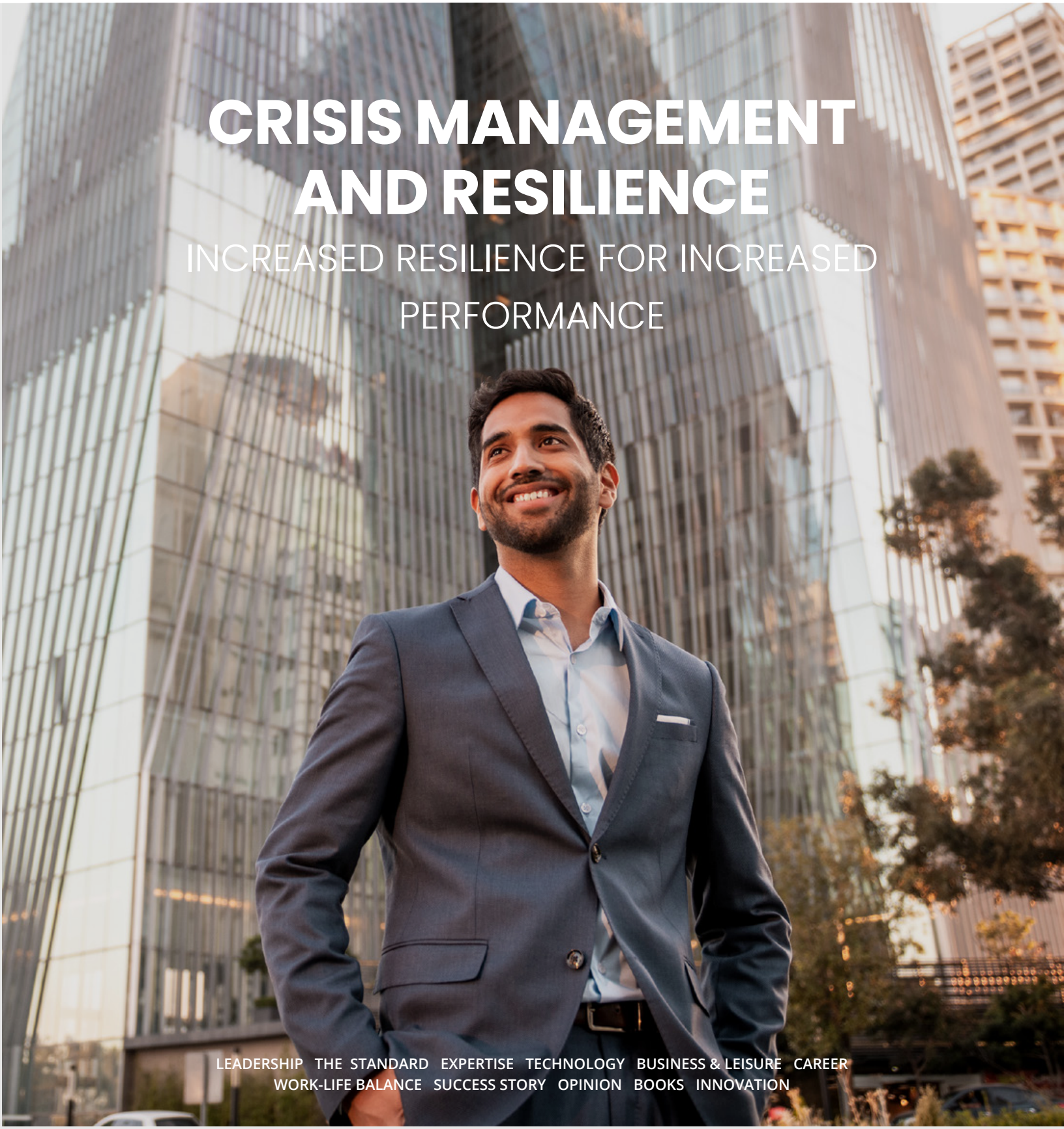
PECB Insights

ISSUE 38 ISO STANDARDS AND BEYOND MAY-JUNE 2022

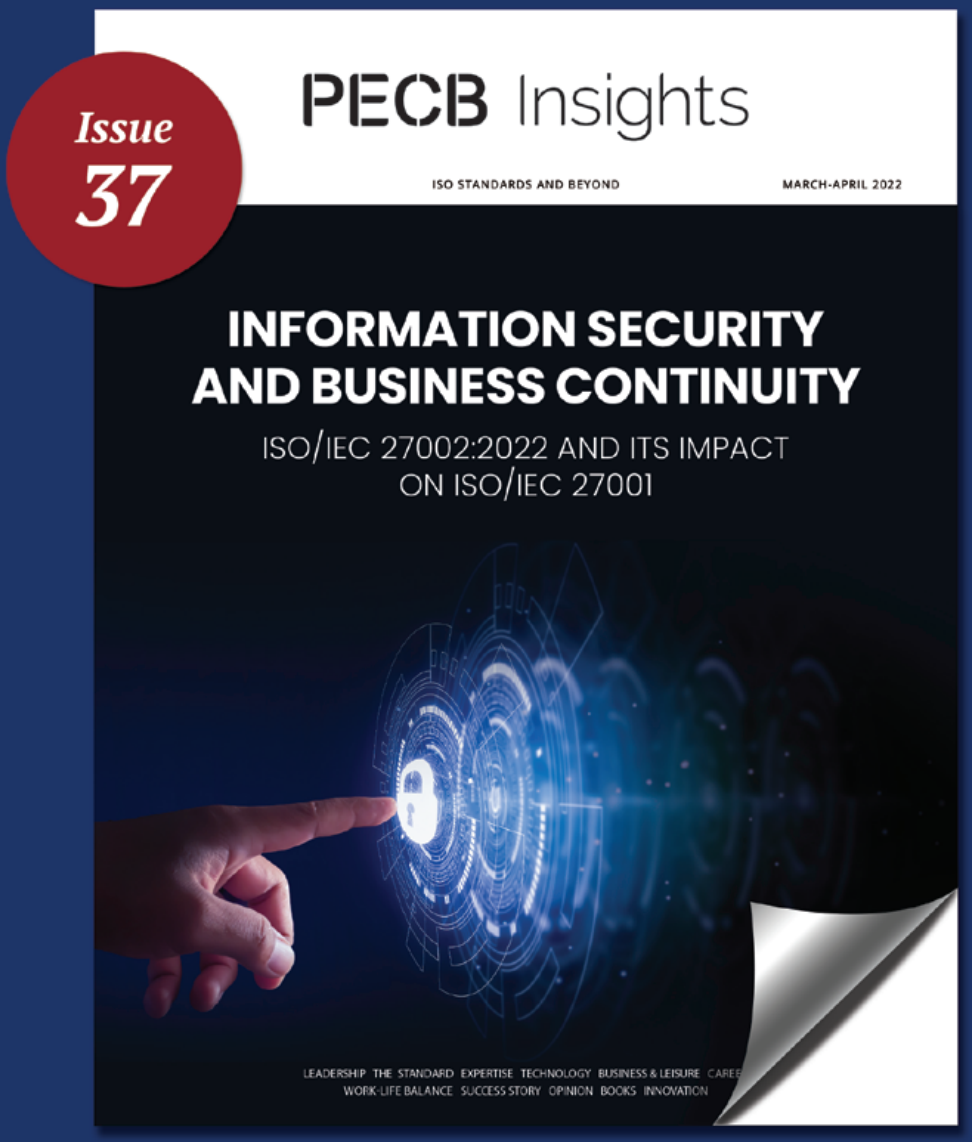
CRISIS MANAGEMENT AND RESILIENCE

INCREASED RESILIENCE FOR INCREASED PERFORMANCE



PECB Insights Magazine

delivered to your mailbox



Subscribe & find out more at

www.insights.pecb.com

In This Issue

> When written in Chinese the word "Crisis" is composed of two characters. One represents danger and the other represents opportunity.

JOHN F. KENNEDY
Former President of the USA

COUNTER-ATTACKS ON CYBERSECURITY

Cyber-attacks are costly, disruptive, and a growing threat to businesses, governments, and society alike. Happily, an arsenal of standards helps stay ahead of the game.

Cybercrime is on the rise. And as we move deeper into the digital age, the era of the so-called Fourth Industrial Revolution, it is also growing ever more sophisticated and severe, with serious consequences. As cyber criminals become more adroit, cybercrime has touched all our lives in one way or another.

Cyber-attacks can range from hacking into systems and social media, phishing attacks, malicious software including ransomware, identity theft, social engineering, and denial-of-service attacks. This is painful both personally and financially, causing untold damage and destruction, as well as leaving society and citizens vulnerable. According to McAfee, the computer security software company, the cost of these cyber-attacks is on the increase, amounting to around USD 1 trillion in 2020.

A GROWING GLOBAL RISK

With the COVID-19 pandemic having further embedded our growing dependence on digital systems, it is not surprising that the Global Risks Report 2022 has yet again included the threat to cybersecurity as one of the growing risks facing the world. Cybersecurity failures, it says, have worsened significantly and threaten long-term prosperity.

But how do we stay one step ahead? Building a good cyber-defence system as well as anticipating threats are key elements in the fight against cybercrime, but neither resilience nor governance is possible without credible and sophisticated cyber-risk management plans. “Cybercrime is both a national and international occurrence that is spreading with great speed, affecting businesses, governments, and society as a whole. The scale and complexity of this criminal activity has far-reaching and detrimental consequences and the situation is blurred as cybercriminals operate, using technical infrastructure, across national boundaries,” says cybersecurity expert

Dr. Edward Humphreys.

> **"Cybersecurity failures have worsened significantly."**

As a result, he adds, international collaboration is essential and International Standards are indispensable for global protection. Dr. Humphreys speaks from his many years of business experience. He is also a senior research fellow specializing in cyber-risk, security, and cyber-psychology research and ISMS innovation studies, and the ISO/IEC Convenor of the working group responsible for the management, development and maintenance of ISO/IEC 27000, a family of standards on information security management systems (ISMS).

SOLUTIONS AND CONTROLS

International Standards provide solutions, he says, enabling organizations to establish frameworks and systems to assess and manage the situation – to protect information, to secure applications and services, and national infrastructure.

The first step in tackling cybercrime is knowing the risks you face and then deciding the controls that need to be implemented to mitigate these risks. Humphreys points to standards such as the ISO/IEC 27000 family, developed by ISO and the International Electrotechnical Commission (IEC), as the de facto choice for any organization wishing to build robust solutions against cybercrime. The suite of International Standards specifies a management system that goes into the risk management process of assessing the risks and then determining the controls needed to treat them.

> **"The first step in tackling cybercrime is knowing the risks you face."**

"There are a range of standards supporting ISO/IEC 27001, such as ISO/IEC 27005 on information security risk management and the ISO/IEC 27003 implementation guidelines," he says. "And there are many other standards that provide technical support for ISO/IEC 27001, for example to secure networks and embed security features into technology, services and applications."

BEING PREPARED

Dr. Humphreys reiterates the need for companies to be prepared and ready to face these attacks. "Cyber-attacks can take place anytime and anywhere, and what is certain is that these attacks are sure to happen but we can never be sure when or where," he says. "Being ready and prepared is an essential business activity for survival. It involves a business having in place a process to be able to anticipate and identify, detect and report incidents, and to analyze these incidents to decide how to respond to them." This all needs to be done in a quick and timely manner to limit the impact the incident could cause.

> **"Cyber-attacks can take place anytime and anywhere."**

So how can businesses be better prepared? Once a business detects the presence of a malicious code attack or a denial-of-service attack, the faster it responds with appropriate security measures, the greater the chance of limiting the spread of these attacks as well as limiting the impact and damage.

And, as Dr. Humphreys says, there are standards that help businesses to become ready and better prepared to respond, such as the incident management standard ISO/IEC 27035, the standard for business continuity management ISO 22301 and the ICT readiness standard ISO/IEC 27031.

COLLECTIVE ACTION

In an already uncertain world, cybercrime can be financially devastating, disruptive to business operations and national infrastructure, as well as affecting citizens and society. For example, an attack on one part of a supply chain may spread and disrupt and damage other parts of the chain. In order to foster more secure and resilient cybersecurity systems, Dr. Humphreys says the management of a supply chain is a good example of where collective action is needed across all parts of the chain to keep it secure.

"Again," he says, "there are standards that help with supply chain security, such as ISO 28000 and ISO/IEC 27036. Collective action is also needed in various scenarios that involve business relationships and communications with other organizations. There is a group of management standards that will help with building resilience to counter business disruption and ensure survivability and system of governance. These include ISO 22301 (business continuity management systems) and ISO/IEC 27001 (information security management systems) and ISO/IEC 27014 (information security governance)."

With the growth and dependency on connectivity for business, the infrastructure that supports it, and the use of the Internet and mobile devices, there is an even greater need for system security and resilience. Dr. Humphreys acknowledges that standards need to evolve to match the rapid advances in technology. "The third edition of ISO/IEC 27002, for instance, was published in the first quarter of 2022. This high-profile standard deals with information security controls and has been updated to match the advancement in technology, business developments and practices, and new laws and regulations."

In 2021, he adds, there were many other developments in standardization, including Internet of Things (IoT) security and privacy, big data security and privacy, artificial intelligence security and privacy, and biometric information protection.

All these are complemented by recent technical specifications such as ISO/IEC TS 27570, which provides guidance on smart city ecosystem privacy protection, and ISO/IEC TS 27100, which specifies how to create or refine robust cyber systems to protect against cyber-attacks. The complete ISO/IEC 27000 family of standards and these technology-focused specifications are the foundation for building and managing a secure future.

Why Organizations Are Moving Towards a Zero-Trust Model?

BY ROHIT KUMAR

Organizations, for a very long time, have been struggling to balance security and openness to run the business efficiently.

The issue has been put to trial when organizations started using a large number of workforces to modernize business, once again when organizations had to use offshore resources to reduce costs of development and maintenance of the enterprise, and finally when they had to allow the remote working based on the global developments of the past two years.

Also, the past few years have not been kind to organizations, who must constantly evolve their business practices to be more agile and dynamic. Organizations rather than allowing only a few sections of the users to work “outside the perimeter” must now implement the open-access architecture, as practically the perimeter has vanished.

This is the slow change that was foreseen by few analysts over a decade ago and has been the talk of the visionaries for a long time now.

Introduction to Zero Trust (ZT)

Zero Trust is a set of cybersecurity principles used to create a strategy that focuses on moving network defenses from wide, static network perimeters, to focusing more narrowly on subjects, enterprise assets (i.e., devices, infrastructure components, applications, virtual, and cloud components), individuals, and other non-human entities that request accesses to resources.

These principles are designed to prevent data breaches and limit internal lateral movement, in case of an attack from an external threat actor or malicious insider.

Before we proceed further, there is a basic concept we must be aware of. The term Zero Trust means Zero "Implicit "Trust.

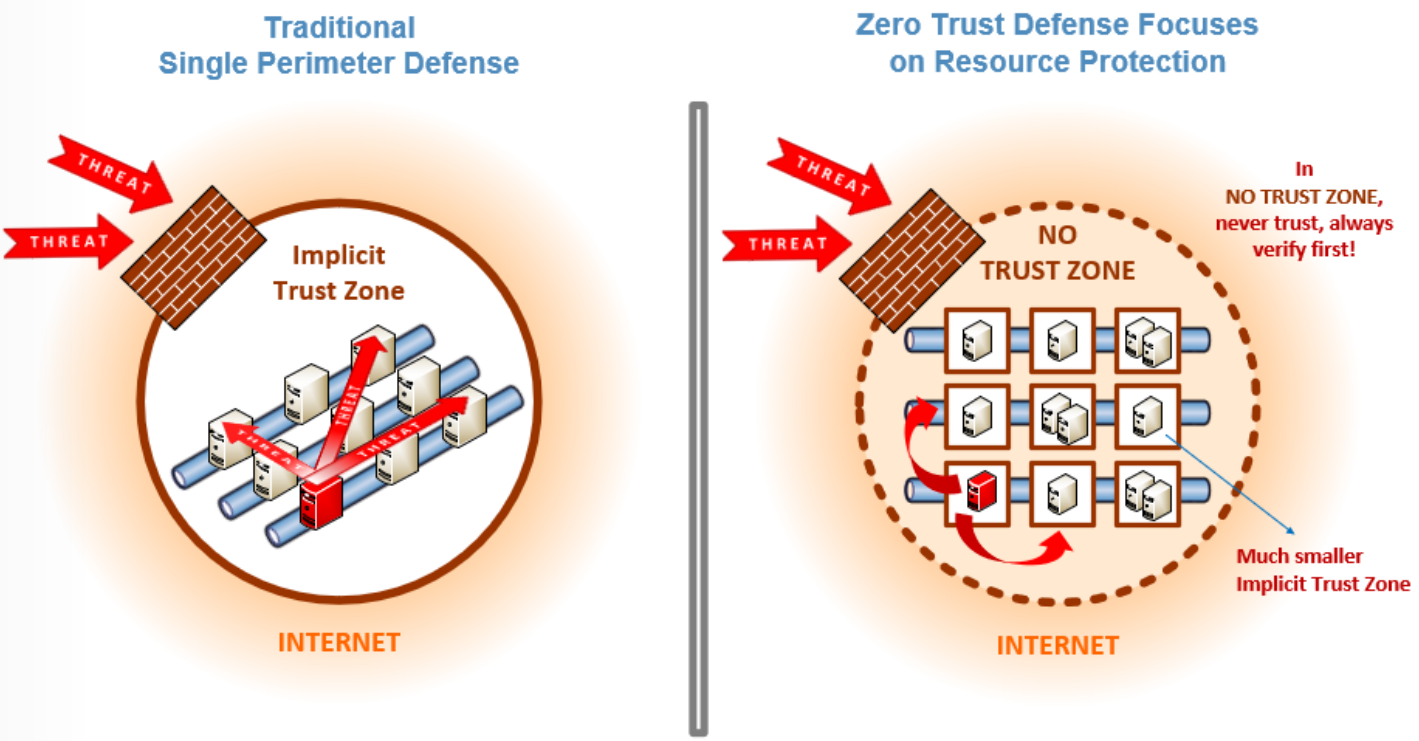


Fig: Traditional vs Zero Trust Defence Mechanisms

Image reference: https://www.nist.gov/image/zero-trust

This is important for understanding what the analysts and research teams imply in their discussions and it is one of the issues that we will discuss later in this article. For now, let us have look at the tenets of ZT and what does it really mean for businesses:

- Principle 1 – All entities are untrusted by default
- Principle 2 – Least privilege access is enforced
- Principle 3 – Comprehensive security monitoring is implemented

In accordance with NIST, the following principles are the technical extensions of the basic principles mentioned above:

1. All data sources and computing services are considered resources
2. The enterprise ensures all owned systems are in their most secure state possible
3. All communication is secured regardless of network location
4. Access to individual enterprise resources is granted on a per-connection basis
5. User authentication is dynamic and strictly enforced before access
6. Access to resources is determined by policy, including the observable state of the user, system, and environment

Now, these might not look very complicated, and that we have been doing them for a long time, but you must remember that these policies must be implemented with a business use case as the driving force and basic security parameters in mind, as in you would not spend $100 to protect a resource that is worth $50. Essentially, context matters and we must carefully design the enterprise architecture so that we can have complete information about resources, users that are trying to interact with it, activities that are done in said interaction, and all related policies that are implemented to inhibit all users that are not supposed to access the resource in the first place.

The evolution of Zero Trust, essentially, is the natural progression of security posture management for organizations. This is the agile way of handling security as it focuses on users, assets, and resources rather than perimeter, because traditional mechanisms were not dynamic enough for an organization to function effectively and securely. It has been an extreme pleasure to see that organizations have become more aware of the fallout from security breaches, and thus, actively discuss security requirements with business teams. Zero Trust Architecture (ZTA) has been in the making for over a few decades now and will continue to evolve based on the requirements and risk appetite of organizations.

As previously mentioned, we must pay extra care to the *implicit* portion of the Zero Trust. This, simply put, helps us define the portion of the resources that can still allow access to the users based on the previously established trust. This, again, paired with the risk appetite of the organization usually drives the use case requirements of the organizations. Thus, they must have a detailed risk analysis of resources, to derive inherent risks of components that make the enterprise applications. This will help organizations to better allocate time and efforts to have continuous diagnostics and mitigation plans for attacks on resources.

Now, this brings us to a very important portion of the discussion. Continuous monitoring, PKI, IAM, SIEM, UEBA, network micro-segmentation, etc., are the usual terms that are thrown across, and somehow, we are not able to make the impact we thought that we would.

These have been around for a long time now, so what are we trying to achieve here? We are really missing the term context in these discussions, which can help us better drive the message home. With adequate context, organizations would be able to better decide if a user; is trying to access the application as a normal or as a privileged user, is executing commands and actions that follow their usual behavior, is permitted to execute the commands from a network or geolocation they are currently present at, has enough proof to prove that they-are-who-they-say-they-are and the organization has no proof to believe otherwise. The details to which an organization should follow can be derived from industry compliances that are binding to the organization. With these additional contexts, now the situation might seem complicated.

There are no two ways that an organization must do things to get it right. Usually, it is just a matter of creation and deployment of the security policies that would help organizations to be a bit more proactive rather than reactive as organizations have been on this path for a long time now and unknowingly majority of them have already completed the heavy lifting. We should now delve a bit deeper to understand why ZTA is the best refuge for security teams, in the era of constant change.

