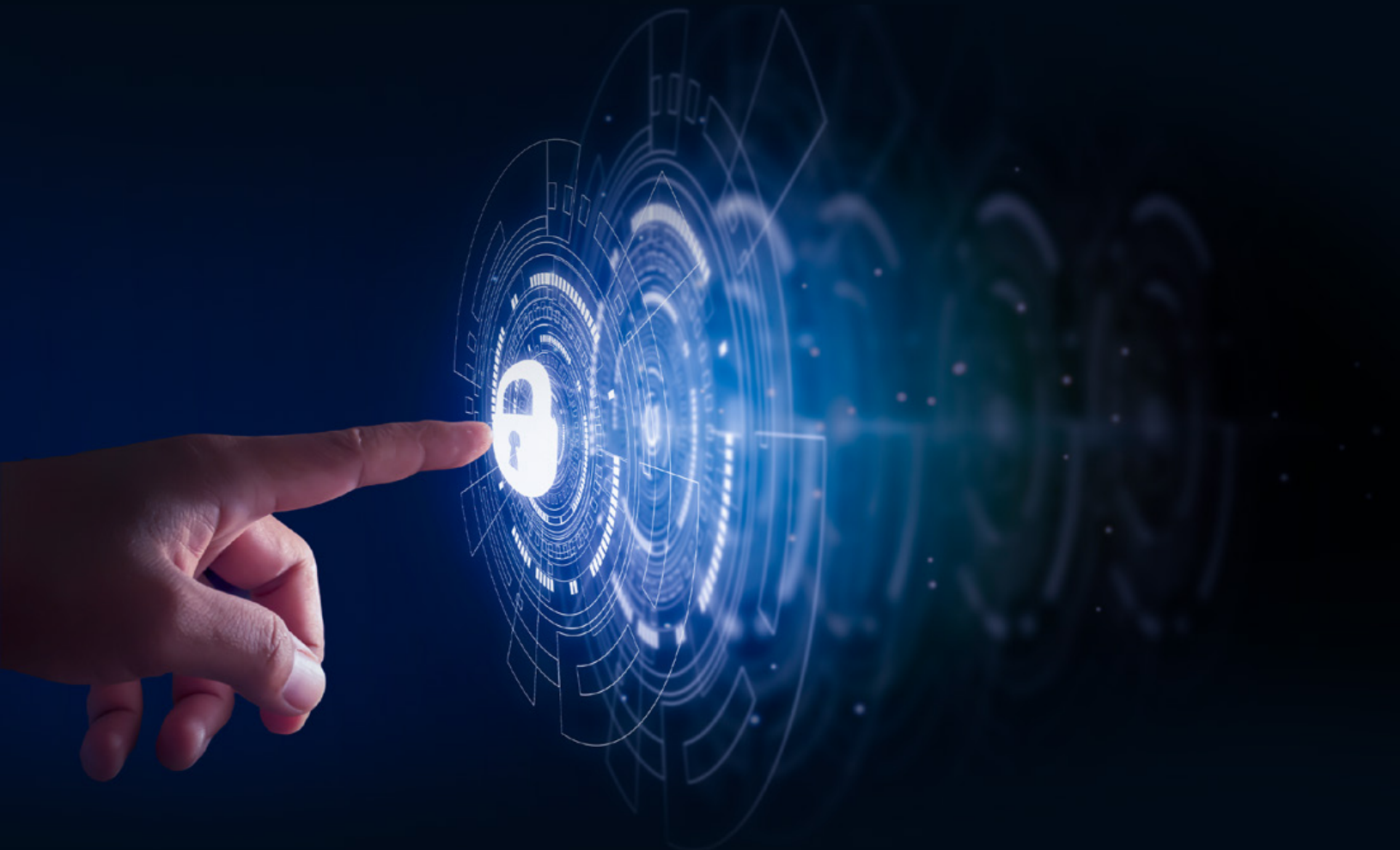


INFORMATION SECURITY AND BUSINESS CONTINUITY

ISO/IEC 27002:2022 AND ITS IMPACT
ON ISO/IEC 27001



PECB Insights Magazine

delivered to your mailbox

Issue
36

PECB Insights

ISO STANDARDS AND BEYOND

JANUARY-FEBRUARY 2022

CMMC, IT SECURITY, AND CYBERSECURITY

WHAT TO EXPECT

LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISURE
WORK-LIFE BALANCE SUCCESS STORY OPINION BOOKS INNOVATION

Subscribe & find out more at

www.insights.pecb.com

In This Issue



6 The Standard

Social Media in Emergency Management

8 The Expert

Supply Chain Cybersecurity Trends
– Staying Resilient

14 Opinion

How Does the New Revision of
ISO/IEC 27002 Affect ISO/IEC 27001

20 Success Story

Passion in Every Step:
Joshua Rey Albarina's Success Story

22 Work-Life Balance

The Lifestyle of An Information Security Expert

28 Leadership

When Cybersecurity and Business Continuity Converge:
A Security Leader's Perspective on How Organizations
Can Thrive

38 Innovation

Is AI Favoring Data Protection and Authentication?

42 Business & Leisure

Exploring Paradise on Earth

48 Books

A Deeper Look Into Our Technology Advanced Era

50 Career

Top Five High-Paying Job Positions You Can Pursue with
an ISO 22301 Certification

54 The Expert

Business Continuity and the Impact on HR Leaders

**“ Knowledge is
of two kinds.
We know
a subject
ourselves,
or we know
where we
can find
information
upon it. ”**

SAMUEL JOHNSON

English Writer







Social Media in Emergency Management

A new ISO standard gives guidance on the right way to keep people informed in a crisis. For many organizations and businesses, social media is a valuable opportunity to reach out to the people that matter to them. The speed with which information can be made available also means that social platforms are an invaluable way to give updates in an emergency.

Unfortunately, the wrong kind of information can spread just as rapidly, with potentially disastrous consequences. For challenging situations that demand effective communication, guidance is now available from [ISO 22329](#), Security and resilience – Emergency management – Guidelines for the use of social media in emergencies, the latest International Standard from the ISO technical committee entrusted with [these questions](#).

The new International Standard is a game-changer when it comes to making the best use of the wide range of platforms available today and getting the right information to people at the right time.

**“Social media is the first place that many people go when they need information or they need to let people know what’s happening in their lives. In a crisis, it’s essential to make sure that the information can be relied upon.” - Åsa Kyrk Gere
Chair, ISO/TC 292, Security and Resilience**

As well as giving guidance on the use of social media in emergency management, the new ISO standard also helps organizations and the public to effectively use, and interact through, social media before, during, and after an incident. It also covers the ways in which social media can support the work of emergency services.

ISO 22329 can be used by anyone involved in emergency management and crisis communication, including governmental and non-governmental organizations and businesses. It was developed by ISO technical committee [ISO/TC 292](#), Security and resilience, whose secretariat is held by [SIS](#), ISO’s member for Sweden. The standard can be purchased from your national [ISO member](#) or the [ISO Store](#).

Supply Chain Cybersecurity Trends – Staying Resilient



BY MOHAMED GOHAR

Supply chain security activities aim to amplify the security of supply chains, transport, and logistic systems for the world's cargo and to facilitate legitimate trading. Their objective is combining traditional practices of supply chain management with the security requirements driven by threats, such as; terrorism, piracy, and theft.

Digital supply chain security indicates the efforts towards the enhancement of cybersecurity within the supply chain. Supply chain cybersecurity is a subgroup of supply chain security, its focus is on the management of cybersecurity requirements for information technology systems, software, and networks, which are driven by threats such as; cyberattack, malware, data theft, and the advanced persistent threat (APT). Its most important aim is to defend against supply chain attacks and protect business assets within the supply chain.

A supply chain attack is not limited to certain industries, it can happen in all fields; from financials sectors, the oil industry, to bigger scales such as the government sector. It is a cyberattack that aims to damage an organization by targeting its less-secure components. Cybercriminals often meddle with the manufacturing process of a product by installing rootkits or hardware-based spying elements. A [report](#) by [Argon](#) an [Aqua Security](#) company states that supply chain attacks increased by 300% in 2021.

The Target security breach, Eastern European ATM malware, as well as the Stuxnet computer worm are examples of supply chain attacks.

The Proliferation of Supply Chain Cyberattacks

[ENISA \(European Union Agency for Cybersecurity\) Threat Landscape for Supply Chain Attacks](#) report published on July 29, 2021, aimed at mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021.



Based on the trends and patterns observed, supply chain attacks increased in number and sophistication in the year 2020 and this trend was expected to continue in 2021, posing an increasing risk for organizations. It was estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and therefore there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.



The report presented ENISA's Threat Landscape concerning supply chain attacks, created with the support of the Ad-Hoc Working Group on Cyber Threat Landscapes. The main highlights of the report included the following:

- › A taxonomy to classify supply chain attacks in order to better analyze them in a systematic manner and understand the way they manifest is described.
- › 24 supply chain attacks were reported from January 2020 to early July 2021, and have been studied in the report.
- › Around 50% of the attacks were attributed to well-known APT groups by the security community.
- › Around 42% of the analyzed attacks have not yet been attributed to a particular group.
- › Around 62% of the attacks on customers took advantage of their trust in their supplier.
- › In 62% of the cases, malware was the attack technique employed.
- › When considering targeted assets, in 66% of the incidents attackers focused on the suppliers' code in order to further compromise targeted customers.
- › Around 58% of the supply chain attacks aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16% at gaining access to people.
- › Not all attacks should be denoted as supply chain attacks, but due to their nature, many of them are potential vectors for new supply chain attacks in the future.
- › Organizations need to update their cybersecurity methodology with supply chain attacks in mind and to incorporate all their suppliers in their protection and security verification.

