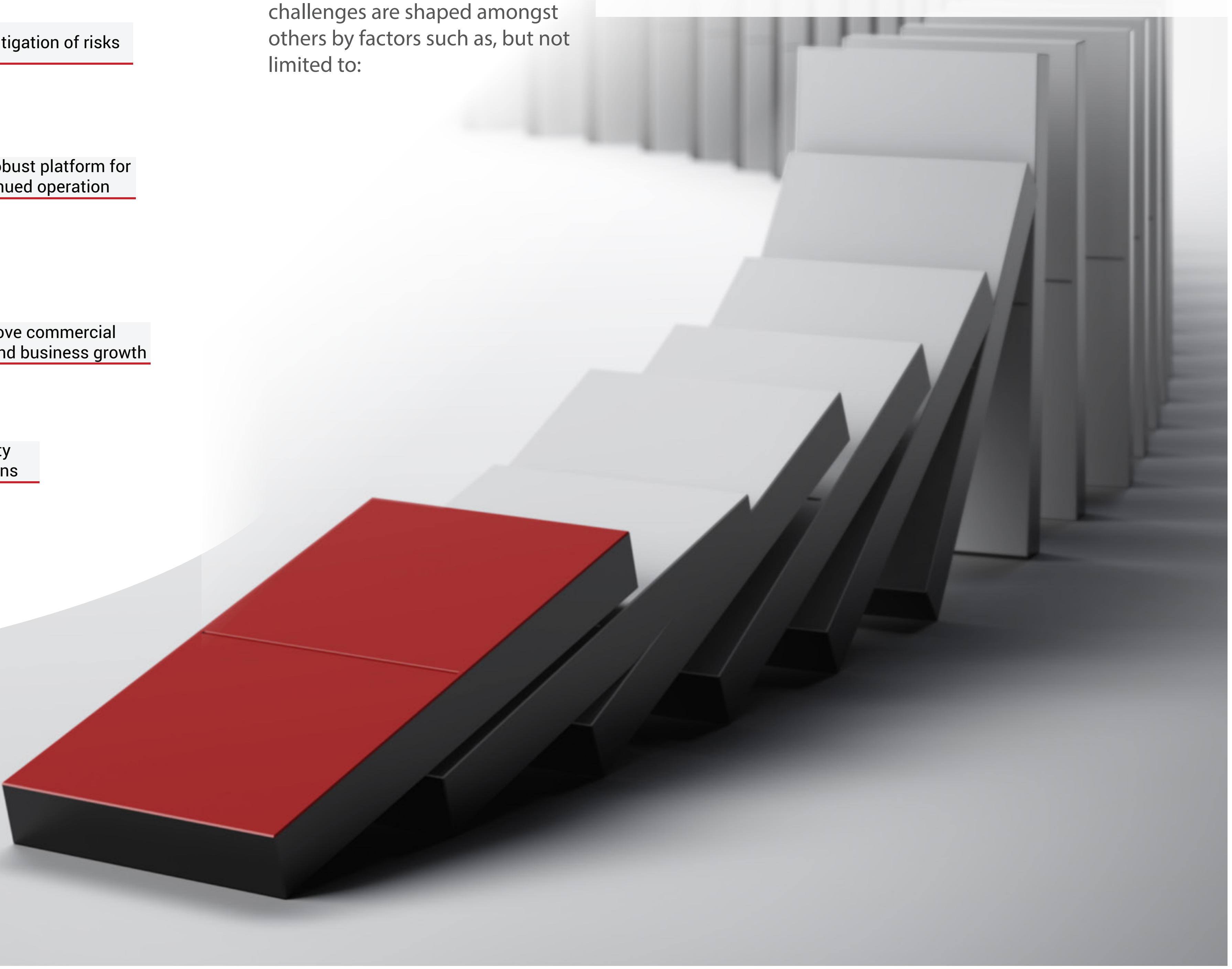
2 SME's leadership not appreciating the value of having continuity programs;

3 Lack of interests into continuity programs as there are no compelling legislation for the SME's to implement continuity programs;