- **Choice of security methodology:** Organizations can pick and choose from a variety of ZTA approaches, which suits them best, as well as which can be implemented without any changes to the business flows (with obvious changes to the security flows). This is needed as any major disruption in the current business flow can cause more issues and can lead to resistance from the management teams, ultimately leading to the non-success of projects. A full ZT solution will include elements of all three approaches, i.e., enhanced identity governance driven, logical micro-segmentation, and network-based segmentation. These decisions about which approach best suits the organization are usually driven by the use cases that the organization wants to cater to, their

existing business, and security policies.
This presents a great opportunity for organizations to better adopt a framework with the least resistance from business teams.

- **Excellent user experience without compromising security:** Usually it is tough for organizations to balance the security with openness of the resources, which usually causes friction once new security measures are introduced. However, the framework allows organizations to enhance user experience, in the same way as the introduction of passwordless logins, while simultaneously allowing security teams to be proactive in their detection of user's network and geolocation, as well as permissions to log in to resources with desired rights on respective resources.
- **Customer and Business data protection:** With the definition of data as a resource being ingrained in the principles of ZTA, it finally receives the attention that it deserves. This helps organizations to have better knowledge and control over the data being handled, allowing them to create a detailed map of data, their types, their custodian, their retention policies, etc., and tying all of them back to a user and their activities over them. This holistic approach of handling data along with identities, again, has been in the making for the past couple of years, giving rise to data access governance which can complement audits of users' access to other resources.
- **Detect breaches rapidly by gaining greater visibility of enterprise traffic:** This may seem like a regular activity for an enterprise, but the visibility that the security teams needed in the network traffic had been blurred by the implicit trust zones that existed in previous modules. This usually led to difficulty in understanding if their trusted user is malicious or not, if service accounts created for applications were being used by a person or not, whether a user's location and activities were consistent with the past behavior or not, etc. Discussions of these parameters, along with the availability of logging from last-mile resources are helping organizations to have a holistic view of resources spread across the enterprise and defining detective and corrective actions for breaches.

There are various firms that have created solutions for ZTA methodologies, which can cater to the security requirements of hybrid infrastructures as well. The recent increase in the adoption of cloud services has also led to a host of solutions that can dramatically increase the reach of security teams, without needing costly deployments that used to take years. This has not only reduced the complexity of the implementation of security policies, but also eliminated security product fragmentation while reducing the number of trained resources needed to manage the complete infrastructure. ROI, on these solution deployments has, thus, been generally positive (within months of deployment), allowing the business team to pay proper attention to the security team's requirements.

Is it just another buzzword?

Zero Trust is not just another buzzword in a never-ending list of tech trends. When Zero Trust principles are implemented in any environment, it does lead to minimal exposure to cyber-attacks, higher continuity of critical processes, increased and cost-effective compliance, and a 'future-proof' architecture that is agile enough to keep up with businesses' requirements.

ZTA principles have allowed security teams to be abreast with business requirements and act as a support mechanism to businesses rather than a deterrent. Lesser fragmentation in policy implementation, lower deployment costs, faster implementation, increased policy coverage, increased ROI, etc., are some of the pointers that are helping security teams to drive the conversation, rather than living in constant fear of attacks and exposures.

All good things come with associated snake-oil sellers and their fake promises. For them, ZTA is a product that is the answer to all the "hacks", which only they can make.

We should also be aware of the term "Pure ZTA" implementation, which can be twisted to sound that there is only one right way to reach the destination of ZTA and all other approaches are meaningless. The idea is to make you aware of the situation and firms that are disingenuous in their messaging and often use loosely-coupled implementation approaches of ZTA to cause confusion. Even though the terminology and some of the concepts might feel new, organizations have been on the path of implementation of ZTA, without even knowing it. Some of the examples can be; the implementation of Data Access Governance, UEBA, context and attribute-based authentication, etc. These, again, have been the priority for many organizations for the past few years now and security teams have been gearing towards them.

This is the natural evolution that security policies, for any organization, and the primary reason it has so many routes, is because these all lead to the same idea of reduction of the trust zone that a system or a person enjoys within the enterprise environment.

Technically, ZTA is just a control plane working on the data plane to create a very limited implicit trust zone. This would, thus, allow organizations to have a unified

policy for Data Access, PKI, IAM, SIEM, etc., across all the resources, centrally created, deployed, and managed. These systems can be complemented with threat detection, remediation, and threat intelligence solutions, which can provide additional context to security teams and help them identify threats faster, minimize false positives, and reduce the time needed to respond to attacks.

However, ZTA, just like other principles, does have some drawbacks that an organization must be aware of:

1. **Subversion of ZTA Decision Process:** If the system owner does remove a system before policy enforcement, the systems would continue to work and operate outside unified policies. This will cause a blind spot for security teams as it might not be possible for them to exercise direct control over these resources. Thus, it is always suggested to have continual audit of resources and record any configurational change made to them.
2. **Opaque Network flow:** There are many network communications that do not allow deep packet inspection, which can obfuscate the attacker's communication with resources.
   The issue can be exasperated if devices being used are not owned and managed by internal IT teams, who can apply agents that can help teams to have visibility into the network traffic.

This can be mitigated with the help of analysis of metadata related to network flow, which can provide context to detect attacks on resources or any other malicious communications.

3. **System and Network information storage:** Storage of information system, network, and resources are very important as it is needed to run the enterprise seamlessly. However, these become the easiest target of attackers, and thus, must be protected as valuable enterprise data, which comes with the associated access governance policies.
4. **Authentication issues:** There are two aspects to authentication issues that an enterprise can face, the first being stolen credentials and insider threats, and the other being the usage of standard authentication mechanisms for APIs. These issues exist even in other security principles, however, some of these issues can be easily mitigated with the use of modern IAM policies like passwordless, context, and attribute-based authentication. On the other hand, extensive use of automation, which in turn depends on APIs, can cause lenient authentication mechanisms to be used, like the use of API keys. These can be exploited by attackers who can use these keys to interact with resources with higher privileges and far less scrutiny.

ZTA is not the silver-bullet that organizations could use once and conclude the activity.

This is an evolving journey that requires organizations to take definitive steps to understand the use case at hand and best-suited methodologies that can be chosen for them, audit their systems to understand effectiveness, coverage, and changes that are needed to make process flows streamlined which are in compliance with business requirements.

Organizations have this golden opportunity to finally bring two sides of the coin together by working in harmony, where the security teams allow business teams to access all resources that they need, from places that they are designated to access from, after irrefutably proving their identity, and not spilling this trust to any other resources, essentially, keeping infrastructures safe from inherent harms of opening up.

Rohit Kumar
CISSP, MSc – Cyber Laws and Cyber Security

Rohit has over 12 years working experience with IAM and ZTA methodologies and is currently associate with EY as solution architect for emerging technologies. He also has working experience on application virtualization, server virtualization, DevSecOps, and has worked with customers in various domains like BFSI, education, Oil and Gas, healthcare, etc.

How Does the Implementation of ISO 22301 and ISO 22316 Affect Your Organization?

BY CARLOS FLORES ROCA

The implementation of ISO 22301 – Business Continuity Management System (BCMS), ISO 22316 – Security and Resilience and Organizational Resilience (OR), can be adapted into any type of organization, regardless of the size or line of business, and it is imperative for an organization to prosper in the long term. Every organization must aim to be more resilient. Considering that currently every organization operates in a more demanding environment, organizations must obtain competitive advantages by offering services or products continuously, and controlling disruptions in their production or business chain.

Said standards provide the guidelines, in order for organizations to grant their services or products continuously, with a focus on preventing disruption events in critical business processes.

Currently, there are companies that have not implemented a BCMS or Organizational Resilience, therefore, having an impact caused by a disruptive event may not leave them in a good economic position, meaning that the recovery capacity often occurs with excessive time. That is why the establishment of BCMS and OR must be a priority.

Important points that the organization must take into account when implementing ISO 22301 – BCMS and ISO 22316 – OR:

1. Analyze the needs of the organization (analysis in the internal and external context), as an important pillar to establish the direction of BCMS and OR within the organization.
2. Analyze the needs of the interested parties.
3. Emphasize establishing policies, which will allow the organization's collaborators to align them towards the same path, granted that they are established by the strategic direction of the organization.

4. Emphasize defining its processes and structuring how the organization will support and maintain the BCMS and the OR. Likewise, establishing a team of collaborators that will fulfill certain roles and responsibilities within the scope of BCMS.
5. Leadership, focused on all collaborators of the organization as support to the BCMS. Similarly, resources must be allocated to maintain BCMS and OR on an ongoing basis.
6. More effective communication between all collaborators and interested parties.
7. Define objectives, goals, and indicators, which must be monitored and evaluated in the performance of BCMS.
8. Additionally, when implementing ISO 22316 – OR, the following must be taken into account:

   a. Organizations must define an agile and flexible corporate governance and communication scheme, defining clear communication channels, responsibilities, and work under a process approach. In this context, an adequate level of resilience contributes to the ability to anticipate and address risks and vulnerabilities.

   b. Maintain organizational resilience holistically. Carrying out a risk assessment from a holistic approach, consolidating a culture of resilience, and having as its main axis the context analysis of the organization.

   c. Establish a Strategic Organizational Resilience Committee, responsible for analyzing and making decisions at the highest level, they identify the most resilient scenarios, determine the most critical actions and initiatives, and the ability to adapt with the least negative impact.

Incorporation of BCMS in the organization

BCMS and OR are adaptable and scalable to all management systems that the organization implements, considering that all management systems aim at prevention, based on the risk analysis integrated into business risk management. Under this scheme, business continuity is reinforced, considering profitability for the organization's shareholders as a premise.

For this adaptability of BCMS and OR, the organization can use the methodology based on the Deming Cycle (PDCA).

Business Impact Analysis (BIA) role in organizations

The first action is to carry out a good context analysis of the organization. Aligned with said analysis, the organization must determine the types of impact in relation to certain risks identified in its critical processes. Likewise, implementing BCMS and OR implies the development of specific plans and procedures to control the types of incidents, impacts, and the respective levels of risks.

The preparation of BIA must establish:

1. Criteria that determines the maximum acceptable recovery time (MTPD – Maximum Tolerable Period to Disruption), in order to provide continuity to services and products to customers.
2. Define the recovery time objective (RTO – Recovery Time Objective).
3. Business continuity plans, based on the recovery of critical activities defined by the organization. Said plans must be flexible in the face of any eventuality and must allow continuity of service in an objective recovery time.

Organizational Resilience and Risk Management

The vast majority of organizations have an implemented risk management system, therefore, the adaptation to a new framework defined in the ISO standards has to be compliant with the principles or models of the Organizational Resilience, and must be adopted and adjusted as strategic support in the recovery plan of the organization, in order to provide continuity of operations and critical activities of the organization.

Based on the resilience model implemented by the organization and the maturity level of the risk management system, gaps and activities or actions must be determined to consolidate the resilience model within the organization. As such, to achieve greater integration of resilience in the organization, it is imperative to adopt crisis management, business continuity, risk management, and change management, hence why we must periodically analyze our context, taking into account technological advances, demographic changes in the organization's operations, political framework, etc., and thus, be able to preventively identify improvement actions to address the various situations or scenarios in order to establish controls that avoid disruptive events.

Benefits of implementing BCMS and OR

1. Generate trust and positive expectations for your stakeholders, customers, and shareholders
2. Help meet the strategic objectives of the organization
3. Increase your reputation with your stakeholders and customers
4. The organization remains resilient in the context of the organization
5. Helps to meet business objectives, supported by BCMS and OR
6. Protects the entire financial system, by identifying benefits and being prepared for any disruption that occurs in the process
7. Identifies vulnerabilities and threats to the critical processes of the organization and is able to control them proactively

Conclusions:

1. A BCMS seeks to determine the threats that could affect or generate a disruptive event, with which the organization must implement continuity plans to continue operating.
2. In a BCMS, plans or procedures must be developed in line with the context analysis of the organization.
3. Launch ongoing exercises to validate business continuity plans and measure their performance within the scope of BCMS.
4. In order for business continuity and operations to be maintained over time, it is necessary for the organization to incorporate business continuity into its organizational culture.
5. The organization should benefit from a structured approach to resilience, based on the competitive environment that currently unfolds.
6. Organizational resilience is closely linked to BCMS, where continuity plans and disaster recovery plans are established, all supported by the development of the BIA, risk analysis, and strategy development.

Carlos Flores Roca
CEO of Grupo Concepta

Carlos is an Industrial Engineer, Master Business Continuity ISO 22301, Master Business Continuity Planner (MBCP), Member of Business Continuity Institute (MBCI), Business Continuity Maturity Model (BCMM), Certified Business Continuity Lead Auditor NFPA 1600 (CBCLA), Certified Risk Management Professional (CRMP), and Cyber Resilience Professional (CCRP), and a Lead Auditor and Lead Implementer ISO 22301. He is an approved instructor by the Disaster Recovery Institute International, Professional Evaluation and Certification Board, as well as an international certification auditor and university professor.


10500
20100

Jacob McLean's Success Story

Kaizen Training and Management Consultants Limited (KTMC), located in Jamaica, in the Caribbean, has been a proud partner of the Professional Evaluation and Certification Board (PECB) since 2014, in the capacity of a Reseller. As a Principal Consultant and a Certified Trainer with PECB, I have seen and experienced exceptional growth and development as an individual and have seen my company grow to the highest level of professionalism and excellence through the association with PECB.

My first PECB class in 2014 consisted of just two participants, however, through extensive marketing and personal selling and the spread of good words by our satisfied customers, we saw steady growth which peaked in 2018, when I was awarded the PECB English Language Trainer of the Year.

Success has come because of significant factors. Included among these are the credibility and prestige of the PECB brand, the support from the PECB marketing department, excellence in training delivery resulting in repeat business, and passing on of the word about customer satisfaction obtained.

Without doubt, PECB's offerings rank highest among competitors within the markets that we operate in. Not only are training materials at best practice levels but PECB's emphasis on continual improvement ensure that clients are assured of getting cutting-edge materials that meet their training needs and enable them to be competitive and remain satisfied.

When I tell participants at the end of a training session that they can immediately start implementing what they have learned, and they get to see results themselves, word gets around. The PECB trainings that I offer have been the door opener for numerous participants, including young university graduates who needed to demonstrate that they can immediately add value to prospective employers.

One strategy that I have been able to use successfully was the offering of payment plans to young graduates who could not afford to pay upfront for their training. The in-demand courses that this strategy was particularly effective in, included ISO 45001 and ISO 9001. By offering these plans, I was not only able to attract more participants but I was able to enhance the life chances of individuals who would hopefully remember and create a multiplier effect, thereby, benefitting society as a whole.

The success of participants on the job has also been a key factor in giving my company a good reputation. Armed with cutting-edge competence, knowledge, skills, and appropriate behavior, participants have been able to quickly make their place, justify added value to employers, and become upwardly mobile.

PECB has been consistent in offering strong marketing support involving the crafting of promotional materials and co-branding relevant to my geography and context. This has helped greatly in attracting clients, as it leaves my company standing as a true partner of a highly successful global company, by instantly creating a positive perception in the minds of potential participants, which then, I am able to deliver those expectations in reality through a first-class session that meets their needs.

With the best training materials in the world, without the ability to effectively impart knowledge, there would be no success. From the outset PECB offered me the opportunity to achieve the kind of success that I had always longed for, which is being able to develop my personal competence and facilitate the onward development of competence in others. In the first case, the opportunity to self-study and gain a wide range of credentials, enabled me to leverage my many years of experience working in diverse fields such as risk, quality, environmental, business continuity, health and safety, and compliance management.

I enjoy the delivery of knowledge. My enthusiasm and passion as a trainer come through and my clients know that I am committed to their success. It is never about remuneration; it is always about making myself proud, representing PECB well, and gaining the satisfaction of a job well done. I believe in excellence, defined by me as being my best in what I do.

I have been able to venture into disciplines in which I had limited knowledge such as; information security, records management, anti-bribery management system, and supply chain security management. Currently, I am certified to train in the following standards:

- ISO 9001 Lead Auditor and Lead Implementer
- ISO 14001 Lead Auditor and Lead Implementer
- ISO 22301 Lead Auditor and Lead Implementer
- ISO 31000 Lead Risk Manager
- ISO 37301 Lead Implementer
- ISO 45001 Lead Auditor and Lead Implementer

Although I have gained credentials in a number of other standards, I have not sought certification to date in a number of them, and in one instance, I have surrendered a credential. Acting with integrity in keeping with the PECB Code of Ethics is important to me as it resonates with my core values.

Like most businesses, KTMC has been severely negatively impacted by the pandemic. Notwithstanding, we have managed to continue to achieve success though at a lower level compared to our highest achievement in the past. Currently, KTMC is a Silver Partner, not where we would like to be, but nevertheless, still rearing to go and prepared to deliver value to our customers.

Anyone in the know would realize that a key driver that has enabled PECB to be at the leading edge is innovation. This is not limited to technology but also includes the creation of new course offerings. The latest certification that I have obtained is ISO 37301 Lead Implementer. Having become certified based on my years of experience in the discipline of compliance management in major corporations, my company was able to offer training services at the Introduction and Lead Implementer levels to an international client.

I will shortly be doing the ISO 27002 Lead Manager training course, another innovation by PECB, and this too will enable my company to be able to offer training and/or consultancy services in this very much in vogue discipline.

The drive by PECB to offer objective-type exams in various management system standards, a continuous improvement initiative, will ultimately enhance the marketability of training courses, as it will add a new selling point. The upgrades to the PECB platform and technologies in use also provide me with an incentive to keep abreast with the technology in use, and therefore, to remain relevant.

The overall support provided by PECB includes webinars which are offered once a month. These have proven invaluable in my further competence development and enlightening me on current trends in various disciplines. Equally value-adding are the conferences that PECB organizes throughout the year.

Success invariably comes with challenges. Among the many possibilities are competitors and the temptation to lower standards in order to gain even more success. Numerous PECB competitors have sought to do business with KTMC, however, having achieved success with PECB, it would be disingenuous to seek to partner with others whose track records cannot be vouched for. The incentive offered is usually of a financial nature, however, this should never be the deciding factor in making choices. PECB has proven to be a reliable and dependable partner that is interested in its Resellers. This, among other factors mentioned, has engendered loyalty and commitment.

PECB's devotion to the highest industry standards has had the most positive effect on me personally. The organization does not cut corners and does not compromise on quality. This means that the Reseller that wants to be in step must do likewise. In this regard, the PECB Code of Ethics, referred to above, is a motivation to stay on the "straight and narrow" road to remain in alignment with the organization.

The future of training is being determined and shaped by current events, including the pandemic, which is not over yet. Other factors likely to severely impact negatively include the strong possibility of global food shortage, inflation, and a possible worldwide recession. The ultimate test of resilience is not just survival but the ability to come back stronger with the motivation to overcome adversities. Whilst no one knows the future for sure, there are enough markers that indicate that there is a reason for caution and to have in place effective business continuity measures.

Having a partner such as PECB is a key factor to success and so is the determination and will to succeed, the thirst for knowledge, and the development of competencies that are relevant to the era that the world finds itself in. Business impact analysis, risk assessment, and the development of mitigation are critical components in the professional's toolkit. Likewise, is the willingness to recognize and grasp opportunities as they arise. Balancing the focus on these is a true indicator of future success, despite the gathering clouds on the horizon.

Prepared by, Jacob McLean, Managing Director, Kaizen Training and Management Consultants Limited (KTMC).

DARQ Age is Here

BY JOSE ANTONIO COSTA

DARQ, a term coined by the business consultancy Accenture, stands for **D**istributed Ledger Technology (DLT), **A**rtificial Intelligence (AI), Extended Reality (XR), and Quantum Computing (QC). It represents a new group of powerful and emerging technologies that when combined and boosted by the evolving telecommunications' technologies (5G/6G), will leverage the development of vast and innovative solutions.

Regardless of some of the technologies themselves being in existence for quite a while, the way in which they can be applied and used together has evolved, creating opportunities and threats to what the post-digital world may look like.

As more organizations have been moving forward with the digital transformation, soon it will not be considered as a business advantage, opening space for the post-digital world. More mature markets will demand new highly customized services and products and organizations will compete to fulfill the individuals in every aspect of their lives.

DARQ in a Nutshell

1. Distributed Ledger Technology

Distributed Ledger Technology (DLT) is a distributed decentralized peer-to-peer digital system for recording transactions between parties in multiple nodes simultaneously. DLT deploys cryptography and consensus mechanisms to allow participants to share an immutable replica of the same ledger. A subset of DLT implements smart contracts which are simply programs that run on the DLT when certain conditions are met.

DLT, including Blockchain technology, is on the brink of adoption by several industries leveraged by the advantages this technology offers, as shown in Figure 1, such as increased security, immutability, tamper resistance, and decentralization, therefore, responding to an ever-increasing demand for transparency, traceability, and accurate data between stakeholders that cannot be trusted without relying on an intermediate.