Key Risks of Supply Chain Cybersecurity

Supply chain cybersecurity risks cover a lot of territories. As stated on the [National Institute of Standards and Technology](#) some of the concerns include risks from:

- › Third-party service providers or vendors, from janitorial services to software engineering, with physical or virtual access to information systems, software code, or Intellectual Property.
- › Poor information security practices by lower-tier suppliers.
- › Compromised software or hardware purchased from suppliers.
- › Software security vulnerabilities in supply chain management or supplier systems.
- › Counterfeit hardware or hardware with embedded malware.
- › Third-party data storage or data aggregators.

Supply Chain Attack

The term supply chain alludes to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product. When it comes to cybersecurity, the supply chain regards a multitude of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software.

There are four key elements in a supply chain:

- › **Supplier:** is an entity that supplies a product or service to another entity.
- › **Supplier Assets:** are valuable elements used by the supplier to produce the product or service.
- › **Customer:** is the entity that consumes the product or service produced by the supplier.
- › **Customer Assets:** are valuable elements owned by the target.

An entity can be individuals, groups of individuals, or organizations. Assets can be people, software, documents, finances, hardware, or others.

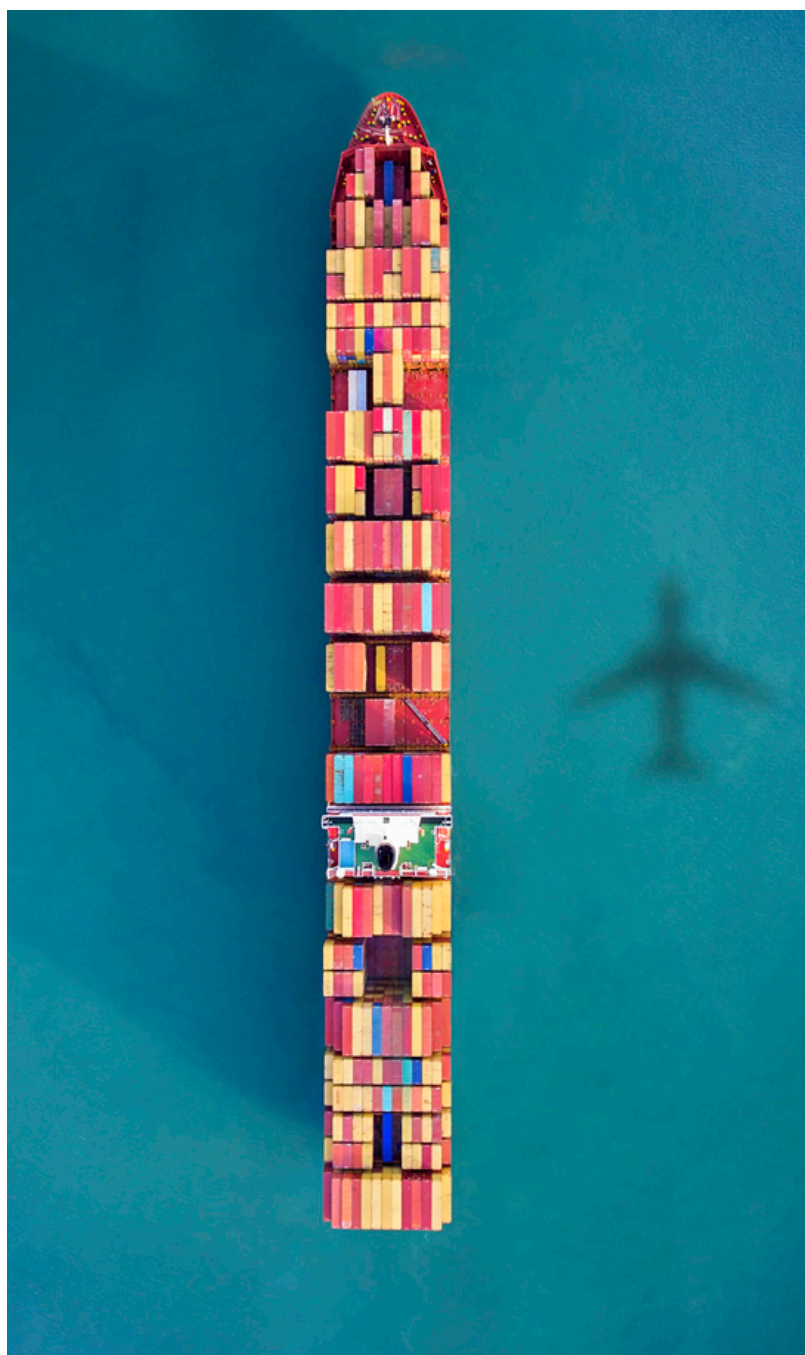
As mention on ENISA's report: Supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targeted.

Attack Techniques, Targeted Supplier, and Customer Assets

The risk becomes evident when a vulnerability of an organization's asset is utilized by a technique to attack or a threat, during this time, the evident risks begin to have a negative effect on the organizations' assets.

Table: Proposed taxonomy for supply chain attacks. It has four parts:

1. Attack techniques used on the supplier,
2. Assets attacked in the supplier,
3. Attack techniques used on the customer,
4. Assets attacked in the customer.



SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supplier	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Malware Infection	Pre-existing Software	Trusted Relationship	Data
Social Engineering	Software Libraries	Drive-by Compromise	Personal Data
Brute-Force Attack	Code	Phishing	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
Exploiting Configuration	Data	Physical Attack or Modification	Processes
Vulnerability	Processes	Counterfeiting	Bandwidth
Open-Source	Hardware		Financial
Intelligence (OSINT)	People		People
	Supplier		

Recommendations for How to Stay Resilient

As stated in an article published by [SecurityMagazine](#): Thoughtful investment in cybersecurity measures goes beyond technology. Not only are digital tools and updated software important, but IT professionals are also essential in building resilient infrastructure.

Industries across the board that utilize cyberspace to any degree are at risk for cyberattacks, so understanding how to use technology and human expertise to both proactively prepare for and reactively combat against threats, is essential.

With experience, both good and bad, comes knowledge. One lesson learned in recent years is how interdependent each section of the global supply chain is on another. If one facility, port, software, or database is interrupted due to a cyberattack, countless companies and consumers can be impacted, resulting in great financial loss and compromised data. In fact, more than 30 billion records were exposed in data breaches just last year.

In an effort to avoid such attacks, individuals and organizations should keep in mind a handful of key steps to becoming more resilient and secure, and senior leadership needs to ensure that they and their team members feel confident in the systems and security they have in place.

On average, about 2,200 cyberattacks occur on a daily basis, so proactive planning is essential in limiting room for threats to come to fruition no matter the source, hence reducing the risks to a level accepted by organizations.

What Should Suppliers and Customers Do?

To manage supply chain cybersecurity risks, customers should:

- › Identify and document types of suppliers and service providers
- › Define risk criteria for different types of suppliers and services (e.g., important supplier and customer dependencies, critical software dependencies, single points of failure)
- › Assess supply chain risks according to their own business continuity impact assessments and requirements
- › Define measures for risk treatment based on good practices
- › Monitor supply chain risks and threats, based on internal and external sources of information and on findings from suppliers' performance monitoring and reviews
- › Make their personnel aware of the risk



To manage the relationship to suppliers, customers should:

- Manage suppliers over the whole lifecycle of a product or service, including procedures to handle end-of-life products or components
- Classify assets and information that are shared with or accessible to suppliers, and define relevant procedures for their access and handling
- Define obligations of suppliers for the protection of the organization's assets, for sharing of information, for audit rights, for business continuity, for personnel screening, and for the handling of incidents in terms of responsibilities, notification obligations, and procedures
- Define security requirements for the products and services acquired
- Include all these obligations and requirements in contracts; agree on rules for sub-contracting and potential cascading requirements
- Monitor service performance and perform routine security audits to verify adherence to cybersecurity requirements in agreements; this includes the handling of incidents, vulnerabilities, patches, security requirements, etc.,
- Receive assurance of suppliers and service providers that no hidden features or backdoors are knowingly included
- Ensure regulatory and legal requirements are considered
- Define processes to manage changes in supplier agreements, e.g., changes in tools, technologies.
- Ensure that the infrastructure used to design, develop, manufacture, and deliver products, components, and services is in accordance with cybersecurity practices
- Implement a product development, maintenance, and support process that is consistent with commonly accepted product development processes
- Implement a secure engineering process that is consistent with commonly accepted security practices
- Consider applicability of technical requirements based on product category and risks
- Offering Conformance Statements to customers for known standards, i.e. ISO/IEC 27001 (or specific ones like the CSA Cloud Controls Matrix (CCM) for cloud services), ensuring and attesting to, at the possible extent, the integrity and origin of open source software used within any portion of a product
- Define quality objectives, such as; the number of defects, externally identified vulnerabilities, or externally reported security issues, and use them as an instrument to improve overall quality
- Maintain accurate and up-to-date data on the origin of software code or components, and on controls applied to internal or third-party software components, tools, and services present in software development processes
- Perform regular audits to ensure that the above measures are met

Moreover, as any product or service is built from or based on components or a software that is subjected to vulnerabilities, suppliers should implement good practices for vulnerability management, as follows:

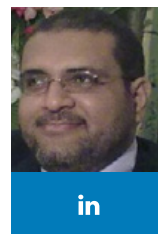
On the other hand, suppliers should ensure the secure development of products and services that are consistent with commonly accepted security practices. Suppliers should:

- The monitoring of security vulnerabilities reported by internal and external sources that include used third-party components

- › The risk analysis of vulnerabilities by using a vulnerability scoring system (e.g. CVSS),
- › The maintenance policies for the treatment of identified vulnerabilities depending on the risk
- › The processes to inform customers
- › The patch verification and testing to ensure that operational, safety, legal, and cybersecurity requirements are met and that the patch is compatible with non-built-in third-party components
- › The processes for a secure patch delivery and documentation concerning patches to customers
- › The participation in a vulnerability disclosure program that includes a reporting and disclosure process

Vulnerabilities should be managed by suppliers in the form of patches. Likewise, a customer should monitor the market for potential vulnerabilities or receive respective vulnerability notifications from their suppliers. Some good practices for patch management include:

- › Maintaining an inventory of assets that includes patch-relevant information
- › Using information resources to identify relevant technical vulnerabilities
- › Evaluating the risks of identified vulnerabilities, as well as having a documented and implemented maintenance policy available
- › Receiving patches only from legitimate sources and testing them before they are installed
- › Applying alternative measures should a patch not be available or applicable
- › Applying rollback procedures, effective backup, and restore processes.