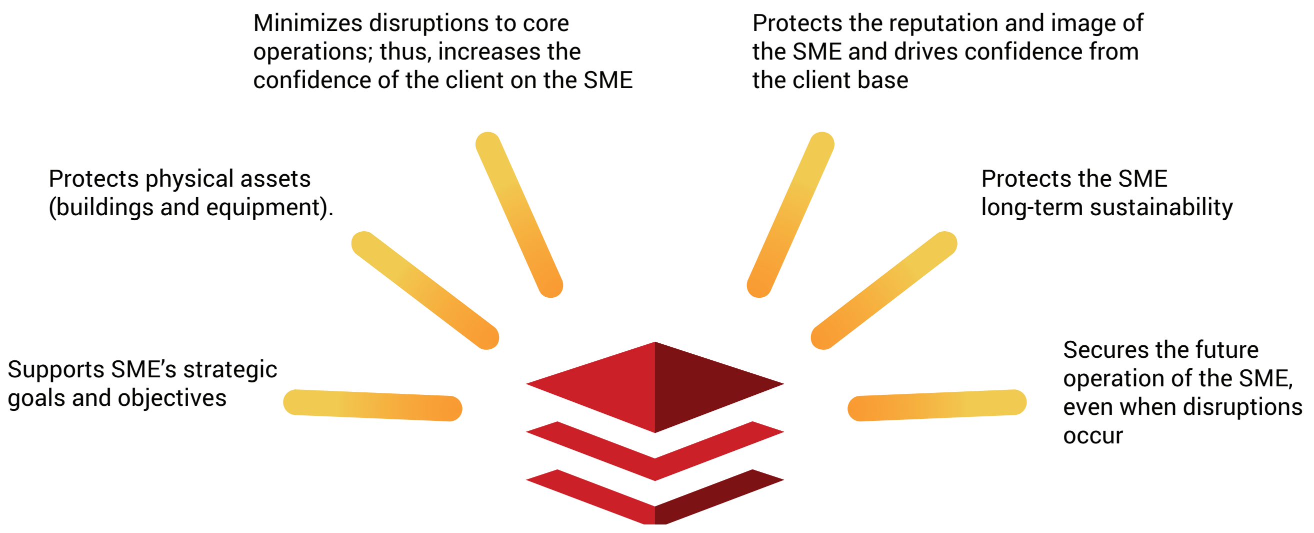
4 Perceptions such as "We have been in business for a long time and nothing has happened in the past. It is possible that nothing will happen in the future, either".

5 A view that BCM is applicable only in "big corporations"; and

6 Business Continuity is only meant to deal with the Information Technology matters and is not applicable to any other parts of the business.



Benefits of implementing BCM by SMEs



Minimizes disruptions to core operations; thus, increases the confidence of the client on the SME

Protects the reputation and image of the SME and drives confidence from the client base

Protects physical assets (buildings and equipment).

Protects the SME long-term sustainability

Supports SME's strategic goals and objectives

Secures the future operation of the SME, even when disruptions occur

How can we optimize the implementation of Business Continuity Plans?

There is then a critical question to ask with an intention to guide and shape the orientation of the SME's Continuity Programs "How can an SME implement and improve its continuity capability in the midst of the aforementioned challenges".

Challenges faced before, during and after the implementation of the Continuity Program present hidden opportunities that could propel an SME to improve its continuity capabilities. There are some critical factors that an SME should incorporate into the continuity program in line with the ISO 22301, being:

Context of the organization

Establish the environment in which the SME operates including internal and external factors that can have an effect on its business continuity plans.

Setting up Continuity Governance instruments

In order to have an effective continuity program in place, a SME should ensure that there are government instruments that are tailor made for its operations in order to guide the program's design, planning, implementation, operationalization, monitoring, review, and reporting. This should be in the form of policy, framework and implementation guidelines.

Interested parties

An SME should establish person(s) or organization(s) that can affect, be affected by, or perceive themselves to be affected by, a decision or activity.

Leadership

The owners of the SME should display their commitment to the implementation of the continuity program through assuring that the program is compatible with the strategic direction of the business, further ensuring that the continuity program requirements are embedded in the business operations, and last but not least to articulate the importance of a continuity program at all times.

Performance evaluation

The organization should constantly measure performance and effectiveness of the continuity program covering the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results.

Embedding continuity culture

In order to build an effective and response continuity program that prepares the SME to deal with any disruption, embedding a resilient organizational culture is crucial.