Figure 2 presents an overview of the DLT. Public DLTs, while

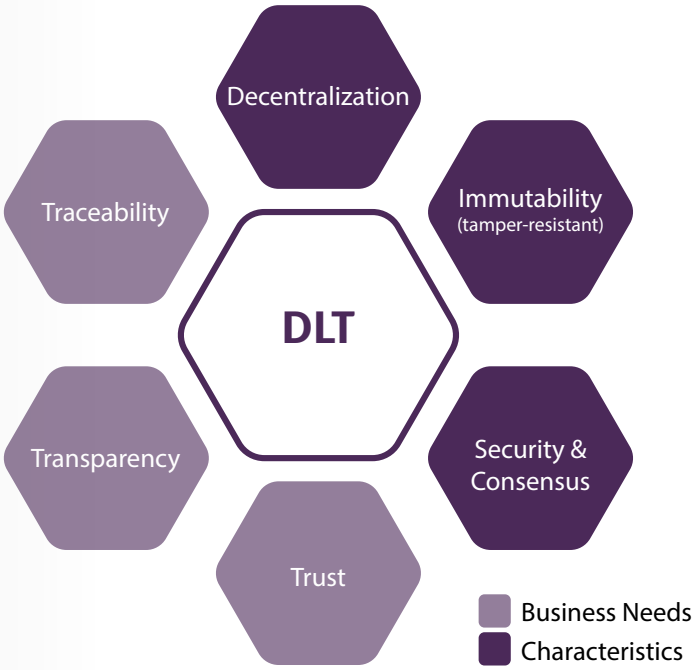


Figure 1: DLT Characteristics and Business Needs

being transparent and resistant to tampering, are slow, being more focused on the security and decentralization and less on the scalability, whereas private DLTs are somewhat centralized but can deliver much higher throughput and speeds, being more focused on the scalability and security and less on decentralization. Hybrid DLTs combine the benefits of both DLT types while trying to limit their disadvantages.

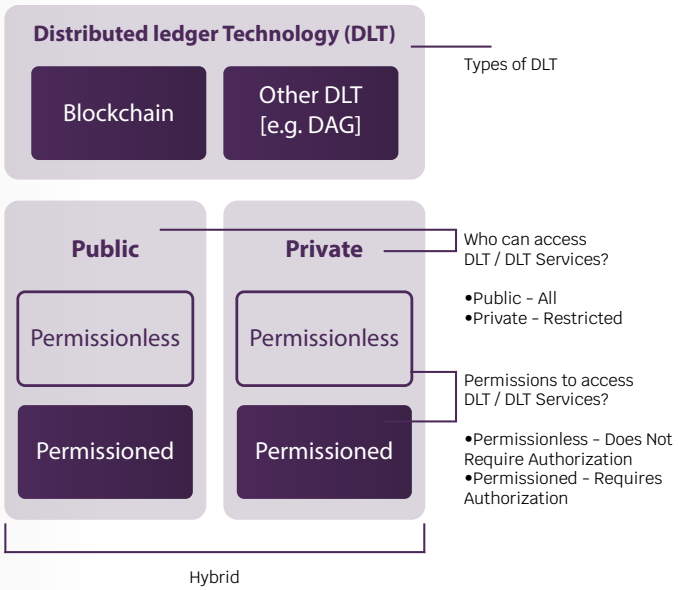


Figure 2: Overview of the DLT

2. Artificial Intelligence

Artificial Intelligence (AI) is the science of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, and computers can execute repetitive tasks with complete precision. Lately, they have been gaining the ability to learn, improve, and make decisions in ways that will enable them to perform tasks previously thought to rely on human capabilities. By automating repetitive tasks, AI is enabling staff to take on higher-value work.

An AI system combines and utilizes machine learning and deep learning and other types of data analytics methods to achieve artificial intelligence capabilities as shown in Figure 3.

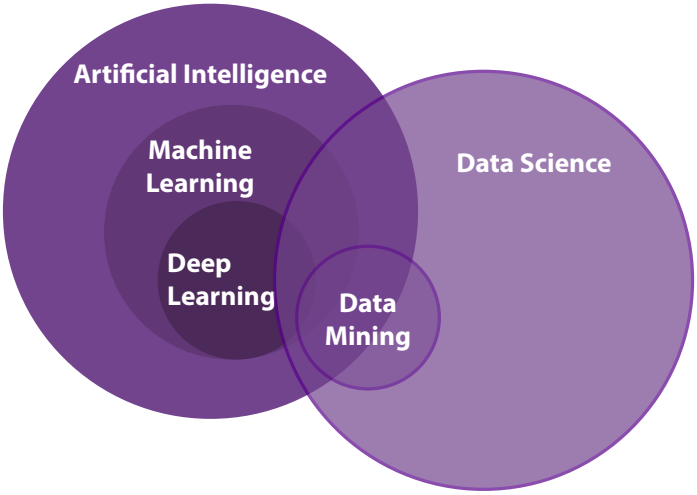
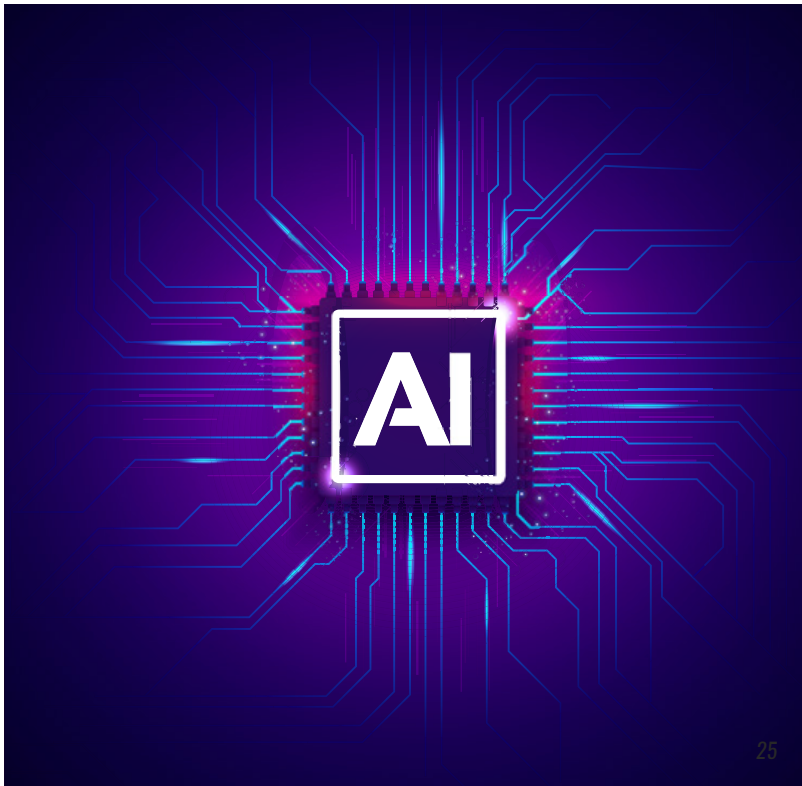


Figure 3: Artificial Intelligence Overview



AI systems can be categorized based on the degree to which they can replicate human capabilities, as follows; Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI), and Artificial Superintelligence (ASI), see more in Figure 4.

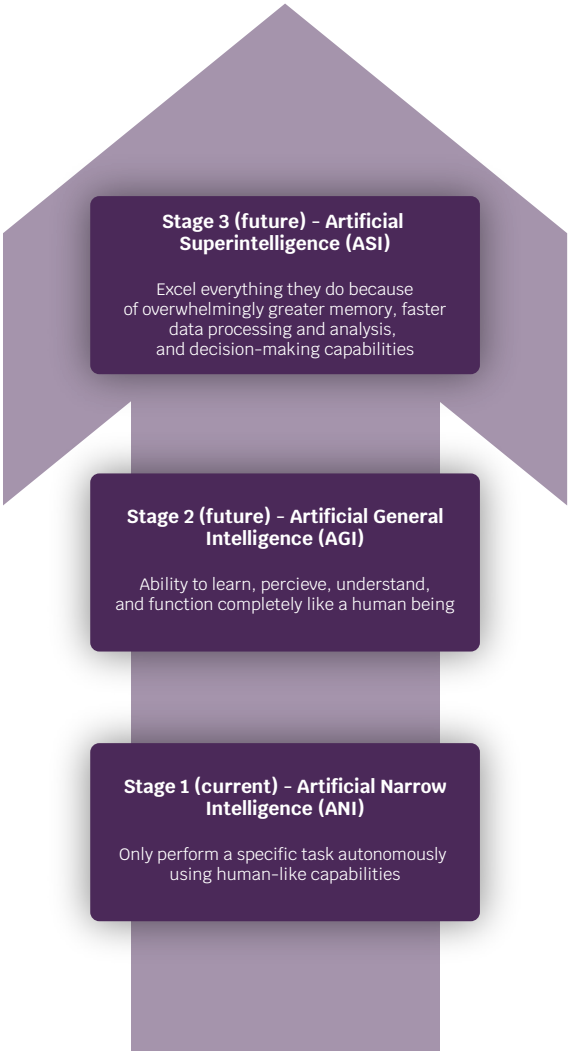


Figure 4: AI Types based on the degree to which they can replicate human capabilities

3. Extended Reality

Extended Reality (XR) is an umbrella for all the immersive technologies, including those already in place today – augmented reality (AR), mixed reality (MR), and virtual reality (VR), as shown in Figure 5, plus those that are still to be created - by extending the reality through either blending the virtual and real worlds or creating a fully immersive experience.

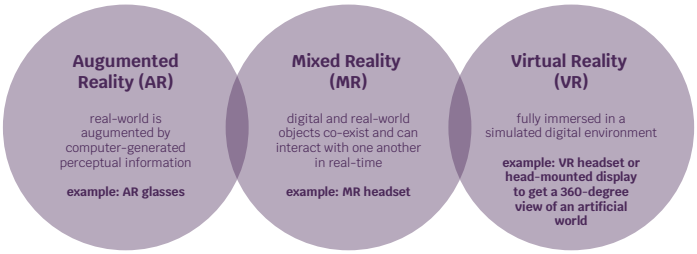


Figure 5: Extended Reality (XR) immersive technologies

4. Quantum Computing

Quantum Computing (QC) is the area of study focused on the development of computer-based technologies centered around the principles of quantum theory.

Quantum computing gains much of its processing power through the ability for bits to be in multiple states at one time.

In classical computing, data must be processed in an exclusive binary state at any point in time – either 0 or 1. These values are binary digits, or bits. As the circuits progress to be smaller and faster, physical limits of materials and the threshold for classical laws of physics apply and quantum computing is a new approach to fulfill these gaps.

In a quantum computer, several elemental particles, such as electrons or photons can be used. Each particle is given a charge or polarization acting as a representation of 0 and/or 1. Each particle is called a quantum bit, or qubit.

For example, a 2-bit register of a classical computer can store only one of four binary configurations at any given time, while a 2-qubit register in a quantum computer can store all four combinations simultaneously as shown in Figure 6.

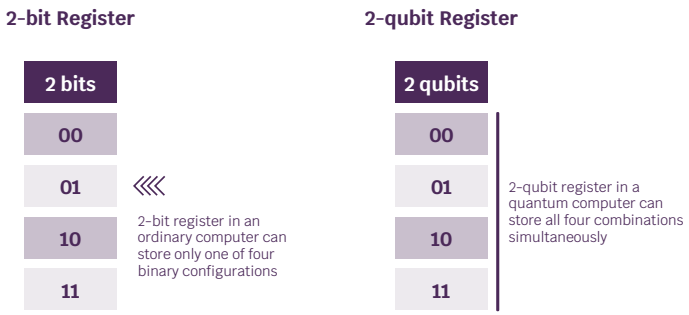


Figure 6: Comparing Classical and Quantum Computing

Getting the Four Technologies to Work Together

As the maturity of each of the DARQ technologies increases, leader organizations already started testing and planning innovative solutions that mix these technologies so that they can take over the competitive advantage in the post-digital era.

The organizations that have acquired the SMAC – social, mobile, analytics, and cloud – competencies during the digital transformation, a pre-requisite to the post-digital era, will benefit from combing and expanding those competencies with DARQ technologies, as shown in Figure 7, driving innovations that will disrupt themselves and the market.

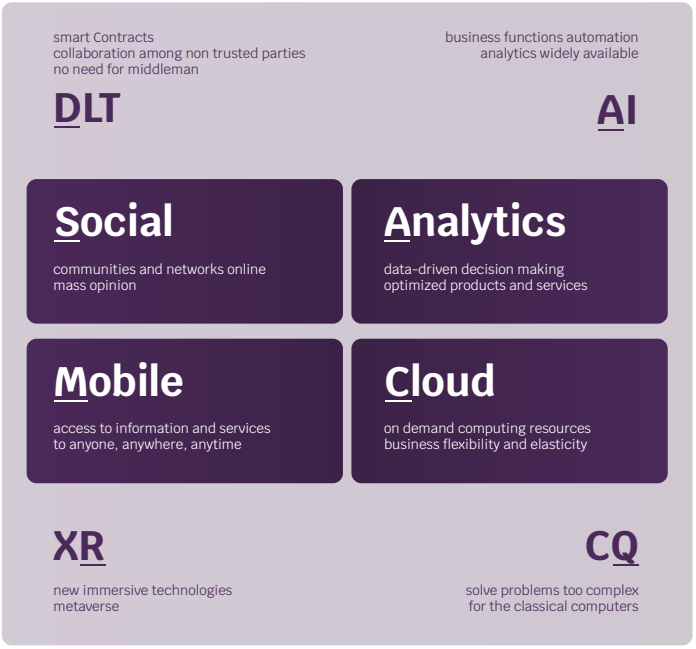


Figure 7: DARQ technologies expanding SMAC competencies in the post-digital era

DARQ – Use Cases

There are already organizations that are testing or using new innovations adopting DARQ technologies in their products or services.

According to Accenture Technology Vision 2019 Report, Volkswagen has been using quantum computing to test traffic flow optimization, as well as to simulate the chemical structure of batteries, hoping to accelerate battery development. The company teamed with Nvidia to add AI capabilities to future models and is also testing distributed ledgers with an eye to protecting cars from hackers, facilitating automatic payments at gas stations, creating tamper-proof odometers, and more. And the carmaker provides step-by-step augmented reality instructions to help service employees repair vehicles.

Tesla has been using DARQ technologies to develop and deploy autonomy at scale in vehicles, robots, and more to achieve a general solution for full self-driving and beyond. Initiatives include Full Self-Driving (FSD), Dojo Chip and Systems, Neural Networks, Autonomy Algorithms, and Evaluation Infrastructure. Regarding DLT, the company has been working with a consortium of cobalt producers to develop a blockchain platform to track the commodity from "mine to the battery." Tesla blockchain platform aims to create a "transparent, open, and global registry" that will track cobalt to ensure its sustainability and help in the tracking of its provenance at the unit level.

DARQ technologies can also be applied to improve efficiency and speed in supply chain management. Modern-day business relies on a complex web of supply chains, with products, parts, and materials often shipped thousands of miles away and from many destinations around the globe.

AI is critical for optimizing these routes and QC can be used to calculate the fastest route for all vehicles considering millions of real-time data points about traffic congestion – quantum routing.

DLT has the potential to transform the logistics, manufacturing, and retailing industries. It can be used to register the transfer of goods between two parties, identified as two addresses in the DLT, including relevant supply chain information, such as location, date, price, and quantity, facilitating traceability.

Smart contracts can be triggered when certain conditions are met. Digital Twins, a virtual representation that serves as the real-time digital counterpart of a physical object or process, can be used together with DLT and smart contracts to enhance the solution.

AR may be used to make the order picking process faster and less prone to error. By using smart glasses, employees can see exactly where items should fit on carts while they are picking orders.

Other scenarios may address transportation handling, storage, and inventory management.

DARQ – Post-digital Era Roadmap

Organizations should start planning the roadmap for the post-digital era if they want to keep up with innovative products and services so that they can be leading the disruption that DARQ technologies can bring. Opportunities and threats should be cautiously considered with regards to the specific technology itself, as well as to the technologies working collectively as a system.

The program(s) in the roadmap should be defined and be closely aligned with the business strategies. Constant feedback loop should be established that can be used, for example, to validate if the program(s) outcomes are contributing to the business strategies, if the business strategies are helping to prioritize the program(s) outcomes, or to inform about new strategies to consider.

It is advisable to adopt an innovation framework to support the planning, design, development, and deployment of the post-digital era roadmap.

DARQ – Emerging Risks

Since businesses are going to use DARQ technologies to reach further into peoples' lives, impacts related to safety, security, privacy, ethics, fairness, bias, liability, and transparency should be considered.

When managing risks – threats or opportunities – related to DARQ technologies, an emerging risks' framework should be used. As defined by Stanford University, emerging risk is a new or unforeseen risk that has not been yet contemplated. This is a risk that should be on the radar, but is not, and its potential for harm or loss is not fully known.

Figure 8: Emerging Risks Categories according to IRGC

International Risk Management Council (IRGC) suggests a categorization of emerging risks, as shown in Figure 8, according to three prototypes in relation to the potential impacts of the emerging risks and to the management strategies that will be recommended.

DARQ – Governance Aspects Related to DARQ Technologies

Figure 9 presents some governance aspects related to each of the DARQ technologies that should be taken into account by the governing bodies, or equivalent structure that has been established to ensure the accountability and the direction, monitoring, and evaluation on the use of the technology, as it is the case for the DLT systems. When the technologies are used collectively some new considerations may arise that should be addressed by the governing bodies or equivalent structure.

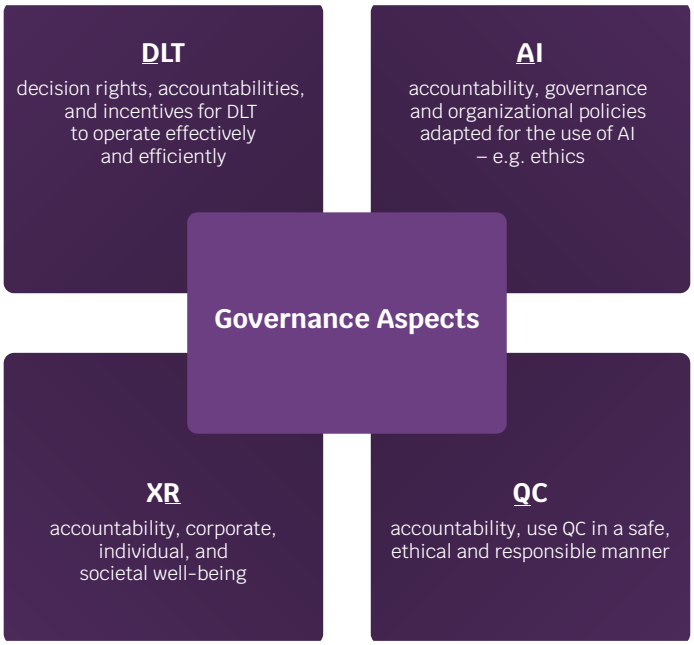


Figure 9: Governance aspects related to DARQ Technologies

DARQ – Regulation

Specific regulation is another aspect that should be considered when using DARQ technologies. Since they are new technologies, different regulations are mostly under development or discussion, and they should be closely followed for new updates due to the impact of not being compliant.

As stated by the International Telecommunication Union (ITU), DLT regulation includes different categories of legislation, such as code and intellectual property; governance; DLT use cases such as cryptocurrency, tokenomics, anti-money laundering and privacy, and consumer law; civil liability and consortia; and legislation that addresses the different layers of DLT structures. Digital assets, including digital currencies, are of importance in the DLT context, and as such various initiatives are currently undertaken, if not approved and enforced yet, to regulate them in many jurisdictions. Central Bank Digital Currency (CBDC), a digital currency issued by a Central Bank, is another relevant topic currently under discussion, development, implementation, or already in operation.

European Commission issued on 24.09.2020 COM(2020) 594 final, a proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology to create an EU framework, that both, enables markets in crypto assets, as well as the tokenization of traditional financial assets, and the wider use of DLT in financial services. Legally binding smart contracts, also have to be considered in terms of compliance with the applicable laws.

Examples of regulatory initiatives related to AI are; EU Artificial Intelligence Act (proposed on 24.04.2021 COM/2021/206 final), UK AI Strategy (to develop UK AI Regulation), the Government of Canada's Directive on Automated Decision-making (begun considering AI and ADM Regulation), Brazilian AI Law (Bill nº 21/20 approved on 29.09.2021).

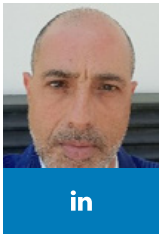
It is of importance that regulators and other stakeholders – researchers, businesses, and legislators – get together to develop DARQ technologies related regulations striking to get the right balance between supporting innovation and protecting against adverse situations. Existing regulations may also need to be revised to accommodate DARQ technologies due to the impact these technologies has on them.

DARQ – Conclusion

Since DARQ technologies are at their early stages, some more developed and matured than others, urge for work to be done by the appropriate stakeholders to encourage the innovation on one hand, and to prevent negative impacts on safety, security, privacy, ethics, fairness, bias, liability, transparency, or other related risks in another hand.

Businesses that wish to remain at the forefront of innovation in the post-digital era should start as soon as possible or keep investing in DARQ technologies taking into account the businesses' opportunities and threats they can bring.