Mohamed Gohar
Principal Trainer, Consultant, and Auditor of ISM/ITSM

Gohar has over 25 years of experience in IT, he is a principal trainer, consultant, and auditor of ITSM, ISM, and BCM.

Gohar is a Subject Matter Expert at ISACA since 2015, he participated in reviewing many ISACA certification review manuals like CISA 26th, and 27th editions, CISM 15th, and 16th editions, CGEIT 8th edition, and CRISC and CISM online courses.

Gohar is cooperating with ITpreneurs in reviewing their ITIL 4 courseware like ITIL 4 Foundation, he is also an exam item writer at EC-Council for CEH v10, and v11 certifications.

Gohar is an approved trainer by ITpreneurs, PeopleCert, and The Open Group, he is also a certified trainer at PECB and Management Systems Auditor at MSEC.

How Does the New Revision of ISO/IEC 27002 Affect ISO/IEC 27001



PETER GEELEN

OPINION

With the publication of the new ISO/IEC 27002:2022 in February 2022, ISO kicked off the long-awaited update cycle of information security standards covered by the ISO 27000 family. In this article, we will look into the consequences for the global security professionals' community that try to keep their environment as secure as possible.

But the story is a bit more complicated than just updating a series of global information security standards. Since the 2013 publication of the previous generation, the world of information security has changed drastically because of the increased pressure on cybersecurity and cloud security.

And I have not mentioned the new world of data protection and privacy yet, GDPR has not only pushed the data protection expectations in Europe, but many regions have also assimilated similar data protection rules.

In this new era, there is no privacy nor data protection without cybersecurity. And a well-built information (cyber) security management system – in whatever format – is an absolute requirement to protect yourself, your organization, and your peers. It is not only about your own protection anymore.

To understand the impact of the ISO/IEC 27002 update, allow me to take a step back first.

ISO/IEC 27001 as the reference standard for many security approaches

First of all, it must be said that ISO/IEC 27001 (a.k.a. Information Security Management System – ISMS) version 2013 is the current master standard, although it has been updated with 2 minor corrections in 2014 and 2015, consolidated in version 2017, but these were rather non-essential cosmetic updates.

Considering the 2013 version, compared with the current state of technology almost 10 years later, it was quite obvious that the standard needed a revamp.



And normally an ISO standard is reviewed every 5 years, therefore, in that perspective as well, it was long overdue, which raised a lot of criticism from the field.

On the other hand, the topics, sections, controls, and measures in the current standard still have a robust, valid general approach. That can be complemented perfectly with other more detailed technical frameworks (like NIST, CIS controls, COBIT, CSA, etc.) and best practices to match the current state-of-the-art security requirements.

The standard has been built from various global security practices. And it still is the common ground that glues them together.

The goal of this standard is to support an effective security, not just a compliance checklist, as many think.

Do keep in mind that ISO/IEC 27001 is also a global reference standard for many other derived frameworks. Some are more lightweight, whereas others focus more on specific sectors or target specific organizations for instance small and medium-sized enterprises or businesses (SME/SMB).

The ISO 27000 pack of standards

For a long time, ISO/IEC 27001 has been the main auditable and certifiable standard for information security.

ISO/IEC 27701 was added a few years ago (quite recent in ISO terms), to extend the enterprise security approach with data protection and privacy. In fact, ISO/IEC 27701 ties together the requirements of ISO 29100 (privacy), GDPR, and the ISMS approach.

These certification standards are complemented with a collection of essential guidelines, code of practices, and metrics on activities you need to implement to make the management system work, including risk management, incident management, business continuity, auditing, assessments, building and protecting evidence, measurements, or application development.

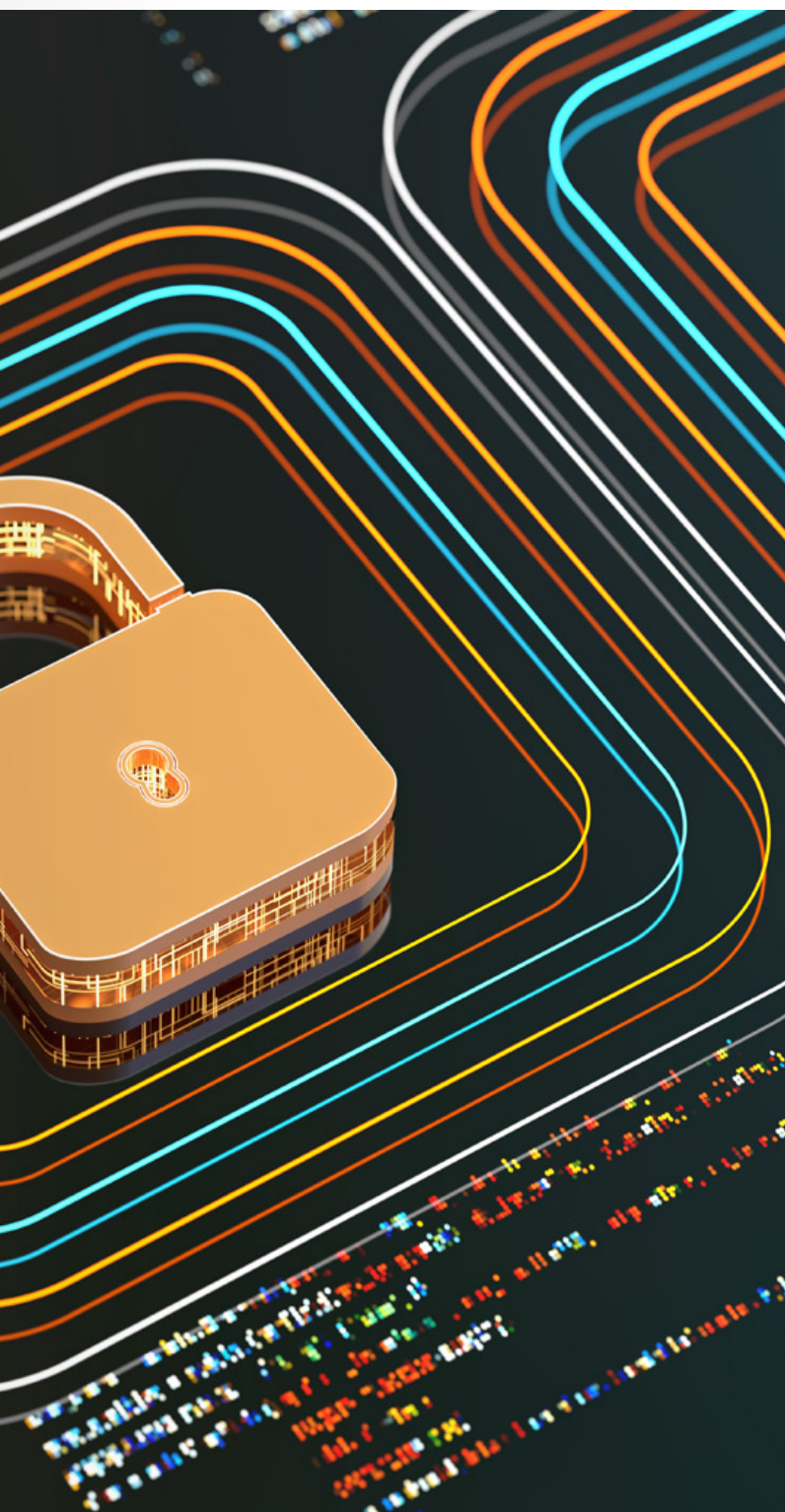
Many are derived from other main ISO standards, like ISO 31000, ISO 22301, ISO 29100, ISO 20000, while many refer to ISO/IEC 27002.

It is quite clear that the latest update of ISO/IEC 27002 will have a major impact on these other essential guidelines. Firstly ISO/IEC 27001, but many more to come.

What is the connection between ISO/IEC 27001 and ISO/IEC 27002?

You might think that question is rhetorical, or in contrast you may find the connection obvious, however, it is not.

Many think that ISO/IEC 27001 is the main standard and that the ISO/IEC 27002 provides additional, in depth guidelines to ISO/IEC 27001 Annex, but that does not stand correct.





In fact, the first thing that is mentioned in the ISO/IEC 27001 Annex A (normative) is: “The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.”