Maximum Acceptable Outage (MAO)

The time it would take adverse impacts to become unacceptable. This is the same as 'maximum tolerable period of disruption (MTPD)'.

Minimum Business Continuity Objective (MBCO)

The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.

For the SME to ensure that the best value is derived from the continuity program, there is, therefore, a need to implement programs that drive the SME's strategic objectives in an efficient manner to support the critical priorities. The set of defined strategies informed by the Business Impact Assessment should guide the SME in determining the continuity strategy for specific areas such as technology, supply chain, business processes, facilities etc. In determining the continuity strategies, an SME should focus on the ensuring that there is provision for:

- Secure and stable information processing facilities and office locations with adequate physical and environmental safeguards;
- Redundancy in identified information technology systems and applications;
- Maintained data-protection procedures and conducted regular backups of critical applications, platforms, configurations, and data with off-site rotation;
- Cases where external service providers are utilized, there should be multiple suppliers in order to limit a single point of failure in the event of a disaster;
- Constant monitoring of the external service provide continuity capability;
- The monitoring of the key critical business process against the key criticality determinants such the legislative requirements;
- The Formulation and documentation of emergency procedures considering the necessities of life;
- The Identification of an alternate site for the recovery of an operation within an acceptable distance from the primary site of operations.

Business Continuity Standardisation

Whilst acknowledging that BCM is still a new concept in the developing world, implementation of the programme can be simplified without compromising the value embedded therein. Internationally recognized standards such as ISO 22301 provides a base upon which SME can derive the core principles for a robust BCM programme. Core principles defined in ISO 22301 are critical to ensure that the SME is guided from the implementation of the continuity strategies to the training of employees.

Deriving Value from BCM

Implementing a BCM programme is argued essential, however, such does not complete the picture of resilience and continuity. Deriving value from BCM remains the major differentiator compliant SME and resilience SME. Value will be realised once the culture has been embedded into SME's operations, employees are able to manage through an in-depth understanding of their responsibilities towards BCM; and even to a greater degree the SME being able to plan, design, develop and implement continuity strategies that are translated to resilience of the SME operations that conduct achievement of the objectives.

UT THE AUTHOR

PECB

Despite the negligence of many companies towards Business Continuity planning, the ISO 22301 has found application to a substantial number of organization, while leading incident management and founding resilience. Besides this, ISO 22301 courses have contributed to increasing the competence of individuals implementing and maintaining resilience within the organization.

A Senior Manager Business Continuity at eThekwini Municipality of Durban, South Africa, **Justice Nepfumbada** is responsible for driving the implementation of Business Continuity Management, Good Governance initiatives, research as well as stakeholder engagement. Further, he is engaged with the program focused on Critical Infrastructure Resilience and secured critical infrastructure. With extensive experience in Risk Management, Governance, and Compliance, Mr. Justice has worked in numerous projects ranging from the implementation of the National Credit Act within the industry, Information Technology Governance structure implementation, and Regulatory Impact Assessment and Risk Management. Also, Mr. Justice has been a researcher with the National Planning Commission during the process leading to the National Development Plan.

THE GROWING THREAT OF BUSINESS EMAIL COMPROMISE SCAMS

Today's digital frontier can be very much likened to the old days of the Wild West. In this present era identified by the ubiquitous nature of the Internet, cybercriminals are calling the shots; constantly blazing new trails in increasing sophistication in cybercrime and profiting unscrupulously off the backs of unsuspecting victims who rarely know what hit them until it is too late.

These cybercriminals are constantly pushing the boundaries of organized crime and keep on coming up with new ways to expand their business operations and increase profits. They come up with schemes and rackets that encompass almost all aspects of traditional crime including fraud, extortion, theft, hijacking and even blackmail in the digital world; long before law enforcement agencies and security professionals are able to discover and eventually catch up to them.
It is therefore not surprising today, that most of us can now say goodbye to the traditional 419 scam which is slowly fading away into a thing of the past and say hello to the future of a much more insidious form of email scam which employs the use of social engineering, malicious software and computer intrusions, known in the information security community as Business Email Compromise Scam.

Yes, you can forget about the almost extinct forms of traditional 419 scams where you typically receive an email from a window or self styled investor promising you a huge payout usually in the millions of dollars, for your assistance in transferring funds belonging to some deceased wealthy corrupt government official or other important notable public figure.