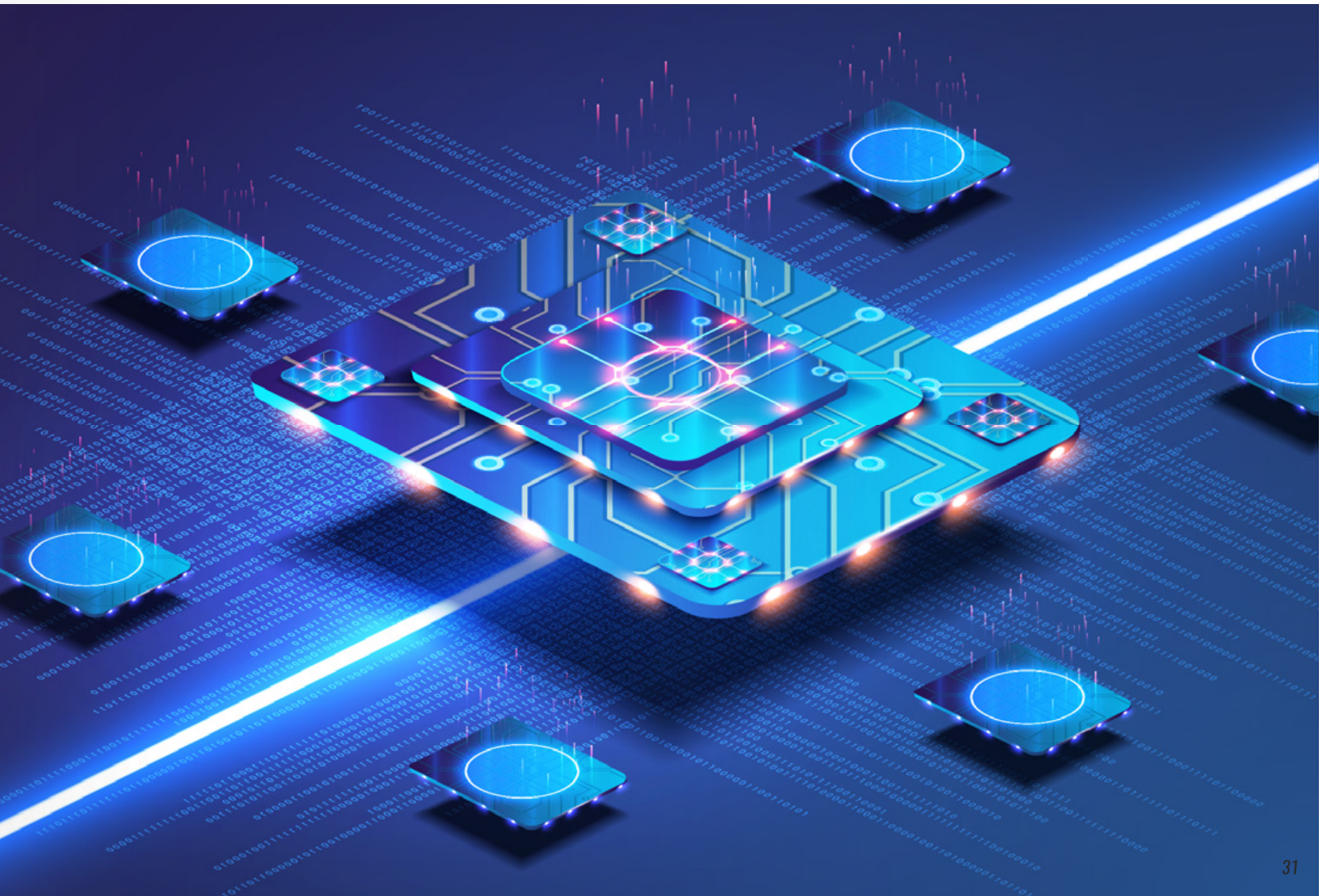
The DARQ age is here!



Jose Antonio Costa
Governance, Risk, Compliance, Privacy, Cybersecurity, Blockchain and DLT - CISA, CGEIT, DPO – CISA, CGEIT, DPO

Jose has over 30 years of experience in IT, mostly in the financial and telco sectors. Being an IT Governance, Risk, Compliance, Privacy and Cybersecurity expert, have led him to have deep knowledge, understanding, and experience with ISO 31000, ISO/IEC 38500, ISO/IEC 27000, and ISO/IEC 20000 series of standards together with ITIL and COBIT.

He has been collaborating very closely with ISO/IEC, CEN/CENELEC, IEEE, and ITU-T in the past years, helping in the development and dissemination of standards and frameworks related to these fields. Since October 2017, Jose has been the chair of the Portuguese Committee on Blockchain and Distributed Ledger Technologies (DLT).



Lifestyle of an Organizational Resilience Manager

BY OMON ILABOYA

Organizations continually face internal and external factors that contribute to the uncertainty of whether, when, and the extent to which they will achieve their business or project objectives. These unexpected, harmful events, and other disruptions can lead to huge losses to organizations. The need for organizations to be well-equipped to anticipate and respond to disruptions quickly is essential for their survival. The demand for Organizational Resilience experts has been increasing now more than ever before.

Having worked as one, and been surrounded by many, I will share with you what the life of an Organizational Resilience Manager looks like.

The Drive and Motivation

Change, as they say, is constant. Therefore, in the ever-dynamic business environments, organizations must have the capability to adapt and respond to change adequately to thrive and compete favorably. Organizational resilience is the ability of an organization to anticipate, prepare for, respond, and adapt to everything, from minor everyday events to acute shocks and chronic or incremental changes in order to survive and prosper.

The impact of the COVID-19 pandemic on businesses across the globe brought more emphasis on the domain of organizational resilience, as many organizations had difficulty in recovering from the disruption. Organizations may not be able to prevent some disruptions, but their survival depends on how well they are able to adapt, respond, and recover.

Resilience management encompasses the assessment, implementation, and monitoring of efficient active and passive systems which address an organization's threats, vulnerabilities, and consequences in the face of an extraordinary event. This provides a basis upon which businesses can undertake sound decision-making towards achieving their strategic objectives. This has now become more important in a global business environment where

organizations and governments are increasingly focusing on effective risk management to deploy capital and attain competitive advantage, recover quickly from business disruptions, and improve their organizational resilience.

Who Is an Organizational Resilience Manager?

An Organizational Resilience Manager is one who is responsible for helping an organization anticipate, prepare for, respond, and adapt to incremental change and sudden disruptions in order to survive and prosper. In simple terms, the job is to make the organization more resilient.

Such a manager would need to have adequate knowledge and skills on how to identify, assess, and manage strategic, organizational, environmental, and technological risks, as well as threats presented by unpredictable situations.

The Organizational Resilience Manager's job involves the integration of various disciplines such as;

- Business continuity
- Information security
- Risk management
- Facilities management
- Emergency and crisis management
- Environmental management
- Health and safety
- Supply chain
- Reputation management
- Fraud control Information, communications, and technology (ICT) continuity
- Change management
- Physical security
- Asset management
- Human resource planning
- Financial control
- Quality management

This also involves ensuring that knowledge is actively shared across internal organizational boundaries. Anything that could directly or indirectly affect the organization is ground for consideration.

Advising on emergency, disaster, or crisis management strategies, the latest regulations on information security, data protection, health, safety and environment, business impact analysis, risk assessment, testing and exercising business continuity plans, coordinating awareness programs for staff, launching an investigation for incidents, or onboarding a new contractor, could all fill up a day in the life of an Organizational Resilience Manager.

It is a job that carries with it a fair amount of pressure at times, as these professionals must be proactive in

anticipating what could disrupt the organization's operations, and be able to lead the organization in recovering from them if they occur, as it is their judgment on the appropriate strategies, plans, and responses that will drive important business decisions and performance.

Depending on the size of the firm, the Organizational Resilience Manager may have the opportunity for more regular dialogue with the C-suite level to discuss resilience issues. Either way, it is important for Organizational Resilience Managers to have a broad understanding of the business across all levels.

A substantial amount of your time would be spent monitoring and maintaining the controls you have established to mitigate organizational risks. So, expect part of your day to be data-focused as you go through the information collated to identify any trends or emerging risks to the business. They conduct substantial research and analysis by gathering intelligence (information, opinion, and data) from varied sources, making sense of it, testing its validity, and drawing conclusions that can lead to practical benefits. Should anything pertinent arise, they may have to be heightened to the Board along with their recommendations for any policy or procedure, amendments, or training for the organization's employees. They would then organize those training and development sessions accordingly. Documentation is part of life too, from reviewing client files and press articles to preparing and revising procedure manuals, and screening information pertaining to supply chain elements.

Organizational Resilience Manager jobs are anything but dull. An exciting component of the role is the diversity of opportunities to interact with different functions, parties, and agencies, internal and external, to the organization. This helps to forge valuable skills to meet the challenges of the job on a daily basis. Furthermore, Organizational Resilience professionals are known for their commitment to educating their colleagues enterprise-wide on policies, procedures, and plans to prevent disruptions, as well as sharing lessons learned from incidents to help improve subsequent performance.

What Skills Are Required?

Beyond the primary need of the Organizational Resilience Manager to possess risk management and other technical skills, essential behavioral and non-technical, are also required for the job. An Organizational Resilience Manager must:

- Be a good communicator to clearly provide written information and verbal information to relevant stakeholders
- Be able to manage stakeholders across various functions and levels
- Be good planners and organizers – proactively thinking ahead, managing time, priorities, risk, and developing structured approaches to delivering results to a high standard
- Be problem solvers – being able to analyze and interpret problems from multiple viewpoints and develop effective solutions
- Keep a perspective – not turning an event into a crisis. Rather, they view problems from different perspectives and analyze them by taking various factors into consideration
- Respond and adapt positively to pressure and change to sustain performance when situations change, workload increases, tensions rise, or priorities shift

Work-life Balance

The need to constantly keep up with changes in the business environment, backing awareness on policies, testing and exercising plans, conducting business impact analysis, risk assessment, monitoring risk controls, responding to accidents, crisis, or disasters, etc., can sometimes take a toll on Organizational Resilience Managers as they work sleepless nights often, between self-education, writing reports, or meeting deadlines. These may lead to negative trade-offs costing them precious time to rest, spending time with families, or engaging in their hobbies. Work-life balance requires us to manage the stresses of work and personal life.

When the stress associated with one of them becomes overbearing, it can lead to an imbalance. As an Organizational Resilience Manager, it is important to be able to avoid tilting far toward either end of that equation. Too much work leads to burnout, and too much entertainment leads to poor productivity and lack of fulfillment.

What a conundrum! Organizational Resilience Managers also need to build personal resilience, because good health, energy, and focus are essential for productivity and motivating the people you manage.

Achieving a good work-life balance is important for managers. This can be achieved by consciously making efforts to delegate more responsibility to other team members and empowering them, taking work breaks, holidays, or vacations to unplug and refresh. Paid time off, holidays, and vacations should be spent relaxing, not working. It is also helpful to maintain a consistent and predictable workday by setting a daily work schedule. Managers have to be intentional about focusing on mental health and well-being by adopting a healthy lifestyle that reduces the impact of work overload, such as scheduling frequent breaks, eating healthy meals, spending quality time for personal priorities and relationships with people you care about.

Maintaining a balance between work and personal life can be quite challenging, particularly for managers during crisis. However, if you find yourself to be physically exhausted or mentally stressed, it is more important to remember that it is necessary to disconnect, rest, and find appropriate ways to recharge or rejuvenate. It is important to also nurture your own resilience, whatever you do, remember to “recharge your batteries”. Building your personal resilience will help enhance your ability to influence positive outcomes for your personal life while being productive and refreshed at work.

in

Omon Ilaboya
Risk and Organizational Resilience Consulting

Omon is an Organizational Resilience professional. Leading consulting teams, he has successfully guided organizations on over 50 distinct projects to achieve enhanced business process performance, compliance, and the adoption of certification to ISO standards with a strong track record of facilitating positive safety cultural change, improving business continuity capabilities, organizational resilience, and information security performance. He has accomplished this through his vast experience in Advisory, Training, Audits, and Exercising support to enhance Risk and Resilience architecture across Africa, Europe and North America. His core expertise is in governance, risk, and compliance. You can contact him through www.augeanstablessolutions.com

PECB INSIGHTS 2022 CONFERENCE

PECB Insights Conference 2022 Is on Its Way!

As we conclude the first-ever Quality Management Conference 2022, we would like to thank everyone that has attended, and we invite you to stay tuned for the conference recordings to be published on YouTube shortly!

Following the great success of the Quality Management Conference 2022, PECB has announced that the Insights Conference 2022 is well underway, and returns to in-person conferences after a three year period. The 8th edition of the Insights Conference is to be held in the lively city of Brussels, on **17-18 November, 2022.**

The conference brings a remarkable opportunity for all individuals wanting to challenge current global perceptions through the exceptional discussions conducted with some of the world's leading experts on the tracks of Information Security, Digital Transformation, Artificial Intelligence, Blockchain Technology, and so much more!

To advance the skills and competencies of participants, this conference will also deliver the following pre-conference training courses on **14-16 November, 2022**:

1. Digital Transformation Training Course
2. Lead Crisis Manager Training Course

The PECB Insights Conference 2022 will be full of informative and immersive sessions that convene the world's most influential and brightest minds across industries. By building bridges between experts from different industries, we are aiming to create a community that is willing to embrace changes and join forces toward a safer world.

Stay tuned for more information on tickets to be published soon!

Creating a Well-Structured Crisis Management Plan

BY GARTH VINCENT

Before delving into the structure of a crisis management plan, I will share an example of a previous case, in order to put the importance of a crisis management plan into perspective.

United Airline 2017 Crisis

In early 2017, social media erupted with the news that United barred two teenage passengers from boarding a flight because of the leggings they wore. The situation quickly escalated as a nearby traveler tweeted about the incident. Far from apologizing, United released a series of tweets defending the gate agent's actions and claiming that this was standard procedure for passengers flying as "pass holders". The "pass holder" reasoning seemed to mollify some, but all agreed that the situation had been poorly handled.

The leggings scandal was nothing compared to what happened a few weeks later, however, when video surfaced showing a United Airline customer being brutally dragged and bloodied from a flight. While initial speculation was that the paying passenger had been asked to give up his seat because of overbooking, it was soon revealed that the seats were being repurposed for United's own employees.

Despite having a swift response, United Airline CEO Oscar Munoz released a statement via social media where he defended the actions taken by the flight crew, in both cases lacking any sort of empathy and compassion for the battered and bruised passenger but did apologize for "re-accommodating these passengers". In just 24 hours of this incident, United Continental Airline shares had lost $800 million dollars in total value.

CEO Oscar Munoz then made several follow-up statements shifting his tone to a more apologetic approach but his main stakeholder, the public, was not receptive to his sentiments, what occurred here is what can simply be called too little too late.

Since simultaneously circulating on social media, the lawyer for the battered passenger stated he has suffered

from a concussion, a broken nose, and several teeth missing and he would require reconstructive facial surgery to repair the injuries sustained. United Airline demonstrated they had an unstructured Crisis Management Plan by how they responded to both situations and paid the ultimate price a major loss in company revenue and severe damage to their reputation.

In this article, we will examine the definitions of crisis management, the different types of crisis that can be experienced by organizations, and problems that can be experienced from having a poorly constructed crisis management plan. We will then examine the ten components that are needed to develop a well-structured crisis management plan. In addition, why an organization can use the ISO 22301 Security and Resilience — Business Continuity Management Systems, ISO/DIS 22361 Security and Resilience – Crisis Management, and the updated ISO 22329 Security and Resilience – Emergency Management.

Crisis Management (CM) is the overall coordination of an organization's response to crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate and often involves the need to make quick decisions on the basis of uncertain or incomplete information. Crisis Management includes the development of plans, based upon an integrated approach with internal and external interested parties, to reduce the risk of various crises occurring. The implementation of crisis plans will minimize the impact of the crisis you are dealing with and assist the organization to recover and restart its normal activities as quickly as possible.

Let us briefly examine what type of crisis can impact many organizations:

Organizational Crisis: Product recall, dangerous goods or material spills, general employee safety concerns, public relations blunders, active shooter incidents, acts of terrorism, civil unrest, and communicable disease outbreaks.

Environmental Crisis: Earthquakes, fires, floods, and hurricanes.

Personnel Crisis: Workplace violence, employee strikes, issues regarding harassment, senior leadership errors, omissions and wrongdoings, kidnapping or hostage situations involving traveling for work, illegal or unethical misconduct.

Financial Crisis: A drop in demand for the company's product or services, bankruptcy, stock price concerns.

Technological Crisis: Cyber-attacks, data loss, mishandling of confidential or proprietary information.

One of the major elements missing in most companies' Crisis Management Plan, is the lack of trained and competent Crisis Management Team members to manage incidents. This has been shown as the main drawback in managing various types of crisis. The Crisis Management Team is largely responsible for creating the Crisis Plan. All team members have input, and the team also consults other stakeholders, such as the operations staff and senior management. The plan spells out important roles in the crisis response and each person's responsibilities. Without an effective and competent Crisis Management Team the development and execution of a well-structured Crisis Management Plan is virtually impossible.

Deborah Hileman, President and CEO of the Institute for Crisis Management stated that: "A good crisis plan possesses a variety of elements that prepare crisis team members to effectively perform their duties when a crisis occurs."

10 Elements of a Crisis Management Plan

The graphic above lets us examine the 10 key components of a well-structured Crisis Management Plan:

1. **Risk Analysis**: Outline the scenarios you think your organization could be impacted by. Having a more specific sense of these potential occurrences will guide your planning. You do not need to include every conceivable risk, but cover a broad range, such as; a natural disaster, a cyberattack, a loss of utilities, a technology failure, a financial crisis, an operational accident, or a product failure.
2. **Activation Protocol**: Include numerous event triggers for the Crisis Management Plan. Triggers in the crisis and business continuity context are the natural first reactions to an emergency by an organization and have a major numbing effect. Using tier levels of urgency (Tier 1, 2, and 3) as your criterion, define the circumstances that activate a particular crisis response. Based on the type or location of the incident, the protocol should also direct your staff on how to respond. The protocol should establish some type of communication that signals the end of a crisis, as well.
3. **Chain of Command**: Include a crisis management-related organization chart in your plan, so it is clear who has final authority and who reports to whom.

Creating a well-defined organizational chart that supports coordination and consistency, is something that some decentralized organizations sometimes struggle to achieve. Depending on the seriousness of the event, your plan may call for additional layers of command.

4. **Command Center Plan**: Determine what will serve as the base of operations for the team during a crisis. The establishment of Emergency Operations Center (EOC) is critical for the Crisis Management Team to execute the strategic aspects of the crisis management plans. In addition to the primary EOC, companies must have an established secondary Emergency Operation Center in the event the primary location has been compromised by the crisis or incident.
5. **Response Action Plans**: Organizations need to perform detailed planning around how Crisis Management Teams (CMT) will respond to various scenarios. This planning includes assigning responsibility for each task as identified. Think of these response actions as modular elements that you should employ as the situation requires, intellectualizing crises in a way that your crisis management can be made scalable and adaptable.
6. **Internal Communication Plan**: An effective internal crisis communication plan ensures your employees are prepared for and actively help to mitigate or reduce crisis situations, and have the necessary information, processes, and channels freely available if anything happens. It is just of such importance that they understand what is expected of them should a situation arise. You must also establish ways to disseminate urgent information to all employees, such as using a notification provider to send texts and automated calls or implementing a method for your employees to check in and report their safety and whereabouts.
7. **External Communication Plan**: Define plans for communicating with the public and other key external stakeholders or interested parties by appointing a spokesperson. Write detailed instructions, including whom you will notify (e.g., media outlets in a particular geographic area), also draft holding statements, the details of which you can fill in later, once you have the relevant information.
8. **Resource Management**: The Crisis Management Team is responsible for identifying, organizing, and coordinating resources and logistical support needed during an organizational crisis. This can be broken down into two broad categories of people, equipment, and supplies that are needed to create an effective crisis communication strategy.
9. **Training**: Being able to execute your crisis management plan quickly is paramount, therefore, holding drills and exercises with the Crisis Management Team is crucial to that goal. Rehearsals or even tabletop drills can reveal flaws in the plan, practice will help the crisis team become comfortable with their individual roles and work together. Make sure to stay current by doing regular training.
10. **Review**: Create a structured review process in order to schedule regular follow-up enhancement regarding your crisis management plan. Organizations need to implement Plan-Do-Check-Act (PDCA) cycle which is the process that encourages continuous improvement of the organization, section, or department. Because of its emphasis on continuous improvement, it aids in the reduction of waste and maximization of efficiency, it has become an important element of the lean management system of organizations.

The Use of ISO Standards to Manage Crisis

ISO 22301 Security and Resilience — Business Continuity Management systems is designed to help organizations prevent, prepare for, respond to, and recover from unexpected and disruptive incidents, and a Crisis Management Plan usually accompanies this plan along with the IT Disaster Recovery Plan and the Emergency Response Plan. The ISO 22329 Security Resilience – Emergency management – Guidelines for the use of social media in emergencies. It gives guidance on how organizations and the public can use and interact through social media before, during, and after an incident, as well as how social media can support the work of emergency services. This standard is applicable to governmental and non-governmental organizations involved in emergency management and crisis communication. This standard aids the use in counteracting social media misinformation and disinformation which can be used to damage the reputation of organizations and requires a crisis management plan to deal with a structured response.

At present the ISO/DIS 22361 Security and Resilience Crisis Management Guidelines for a strategic capability is being developed and this standard is to aid in the design and ongoing development of an organization's crisis management capability. It sets out principles and practices needed by all organizations.

As such, organizations should adopt a structured approach to crisis management by applying a set of principles on which a crisis management framework can be developed. This should include elements of organizational culture, leadership, competencies, and structure that supports the implementation of a crisis management capability in a purposeful, consistent, and rigorous manner.