This means that ISO/IEC 27002 is the Code of Practice as the main guide for the requirements listed in ISO/IEC 27001, or said differently, that the requirements in ISO/IEC 27001 are a compacted list of ISO/IEC 27002. Consequently, if the ISMS requirements must be updated, the ISO/IEC 27002 update comes first.

The most prominent changes in the new ISO/IEC 27002?

There have been many posts, articles, and webinars on the ISO/IEC 27002 update, therefore, I do not wish to overelaborate. But the best news is: ISO/IEC 27002:2022 contains a matching table to explain the match between the 2013 and 2022 version, and also the other way around.

For clarity let me quickly point out the main differences.

New organization of the security controls

From ISO/IEC 27002:2013		To ISO/IEC 27002:2022
Number	Security control clause	Security control clause
5	Information security policies	Organizational controls (37)
6	Organization of information security	People controls (8)
7	Human resource security	Physical controls (14)
8	Asset management	Technological controls (34)
9	Access control	
10	Cryptography	
11	Physical and environmental security	
12	Operations security	
13	Communications security	
14	System acquisition, development and maintenance	
15	Supplier relationships	
16	Information security incident management	
17	Information security aspects of BCM	
18	Compliance	



In essence, the most important update is a complete reorganization of the controls main categories. A brief overview: the ISO/IEC 27002:2013 standard contains 14 security control clauses, 35 subcategories with 114 controls. The 2022 version contains 4 main clauses with 93 controls. Essentially, the 2013 version has the controls organized on operational functions, the 2022 version is based on PPT (people, process and technology).

To be specific it is: PPPT: **P**olicy, **P**eople, **P**hysical and **T**echnology.

New approach to control classification

So there is one less level of organization, this oversimplification is not necessarily an improvement. Regardless, the new ISO/IEC 27002:2022 covers this lack of organization by using attributes (including Operational capabilities), explained in Annex A of ISO/IEC 27002. The interesting part of this approach is that you can easily match your existing ISO/IEC 27001 implementation controls with the new ISO/IEC 27002 structure.

New controls in ISO/IEC 27002:2022

ISO/IEC 27002:2022		Improvement driver
Number	Security control clause	
5.7	Threat intelligence	Cybersecurity
5.23	Information security for use of cloud services	Cloud security
5.30	ICT readiness for business continuity	Cyber, cloud & data protection
7.4	Physical security monitoring	Cyber, cloud & data protection
8.9	Configuration management	Obviously missing from ITIL/ISO2000 approach
8.10	Information deletion	Data protection
8.11	Data masking	Data protection
8.12	Data leakage prevention	Data protection
8.16	Monitoring activities	Cybersecurity
8.23	Web filtering	Cybersecurity
8.28	Secure coding	Application security

Merged controls

In essence, no controls are removed from the 2013 version, but duplicate or similar controls are merged to end up with 93 instead of the previous 114 controls.

What about the ISO/IEC 27001?

For the moment, at the publication of ISO/IEC 27002:2022, ISO/IEC 27001 is not changed yet, this means that the current certification standard stays put with the old controls until republication. However, in early February, just before the final publication of ISO/IEC 27002:2022, ISO launched a review cycle of ISO/IEC 27001:2013 to update the standard with the new Annex from ISO/IEC 27002.

This review will take 12 weeks, which is a fixed ISO procedure. So you might expect some official news sometime in May – June 2022.

A small surprise: the new update will not be a new version but an amendment, which is a minor update not a complete overhaul or new version.

Just keep in mind that the main clauses in the ISO/IEC 27001 are "management" clauses, aligned with the PDCA cycle of ISO 9001 (which also has been kept in place, unchanged from the 2015 version). In this case, the amendment is clearly a replacement of ISO/IEC 27001 Annex, with a condensed table version of ISO/IEC 27002:2022, with the previously discussed controls.

What about your existing ISO/IEC 27001 certification?

So far, the first signals are correct and confirmed, there will be a shorter update cycle for existing ISO/IEC 27001 certifications.

Instead of the typical 3 years, there will be a required update within 2 years. But in reality, most – if not all – implementations are already enforcing the security controls of the new version. Just double-check on the new controls in the 2022 version.

So, in conclusion: implement a few extra security controls (which you should have already), update your Statement Of Applicability, rename the controls or cross-match the existing controls with the 2022 version, then you are on the clear to proceed with an updated certificate on the next external audit cycle, even a surveillance audit.

And the other standards?

It is not clear yet what will happen with the other ISO/IEC 27000 standards in the pack, but it is likely that they will get a similar review to match up with ISO/IEC 27002:2022.

However, as they all will need to pass through the same official review, it will take some time to have them all aligned.

Certainly for ISO/IEC 27701 (PIMS), this is an important concern. But in the strictest sense, ISO/IEC 27701 requirements point to the ISO/IEC 27001 clauses, and the normative Annexes (Annex A for PII Controllers and Annex B for PII Processors) do not mention ISO/IEC 27002. Hence, once the ISO/IEC 27001 is officially updated, ISO/IEC 27701 recheck should be fairly straight-forward.

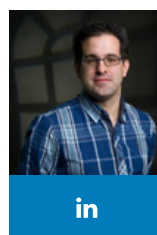
Epilogue

Except for a growing set of standards in the ISO 29100 area, with new and updated guidelines for privacy/data protection management, there is a new section you should keep an eye on.

That is [ISO/IEC TS 27100 Cybersecurity – Overview and concepts](#), [ISO/IEC TR 27103:2018 Cybersecurity and ISO and IEC Standards](#), [ISO/IEC TS 27110:2021, Cybersecurity framework development guidelines](#).

Ergo, except for important updates on information security, privacy and data protection, also cybersecurity will get its fair needed changes accordingly.

PECB makes staying up-to-date with such updates simple, with easy-to-follow training courses on ISO/IEC 27001, ISO/IEC 27002, GDPR, and much more.



Peter Geelen

Director and managing consultant at CyberMinute and Owner of Quest for Security, Belgium. For over than 20 years, Peter has built strong experience in enterprise security and architecture, Identity and Access management, as well as privacy, information

and data protection, cyber and cloud security. During the last few years, the focus is on ISO/IEC 27001 and other ISO certification mechanisms. Peter is an accredited Lead Auditor for ISO/IEC 27001, ISO/IEC 27701, ISO 22301, and ISO 9001, PECB Trainer and Fellow in Privacy. Committed to continuous learning, Peter holds renowned security certificates like ISO/IEC 27001 Master, ISO/IEC 27701 Lead Implementer/Auditor, Sr. Lead Cloud & Cybersecurity Manager, ISO/IEC 27002 Lead Manager, CDPO, Lead Incident Manager, Disaster Recovery, and more.



Passion in Every Step: Joshua Rey Albarina

My journey with PECB started when I became a certified trainer and a Risk Manager. Prior to this, I was engaged in management best practices on non-government-funded projects as a trainer and consultant for both; manufacturing and service industries. Since I joined SAS Management as a Senior Consultant, I was given the opportunity to build a strong presence within the country for promoting ISO standards and the value it brings to every organization, exploiting more on how it can leverage business regardless of strategy.

The Impact of being certified by PECB

Ever since I got my PECB certifications, I was engaged mostly in numerous consulting projects and trainings. Few of the many milestones I have that created a positive impact on organizations was when we first introduced the ISO 31000 certified risk manager program after achieving certifications, both the program and becoming a PECB certified trainer, it was at that time that we pioneered the certification course related to Enterprise Risk Management within the country, with three participants on its first launch. Since then, by promoting the cause of having the right mindset towards risks, it became a popular course, with more than ten participants every session, as it became a need for most organizations to have someone lead their risk management frameworks from various industry contexts and lead industries to promote adopting and adapting risk management practices within the country. Aside from trainings, we extended our services further by helping organizations create their risk management frameworks and choosing appropriate risk assessment techniques that help in being critical with respective risks.

Following the years after promoting risk management, we went on to meet organizations' needs in terms of data privacy practices. Having been certified as Lead Privacy Implementer and ISO/IEC 27701 Lead Implementer gave me the necessary leverage to serve and support organizations in the implementation of data privacy frameworks and controls to ensure that they are compliant with state laws, especially in compliance with the Data Privacy Act here in the Philippines.



Having been certified with ISO/IEC 27001 as a Lead Auditor, in ISO 22301 as both; Lead Implementer and Auditor, and ISO 31000 as Lead Risk Manager on top of other certifications, became my advantage in taking part in two key IT projects, where I helped initiate and design their enterprise-wide Information Security Risk Assessment, covering thirteen software applications in the scope. It was laborious but fulfilling knowing that they learned a lot from the experience. On the other project, my role was designing their IT balanced scorecard, which was a primary tool in their steps to practicing IT Governance, which was a key need considering that the nature of their business is heavily dependent on technology.

Fueling success

Throughout my career as a consultant and my credentials being recognized through PECB, having the opportunity to coach or train professionals through the courses that we offer and assist them in validating what they have practiced for them to achieve certification was both an honor and a privilege. By promoting an effective risk management practice as a personal advocacy for organizations and professionals, this got me far in my career through getting invited in speaking engagements, group discussions, or forums, where some were organized from my previous participants or organizations. It also helped me broaden my perspective, which in turn helps me improve my practice and get more endeavors, whether here or abroad.

These success stories in my career, however, became possible by keeping in mind the following things that kept me on track:

› Have the best mentor

Having the courage and enthusiasm to perform and excel in this field would be very much impossible through the guidance and wisdom shared by my director, who is a really good mentor. Through casual conversations and brainstorm sessions, he made sure that I got to understand the logic behind each scenario and made every effort to give me that push in becoming better at every opportunity at work.