The format of a typical 419-email scam preys on our vulnerabilities as human beings who naturally have a tendency to help one another by using deception, and playing on our susceptibility of our desire to get ahead in life by offering us a get rich quick scheme.

However, today most of us would spot a typical 419 from a mile away. To say the least, these emails usually end up in your spam folder assuming that you use the services of an email hosting provider with basic spam and email filtering rules.

A recent quite interesting 419 scam of a somewhat cosmic and comical proportion tells the unbelievable story of a Nigerian astronaut who needs $3 million dollars to come back to Earth after being stranded in outer space.

What is a Business Email Compromise Scam?

The FBI defines Business Email Compromise (BEC) as a sophisticated scam targeting businesses working with foreign suppliers who regularly perform wire transfer payments in exchange for large quantities of goods. Formerly known as Man-in-the-Email scams, these schemes compromise official business email accounts to conduct unauthorized fund transfers. According to them, BEC scams have cost US victims nearly $750 million dollars and affected more than 7,000 people between October 2013 and August 2015. Globally, cybercriminals scammed more than $50 million dollars from victims outside of the US.

Business Email Compromise (BEC) crimes overshadow by far all other types of crime. These scams are financially motivated and leverage on social engineering tactics; using various forms of computer intrusion techniques targeting business email in-boxes, resulting in financial loss due to unauthorized transfer of funds into fraudulent destination bank accounts.

BEC Scams Come in Three Different Versions

Version 1

This version which will be a focus during the course of this write up can also be referred to as "Invoice Payment Fraud", "The Buyer Swindle", and "Invoice Modification Scheme"; usually involves a business that has an established relationship with a supplier. The fraudster inserts himself in the middle of the email communication exchange and asks the buyer to wire funds for an invoice payment to an alternate, fraudulent account via a spoofed email. A spoofed email is a fake email assuming the identity of a legitimate entity.

Version 2

In this version, the fraudsters identify themselves as high-level executives (CFO, CEO, CTO, etc.), lawyers, or other types of legal representatives and purport to be handling confidential or time-sensitive matters, and initiate a wire transfer to an account they control. In some cases, the fraudulent request for wire transfer is sent directly to the financial institution with instructions to urgently send funds to a bank. This scam is also known as "CEO Fraud", "Business Executive Scam", "Masquerading", and "Financial Industry Wire Frauds".

Version 3

Similar to the other two versions, an email account of an employee is hacked and then used to make requests for invoice payments to fraudster-controlled bank accounts. Email messages are sent to multiple vendors identified from the employee's contact list. The business may not become aware of the scheme until their vendors follow up to check for the status of the invoice payment.

Invoice Payment Fraud Threat Intelligence

Threat intelligence is simply a situational awareness of a particular type of threat including the techniques and tactics employed by the threat actor. This section will try to explain why I choose to focus more on the threat of "Invoice Payment Fraud" in this article.

Working with clients across the African and Middle Eastern regions, I have come across multiple incidents involving Invoice Payment Fraud scams and have ultimately gathered that this version of BEC scam, is more popular in the MEA region.

This is quite likely due to the nature of the region's business and economic ecosystem, which I dare say, largely consists of the importation or shipment of raw materials and supplies used in manufacturing, agriculture and other forms of small scale processing.

The buying and selling of consumer goods by small and medium sized businesses typically drive these economies as compared to the service-based economies of the more advanced developed countries, which revolve around bigger more established business players. These bigger players from my analysis would be more susceptible to versions 2 and 3 of BEC scams.

Coupled with a lower sense of awareness of the risks of cyber security threats, a lack of basic cyber security hygiene and security practice creates the perfect playing field for cybercriminals who are focusing more attacks via invoice payment fraud scams to the region.

This will be our focus in the next sections as this scam has the highest potential to impact many small and medium sized businesses who fit the criteria for invoice modification fraud. A few of these invoice fraud scams I have worked on recently have involved businesses that have incurred losses of up to $100 thousand dollars within a very short space of time. This however, does not mean that this trend will continue to stay the same in the coming future as things change from a global market perspective.