We have seen how important a crisis management plan is to every organization. What is now becoming the norm, interestingly enough, is that most companies are creating an integration between their business continuity plan and their crisis management plan to increase the organization's levels of resilience against all forms of crises and disasters.

Do not let your next incident, accident, or disaster leave you vulnerable, strengthen your preparedness with a well-structured Crisis Management Plan and utilize the various applicable ISO standards to ensure your plan is fit for purpose.

Garth Vincent
Principal Consultant/ CEO Business Crisis Consultants Ltd.

in

Garth has over 28 years' experience in Health, Emergency, and Safety Management Systems. Garth is a former contracted Chief of Emergency Operations for Bp Trinidad. Garth possesses two U.K. Master's Degree in Risk, Crisis and Disaster Management and OHSE (Distinction grade). Silver PECB Partner, Certified in ISO 22301, BCMS Trainer, ISO 45001 OHSMS Trainer, ISO 18788 Trainer Implementer/Auditor, ISO 21000 EOMS, Senior Risk Manager, and ISO 31000 Trainer. Part-time lecturer at Arthur Lok Jack GSB, Energy Chamber TT, IHSEC Dubai, Nations School Guyana &ECATT. Chairman at TTEMAS EW. ILO Trainer Consultant Caribbean region.


Sales
Regional sales
270 000
750 000
250 000
Accumulated
Top
25%

Building An Effective Crisis Management Team

BY GEARY SIKICH

Building a sustainable Crisis Management Team (CMT) requires effective decision analysis capability. You need: *people, tools, and structure.*

What does this mean? It means that the CMT must possess:

1. Common mindset – To accomplish this the CMT has to have a common terminology that is understood by all members and they have to understand that the decision-making process in a crisis is different from normal day-to-day decision making.
2. Training – Critical to becoming an effective CMT is training, this includes classroom, virtual, and other forms of knowledge infusion. In addition to training, effective simulations (tabletops, drills, exercises) should be regularly scheduled and conducted.
3. Recognition of Weaknesses, Hazards, Opportunities, Threats, Strengths, Underlying Plans (WHOTSUP) – Effective baseline assessments that underpin the development of plans should be regularly performed. Risks, threats, hazards, and vulnerabilities are not static; each action taken to buffer against the effects of realization means that the risk, threat, hazard, and vulnerability changes and must be reassessed, buffered, and monitored.
4. Active Analysis – Situational Awareness – Communication – Constant, rigorous analysis, awareness, and effective communication are necessary for the CMT to activate, and transform into crisis mode operations to effectively transition into recovery and return to business operations.
5. Focused efforts that build credibility – Today much scrutiny occurs when a crisis erupts, media, stakeholders, regulators, and others will all be watching what the CMT does or does not do. Reputation Management has become a critical component of CMT operations.
6. Flexible structure that supports long-term functional needs – Incident Command Systems, National Incident Management System, and other forms of structure for CMT operations are critical to

understanding and adapting to your organization's normal operating structure. Transition to crisis operations can be seamless or chaotic; seamless as a result of having a structure that adapts rapidly to evolving situations or chaotic with no clear direction and structure.

The figure below, a reference to Gary Klein's book "Sources of Power: How People Make Decisions", provides an example of some of the key questions that must be answered to form an effective CMT.

Team competencies, team identity, and team cognition create the framework for an effective CMT. Can your organization's CMT answer the questions posited below? If not, perhaps a reconfiguration or restructuring may be in order?

Klein points out two challenges and one explanation for CMTs. He states that your biggest challenge will be:

1. Getting the team to work together when they generally do not function every day as a CMT.

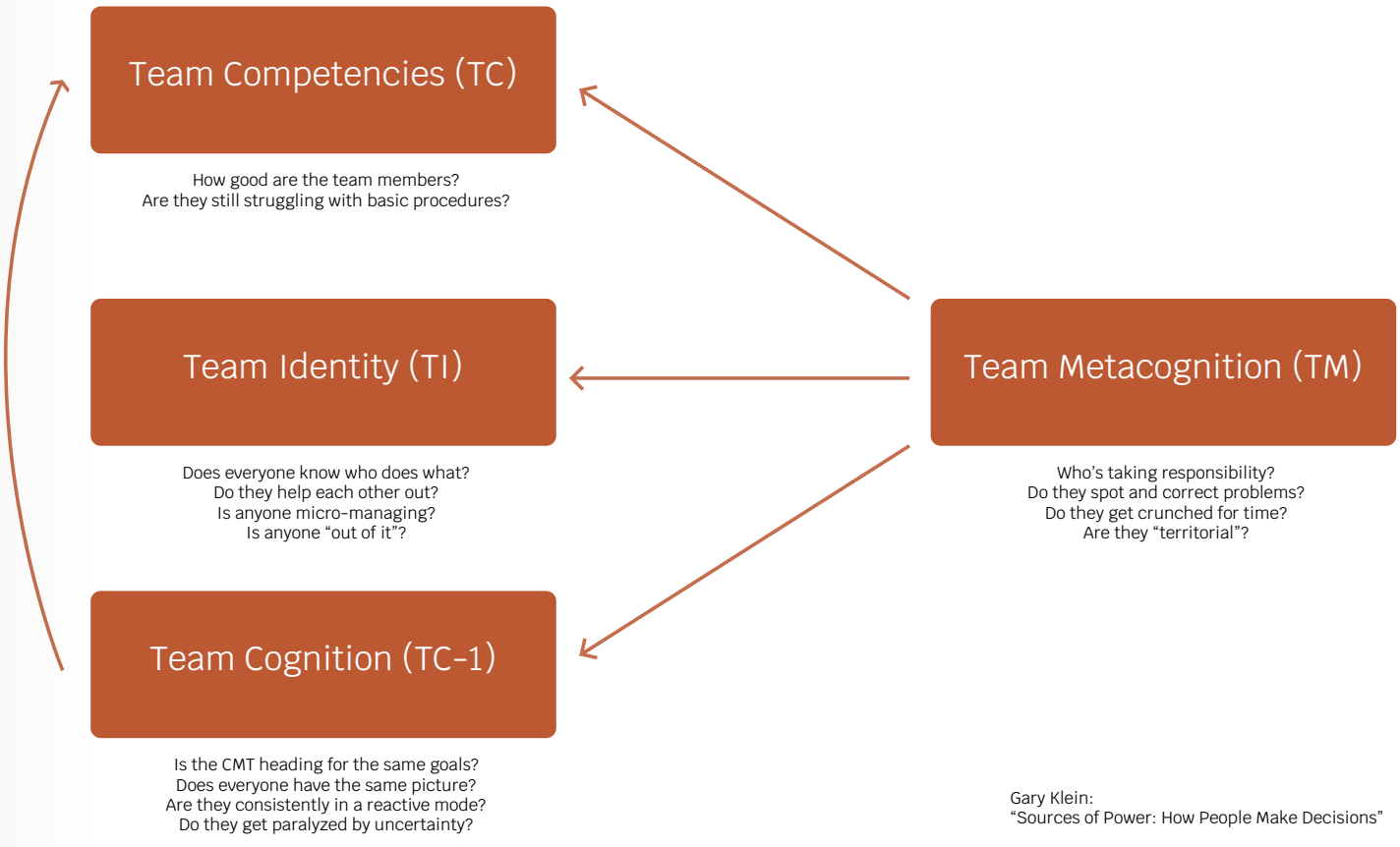
Your next biggest challenge:

2. Getting the team to comprehend their crisis management roles, responsibilities, functions, and how they differ from their day-to-day roles, responsibilities, and functions.

Klein gives five reasons why Crisis Management Teams fail:

- **Crisis Management Team does not know its own reaction time** – Think about how long it takes your CMT to react and begin to function in Crisis Mode.
- **Communications** – The failure to communicate effectively during the initial stages of a crisis and ongoing communication issues lead to more disruptions, delays, and misappropriation of resources. Common terminology and effective communication techniques must become a way of doing things versus an adjunct to CMT activities.
- **Micro-Managing** – If you are not on the scene do not attempt to tell the on-scene (Local Incident Commander) how to conduct tactical operations. You do not know what is going on, so rather than micro-manage, ensure support is provided to the incident location.

Crisis Management Team (CMT)



Gary Klein:
"Sources of Power: How People Make Decisions"

- Decisions are left at low levels – Ensure that decisions are made at the appropriate levels. All too often a decision left at a lower level is going to be second-guessed. Additionally, the decision-maker at the lower level may not be aware of the effect of their decision as it ripples through the organization creating a tsunami of cascading effects.
- **Allowing problems to compound** – Not addressing problems early on can lead to greater disruptions through cascading effects and the creation of collateral damage that could be prevented.

Six Leadership Habits

1. Anticipate

Most of the focus at most organizations is on what is directly ahead. The leaders lack "peripheral vision". This can leave your organization vulnerable to rivals who detect and act on ambiguous signals. To anticipate well, you must:

- Look for game-changing information at the periphery of your industry
- Search beyond the current boundaries of your business
- Build wide external networks to help you scan the horizon better

2. Think Critically

"Conventional wisdom" opens you to fewer raised eyebrows and second-guessing. But if you swallow every management fad, herd-like belief, and safe opinion at face value, your company loses all competitive advantage. Critical thinkers question everything. To master this skill, you must force yourself to:

- Reframe problems to get to the bottom of things, in terms of root causes
- Challenge current beliefs and mindsets, including your own
- Uncover hypocrisy, manipulation, and bias in organizational decisions

3. Interpret

Ambiguity is unsettling. Faced with it, the temptation is to reach for a fast (and potentially wrongheaded) solution. A good strategic leader holds steady, synthesizing information from many sources before developing a viewpoint. To get good at this, you have to:

- Seek patterns in multiple sources of data
- Encourage others to do the same
- Question prevailing assumptions and test multiple hypotheses simultaneously

4. Decide

Many leaders fall prey to "analysis paralysis". You have to develop processes and enforce them, so that you arrive at a "good enough" position. To do that well, you have to:

- Carefully frame the decision to get to the crux of the matter
- Balance speed, rigor, quality, and agility. Leave perfection to higher powers
- Take a stand even with incomplete information and amid diverse views

5. Align

Total consensus is rare. A strategic leader must foster open dialogue, build trust, and engage key stakeholders, especially when views diverge. To pull that off, you need to:

- Understand what drives other people's agendas, including what remains hidden
- Bring tough issues to the surface, even when it is uncomfortable
- Assess risk tolerance and follow through to build the necessary support

6. Learn

As your CMT grows, honest feedback is harder and harder to come by. You have to do what you can to keep it coming. This is crucial because success and letdown – especially letdown – are valuable sources of organizational learning. Here is what you need to do:

- Encourage and exemplify honest, rigorous debriefs to extract lessons

- Shift course quickly if you realize you are off track
- Celebrate both success and (well-intentioned) letdowns that provide insight

The figure below depicts the Three Spheres of Concern that CMTs have to recognize, adapt to, and manage. Your Sphere of Influence is what you bring to the table so to speak – it is the assets and capabilities that can affect the actions of others.

Your Sphere of Interest relates to those assets and capabilities that others possess which can influence your courses of action. Think of internal departments that you have no control over, but that can influence your actions. Recognize that external entities, similar to local, state, and federal government can have a major impact on your carefully laid out plans as well.

Your Sphere of Responsibility relates to your organization's mission, vision, and values. Today, with so much emphasis on reputation, stakeholder management, and the ever-present effect of social media; your sphere of responsibility truly puts your CMT in the spotlight when a crisis occurs.

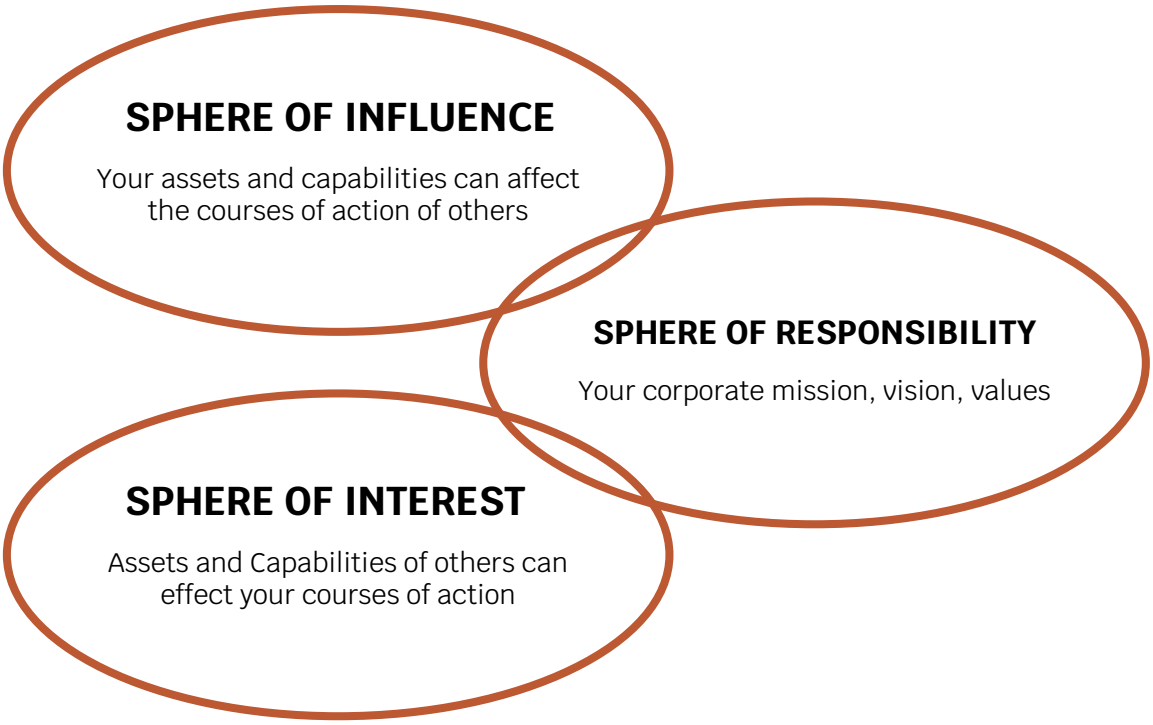
Expectations – Agenda – Focus

The length of time the enterprise will have to react to an event is directly related to the event's perceived impact on the enterprise by its key stakeholders. Three levels of management must be joined into a seamless flow of information, decision making, and action. These are:

Tactical:

- Near Real-time
- Event-driven
- Results Oriented
- Based on the Plan

Three Spheres of Concern



Business agility and resilience are popular buzzwords today. Everyone seems to be asking, "What's the next step in leveraging collaborative business?" Today, it seems that your organization must be poised to respond immediately to any business condition or value chain request and leap on any new opportunity. This creates yet another set of challenges and responsibilities that require executives to view crisis management in a whole new light.

Operational:

- Support to Tactical Response and advising the Strategic Component
- Assessment Driven – Affected and Non-Affected Operations
- Cascade and Collateral Damage Prevention Oriented
- Based on Response Actions

Strategic:

- Broad-based – Stakeholder focused
- Issues Driven
- Results Oriented
- Based on Response and Operational Actions

The OODA Loop

The OODA Loop is the cycle observe-orient-decide-act, developed by United States Air Force Colonel, John Boyd. Boyd applied the concept to the combat operations process, often at the operational level during military campaigns. It is now also often applied to understand commercial operations and learning processes. The approach explains how agility can overcome raw power in dealing with human opponents. It is especially applicable to cybersecurity and cyberwarfare.

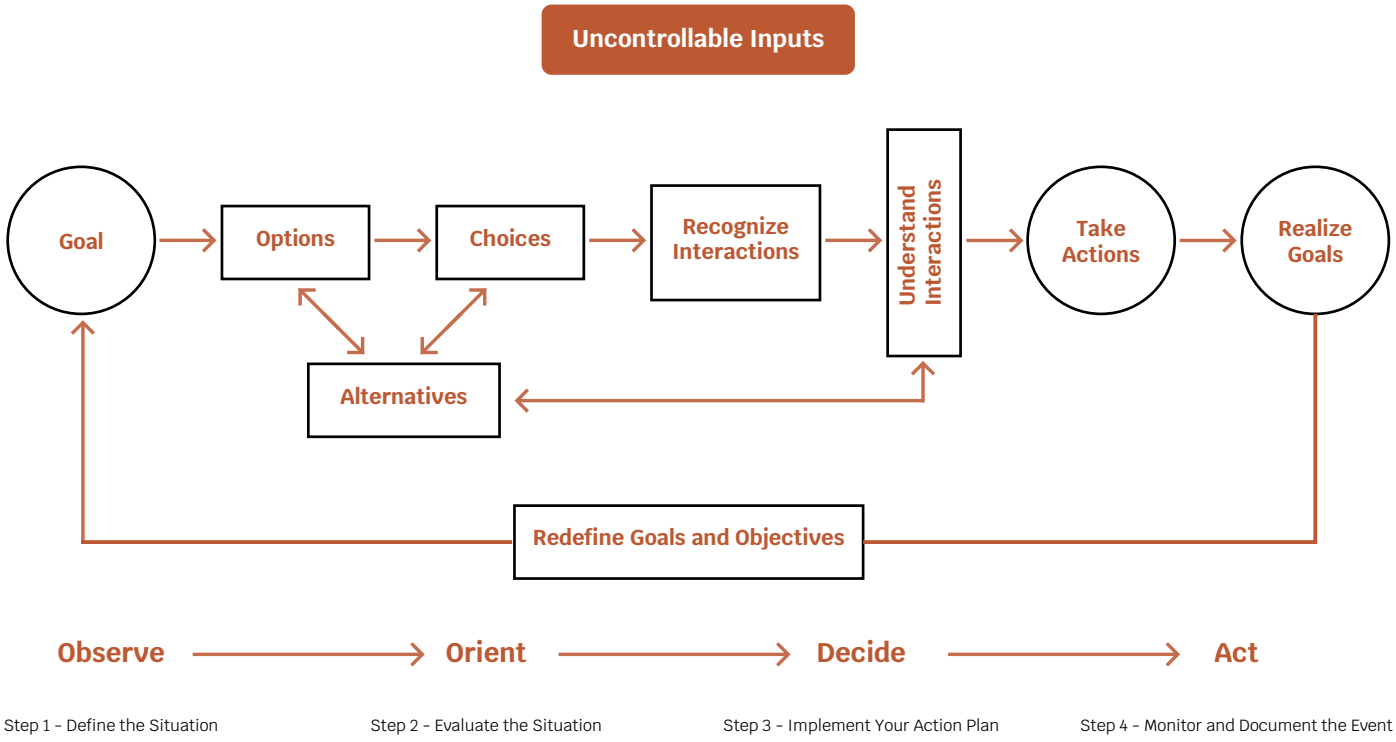
The figure below is a depiction of the OODA Loop applied to decision-making in a crisis. The CMT can benefit greatly by incorporating this decision-making tool into its playbook.

Critical Functions

I have found that the following breakdown of functions can be organized by the CMT to provide structure and understanding of role responsibility for members of the CMT.I breakdown and apply the Incident Command System and National Incident Management System structures into eight areas for CMTs:

1. **Management** – Defines who is in charge and what responsibilities are allocated at the tactical, operational, and strategic levels for decision making and management of the CMT.
2. **Planning** – Short-term immediate needs and long-term needs, planning is essential.
3. **Operations** – What is affected and what is currently not affected? How do you keep the event from cascading and creating collateral damage? Think vertically and horizontally.
4. **Infrastructure** – Internal (what you control) and external (what you do not control). Information Security and Information Technology operations.

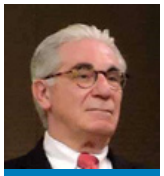
Leadership Decision Making and Situational Awareness



5. **Logistics** – Current needs and extended-period needs. Think food, water, lodging, transportation, etc.
6. **Finance** – Tracking costs associated with the crisis and expediting any services that are required to respond to the situation and for recovery efforts.
7. **Administration** – All administrative tracking for Human Resources, records, privacy, and regulatory compliance issues.
8. External Relations – All levels of government, stakeholders, media, "value chain", etc. Who is the designated spokesperson at the tactical level, operational level, and strategic level? What is the message that you want to convey?

Concluding thoughts

Will your organization have an effective crisis management team or will it fragment and chaos ensue during a crisis? Crisis Management Teams must be able to deal with the "stress of the moment" and come together in a seamless fashion to be effective.



Geary Sikich
Sr. Crisis Management Consultant, Author, and Business Advisor

Geary Sikich is a Senior Crisis Management Consultant. Geary focuses on enterprise risk management, contingency planning, executive education, and issues analysis. Geary developed LMSCARVERtm the "Active Analysis" framework, which directly links key value drivers to operating processes and activities. LMSCARVERtm provides a framework that enables a progressive approach to business planning, scenario planning, performance assessment, and goal setting. Geary has developed and taught courses for Norwich University, University of Nevada Reno, George Washington University, and the University of California Berkley. He is the author of many books, such as: "It Can't Happen Here: All Hazards Crisis Management Planning", "The Emergency Management Planning Handbook", "Integrated Business Continuity: Maintaining Resilience in Uncertain Times", "Protecting Your Business in a Pandemic: Plans, Tools, and Advice for Maintaining Business Continuity", to name a few.