In hindsight, having a mentor to be with you every step of the journey is a valuable experience. In reality, it is a privilege only few can have.

› Keep a 'can do' attitude

As a certification trainer and consultant, I always encounter various personalities in different circumstances, such as having a participant with no experience in information security to someone that has multiple certifications on his credentials (i.e. COBIT, TOGAF, CISO), or on some occasions, working on a single standard for two consulting projects on different organizations. This can be challenging in my case, and I must keep a 'can do' mindset throughout, as to value their time and presence, delivering positive results at every engagement. I do believe that everyone has the capability to perform and excel in every discipline they choose to venture on. But through a 'can do' mindset, a positive and persistent attitude, achievements can go a long way, and this in my part resulted in more training sessions and consulting projects year after year. Personally, this 'can do' mindset became a big factor in helping me achieve all certifications I have up to this day, and why clients trusted us to help them meet their needs.



Picture: Certified ISO 31000 Risk Manager training at Cebu

› Their success is your success

Establishing yourself as a reliable trainer is highly important, especially when dealing with such matters. As anyone who may have any sort of experience with education, you understand how fulfilling and validating it is to be able to witness the achievements of your students, or in my case the attendees of my trainings. As a lot of work is put in, both from the trainer and an attendee, it brings a lot of satisfaction seeing that work flourish into success.

As a trainer, it pays a lot of benefits to ensure that every professional gets the right support and motivation to pass, get certified, and realize the benefits at work or on various opportunities where they can practice them. This may sound subjective, but it gives a good sense of fulfillment to see that they succeeded since they are living ambassadors of the training they get from a credible instructor with sufficient credentials to prepare them for the road ahead.



Joshua Rey Albarina

Business Consultant, Trainer, Risk Manager, Assessor, Strategist

A Senior Consultant for ISO standards and business best practices at SAS Management, Inc. in the Philippines. He is a PECB certified trainer and an ISO 31000 Risk Manager, ISO/IEC 29100 Lead Privacy Implementer, ISO/IEC 27701 Lead Implementer, ISO/IEC 27001 Lead Auditor, and ISO/IEC 22301 Lead Implementer and Auditor.

The Lifestyle of An Information Security Expert



BY ABDELMALEK NAJIH

With the changing economic context that relies more and more on information technologies which need to be secured, the title Information Security Expert has become shiny and luxurious that many have become quite curious about this category of professionals.

In the following, I will share with you what the life of an information security expert looks like, considering I have been surrounded by many of them for years.

The drive and motivation

Upon the evolvement of the number of cybersecurity attacks a few years ago, the light was shed on the domain of cybersecurity in particular, and subsequently, on information security in general, after the higher management of companies around the world also got interested.

Profiles belonging to this discipline were rather required, and thus more students and professionals were seduced to change their field and acquire the most sought-after roles in the job market.

It goes without saying that this category is attracted by a good life, a good role in the company, and a substantial salary.

On the other hand, we find people, students, and professionals, who show unconditional passion for cybersecurity and information security.

Unconditional because they know no conditions nor limits to learn about a new vulnerability or a method to bypass a security measure. Time, sleep, and money are easy to afford when it comes to a CTF (Capture The Flag, a hacking competition) which is typically planned on weekends and commonly lasts all night long.



Is Information Security only about Information Security?

I have been speaking about cybersecurity and information security as if they are two separate things. As many of you may know, cybersecurity is about security related to technologies: laptops and desktops, servers, mobile phones, embedded systems, and many more. The focus is on the information indeed, but the condition is that it should be stored or treated by the above listed things.



Whereas information security focuses on the information regardless of the medium used to store or treat it. Whether the information is stored on a hard drive, written on paper, or in the head of an employee, it should be secured (yes, we can “secure” information within employees’ heads through clauses in their employment contracts called NDA: Non-Disclosure Agreement, and by adding mention to profession secrecy if applicable).

The other difference is that cybersecurity is managed at an operational level, while information security is managed from a governance level, but also at a managerial level and operational level for some processes.

Now, to answer the question asked in the title: no! Many standards and frameworks are serving as tools to manage information security, but an expert should also bear in mind other considerations, such as legal, regulatory, and contractual requirements. It is certainly related to information but not always linked to information security. Sometimes the requirements are related to an influenced decision; or a client imposing a preference during contracting for the service to be provided for instance. Such requirements are not to be guessed, but to be checked and complied with to avoid troubles later, either with clients or with authorities, when things get graver than we wish.

What does it take to get there?

To answer this question, let us have a look at what an information security expert does in a mission of implementing and/or auditing an ISMS (Information Security Management System) in conformity with the ISO/IEC 27001 standard, in this instance, the expert should:

- Meet with the top management, interested parties, managers, technicians, and users
- Make presentations, introduce the project and gain approvals, report progress and results, etc.
- Meet with process owners to secure and document the processes. This includes non-IT processes
- Conduct Awareness and training sessions for users
- Conduct Self-Check, gap analysis, or audits
- Ensure follow-up of action plans, etc.

The incomplete list of tasks mentioned above implies that the information security expert must have information security skills, which is normal, but what most professionals forget about is the non-technical skills required for this job to be done. An information security expert must:

- Be a good negotiator in order to convince the interested parties about the project, or parts of it, to get their approval and engagement.
- Have good communication skills to get the message delivered and understood by your interlocutor.
- Be a good presenter with good presentation skills to be able to deliver the message and grab the attention of your audience through presentation techniques.
- Be a good trainer since your audience will be of various domains and definitely not simply information security. The trainer creates threats by conducting training/awareness sessions when participants attend and do not fully understand the content! An unaware user is a threat in itself to the business.
- Be a good project manager to ensure the steering and the smooth execution of the action plans, as well as meeting the deadlines.
- Be polyvalent. Conduct audits of all of ISMS and be willing to verify the effectiveness of all processes (facilities, physical security, human resources, etc.). You must have at least a general understanding of all those processes.

Besides all of these skills, an information security expert should have real-life experience in information security and IT, preferably in cybersecurity, in various missions for various clients of different business sectors, ideally in different countries. Otherwise, you will only have theoretical skills which do not assist as much as one would think.

Maintaining the level of expertise: A choice or a dilemma?

Some jobs require few updates and learnings whereas some no updates at all. Once a student gets their degree, they are good to go. In information security and cybersecurity, one long pause can make an expert with 20 years of experience a simple information security professional with an outdated skillset.

The issue is that technologies are moving fast, bringing new vulnerabilities, new threats, techniques, and then new frameworks, standards, laws, and regulations.

Which makes it hard for an information security expert to keep his level of expertise.

Getting to the next level is another story. It costs money, time, and effort to learn and acquire new skills. An expert calculates the Return-On-Investment of any advancement or study they want to take each time.

Indeed, an expert cannot choose whether to continuously upgrade their skill set and stay up-to-date, it is their only option.

What is it like to work in the domain of information security?

There are three roles that an information security expert can have: An implementer (also called an adviser or a consultant), an auditor (or an assessor), and finally a trainer (or an instructor).

As an implementer, when the work is done for a consulting firm, they are appreciated as they bring revenue to the company by delivering expertise to clients. This applies to audit and training roles as well. But clients have a different opinion. The mid-management sees them as an overpaid resource, so they are expected to deliver more than internal resources.

As an auditor, it depends on where the auditor is coming from; an authority, a regulator, a certification body, a client exercising their right of an audit, a consultancy firm to conduct a readiness audit as a preparation of a certification audit for example, or from an internal department, for instance, an Internal Audit. Respectively, the auditor has less and less power and independence.

An auditor selected by a regulator to conduct a regulatory audit would not mind sending a report full of red flags, while an internal auditor, in some companies depending on the management, may think twice before mentioning a minor non-conformity in their report, especially when the source of the issue comes from the senior management.

A good trainer knows how to lead the course, they are experts and know how to best explain their expertise. There are instances where the candidates can provoke the trainer, perhaps testing their knowledge, however, those are easy situations to maneuver with professionalism.

In some jobs, the risks are physical, whereas in information security, when a risk scenario occurs and it is not managed as intended, the first person asked questions is the Risk Manager.

Questions can be queries to learn from a mishap for next time, it can be a polite (sometimes impolite) way to accuse negligence or lack of skill, direct accusation of intentional fraud, or theft when it comes to financial transactions in a bank, for example.

Depending on the business criticality and its context (authorities, regulators, clients, and providers), the seriousness of an information security expert's responsibility may vary.

I would say that information security stands for responsibility. It can often be perceived as a profession that does not require an immense amount of seriousness and most people that work in this field tend to be humorous, on that note I would like to clarify the fact that being humorous does not indicate a lack of seriousness, responsibility, and professionalism, on the contrary, it is the opposite, as it takes endurance to get there.

Many information security consultants and professionals who are happy with their job and achievements, complain from time to time, which is natural, nonetheless, they are content.

Work-life balance

Given the amount of news and the changes in technologies, standards, frameworks, laws, and regulations, an expert finds themselves obliged to spend sleepless nights often, between learning new things and working overtime to meet deadlines. That easily leads to time away from loved ones, passions, or hobbies one may have, therefore, being able to create a balanced schedule and manage time correctly is of utmost importance.

Achieving a healthy work-life balance may take some time and determination, as the need to set boundaries for yourself, is fundamental. Being able to manage time correctly, between work and personal life, may be a bit of a juggle initially, but a definite tip from my side would be having a set daily work schedule, realizing your peak productivity hours, and taking advantage of that timing.

Always keep in mind the importance of your health, be that mental or physical. Make sure you are making time for your hobbies, passions, and the things that bring you joy aside from work.