How Invoice Payment Fraud Works

This is quite a complex sequence of events that only those businesses who have supplier relations and are more familiar with these kinds of wire transfer transactions; can easily relate to and will hopefully understand how the attackers will patiently wait, observe and then strike at the opportune time to scam their victims out of huge amounts of cash.

1 The attackers behind these scams use intrusion techniques to attack email servers that have a weak security configuration and sit man-in-the-middle style intercepting and redirecting messages between buyer and supplier business email exchange in order to score a big payout.

2 Once they are inside a compromised mail server they seek out high-value transactions that are in the pre-order phase. Another tactic these cybercriminals use is usually through malware and phishing methods to get employees to click on malicious links, which are then used to download and install a keylogger to record keyboard strokes on the victim's host.

3 Once the keylogger software has been installed the attackers use a message feedback mechanism to alert them when specific keywords are observed from the victims keystrokes such as 'invoice', 'purchase order' etc. to seek out high-value transactions in the pre-order phase which are moving towards the payment confirmation stage.

4 Usually, in these types of transactions buyers send a purchase order to the seller's business email account after which the seller then replies to the buyer's email with an invoice and payment instructions.

5 Upon monitoring the compromised email account or recorded keystrokes which will obviously reveal the username and password of business email accounts; by recording every single keystroke of the victim's infected computer, the fraudster will try to determine who initiates wires and who requests them.

After figuring all this out, the attacker clones both the buyer and sellers email addresses, usually creating a new address that is slightly different but similar to the company they're targeting, in order to spoof emails that

convince the target that they are dealing with the other legitimate party.

One very important aspect to note here is that they will alter the email return path or return address to redirect the replies to their own attacker controlled email accounts after which they can modify the message and forward it to the then intended recipients.

A Real World Example

An example of the email cloning mechanism used by these cybercriminals would be in the form where say; we have a business email address for a sales person from mybusiness.com, a buyer company dealing in the manufacture of plastic chairs to be **kofi.agyare@mybusiness.com**.

The attacker would register a new email address at a different domain and clone Kofi's business email address to kofi.agyare.mybusiness@mail.com which will be controlled by him and also to which he will receive messages from the supplier company that Kofi is looking to source raw materials from and vice versa.

The attackers are then able to modify the invoice and change bank account numbers, location and SWIFT codes needed to complete the fraudulent transaction. They also modify the payment destination account in the invoice document to a fake destination bank account by stating some bogus reason, such as their accounts are currently being audited or the liking and while sitting in the middle, forward this new instruction to the buyer, who then wires money to the attacker-controlled fraudulent account.

Defending Against the Scam

Businesses should stay vigilant and educate employees on how to prevent being victimized by BEC scams and other similar attacks.

"It's important to know that cybercriminals do not care about your company's size - the more victims, the better".

Additionally, cybercriminals need not to be highly technical as they can find tools and services that cater to all levels of technical expertise in the cybercriminal underground. As the world relies more and more on Web services such as webmail, a single compromised account is all it could take to steal from a business. As such, here are some tips on how you can stay protected and secure:

1
Install and maintain a good anti-virus software and use a third party email hosting company that provides a secure mail infrastructure with email filters to reduce some of the phishing traffic and potential malware infections.

2
It is strongly recommended to use the "Forward" function instead of "Reply" or "Reply All" so you can type the email address of your contact and ensure that the correct address is being used and not the attackers spoofed fake email address.

3
Educate and train your employees. While employees are a company's biggest assets, they are also usually its weakest link when it comes to security. Commit to training employees according to the company's best practices. Remind them that adhering to company policies is one thing, but developing good security habits is another.

4
Verify any changes in supplier payment and destination bank account details by using phone verification as part of a two-factor authentication. Confirm requests for transfer of funds by using known business numbers and speaking with familiar or known verified backup personnel.

5
If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised.

PECB

Addressing such scams professionally is mandatory to mitigate various risks associated to businesses internal network. Further, protecting valuable information is equally important to lower the potential of malware vulnerability. Thus, PECB is continuing their contribution to increase awareness and strengthen IT security through the courses provided on ISO 27001 and ISO 27034 and many more.