10 WAYS TO PROTECT OUR ENVIRONMENT

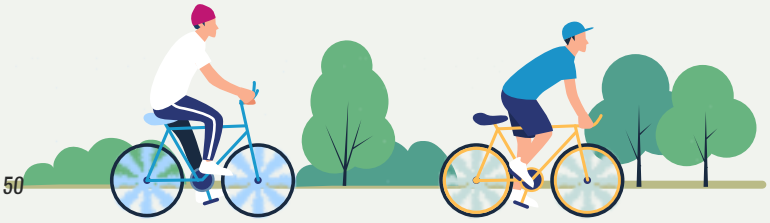
CHOOSE REUSABLE USE PRODUCTS

CONSERVE ELECTRICITY

RECYCLE PROPERLY

BUY LOCAL CHOOSE ECO-FRIENDLY PRODUCERS

WALK, BIKE, OR CARPOOL



CONSERVE WATER

Being mindful of ways that we can benefit our environment will lead to a better-preserved planet for us and for future generations. Becoming more environmentally friendly simply requires a few minor changes to our daily lives.

PLANT A TREE

USE FEWER CHEMICALS

IMPROVE YOUR DIET

COMPOST

DISCOVERING THE WESTERN SIDE OF MADAGASCAR

Madagascar is known for its exceptionally rich fauna and flora. It is one of the places in the world that shelters the most endemic animals and plants.

The vegetation has not gone unnoticed, as is much more important and greener in the east of the country than in the west, where it is very hot, dry, and very desert-like.

But despite this climate, the western side of Madagascar remains a place flooded by travelers from around the world and invites adventure and contemplation, from the natural pools of Isalo Park and its lemurs, or the Kirindy Mitea National Park to appreciate the water birds, lakes, sand dunes or forest islands, to some species of baobabs.

The west coast of Madagascar has a lot to offer. Through the beauty of its landscapes, its cultural richness, and the hospitality of its population, this region does not leave the visitors indifferent to a discovery of unique island culture.


IE
OF
R

Discover the biodiversity of the western side of Madagascar

Must visit places

1. **Tsingy de Bemaraha National Park**
   The Tsingy are huge limestone cathedrals that rose from the earth millions of years ago. The Tsingy de Bemaraha National Park of Madagascar is home to spectacular karst landscapes, never seen elsewhere. Known as the Forest of Stone, the park offers a very special landscape that can only be seen on the red island of Madagascar. This karst forest is a strongly jagged limestone massif forming peaks sharpened like knives. The lemurs like it here and they are easily observed. The park is located 300 kilometers from Tananarive in the center-west of Madagascar.

2. **National Park of Isalo**
   The Isalo National Park is located 269 km from Fianarantsoa and 80 km from Ihosy, it is in the Commune of Ranohira. It is a unique ecological representation within the network of National Parks Madagascar. It is the most visited circuit for its splendid green swimming pool, a true luxuriant oasis fed by a waterfall of tepid water. You evolve in the middle of varied ecosystems going from the cliffs to the plain of Tapia, astonishing trees with multiple uses, while passing by the Bara and Sakalava burials. You travel in a rich and strange culture, through geological ages.

   You can see plants with remarkable adaptations, but also Lemur Catta in the forest of Mangily.

   This visit will make you admire imposing landscapes: massively eroded savannah with strange shapes, Bara and Sakalava tombs, Tapia, and panoramic views.

3. **Kirindy Forest and Special Reserve of Andranomena**
   It is located in the Menabe region, Kingdom of the Sakalava, about 70 km south of Morondava on the edge of the Mozambique Channel and intermittently traversed by the Kirindy River. A true jewel of western Madagascar and a remnant of the primary dry forest.

   The forest is one of the best destinations for bird watching, such as; the red-tailed vanga, Madagascar hawk, Coua, bird of paradise, and the striped-bellied falcon. Birdwatchers will highly appreciate a visit to these unique places.

   It is only at night that you may have the chance to see fossas, these small endemic fawns of Madagascar, the ideal scenario is to prepare a guided night visit, a real playground for naturalists, botanists, or nature lovers.

4. **Baobab alley**
   Trees, more than 800 years old, are called “renala” which means "mother of the forest" in Malagasy. It is the emblematic landscape of Madagascar, nicknamed the red island. A dozen baobabs of 30 meters high and 5 meters in diameter line the dirt road that connects Morondava to Belon'i Tsiribihina in western Madagascar. This majestic alley is located in the Menabe region.

Endemic animals

Madagascar is a dream for young and old explorers. With its varied vegetation and unique climate, the island is home to an incredible diversity of animals, some of which are endemic and rare. Going to Madagascar allows you to discover the most beautiful things nature has to offer by planning a safari, to meet an exceptional animal world.

The lemur: Emblematic animal of Madagascar, the lemur is one of the species that you will cross most often on the island. The most famous star of the cartoon "Madagascar", is the Catta lemur, also called Maki, with its black and white striped tail.

The fossa: The most feared predator of lemurs is the fossa, endemic animal to Madagascar. This big cat is the biggest carnivore on the island. It lives mostly in solitary and hunts by day and by night. Measuring at about 70cm long, it is smaller than a puma and weighs on average 10kg.

The aye-aye: Another curiosity of Madagascar, the aye-aye, is found nowhere else in the world. This primate with large triangular ears, like those of bats, also has a long tail. It feeds mainly on insects that it collects in the holes of trees with its long fingers. It is the largest nocturnal primate in the world, measuring at nearly 90 cm in length.

Where to dive in Madagascar - Westside

Famous for its numerous coral gardens, its multiple species of fish, but also for the observation of larger specimens, the fifth-largest island in the world has something to offer to the lovers of the sea bed.

1. **The beach of Anakao in Tulear:** Located south of Saint-Augustin, south of the city of Tulear, is one of the most beautiful Malagasy beaches. It is bathed in light and sun, surrounded by a warm water lagoon of turquoise color. We come there to swim, snorkel, enjoy nature, and recharge our batteries. The best way to get there is by boat, although it is possible to take a track, considered rather a detour that will make you lose 5 hours of time.

2. **Nosy Ve, off Anakao:** three kilometers off Anakao, in the Mozambique Channel, is Nosy Ve (not to be confused with Nosy-Be). Its particularity lies in the presence of a coral reef, suitable for snorkeling. It is a natural aquarium where visitors can swim with colorful fish, turtles, and stingrays. In addition, there are beach activities, such as lounging and swimming.

3. **Ifaty beach, in Tulear**: located 25 km north of Tulear is a beautiful white sand beach, bordered by pleasantly warm crystal clear water. It is a place of bathing, also favorable to snorkeling and diving, particularly magnificent, since it makes you think of the paradisiacal beaches of the Caribbean. Ifaty beach can only be reached by sea and land.

Avoid cultural misunderstandings

The west side is the ideal region to immerse yourself in the heart of the Malagasy culture and discover the traditions of the population, the ancestral rites of the Sakalava Boeny (Majunga), or the Sakalava Menabe (Morondava, near Tuléar). A little further south, the rites and Antandroy tombs do not escape the visitors.

Here are some tips to avoid clumsiness with a Malagasy:

1. Never despise the Fady (forbidden). It is, thus, essential to be accompanied by a local guide to communicate with the Malagasy and especially to obtain essential information on the "fady" (local prohibitions and taboos).
2. There is no such thing as "tutoiement or informalities" in Malagasy grammar, so it is best to be polite before you have established a close relationship with a person. Slipping a few words of Malagasy into a conversation is always appreciated.

Sample itinerary:

The western tourist circuits will allow you to discover the main tourist attractions of the region.

The western itinerary starts in Antananarivo which is the capital of Madagascar, passing by Antsirabe nicknamed the city of water, the coolest city before joining Miandrivazo, on the contrary, the hottest of the big islands.

Then, you will discover the original descent of the Tsiribihina River by traditional dugout or by motor boat or barge. Landscapes, warm welcome of the locals, camping, waterfall, not to mention the endemic fauna and flora of the region, and many other experiences that the Tsiribihina trip offers you in this western circuit of Madagascar. Apart from that, the famous Tsingy de Bemaraha, a UNESCO World Heritage Site with its cathedral-like limestone massifs over 60m high is a must see. Canyons, panoramic views, possible climbs, long beaches and mangroves, and several endemic species. And as a highlight, the majestic baobab alley, directed Morondava which is the capital of the Menabe passing by the Sacred Baobab, the Baobabs in Love, and the Baobab Avenue at sunset.

Partnership with PECB

Sustainable Management Systems Consulting is a firm specializing in training, auditing, and coaching on international management system standards. We bring a solution to professionals willing to make their structure evolve.

Through our partnership with PECB, since 2005, we support learners by training them until their certification exam.

We are very proud of this offer because it is an opportunity for us to be the market leader in professional training in management systems and ISO standards.

We answer all calls and requests for training on the big island. And it is even an advantage for this profession because it allows you to travel while working, widen your connections, and thus, increase the notoriety.

in

Andry Jean Marc Rakotomanjaka

Having studied computer science, Andry is an environmental advocate. To combine his passion and his studies, he became a national expert on biodiversity informatics and teaches researchers to use scientific data on primary biodiversity. Andry is also a member of several associations where he trains young people on education, information technology, and environmental projects. He founded SMS Consulting, where he teaches, audits, and supports companies in the implementation of management system standards for sustainable development and corporate social responsibility. He is currently working there as l Executive Manager.

A Better Understanding of Modern Crisis

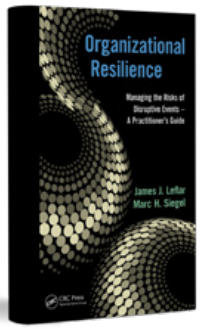
During recent years, we have all been faced with crisis, therefore, all organizations were put in the position of learning how to best become resilient and operate well with no disturbances to services. Reaction time became very prominent, as did the manner of response. Since we are living through a pandemic, the initial management of crisis for all organizations became a priority overnight, finding a lot of organizations unprepared for such circumstances.

Understand crisis management and resilience in such instances better through these books that will provide more detailed information on being prepared, handling crisis, and managing your organization successfully during such occurrences.

1. Crisis Management: Resilience and Change by Sarah Kovoor-Misra

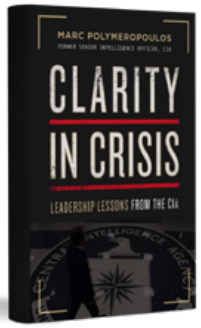
This book presents an up-to-date look at present-day crisis for organizations. The author gives real-life examples of crisis management, through a combination in the material of theory with practical usage, especially regarding the use of social media and the internet. As we have become more of a media-driven society, modern organizational crisis have become more complex, frequent, and diverse, this book provides an introduction to best practices for learning, containing, and preventing such crisis. The author also notes the strengths of existing works on crisis management, such as; leadership, communication, and stakeholder perspective, all the while including aspects of crisis management, such as change, ethical, global, and emotional angles. Additionally, this book also includes chapters on prevention, adaptability, resilience, and rebuilding of organizational reputation in the face of calamity.

2. Organizational Resilience: Managing the Risks of Disruptive Events – A Practitioner's Guide by James J. Leflar and Marc H. Siegel



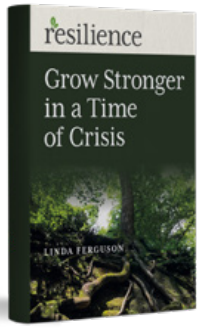
The book serves beginners in this field, advanced security practitioners, and the always increasing group of persons that need to understand, implement, and enforce standards, as well as guidelines produced by organizations like NIST, CEN, and ISO. This book represents a big step forward to better adopt and implement the several standards that get released in the field of Organizational Resilience. The book covers aspects that are valid for all organizations, despite the complexity and the size. The authors define organizational resilience in terms that are easy to understand, while also providing real-world examples. For an organization to move towards resilience, simply implanting policies and procedures will not be enough, as a process, it takes organizations on a winding path that requires patience and tolerance. Through this book a reader will come to appreciate the necessity of any organization, regardless of size, to have a risk management plan.

3. Clarity in Crisis: Leadership Lessons from the CIA by Marc E. Polymeropoulos



Clarity in Crisis speaks of the art of making difficult decisions with a less than ideal amount of information and makes avoiding the consequences of mishandling a crisis, which can escalate quickly and leave irreparable damage to an organization's reputation, easier. Through this book, the author delves into how true leaders should lead in times of crisis and thrive under conditions of obscurity, rather than avoid hard situations. In other words, Marc generalizes the successful methods he used to solidify clarity of mind when making crucial decisions in high-pressure situations. The book provides critical proven strategies and principles that can apply to face any crisis, sharing more in-depth information on the elements of managing a crisis, the understanding of the importance of key fundamentals, implementing guidance, and gaining confidence in your decision-making. The author, a senior intelligence officer in the CIA who has lived these situations, outlines for us what he practiced himself to achieve unshakable clarity in crisis.

4. Resilience: Grow Stronger in a Time of Crisis by Linda Ferguson



Once faced with difficult times, everyone reacts differently, some become stronger, more resilient, and more innovative under pressure. In recent years, most organizations have found themselves midst crisis, therefore, the time to take action and react in favor of your organization was very evident. In times of crisis, knowing when it will pass is unknown to all involved, hence why understanding how human beings function at their best, and their willpower to make changes in behavior and perception with a vision of a better future, is essential. This book allows you to create the conditions that allow your best efforts to come forward, with multiple hands-on exercises that deepen your self-knowledge. As we cannot control the outside world, what we have control over, however, is how we respond. Especially during these times of a pandemic, through this book, you will be able to discover pockets of resilience, learn, and thrive in times of any crisis.

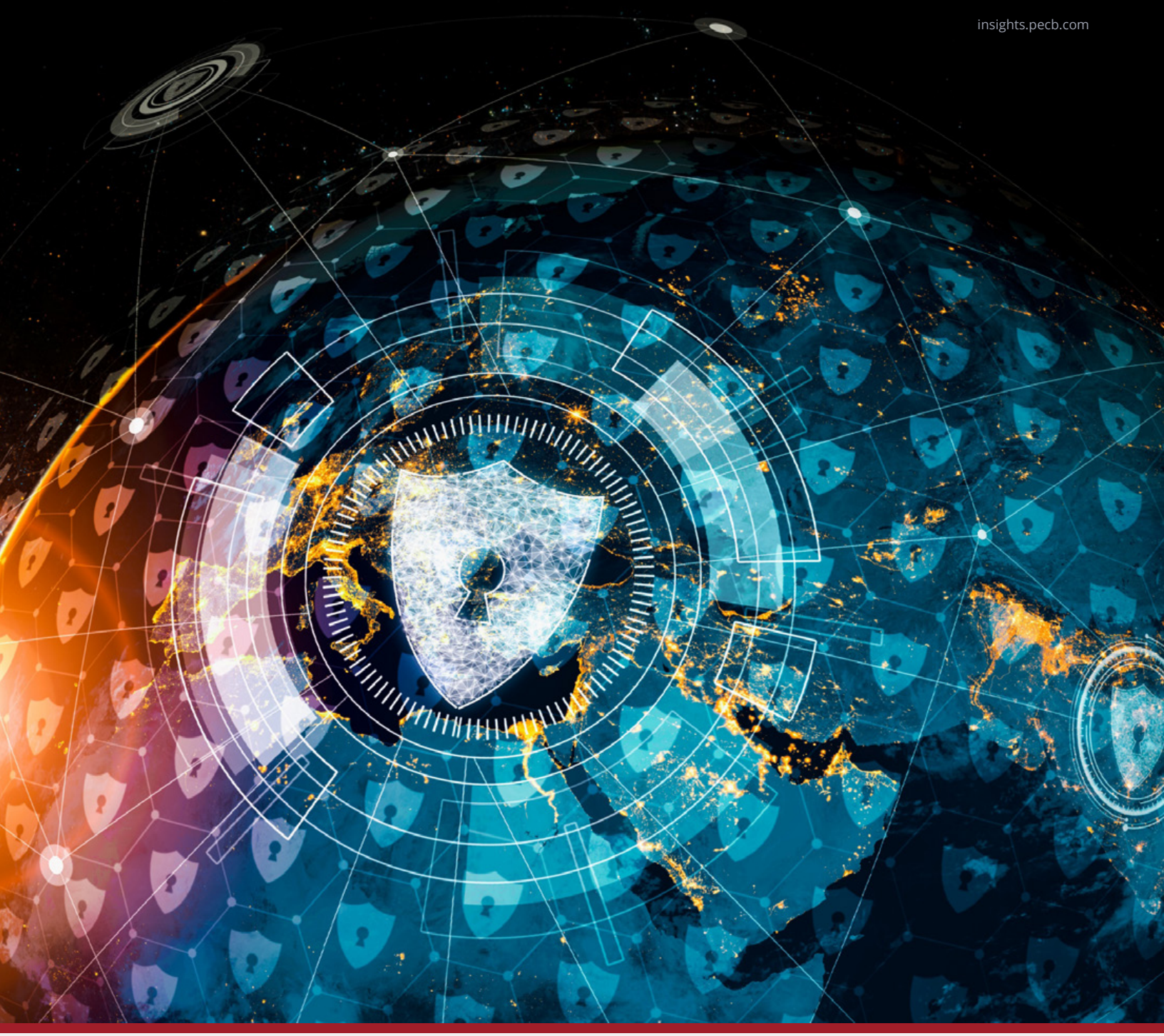
THE LATEST VERSION OF ISO/IEC 27002 IS NOW AVAILABLE!

Understand the benefits of an ISO/IEC 27002 certification

- → Having the knowledge to implement information security controls according to guidelines
- → Understanding the relation between groups of information security, such as; asset management, a human resources, environmental security, etc.
- → Possessing the skills to support an organization in selecting, implementing, and maintaining secur
- → Understanding the process of performing periodic risk assessments and selecting the appropriate
- → Having the knowledge needed to be part of an information security implementation team

Learn more about ISO/IEC 27002

To learn more about this or other training courses, contact us at marketing@pecb.com.



ccess control, operations security,

ity controls in compliance with ISO/IEC 27001
risk treatment

A High-Performance Information System: A Major Competitive Advantage

BY ERIC BERLANGA, ERIC GORMAND, PHILIPPE BLOT LEFEVRE, PARHAM MOILI

Is there internal reluctance for executives to tackle digital subjects and to carry on with it within their company?

As seen from the side of the business manager, IT, digitalizing means always more costs of protection and budget, but let us recognize that the counterpart of digitization means more turnover, more information available, and more productivity. They are, therefore, gains to support these costs.

Digital means it should be complex and the natural tendency is to leave it to specialists: the IT or outsourcing department, SDI – CISO. However, these are players who are rarely integrated into the heart of the company's decision boards and councils (Codir, Comex council administration).

If we see it from the side of the IT department, the main part of the job consists of dealing with emergencies, being focused on productivity service, solving bugs and unavailability.

With very tight staff, these priorities are done to the detriment of more structuring and yet essential tasks, such as updating IS, training users, raising awareness of risks, and typical tasks that enable avoiding cyberattacks or fixing them with as little damage as possible.

As seen under the prism of governance, digital technology, for twenty years, permitted a corporate culture focused on the search for transversality and the fluidity/availability of information, to the detriment of a culture of secrecy.

Moreover, employees are less aware of the risks and the value of information that they hold.

The classification of documents (industrial secret, confidential company, etc.) seems to have disappeared from many companies.

What are the Solutions?

We have measured, during exchanges with leaders that digital subjects from the angle of risk and vulnerability, remain a subject with which business leaders and boards of directors are not comfortable with. Many administrators call for the creation of digital committees so that these subjects are addressed with more pedagogy so that all decision-makers measure the issues better.

The challenges are twofold: to draw up an inventory of the company and its subsidiaries (in the short term), and why not of its main suppliers, and to focus on people by training employees to deal with the culture of the company (a long-term goal).

A 360° INVENTORY INCLUDING AN INTERNAL R'U SAFE SCORING ON BANK COMMUNICATION APPLICATIONS

Companies face some awareness issues when it comes to measuring the vulnerability of their company toward external attacks but also toward the risks of internal fraud; and the latter mainly concerns the treasury departments and executives who, detecting a vulnerability, decide to take advantage of it without necessarily having premeditated their act which is not in accordance with the law.

Companies that have suffered ransomware attacks and have difficulty recovering their data and their level of activity are generally ill-prepared companies that buried their heads in the sand or were in denial with the pretense that: "It happens to others!". For medium-sized companies with a CIO or CISO, the latter is considered an external diagnosis, as an intrusion likely to demonstrate rather than support its recommendations, and budgets commensurate with the challenges with its general management.

It is on the strength of this analysis that we, at R'U SAFE, have developed diagnostics with assessment tools, giving a clear picture of the risk, clearly understandable to general management.

For this awareness to take place, we have combined five areas of expertise within the "PACK R'U SAFE" diagnosis to paint a faithful picture of the state of maturity of the structures. We assess both the quality of the shell but also the corporate culture, the quality of human factors being identifiable by an analysis of the application of the GDPR within the company.

This combination and the links we establish between expertise and the application of ISO 27001 methodologies are unique. 7 days to put it all on the table!

Our "FOCUS R'U SAFE" diagnosis focuses on the two most neglected areas of expertise in the company, even though they concentrate on the greatest vulnerabilities in cash management security scoring and the measurement of maturity and the impact of cybersecurity.

The challenges we identify are to rebalance the circulation of information in companies while maintaining a spirit of sharing. There is too much circulation of sensitive information "unknown" in the company. Just consider this: how many unopened and unclassified files do we have in our mailbox; these are sometimes emails we are in copy, as a report or "just in case, information that we hold "without knowing it" but we are responsible for.