As lovely as a rich professional career is, we must never forget to make time for ourselves, friends, and family.



in

Abdelmalek Najih

Group IT Security Compliance and Threat Intelligence Officer at IQ-EQ Group

Abdelmalek Najih is an Information Security Expert. He has been working as an auditor, adviser, and trainer in the field of information and cybersecurity with clients in various sectors in different countries in Africa and Europe.

Mr. Najih's expertise are mainly oriented toward information security governance, risk, and compliance.

The PECB Anti-Bribery Conference 2022 is over, and we are proud to say that it has been a huge success and an astounding turnout of attendees from all around the globe. We would like to thank you for being part of this incredible journey with us. You can view all of the PECB Anti-Bribery Conference 2022 recordings by [**clicking here**](#).

Following the great success of the Anti-Bribery Conference 2022, PECB has announced the Quality Management Conference 2022 that is going to be held on May 23-24. This will be a two-day virtual event that will feature two sets of two simultaneous sessions per day. The first set of sessions will begin at 3:00 PM CET, and the second set will begin at 5:00 PM. Each virtual panel will last for one hour and will be headlined by quality management experts and professionals from around the globe.

The PECB Quality Management Conference 2022 will feature an extensive program that will contain sessions in English and French. Panels will cover topics from different areas of issues and challenges related to the future of quality management systems, and so much more. To view the entire conference program, please [**click here**](#).

Do not miss out! **Reserve your seat** for free now, and do not forget to invite a friend or colleague.

REGISTER HERE!



PECB QUALITY MANAGEMENT CONFERENCE 2022

When Cybersecurity and Business Continuity Converge: A Security Leader's Perspective on How Organizations Can Thrive



BY RINSKE GEERLINGS

The traditional concept of IT Disaster Recovery (DR), i.e. the solution where an organization sets up an alternate site where servers, applications, and data can be used in case the primary data center burns down, floods, loses power, or otherwise fails, needs to be re-thought completely due to two major developments.

The first one is Cloud Computing, resulting in the IT DR responsibility seemingly being transferred to the shoulders of an external supplier. “We have outsourced our business continuity challenges to a cloud vendor” is a popular comment. Do not be fooled though. As perhaps everything in life, any benefits usually come with a set of new challenges.

Whilst you may have picked a cloud partner with ISO/IEC 27001 and/or related certifications, you will unlikely have full control over their operating procedures, any changes in security practices between audits, their mergers and acquisitions, their staff background checking processes, any temporary skill gaps, any disgruntled employees they may have, exactly where on their systems your data resides, and who else’s data resides on it.

Additionally, many customers of cloud vendors have ‘all eggs in one basket’ when it comes to storing their various data environments (e.g., production, test, development, and DR) all with the same cloud vendor. This is not always the best choice, if we consider the risk of your account being compromised or in case that supplier’s system or infrastructure go out of operation – which even happens to the best of them, as was demonstrated in 2021 when a leading CRM vendor went down for 6-8 hours taking their clients with them. Many of whom had stopped worrying about having a Business Continuity Plan (BCP) including manual work-arounds, because “they had outsourced their BCP to the cloud” – remember?



Without negating the upsides of cloud solutions for BCP, one should just be conscious of the aforementioned issues as well as further downsides, such as the relatively little ability to customize the user interface (compared to in-house software). But possibly the biggest downside is the complete and utter reliance on network connectivity. Whilst in a pre-cloud world, your staff may have been able to continue working on local file and mail servers, now they are no longer able to even email the colleague sitting next to them if internet connectivity is affected. Cloud can absolutely be an excellent choice, only as long as the decision is made with all pros and cons in mind.

The next development that has changed the concept of IT DR entirely is the uprise in information (including cyber) security threats. The traditional 'primary site vs backup site' concept makes little sense if malware has worked its way into both environments. Further complicating this risk is not knowing how far it has traveled, "so let us initially unplug all systems and investigate". A fire, flood, or power outage makes itself heard and seen in an obvious way, but with information security threats, part of the challenge comes with the inability to assess properly what has happened, what components are affected, how to remove the cause, and when a patch may become available. Finding an expert cybersecurity consultancy partner to quickly assist in this process may also be a challenge, particularly in case of a large-scale cyberattack, which means you will not be the only one seeking their help.

In a nutshell, DR is not as predictable as in the past, therefore, having a solid BCP with initial/manual work-arounds and excellent communication procedures and tools is imperative – more so than in the past. However, BCPs and Cyber Incident Response Plans (CIRPs) often exist on paper, rather than actually being embedded across the organization.

There is too much focus on ticking boxes to please auditors or clients, too much paperwork, too much-required effort to maintain such plans, too little hands-on implementation, too little buy-in, too little enthusiasm from staff, too little actual incident readiness, and too little effort put into preparing staff to think 'on their feet' when a disruptive incident occurs.

It affects entire organizations. Senior management ends up with a false sense of security; that everything is covered with technical controls, that risks are managed well, and that staff is ready to act if a cyberattack or other incidents were to occur – and that is if management even understands that the broader workforce must play a part in identifying and reducing information security risks.



Whilst, in reality, only a few individuals, such as the BCP manager, the Chief Information Security Officer (CISO), and any IT (Security) staff keep themselves familiarized with the content of the plans and procedures, or even worse, they are the only staff who even know these plans exist.

Even if organization-wide awareness campaigns are occurring, non-IT/Security/BCP staff are usually getting on with their normal business without understanding the context and how their daily work might incur risk. Until an immediate trigger occurs (e.g., a real-life cyber incident blocking their data, network, or application access), they do not even think about all the issues that could affect them. Often, information (including cyber) security and business recovery procedures only get written or refreshed for audit or other compliance-related purposes. And if staff can avoid being involved, they usually will.

The problem actually starts much earlier than that. BCP managers, CISOs, and IT Security staff tend to work in a solitary way, or mainly involve those in an organization who work directly with them. At best, they may try to have some dialogue with senior management to provide confidence that the risks are managed and ensure the top management can go to sleep at night.

It is often challenging to get buy-in, time, and attention from middle management and the general workforce who are busy 'doing their job'. And that is where the ball stops rolling in many BCP and Cyber Incident Response Planning (CIRP) initiatives.

The result is that mountains of documentation may get produced (including detailed preventative and impact-reducing controls for a range of incidents such as ransomware, DDoS attacks, malware, phishing, and social engineering), but these are written quite generically, e.g., using a standard template 'downloaded off the Internet'.

More 'fit for purpose' style documents (including practical manual work-arounds) are preferred, but these are often invested in just once and then easily get out of date. If a real incident occurs, most staff are oblivious to the incident (or confused), thereby increasing the chance of worsening the impacts. They do not know their role, what to look out for, what treatment options to activate, and/or who has the authority to give them instructions. In a nutshell, they are far from ready.

These problems stem from the following six mistakes:

1. Only the BCP manager, CISO, IT, and/or IT Security staff are fully aware of the plans and these individuals become 'single points of success' without the broader workforce being ready at any time for an incident. Little or no integration exists with broader incident management processes. Or worse, the entire plans have been written by an external party who have not aligned it with the organization's processes, structure, priorities, and culture.
2. In addition to over-dependency on a few internal skilled individuals, there tends to be an over-reliance on (and over-confidence in) external recovery



service providers and Cyber Incident Response (CIR) providers. Will their contractual promises and Service Level Agreements (SLAs) survive a substantial influx in demand for their services if many of their clients are affected by the same incident, such as an industry-wide ransomware attack or widespread flooding? Have you discussed with them how they might juggle their various clients' needs for help and where you are on their priority list? Taking legal action to address their non-compliance and getting compensated weeks or months after the event will not help you to maintain proper service levels and relationships with your own clients – and your reputation in the marketplace.

3. Complicated and jargon-filled procedures sent by technical staff to business divisions, under the expectation that their staff will understand and adopt them without proper guidance. Staff within the divisions are often unclear about their role in the plans and the purpose of some of the treatment options (e.g., password change policies, phishing attack simulations, BCP exercises, and staff training programs), which results in low uptake, attempts to circumvent certain controls and eventually create resistance amongst the broader workforce to help keep the process alive.
4. Top management, whilst aware of the risks and the need to comply with relevant regulatory requirements, often does not commit sufficient time to truly understand their own role in the processes, palms it off as an 'IT thing', is not equipped with the skills to actively guide middle management and general staff and does not commit sufficient resources to embed awareness programmes across the organization.
5. The CIRP and BCP are built as large documents – which are centrally managed by the BCP manager, the CISO, and other Security staff – not regularly maintained and impractical in real incidents, because relevant content is difficult to find. Version control (if any) may be impeded by only one person being able to edit the latest version at a time. And when the IT systems are deactivated as a precaution, the CIRP and BCP documents cannot be retrieved as it sits on a system that is now unavailable.
6. Simulation tests being timed inconveniently, repetitive in terms of the scenario, not including sufficient business context/relevance, and/or having a 'pass/fail' flavor – causing participants to try to look good in front of top management rather than trying to find areas of the plan that need improving.

I have observed organizations spending hundreds of thousands of dollars on consultants, only to find they still make these six mistakes. The resulting problems recur every few years when the documents are out of date, or sooner – and this is much worse – when a real-life flood, fire, data breach, or other incident occurs and the plans (and other controls) do not work – and nobody knows how to activate them.