ABOUT THE AUTHOR

Mr. Glymin is a network and information security professional with over ten years of experience. His specialties are listed under Threat Management, Penetration Testing, Incident Response, Intrusion Analysis, Incident Handling Web Application Security, Malware Behavior Analysis, Malware Traffic Analysis, Memory Forensics Network & Internet Security, Risk Management, Patch Management, Vulnerability Management Security Operations Management, Industrial Control Systems, Advanced Persistent Threats Organizational Culture, Change Management, and SCADA Security. Further, his specialties have added value to Dell SecureWorks, Global Secure Solutions, Ecobank Transnational Incorporated, and Tandem Networks Ltd. among others.

"THE ANNUAL COST OF **CYBERCRIME TO THE GLOBAL ECONOMY** IS MORE THAN $4 BILLION"

Mark Rutte

IMPROVING PROCESS CONTROL THROUGH QMS

Is quality control really improving internal processes?

The purpose of implementing a process approach aims to enhance the organizations level of effectiveness and efficiency to achieve its defined objectives. Simply put, a process transforms inputs into outputs. This is done seamlessly when the process is planned; plans are executed, checked, and acted upon in order to improve the process. Undergoing through such processes also requires some application of quality management systems to be aligned with the processes within the organization.

Additionally, implementing a process based approach to either services or manufacturing industries helps the development of stability in operations and better management. Managing through preventing nonconformities in processes does help the organization gather better information to where the problems are and how they may be actually fixed. What is more, keeping track of operational activities through a process based approach becomes much easier for the organization as well as for the employees themselves.

Quality Management System, from hereinafter referred to as QMS, is also a risk management tool that helps organizations to achieve its intended outcomes: enhancing customer satisfaction and complying with its legal obligations. A quality management system helps to ensure that business processes are continuously improved upon.

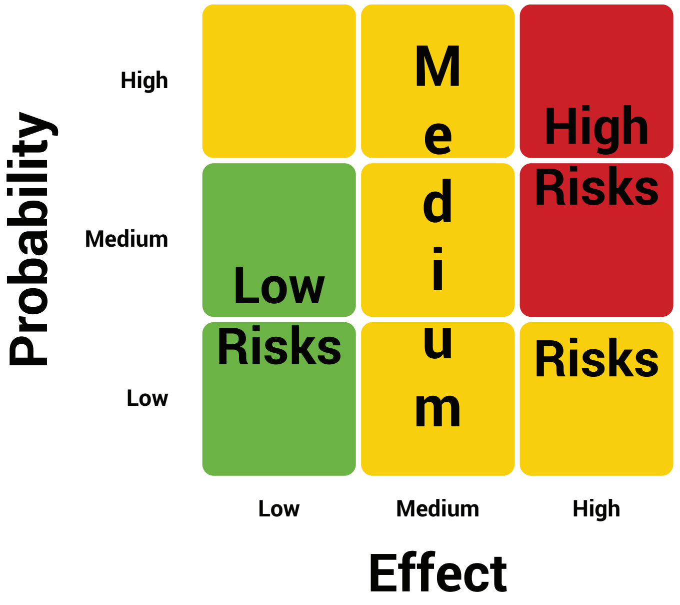
In essence, a QMS is made up of business processes whose final output is product offered or service delivered to the client.