The return to a more selective or confidential culture requires time and a training effort for all employees. It is all about creating a virtuous circle to place the data in a better-controlled environment.It is important to be well trained, and we identify three poles of teaching.

Called data security, the first one concerns cybersecurity issues (iso 27001 and cash management). Some courses are for everyone in order to better share a common language with digital specialists, the others are more dedicated to the IS department and lead to a certification.

The second pole of teaching deals with the respect for employees and customers, leading to the voluntary restriction of personal data: called data compliance. The course is all about principles linked to the European GDPR (General Data Protection Rules).

The third one, and most innovative, concerns data governance, or data management. We envision it for decision-makers and strategists.

More aware, members of committees and boards of directors will better identify the strategic nature of the budgets requested by IS.

The fight against cyber threat has resulted in many companies accumulating protection systems, technical solutions, yet it does not allow the invulnerability of the citadel. Any company is likely to be attacked, it is the resilience and education of employees that must now be given priority.

Considering that security is mainly the business of specialists, i.e. the IS department, is to take the risk of demobilizing or, worse, of not feeling individually concerned by this. In this matter the D&IM will provide new insights to the governance.

The New Function of Companies Entering the Digital Economy Profile – Document and Information Manager (D&IM)

With regard to entrepreneurial responsibilities, the CEO must be omnipresent and omniscient. The impossibility of such an exercise has forced them, since the creation of the first public limited companies around 1865 depending on the country, to delegate their powers according to internal professions that they all had to assume together. Having become overwhelming, these strategic, technical, and coordinating functions of the CEO forced them to delegate what was becoming too complex for one man to assume. Thus, born were COOs, CFOs, CCOs, CTOs, CMOs, etc.

On the threshold of the 2000s, never had upheaval been as sudden and abundant as that of multimedia. In a kind of panic related to new emerging issues, organization, and infinitely advanced technologies, companies have organized themselves by expanding or subdividing existing functions. This "off the cuff" movement does not respond to the problem of Documents and Information (D&I), which requires a height of view, a vision in perspective, and an authority that the 16 main information functions counted in different organizations do not satisfy. And the CEO remains responsible without being able to act with the aplomb or the accuracy necessary to preserve – inescapably and confidentiality, the need to know, the quality of information; and recently, disinformation whose inflation is galloping.

The Substance Justifies the Form

Essentially, it is only by precisely understanding the role and position of D&IM that we appreciate its dimension, which is absent from related professions. On the form side, what does the D&IM function add to the existing one to be more successful?

There are three possibilities:

1. The consideration and implementation of the D&IM function by the CEO
2. The addition of the function within the CODIR,
3. Outsourcing to a consulting partner

What exactly is the D&IM and its function?

- The D&IM function aims to identify, enhance, and control documentary processes in the organization.
- The D&IM is an actor in the governance of the company and a leader at the service of the operational departments in their internal and external activities.
- The D&IM is a change management professional.
- The D&IM is working on the urbanization of the D&I system. It formalizes the organization's documentary policy by verbalizing the cognitive loads, processes, and life cycles of the D&I to guarantee the company with regard to its environment.
- The D&IM works in conjunction with the company's support functions: DOI, DSI, DAF, RM, RSSI, HRD, etc.

General Principles – The Function of D&IM

The D&IM performs a transversal function of the organization. Today, it imposes itself on the company by:

- The competitive advantage provided by the control of Documents and Information (D&I)
- The growing volume and complexity of information, digital, and paper media to be mastered within the organization
- The criticality of the documents in the organization's environment (technical, legal, regulatory, capital value, disinformation, etc.)
- The control of costs and risks (creation, production, software and hardware tools, flows, reuse, use and authorization, restitution, destruction, etc.)
- The technical and economic obligation to control the life cycles of documents
- The complexity of today's organizations (VUCA) regardless of their size

The D&IM does not necessarily have a direct hierarchical position, vis-à-vis the various actors of the organization, but always a role of governance. They exercise local and international leadership on all D&I matters. The hierarchical position of the D&IM in the organizational chart of the organization is a direct or functional attachment to the general management which entrusts it with its mission. They are aware of and can participate in the definition of the company's overall strategy.

They are the guarantors of the application of a D&I policy in line with the strategy of the organization.

The function of the D&IM is recognized as essential for the governance of the organization by the general management and by the operational departments.

Since the D&IM is the link between the actors involved who are responsible for the operational implementation of the D&I strategy and the actors concerned who are the users of the information assets:

- The D&IM belongs to the general management. As members of the Management Committee, they are directly involved in the company's strategy. They are committed to the result.
- The D&IM intervenes at the level of the operational departments. They participate in the project launch committee and in the steering committee. However, they are not responsible for the operational implementation, nor for the management of the operational teams, or for the budgets of the departments involved.

D&IM Missions

The missions of the D&IM are thus to guarantee the correct identification of documentary sources, their uses, the risks, constraints, and challenges; to define the D&I strategy in line with the company's overall strategy. The D&IM declines the D&I strategy for the entire "D&I Network", the organization, and for each operational department. He steers the implementation of the D&I strategy and reports to General Management and the “D&I Network”. Therefore:

- The D&IM issues a detailed opinion on the technical and legal tools of the “D&I Network”
- The D&IM qualifies and guarantees control of the D&I relationship with the organization's third parties
  - monitors the implementation and compliance with the guidelines
  - proposes areas for improvement and be a vector of documentary innovation

At the level of the operational departments:

The D&I strategy is broken down into an action program for each operational department (tactics for the implementation of the D&I strategy) materialized by measurable objectives in the short and medium terms, achieved in collaboration with operational departments and third parties. Dashboards are set up, including performance indicators (KPIs) and monitoring of the achievement of objectives/performance).

This strategy is updated according to the indicators (human, time, financial, etc.). It oversees the D&I coordination of the departments with their operational departments (equivalent to a D&I steering committee). It exercises monitoring and control of D&I action programs (guarantor of compliance with the strategy), such as participation in steering committees, monitoring of dashboards, etc. It monitors compliance with common D&I standards.

Change management:

- The D&IM animates the D&I network. It is a role of federating actors: communication, promotion, and education of the function, with the establishment of a D&I community of practice and rights of use to be reserved for them. The D&IM proposes and holds, if necessary, training courses, seminars, webinars, etc.
- Resources and outsourcing
- The D&IM must have the resources in relation to the objectives retained in its missions for the organization. These resources are external, internal, and financial. They include the animation of a network and an ad hoc staff.
- Like all the major departments sitting on the CODIR, the D&IM presents an operating budget (operation, R&D, etc.), and an investment budget correlated with the other departments.
- The D&IM function may be entrusted to a third party, but in order to be operational and able to exercise its right of veto, to any of the departments sitting on the CODIR, other than the CEO. It is, therefore, up to the latter to subcontract the function to an external firm, duly authorized to exercise it and report to it.

What are the limits of the consultant compared to a D&IM

- In large companies, the consultant often only has a fragmented vision of the organization. They will never have the culture of the organization or the links with the various actors. They will also not be aware of opportunities to promote the D&I documentary function. They are present only occasionally and only have an advisory role: they are not a decision-maker and the CEO, to whom they report risks never put the D&I issue at the forefront of decision-making. In essence, nothing will really change but it is a gradual way to persuade the CEO to start the process.

The return to a more selective or confidential culture requires time and a training effort for all employees.

It is all about creating a virtuous circle to place the data in a better-controlled environment. Culture, as well as new tools, will help.

Tackling the Cyber Risks with a three in one automatization

Organizations are subject to strong competition and are looking for levers to increase their productivity, and thus, gain market share.

One of the highlighted areas is the digitization of business processes and working tools, this digitalization results in the transformation of activities within the organization.

This quick digitalization, also called Industry 4.0 in the concerned industries, leads to the adoption of more and more software, and therefore, increasing dependence of the organization on its information system.

This dependence results in strong demand by the organization for its information system, which requires it to deliver the highest level of infrastructure, availability, and business application, while controlling its costs.

Cyber Risks: Damocles' Sword Hanging Over the Organization

The information system is central and vital for the organization. It becomes a privileged target: industrial espionage, data theft, voluntary destruction, encryption, and ransom. As these cyber risks become increasingly prevalent, many laws and regulations tend to impose the adoption of adequate measures to mitigate risks: Bâle, GDPR (RGPD), SOX, NADCAP, ISO 27001/2, etc.

This triple constraint: company requirements, regulatory requirements, and consideration of cyber risks, oblige the information systems to adopt a virtuous approach, maintaining regularly updated systems and software.

Without going into details and technical considerations, the information systems and their underlying rchitectures are increasingly complex and nested (On-Premise, Cloud, Hybrid, Virtualization, Containerisation, etc.).

Cybersecurity Recommendation: The Critical Importance of Implementing Updates

The complexity of information systems raises the possibility of an increase in risks due to loss of control.

The French Agency for Information Systems Security (ANSSI) supports French companies by providing them with a guide to take back control of their risks and information system.

This guide proposes 42 technical and organizational measures, which can serve as a basis for an action plan to increase the overall information system security level.

Essential Measures

The information system security level is equal to the lowest security level of one of its components. This is why mastering the information system urbanism is essential.

One of the essential steps to achieve this mastery is the modeling of an application mapping, allowing to identify the place and the role of all the tangible and intangible assets of the information system, thus the identified data allows the application mapping to conduct impact studies, implement defense strategies, and draw up maintenance and update plans.

More than 40% of global security incidents are caused by a lack of updates on the targeted equipment. With the help of application mapping, it is important to reconcile, on one hand, the economic stakes of the organization and the consequences due to the unavailability of its information system, and on the other hand, scheduling regular updates of all information system equipment.

An organization's productivity loss caused by the downtime of information systems can be reduced by increasing communication (planning and reminding) between the technical teams and the business teams.

This communication facilitates the acceptance of measures, improves the business's confidence in the information system, and allows business teams to organize in the absence of their digital tools.

Monitoring the proper application and effectiveness of the measures is essential in order to build a solid safety policy.

These measures, which are central to ISO/IEC 27001 and ISO/IEC 27002, can be implemented in successive iterations, materialized by the famous Plan Do Check Act, and thus limit the burden on the technical teams to implement them.

Regular audit results highlight the strengths and weaknesses of the measures in place, help consider corrective action plans, and identify regressions if they occur.

Internal and external auditors rely on factual evidence to establish their ratings and recommendations. The measures described above strengthen the maturity of the information system and provide the elements of response to the auditors.

When drawing up the Master Plan for the information system, it is essential to integrate the implementation of measures for each project.

Moreover, since the application mapping is central to considering an effective security policy, it is important to transcribe each information system evolution in the application mapping in order to remain accurate.

The Cloud – A Finality?

We observe a process that aims to see many scopes of the organization's information system migrate from a traditional model, also referred to as on premise, to spaces belonging to third-party entities, also known as the cloud.

Under the generic name cloud, it is necessary to distinguish the two different concepts. On one hand, the remote Datacentre allows hosting all or part of the servers that make up the Enterprise Information System. On the other hand, the SaaS (Software as a Service) and IaaS applications (Infrastructure as a service) are entirely the supplier's responsibility.

In both cases, the objectives pursued by the companies are transferring the associated risks, responsibilities, and costs, and switching the investment budgets (CAPEX) into the operating budget (OPEX).

The purpose of these suppliers, like any organization, is to lead economic logic to make profits. The choices and investments that are necessary to maintain a high level of security, are often not communicated thoroughly, only through displayed labels which suggest that they follow the main recommendations. At the same time, they face the same difficulties in recruiting and retaining qualified technical profiles.

Finally, they are privileged targets of attackers because they centralize large volumes of data.

The keyword for deciding on a cloud migration of an information system component is pragmatism. Is the tool critical? How long can we do without it? Is the data sensitive or critical for the company, for its activity? Consequently, not all components of the information system are intended to leave the organization.

Take the case of a classic industrial site with production units, quality department, logistics, and finance.

What happens in case of communication loss? Do the degraded procedures ensure, at a minimum, continuity of services and that the company meets its obligations to its customers? Are the business teams prepared for this possibility?

The same questions apply to a healthcare facility where all information and healthcare devices are controlled by the information system?

The hybridization of the information system makes it possible to take advantage of the best of both approaches.

Process Automation: An Essential Tool

The information system maintenance operations, mainly the application of updates, are becoming more and more numerous and complex to apply.

Human intervention must be kept to a bare minimum to ensure a high level of reliability. The adoption of automation tools is now becoming indispensable within the information system.

It allows technical teams to model maintenance operations and also formalize knowledge and practices that were not transcribed but only transmitted orally.

The adoption of automation tools allows the IT department to become more mature, from both, a technical and an organizational point of view.

The choice of tool depends on the organization's constraints. In a simple scheduler or more advanced orchestrator, the need to control triggers between different sequences and operations is a decisive selection criterion.

However, the development of these processes requires numerous skills:

- Mastery of the technical environments and dedicated technical languages allowing the automation of tasks
- Maintaining a high training level of the involved resources

At the same time, the information system is constantly evolving, meaning that this change requests migrations, promotion of environments, new business tools, etc.

As a result, automation chains must be constantly reviewed and refined to take into account the new constraints.

Any new project within the information system must include an impact analysis and an update cost of the automation task.

The more complex and interwoven the information system is, the more difficult it is to define maintenance processes that take into account the many constraints.

In addition, any need to modify these processes quickly becomes extremely complex.

In this context, Robotic Process Automation (RPA) allows efficient response and sustainably to the modelling of complex environment maintenance processes.

Robotics enables the generation of entire processes without any human intervention, through a no-code approach. The adoption of automation is, thus, facilitated because it requires little technical expertise. The processes obtained are optimized to guarantee a minimum downtime of the business applications.

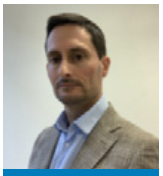
Whether the Enterprise Information System (EIS) is On-Premise or partially migrated to the Cloud, the mastery of application mapping is a prerequisite for any development of a security policy.

Armed with this mapping, the analysis of data flows of the information system serves as the basis for the writing of all processes that will allow keeping all equipment up to date.

The adoption of a scheduler or an orchestrator makes it possible to automate all the sequences and operations that contribute to maintain operations. To overcome the complexities of setting up and supporting automation, the use of robotics will ensure that processing times are reduced, the error rate is reduced and security is strengthened.

The solution published and distributed by xSécu makes it possible to put in place concrete measures, check their proper application, and measure their effects:

- Application mapping
- Robotics and Orchestration of maintenance processes
- Automatic communication of maintenance schedules to the business teams
- Ongoing audit of key equipment control points
- Automatic alert on thresholds crossed or events detected
- Reports being provided to publishers to disassemble the implementation of the measures



in

Eric Berlanga

Eric is an Information Systems Manager, software engineering expert, and founder of a publisher of cyber security solutions. For over 20 years, he has put his technical expertise and his functional perspective at the service of customers from all perspectives of life, such as; banking, finance, transport, medical industry, digitization of business processes, diagnosis of IT maturity, development, and implementation of cyber defense strategy.

in

Eric Gormand

Eric Gormand defines himself as an entrepreneur, but he has evolved over the last thirty years in positions of responsibility in the public service, in a large industrial group, and in the management of SMEs. His aeronautical training, as a combat pilot, gave him a pragmatism, adaptability, and resilience that allows him to accomplish his "missions" (deliverables) including in degraded mode. Curious and agile, he acts as a project manager and has expertise in the field of governance.

in

Philippe Blot Lefevre

Philippe is a serial entrepreneur in risk management. By working with people, he raised Concept-Consolidation, his financial reporting software package, to rank No. 1 worldwide. Mentor and coach of change management, he takes into account our supersensitive dimension to reduce the divergences between individual and collective interests, and increase performance.

In the 2000s, he defined the profile of the Document & Information Manager (D&IM), a member of governance who guarantees the quality and use of Documents & Information, their life cycles, risks, human constraints and techniques, and the issues. Philippe has published “Right of Use and Protection of Digital Information” (ed. Editea 2007).

in

Parham MOILI

Parham is a senior certified ISO/IEC 27001 lead auditor and lead implementor. For more than 25 years, he has been wearing new uses and new technologies within large companies and supports the digital transformation of organizations, business processes, and information systems. His excellent knowledge of banking communication applications and Electronic Data Management (EDM) allowed him to create 2 Scoring repositories on Cash Management administration (AUSECAF) and Security of the EDI banking platforms (SECEDI). He is the founder of the PECB certified training AUSECAF (Anti-fraud security audit on banking communication applications).

For more information on this global article, you can reach Parham at +33 (0) 650 00 03 89 – pmi@rusafe.fr

PECB eLearning

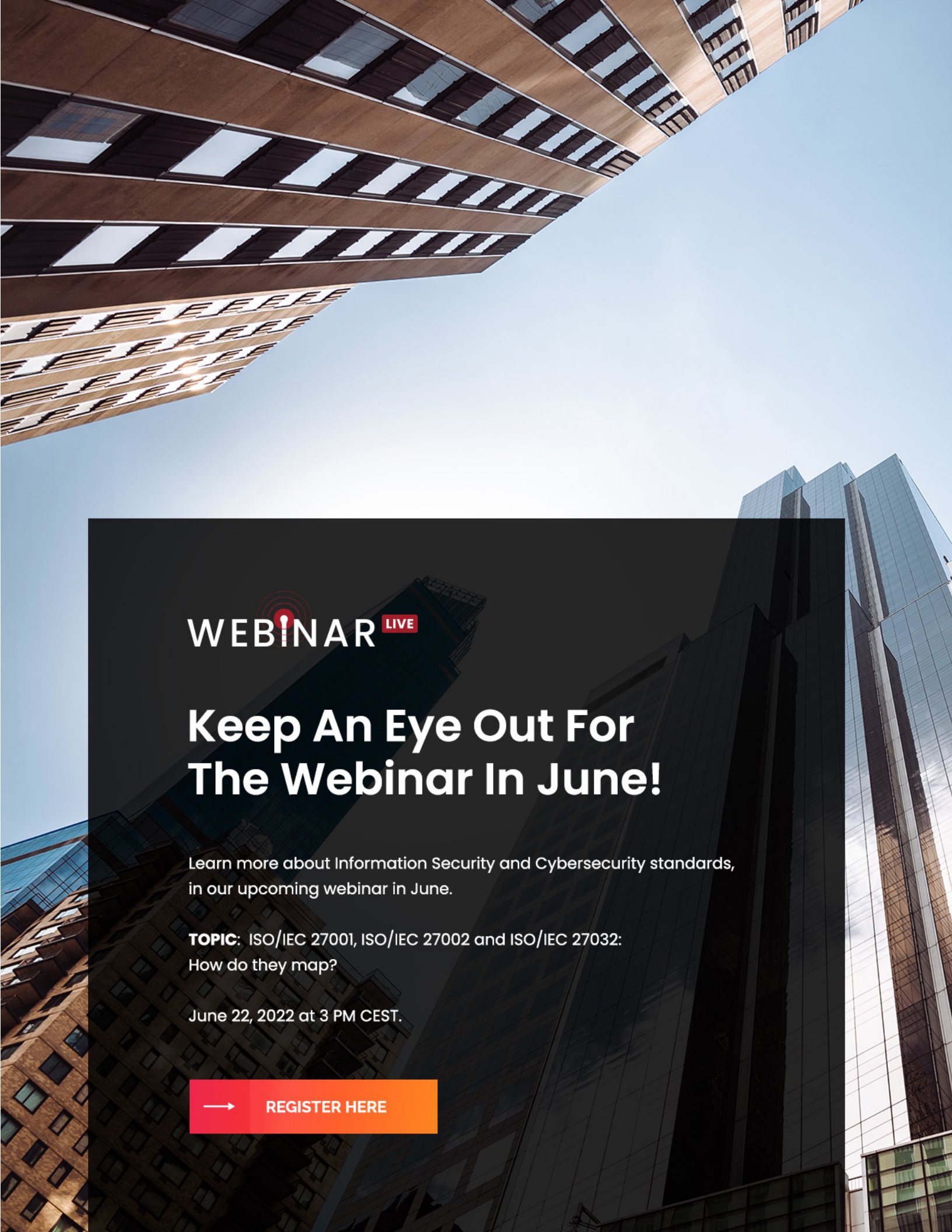
ISO 22301 Lead Auditor eLearning Training Course in English Available!

Enrich your portfolio with this excellent opportunity to get your certification in ISO 22301 – Business Continuity Management System, through the comfort of your home.

As an international standard, ISO 22301 is designed to protect, reduce the possibility of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. With a Business Continuity Management System, your organization is prepared to detect and prevent threats.

CHECK THE BROCHURE!

To learn more about our other eLearning training courses, please **click here**.


WEBINAR
LIVE
Keep An Eye Out For The Webinar In June!
Learn more about Information Security and Cybersecurity standards, in our upcoming webinar in June.
TOPIC: ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27032: How do they map?
June 22, 2022 at 3 PM CEST.
REGISTER HERE

Top Five High-Paying Job Positions You Can Pursue with a Crisis Management Certification

During the last two decades, technology has been developing rapidly, leading to an impact on other areas and ultimately changing the way organizations conduct business. However, regardless of how useful these changes have been, organizations still deal with different disruptions, be it from natural or human causes. Hence, the need for organizations to ensure resiliency and business continuity when dealing with disruptions is present and is increasing.

Every organization might be susceptible to disruptions or crises, which may impact the relationships with their stakeholders, as well as their reputation. Thus, organizations should emphasize the creation and establishment of proper ways to respond to crises.