Equipped with a short, sharp, dependable BCP and CIRP (integrated where possible, in terms of key decision-makers and related teams), your business will be in a far better position to respond confidently in an actual incident, protecting its brand and reputation, meeting its legal responsibilities, and ensuring the needs of its staff, clients, and stakeholders are met. To achieve this, senior management needs to commit to these processes 'all the way'. In a nutshell, the right approach includes the following elements:

1. A 'superhero' team is established, consisting of BCP coordinators, IT (Security), as well as key business unit representatives, to assist in creating the response plans, engaging with staff across the organization, planning/facilitating training and awareness programs and conducting rehearsals/tests.
2. Scenario-based discussions are held with external providers prior to selecting any of them. Once realistic promises regarding their response times and capabilities have been agreed upon, these are then validated.

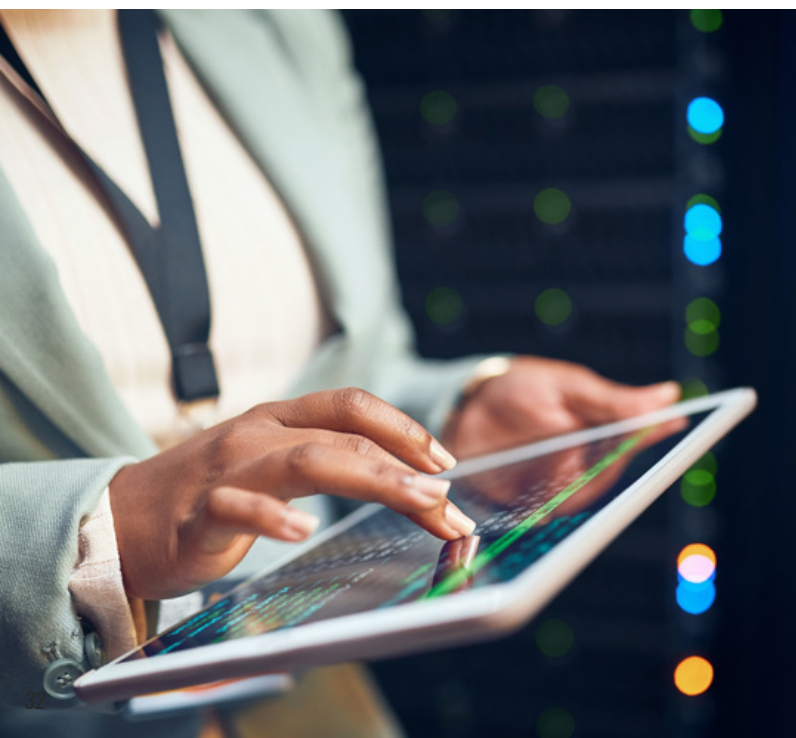
Where gaps come to the surface, further collaborative work is conducted together with them, to align mutual expectations and promises – and related (standby/retainer and/or activation) fees. Providers are included in any plan walk-throughs and/or exercises/tests, so they understand the internal mechanics of your organization, as well as key deliverables and roles relevant in an actual incident.

3. Middle management and general staff are engaged in concise but highly interactive workshops, so they start engaging hands-on with the BCP and information security processes, in an effort to assist with choosing preventative controls that their teams can practically implement and maintain. This could include the encouragement of a true “if you see something: say something” habit amongst staff, and the development of practical work-arounds in case of a disruptive incident.
4. Top management is trained in its governance role, as well as its decision-making role in the event of an emerging or evolving incident. By means of workshops using mini-scenarios, they share views on their organization’s risk appetite and related risk evaluation criteria. These can then be utilized by staff down the line to select feasible and reasonable treatment options.
5. BCP and Information Security documentation is simple to maintain (e.g. by using color coding, bullet-style checklists and Quick Reference Cards) and based on a top-down holistic approach (e.g. by working with a small number of impact-based scenarios). It resides on an interactive, common platform such as the organization’s Sharepoint/LAN/ Intranet site (i.e. one that the broader workforce already uses in their daily life) and has a remotely accessible copy in case IT systems are down.



6. Rehearsals or simulations are entertaining and actually allow participants to make mistakes. They aim to identify gaps instead of covering them up (for these to then surface during a real-life incident when it is too late). Exercises include audio-visual tools and a range of practical challenges and injects (including realistic testing of decision-making processes and staff notification systems if IT services are not to be used) in order to ensure management and staff develop true incident readiness.

The goal is for everyone to be able to sleep soundly at night knowing that, not only are good plans in place, but also that they are up to date, and that everyone knows what to do should an incident occur.



Rinske Geerlings
(MBCI ISO 27001 / 22301 / 31000)

Rinske Geerlings is an internationally known, award-winning consultant, speaker, and certified trainer in Information Security, Risk Management, Disaster Recovery and Business Continuity with over 20 years’ global experience. She implements, audits and trains staff in ISO/IEC 27001, ISO 31000 and ISO 22301 and related best practices.

She was awarded Risk Consultant of the Year 2017 (RMIA – Australasia) and Outstanding Security Consultant of the Year Finalist 2019 (OSPAs Australia). To build Business Continuity Plans (BCPs) and Cyber Incident Response Plans (CIRPs) that actually work when you need it most, contact Rinske via www.businessasusual.com.au.



Building Trust in Technology Using Confidential Computing

 BY NIKHIL AGARWAL

The Trust in Technology Adaption

Cloud Computing, 5G, IoT, edge computing, and AI are all driving innovation, but widespread adaption is hampered by a basic lack of confidence. The hesitation derives from a lack of trust in the capabilities of each technology to preserve data. However, a new data security paradigm promises to relieve businesses' major fears about data leakage. It is known as "confidential computing" and as a new way of securing data when it is in use and most vulnerable, by executing computations in a secure, hardware-based environment that is maintained segregated from the rest of the system.

Why would enterprises believe, at face value, the cloud's security guarantees? Enterprises have varying levels of faith in their service providers. Some people may have complete faith in it to keep their data safe, while other enterprises can be worried about other residents, software vulnerabilities, or insider assaults (for example, from data center technicians).

Some may demand rigorous adherence to privacy standards, some may also have reservations about the cloud provider's desire or ability to implement its stated security policies — for example, ensuring that their data would never be used without their consent — or fear subpoenas and other legal threats in the jurisdictions where the cloud operates.

Because a breach at a lower layer can affect security at any tier of the computing stack, security solutions must exist all the way down to the hardware's processing components. Suppliers of operating systems and device drivers, platform and peripheral vendors, and service providers are all removed from the list of needed trusted parties as a result of this action. This reduces the risk of other host programs, the host operating system and hypervisor, system administrators, service providers, and even the infrastructure owner posing a threat.



Modern Data Security Challenges

It is turning out to be progressively uncommon for seven days to go by without fresh insight about a huge data breach. Organizations are crawling to answer developing dangers and worries about large information security, however, they should initially comprehend the significant threats they face. Executives can further develop response activities by better understanding the most genuine risks.

Data can exist in one of three forms: It is either on transit, in rest, or being used. Confidential computing addresses the "being used" security case. Every one of the three forms requires safety efforts to be set up to guarantee that unapproved elements cannot get to the data. At the point when data is on the way, among applications and servers, or at rest, there are various measures accessible to safeguard it, including encryption, ransomware, and infra security.

Data being used is more muddled on the grounds that for applications to compute, they should approach decrypted, unsecured data. It is in this insecure form, when data is being used, that it is especially defenceless against root users and malware that can access and take the substance of memory.

The burning question here is; what can enterprises do to take the benefits of cloud and such other technologies while balancing a secure environment for their most sensitive data? Accepting the problems is the first step toward finding practical solutions. The succeeding step is to select suitable technologies and solutions to tackle these cloud security challenges.

Cybersecurity risks and challenges in cloud computing and other similar technologies are not overwhelming. Enterprises can take benefits of cloud technology with the correct cloud service provider (CSP), next-gen technology, and due diligence.

Remarkable Development in Confidential Computing Space

The IT industry has recognized a new class of threat actors for whom no amount of external security or firewall protection will prevent a data breach, resulting in the coining of a new phrase in the security world: Confidential Computing. Businesses and government agencies are looking for a new approach to keep their data safe in the cloud these days.

Financial services clients, vehicle manufacturers, health insurance providers, and telecommunication service providers all benefit from this. Data privacy has become more critical than ever as a result of the worldwide pandemic, which has prompted the development of public and hybrid cloud services. Specific compliance regulations, as well as a rising number of broader data protection rules, apply to certain industries.

Several significant IT companies, including Google, IBM, Huawei, Arm, Intel, Microsoft, Oracle, Red Hat, Nvidia, Fortanix, and VMware, are members of the confidential computing consortium and have invested heavily in Confidential Computing, bringing new and creative solutions to the enterprise.





As a result, organizations in these industries must adhere to what is referred to as the "three pillars of data security": data security at rest, in motion, and in use. These principles also apply to cloud computing security. The first and second have been managed using encryption and tokenization, among other approaches, over the years.

However, the last one has proven to be more challenging to achieve, particularly in the cloud. Data must not be protected in order for computation to take place. As a result, attackers have the opportunity to dump the contents of memory and steal important data.

And this is where confidential computing comes in, assuring organizations and leaders that their data in the cloud is safe and secure.



Relevant Confidential Computing Use Cases

Finance 	Healthcare 	Industrial 	Emerging 
Regulatory compliance Anti-money laundering Data Analytics Blockchain Cross-border analytics	Electronic health records Supply chain Genomics Drug discovery Federated learning	Data Sharing Industry 4.0 Supply chain Securing IP Service Attestation	Industrial Retail loyalty Supply chain Edge compute Telecoms
Most regulated industries looking to adopt cloud economic models but restricted by privacy concerns			

The high-tech industry benefits greatly from confidential computing. Confidential computing primarily tries to give businesses more assurance that their data in the cloud is secure and private. It encourages businesses to use public cloud services for more sensitive data and computational tasks.