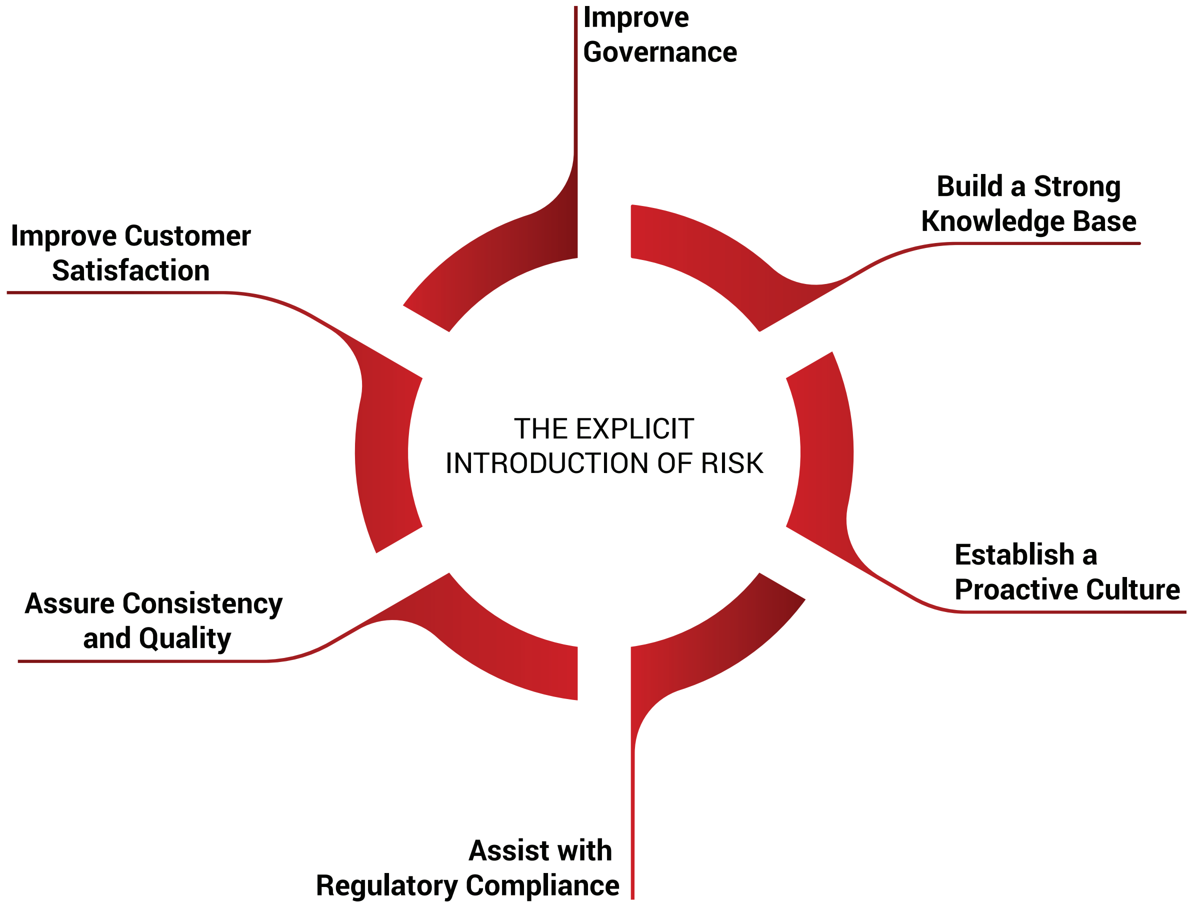
QMS contributes to improving process control because it defines requirements that need to be met via process controls in order to ensure process optimization. Moreover, a QMS is established using the Process Approach via the Plan – Do - Check – Act cycle and Risk-Based Thinking. Further, extra precautions are factored into the processes on a consistent manner.

Differently, the PDCA cycle may be referred to as being the basis of continual improvement, which in process based thinking, becomes crucial. The integration of continual improvement to the benefit of efficiency of processes must follow its process including, reasons for improvement, current situation, analysis, identification of possible solutions, evaluation of effects, implementation and standardization of the new solution, and evaluation of effectiveness after improvement. For all these points, a quality journal is advised to identify, keep, measure, and improve the occurring problems while comparing them to the previous ones.

The explicit introduction of Risk–Based Thinking in ISO 9001: 2015 is the next best thing that ever happened after chocolate and vanilla ice cream! The advantage of this concept in the new standard cannot be over emphasized.

Implementing risk–based thinking helps improve quality control because interested parties requirements are considered and used in line with the context of the organization to plan, and address the risks inherent to the process. Additionally, installing a proactive approach to both the process based operations and organizational culture is a principle of risk-based thinking. Prioritizing risks as much as having an action plan to tackle risky problems should be at the core of implementing a process based approach to improve process controls and eliminate risks.




Improve Governance
Build a Strong Knowledge Base
Improve Customer Satisfaction
THE EXPLICIT INTRODUCTION OF RISK
Establish a Proactive Culture
Assure Consistency and Quality
Assist with Regulatory Compliance

Challenges being faced in Nigeria's stem are two faceted. One is from understanding and implementing the requirements of the standard as a part of the organization's business processes, while the other is from understanding the benefits of being certified by an accredited certification body with audits conducted by competent auditors. Most businesses in this region do not understand that business process controls can be improved through the implementation of QMS. This can be corrected by ensuring that training is provided by competent people and the trainers; being continuously trained and retrained to ensure consistency in interpreting the requirements of the standard. Certainly, certification by an accredited certification body, attributed to a risk – based thinking strategy, can also help optimize the process.