In order for organizations to manage crises effectively, they should anticipate potential crises and determine the strategies they will use to address those crises. Having competent personnel is also a necessity when striving for effective crisis management. Additionally, organizations need to establish strategies for communication before, during, or after a crisis in order to build trust between their personnel, stakeholders, and customers.

1. **Disaster Recovery Manager**

According to Glassdoor, ZipRecruiter, and Salary.com, the average salary of a disaster recovery manager is **$110,110 per year.**

2. **Business Risk Manager**

According to Glassdoor, PayScale, and ZipRecruiter, the average salary of a business risk manager is **$102,401 per year.**

3. **Crisis Management Consultant**

According to PayScale, Glassdoor, and SalaryList, the average salary of a crisis management consultant is **$78,535 per year.**

4. Emergency Manager

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of an Emergency Management is **$74,546 per year.**

5. Emergency Management Analyst

According to Glassdoor, PayScale, and Salary.com, the average salary of an Emergency Management Analyst is **$74,365 per year.**

A crisis management certification will demonstrate that you possess the necessary knowledge and skills to deal with emergencies and disruptions that many organizations deal with nowadays.

It can pave the way for new job opportunities in organizations for whom crisis management plans are of fundamental importance.

Note: The salaries presented in this document are not definitive and may change with time and industry development.

We are in the process of developing the Crisis Management training course training course, as such, it is not ready for distribution yet. Please contact us at marketing@pecb.com to get information about the publication date.

Disaster Recovery, Crisis Management, and Business Continuity: Does the Terminology Convey Shared Meaning?

BETTY KILDOW

"A rose by any other name would smell as sweet." - William Shakespeare, Romeo and Juliet

In our profession, like most others, we have developed our own terminology, jargon, buzzwords, and acronyms used to discuss what we do, how we do it, and the end product of that work. If there is one thing that has remained consistent throughout the history of business continuity and its related practices, is the inconsistency of how we define and use terms. In my perspective, the most long-term (multi-decade) example of this has been Disaster Recovery and Business Continuity with these terms historically being misused, confused, and used interchangeably. While after a few good years this example does seem to be getting sorted out, as we continue to evolve and mature, new inconsistencies have created the same fuzziness. Ask a random group of practitioners to define business continuity and crisis management. You are likely to get varied responses. Some will say they are interchangeable terms, others will say that one is a subset of the other, while others will absolutely declare that they are two quite different things.

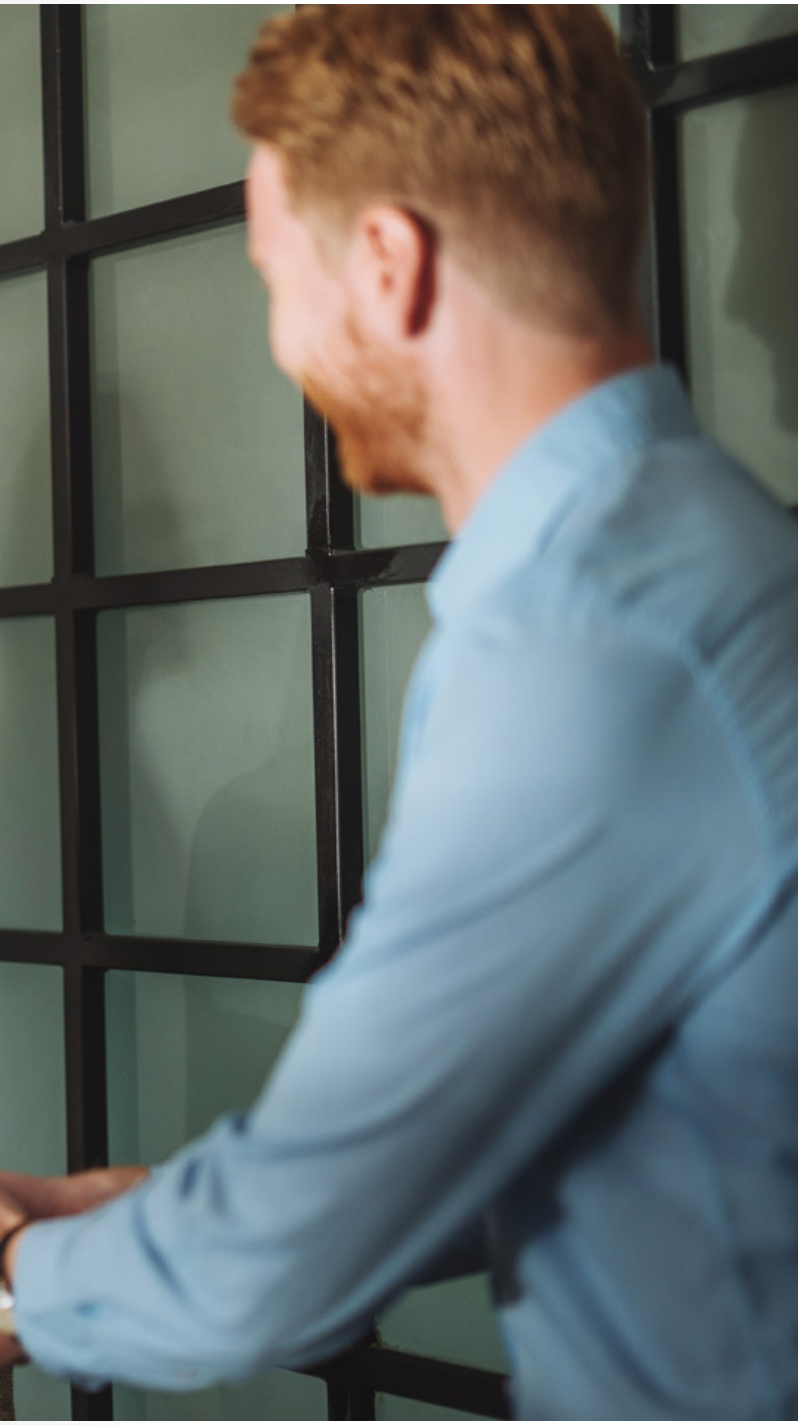
In approaching what for some may be a controversial subject, someone might warn me to avoid dealing with this potentially touchy subject. As my grandmother used to say: "Don't poke a stick at a hornet's nest."

But as fools rush in, here are some thoughts on this topic. To start, here are some brief definitions of three of our commonly (though not necessarily consistently) used terms, Disaster Recovery (DR), Business Continuity (BC), and Crisis Management (CM), with a couple of basic descriptions of each.

It is almost a given that some of those reading these descriptions will disagree with even these very elementary definitions. For those who do not like or agree with these,

they are only a small sampling of the thousands that can be found with a quick internet search. In addition, to verify that they are in fact important terms, each has a recognizable acronym.

- Disaster Recovery (DR) is the technical aspect of business continuity. A collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications, and data).
  - Disaster Recovery (DR) focuses on the ability to recover the IT infrastructure in case of a disruption, whatever the cause – natural disasters, cyberattacks, technological failures, or human error. It is viewed as being both proactive and reactive.



- Business Continuity (BC) is the capability of the organization to continue or restore delivery of products or services at acceptable predefined levels following a disruptive incident.
  - Business Continuity (BC) has as its goal ensuring that operations continue to enable products and services being delivered at pre-agreed upon levels when disruptions or disasters occur. Seen as being proactive.
- Crisis Management (CM) is the overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.
  - Crisis Management (CM) is responsible for ensuring timely, accurate decision-making to determine if the event is a problem, disruption, or disaster while managing the crisis, and it has the appropriate authority to declare a disaster, make notifications, activate teams, allocate resources, and oversee the management of the event. Viewed as being reactive.

It is a given that each of these three plays a critical role in protecting people, operations, physical property, and intangibles, such as company reputation, brand, and market share. Each contributes to creating a resilient organization.

The purpose, roles, and responsibilities under the heading Disaster Recovery have now been relatively agreed upon – with the possible exception of whether cybersecurity is part of DR or a separate entity – for now, let us take a look at business continuity and crisis management which I have noticed have recently become a topic of significant interest and discussion due to a lack of agreement on the roles of each, who is in charge, and how each best fits in the bigger picture of organizational resilience.

You have also quite likely noted the uptick in interest, as has Ashley Goosman, MBCP, MBCI, who noted in her Disaster Empire post “Business Continuity vs Crisis Management”: “People around me are taking opposing views about whether business continuity and crisis management are the same thing or not. One group sees crisis management as part of an emergency management structure.

They believe that business continuity only focuses on helping business operations to recover from an outage. Others, like the Disaster Recovery Institute International (DRI), see crisis management as part of an overall business continuity management program. Both sides believe they are right.”

Some might ask if we actually need a separate crisis management team plan, as it creates a new layer, one that perhaps overlaps with business continuity. In response, others might call attention to the fact that crisis management addresses situations where disruption may or may not pan out to impact operations to the extent of requiring business continuity activation, though may demand monitoring and perhaps media and social response to a threat to the company's reputation.

Another response from those questioning the value of a separate Crisis Management team would point out that a crisis management plan is one of a group of other specialized plans which belong under the BC umbrella, such as a pandemic plan, continuity of operations plan, or a product recall plan. On the other hand, some will say that business continuity should report to crisis management with crisis management taking a disruptive event under its control while business continuity enables operations to continue at an acceptable level.

Equally important, if both entities exist, do they work jointly, does business continuity report to crisis management or vice versa? Are responses initiated by crisis management and then turned over to business continuity? If so, at what point? In the meantime, what are the communication requirements between the two? What are the coordination points?

Perhaps this requires a review from a governance perspective where the business continuity organization is established, also roles and responsibilities are assigned to ensure that the current continuity organization reflects established governance. An important purpose of a business continuity policy is to provide a definition of what top management wants to achieve with the business continuity program. Does the approach we are taking meet the requirements established in our business continuity policy?

Are overall ownership, points of accountability, oversight, and support as originally established still valid, and are assigned roles and responsibilities still appropriate?

In some organizations following a negative event, disruption, or disaster, crisis management has as its focus communication – reputational management, public relations, media, and social media management to provide a unified response to protect the brand, reputation, and public image. For others, this is an element of crisis management. For others, this responsibility is yet another separate team that reports to top management and in some cases is titled crisis communication team.

One thing I believe we can agree on is this; neither business continuity, nor crisis management, nor disaster recovery, or any of the related functions can be viewed as a stand-alone separate discipline. Each plays a key role in building a resilient organization, in ensuring a capability to plan for, respond to, and recover from the multitude of risks that we all face today. Silos do not work; turf wars are counterproductive.

Keep in mind that even standards and best practices are meant to be a framework and to provide guidance, not a do it this way or else proposition. For example, ISO 22301: *"... provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities".*

While standards and best practices provide a framework, they do not dictate details for exactly how each and every organization is to apply the framework. The emphasis must be on what works for the organization, not what has always been done before, what other organizations are doing, the latest trend, or guidance that was chosen at random or because it was a perfect fit another company.

It is likely that full consensus on this subject will not be achieved any time soon. My question then, is it required that every organization take the same approach? I believe that this is not necessarily a case of absolute right or wrong, rather what is best for the organization.

If we can accept this, then whether to have separate business continuity and crisis management programs or a business continuity program that incorporates the crisis management functions or vice versa, is a decision to be made, not a foregone conclusion.

Either way, here are some questions that may be worth some thought:

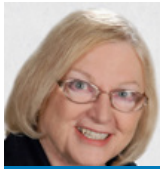
- Is our company's continuity organizational structure right for us? – No, two continuity organizational charts will be identical when organization size, type of business, location(s), products and services, resources, and culture are taken into account.
- Does the current continuity organization meet the requirements established in our business continuity policy and any other applicable policies? – If not, perhaps there is reason to revisit the policy or the continuity organization, or both.

- If changes have been made to the continuity organization, were tests conducted that prove that no gaps or overlaps in responsibilities and authority have resulted? – A change in any part of the organization will most likely require changes in others.
- For smaller organizations, have functions been combined, e.g., business continuity and crisis management, based on personnel resources?
- Are there built in mechanisms to ensure full communication, cooperation, collaboration, and coordination before, during, and following any disruption or disaster?
- Have you adopted a shared glossary of terms, acronyms, and definitions for use across your organization so that everyone understands and shares the same meanings for business continuity, disaster recovery, crisis management, and related terminology?

More importantly, keep the focus on the overarching goals of your program which likely include continuing the company's mission without major disruption, managing operations if the company experiences a significant disruption or disaster, continuing to meet customer and other stakeholder needs, and mitigating damage to reputation, or brand, legal, and regulatory issues.

Yes, shared terminology and agreement on what is the best organization for our company's resilience-related business units are important. Just do not let the focus stray from why we do what we do, to create and maintain a more resilient organization.

> **"I know you think you understand what you thought I said but I'm not sure you realize that what you heard is not what I meant." - Alan Greenspan**



Betty A. Kildow
FBCI, CBCP

Betty has specialized in business continuity and supply chain continuity consulting for more than twenty years, working with a wide-ranging variety of businesses and organizations. She is a PECB ISO 22301 Master, ISO 28000 Lead Implementer and Lead Auditor, and Certified Trainer, as well as a Certified Business Continuity Professional (CBCP) and a Fellow of the Business Continuity Institute (FBCI). Betty is a frequent conference speaker, a skilled trainer, and has written articles that have appeared in professional publications in North America, Europe, and Asia.

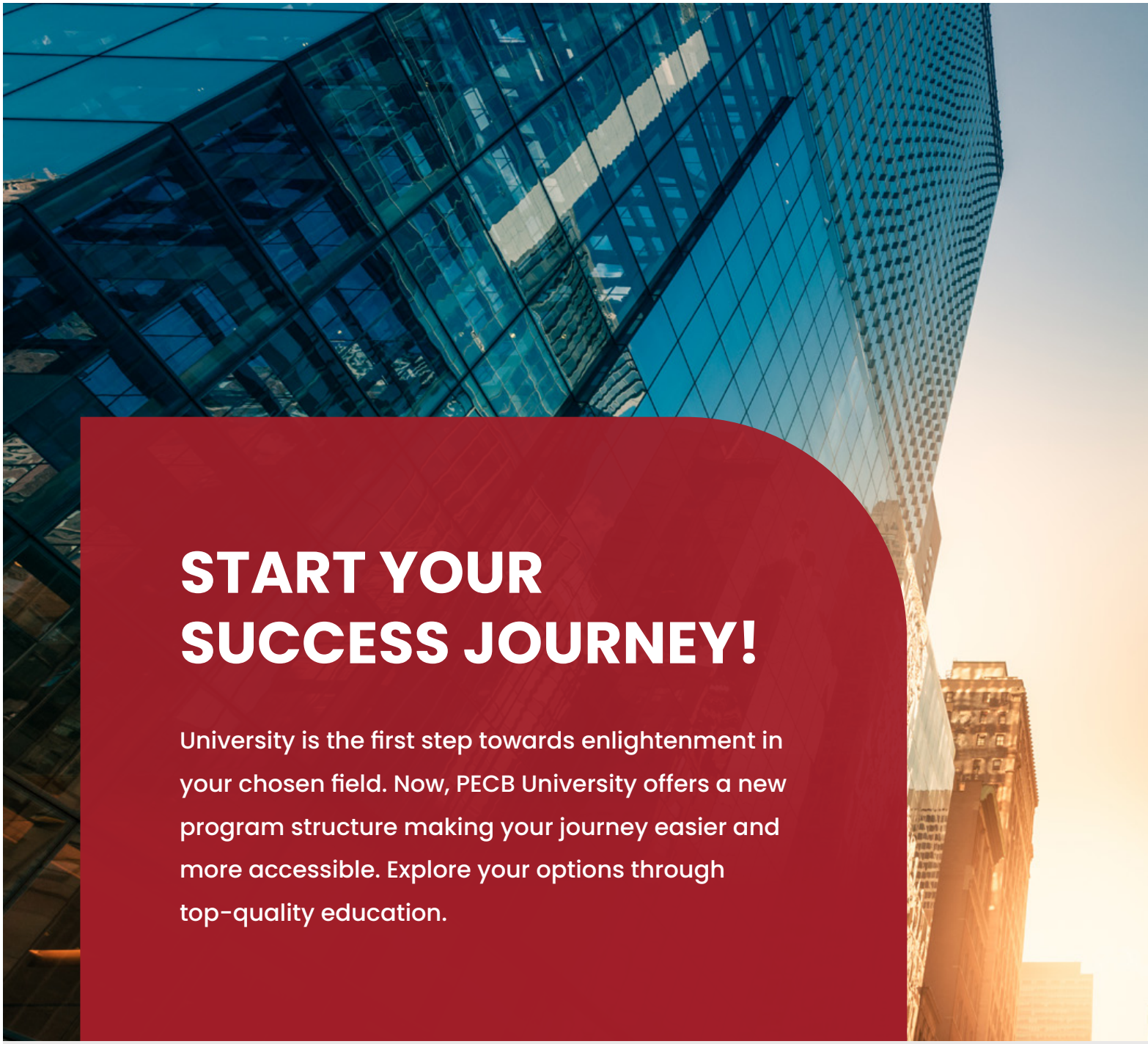
World Accreditation Day

With an aim to raise awareness of the value of accreditation, World Accreditation Day is annually observed on June 9, with different events taking place worldwide.

As a way to demonstrate quality and competence, some of the benefits of accreditation are:

- ✓ Providing greater safety for customers
- ✓ Increasing competitiveness
- ✓ Simplifying global trade
- ✓ Providing orderliness of activities
- ✓ Minimizing the risk of error

Check PECB's Accreditation



START YOUR SUCCESS JOURNEY!

University is the first step towards enlightenment in your chosen field. Now, PECB University offers a new program structure making your journey easier and more accessible. Explore your options through top-quality education.

Executive MBA Programs

Executive MBA in Cybersecurity

Executive MBA in Governance, Risk, and Compliance

Executive MBA in Business Continuity Management

Visit the PECB University Website to get better informed or contact the PECB University counselor at university.studentaffairs@p

STRENGTHEN YOUR COMPETENCIES, FOR A BRIGHTER FUTURE

Benefit from PECB's new and updated training courses!
Contact us at **marketing@pecb.com** or visit our **website** for more.

New and updated training courses

Training Course	Language	Status	
ISO/IEC 27001 Lead Implementer	English	Updated	→
ISO/IEC 27001 Lead Auditor	English	Updated	→
ISO 9001 Lead Implementer	English	Updated	→
ISO 37001 Introduction	English	Updated	→
ISO 22000 Introduction	English	Updated	→
ISO 31000 Risk Manager	Spanish	Updated	→
CMMC Certified Professional (CCP) *Note: Based on CMMC v1.0*	English	New!	→
ISO 37101 Foundation	English	New!	→
ISO 37002 Introduction	English	New!	→

EXPLORE THE BENEFITS OF ISO/IEC 27002:2022

Make progress in your field and give yourself a professional advantage by getting certified against **ISO 22301:2019** Security and resilience — Business continuity management systems.

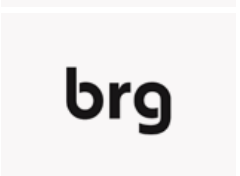
Find all the needed materials, which are designed to make your advancement process easier.

SHOP NOW! ▶

SPECIAL TI

TITANIUM

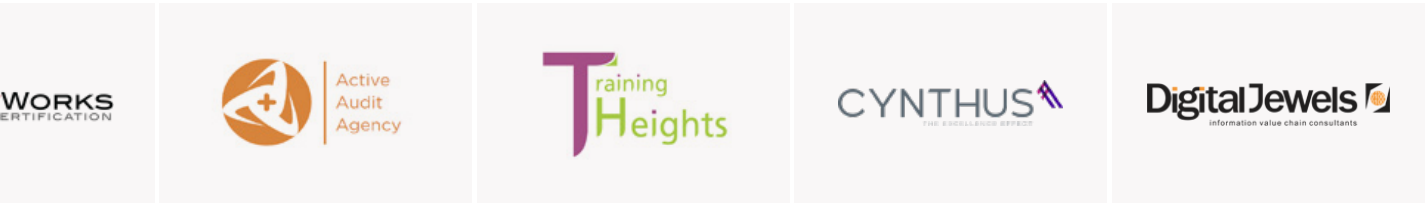
GOLD PA



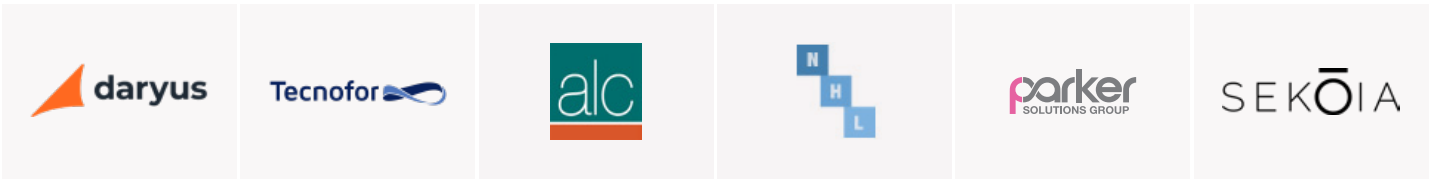
Note that PECB Partners are listed as per the credits

HANKS TO

PARTNERS



ARTNERS



acquired from January 1, 2021 to December 31, 2021.

STAY PROTECTED, REINFORCE YOUR ORGANIZATION

Keep an Eye Out for the Upcoming
Lead Crisis Manager Training Course!