ABOUT THE AUTHOR

PECB

The aim of maintaining a positive attitude towards implementing ISO 9001, as referred to by PECB, is the foundation of increasing quality of operations within your organization. With a direct effect to customer satisfaction, certifying against ISO 9001 would clearly increase your credibility and assurance towards customers. Further, integrating "risk-based thinking" methods, and applying the process approach would build a strong knowledge base, while establishing a proactive culture for improvement.

Currently a Divisional Head of QMS (Manufacturing) at Standards Organization of Nigeria, **Amina Deji** – Logunleko is a Lead Auditor, Implementer and Trainer of ISO 9000, 14000, 22000 and 18000. Her contribution at Standards Organization of Nigeria has been also evident through holding other key positions such as Principle Standards Officer, and Divisional Head of OHSMS, Multi Systems, and IMS. Additionally, her experience extends to being an auditors evaluator for both Oil and Gas industries.

SPECIAL THANKS TO

OUR EXCLUSIVE PARTNERS

PECB NORTH AMERICA

PECB SOUTH EAST ASIA

PECB OCEANIA

PECB NORDICS

PECB UK & IRELAND

PECB EUROPE

PECB UKRAINE

Sedika TECHNOLOGIES

OUR PLATINUM PARTNERS

PECB AUTHORIZED PARTNER PECB PLATINUM PARTNER

ContinuityLink

DigitalJewels
information value chain consultants

OUR GOLD PARTNERS

PECB AUTHORIZED PARTNER PECB GOLD PARTNER

LITAC AFRICA
Certifying Corporate & Business Professionals

KTMC LTD KAIZEN TRAINING & MANAGEMENT CONSULTANTS LTD

SecurCert

BIT
Business and Information Technology

ITpreneurs™
Effective Learning Solutions

KPMG

neam
IT-Services GmbH

NUMERIC TECHNOLOGIES LIMITED

AJL Consults LTD.
RC:1222233

DATAPROTECT
Security is our commitment

analytix

protiviti®

SecuraStar
ISO 27001 EXPERTS

iMACERT

cirosec

WHAT IS HAPPENING IN FEBRUARY

The new updates from PECB come with a considerable number of new course offerings and updates. Facilitating the distinct materials of study, we assure to continue supporting our belief of providing you with qualitative and credible education. With a constant growing number of partnerships, we must highlight the necessity of continuing our personalization journey.

THE NEW COURSES OFFERED FROM FEBRUARY 2017 INCLUDE:

- PECB Certified ISO 22320 Emergency Management Foundation
- PECB Certified ISO 22316 Organizational Resilience Foundation
- PECB Certified ISO 22317 Business Impact Analysis Foundation
- Business and Supplier Relationship Management Foundation
- Budgeting and Accounting for Services Foundation
- Hazard Identification and OH&S Risk Assessment Foundation
- Sustainable Product Design Foundation
- Consumer Product Safety Foundation
- Customer Satisfaction Foundation
- Quality Assurance and Control Plan Foundation
- Accident Investigation Foundation
- Pandemic Plan Foundation
- Root Cause Analysis Foundation
- Finance for IT Professionals

IMPROVEMENTS AND UPDATES HAVE BEEN IMPLEMENTED ON:

- PECB Certified ISO 13485 Lead Auditor (English)
- PECB Certified ISO 27001 Lead Auditor (French)
- PECB Certified OHSAS 18001 Lead Implementer (French)
- PECB Certified ISO 14001 Lead Auditor (French)
- PECB Certified ISO 14001 Lead Implementer (French)

PECB PROVIDES YOU WITH AN ADDITIONAL SET OF TRANSLATED COURSES

Advanced Auditing Techniques
Now available in Spanish

PECB Certified 22301 Lead Implementer
Now accessible in German

PECB Certified ISO 27001 Lead Implementer
Translated to Brazilian Portuguese

PECB Certified ISO 31000 Risk Manager
Also translated to Brazilian Portuguese

PECB Certified ISO 27005 Risk Manager
You may also access this course on Spanish

www.pecb.com

When Standards Matter...