Because many edge and IoT devices must safeguard in-use data, confidential computing can be employed outside of the cloud as well.

A store and a credit card firm can use confidential computing to cross-check their customer and transaction data for potential fraud while none of them has access to the original data. CC ensures the privacy of their customers' sensitive data throughout the process. Confidential computing allows for secure multi-party AI training for many reasons. For example, many hospitals may pool their data to teach AI to detect diseases based on CT scan images.

Throughout the process, the data of the patients is kept private. Sensor data from networked automobiles may be gathered and processed using confidential computing in an end-to-end encrypted and verifiable manner. It is theoretically guaranteed that no relevant judgments about individual drivers can be formed from the output data.

Industry 4.0 refers to a strategy for increasing productivity by deploying a large number of sensors and analyzing the data collected. Companies, on the other hand, are often unwilling to share or process their data in the cloud. Confidential computing has the potential to change that.

Most specialists in the sector believe that this technology is the way of the future. In the coming days, the software landscape of new technology will be shaped by cloud computing paired with confidential computing, which provides data security benefits. Confidential computing may become the de facto technology for computational security as a result of the necessity to safeguard and manage sensitive data throughout its life cycle, as well as industrial legislation and the expansion of cyber risks.

Confidential Computing Becomes the Organic Solution With Growing Data Security Concerns

When businesses started their cloud excursions several years ago, early adopters did not rush things. For the most part, it was simply a matter of moving a few simple workloads to the public cloud. However, we are now in the second chapter of the cloud, and we are trying to migrate the remaining workloads. This entails transferring sensitive data to the cloud while attempting to prevent the ransomware and other threats that plagued the cloud's first chapter.

Additionally, confidential computing creates new commercial options. Without having to worry about storing and processing their data, businesses can choose a cloud service provider that best matches their needs. Organizations can also collaborate with other businesses to develop innovative solutions without revealing intellectual property or other sensitive information.

Running workloads in secure enclaves allows for entirely new security requirements to be implemented, preventing



breaches, viruses, malicious insiders, and hackers. By applying this to cloud infrastructures, businesses may utilize the cloud almost like on-premises if they operate everything in secure enclaves – because no one, including cloud providers, has access to your data or code, removing the need for trust.

This could become the key use case for Confidential Computing in the next years, affecting how businesses set up their IT infrastructure and we will definitely see more businesses shifting toward confidential computing.

Confidential Computing is the logical choice for businesses concerned with cybersecurity and the protection of their data, employees, and customers at all levels. We believe that when you learn more about this immature but rapidly growing technology, you will find that it is a viable answer for your business security needs.



Nikhil Agarwal

Technologist, Cyber Security Advisor & Penetration Tester

Nikhil is an innovative avant-garde information security leader & technology evangelist, currently working as Senior

Solution Architect with Fortanix Inc., and leads large-scale confidential computing projects helping clients solve their data security challenges. Nikhil was ranked 18th in Cybersecurity, 10th in Emerging Technologies, and 3rd in Cloud Security amongst the top 25 consulting leaders by Analytica in the Consultancy Industry, globally.

As a noted technology expert, who passionately shares knowledge with the community, Nikhil has proven ability to work across cultures and serve clients globally while working in Europe (Germany), Africa, MEA, JAPAC countries amongst various client industries.



Is AI Favoring Data Protection and Authentication?

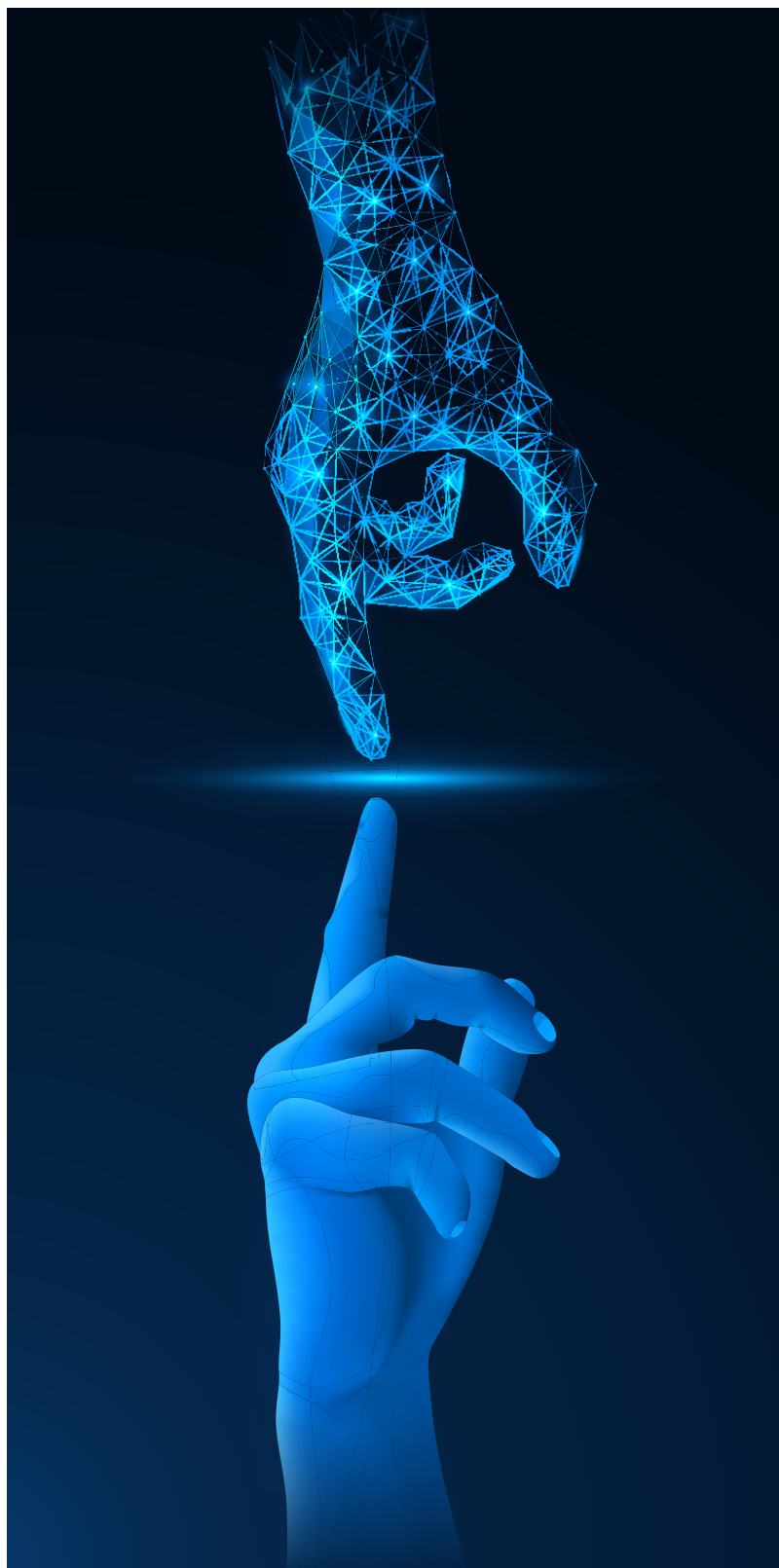
 LÁSZLÓ GRAD-GYENGE

Can AI help us to protect our data?

The answer is more or less straightforward as there are already examples of applied AI algorithms in this topic. I suppose the first online data protection technique is well known to the reader. The purpose of this tool is to typically prevent automated access to online systems by inserting a human check into certain parts of the online workflow. This method is well known by its abbreviation: CAPTCHA. The early solutions did not involve AI algorithms on the protection side but involved AI algorithms on the hacking side. Nowadays, there are various solutions on the market. The most widely used technique - reCAPTCHA - involves AI. In this case, the primary role of AI is not the classification between humans and bots but dataset building. When a visitor solves a CAPTCHA presented by reCAPTCHA, the images are automatically annotated by a no-cost human workforce. The software probably presents those images which cannot be labeled with high confidence by an AI algorithm.

Biometric identification is also involved in commercial products. Some smartphones and laptops already offer face and fingerprint identification solutions. In addition to such techniques, alternative solutions are also possible, for example, skin impedance-based identification and breath analysis based on exhaled biomarkers. The mentioned techniques strongly rely on AI algorithms. The application of such solutions can be applied in law enforcement and financial scenarios mainly, at the moment.

The device/browser fingerprinting is also a rich source of information. The fingerprint contains relevant information about the user that can be acquired online. Such user attributes can be, e.g., browser type, browser subversion, IP address, geolocation, and also the history of these values. AI algorithms can be applied to such data to conduct account fraud detection, protect payment processing, etc.



In addition to user account protection, enterprise grade solutions are also applied in practice. Enterprises are not trivial to protect, due to the relatively high success rate of social engineering. The typical application areas of AI algorithms can be found, in this case, in antivirus software and smart firewall systems. The specialty of antivirus classifiers is the need for an extremely low false-negative rate. The hardness of smart firewall systems can be found in the heterogeneous and distributed data such systems rely on.

Can AI help with data acquisition activities?

As already mentioned, AI can be used to overcome automated and human-operated IT protection. The mechanisms of such attacks can be, for example, database acquisition, propagation of fake news, breaking data protection, cracking passwords, identifying weak spots, finding targets of social engineering, impersonating people (voice, video).

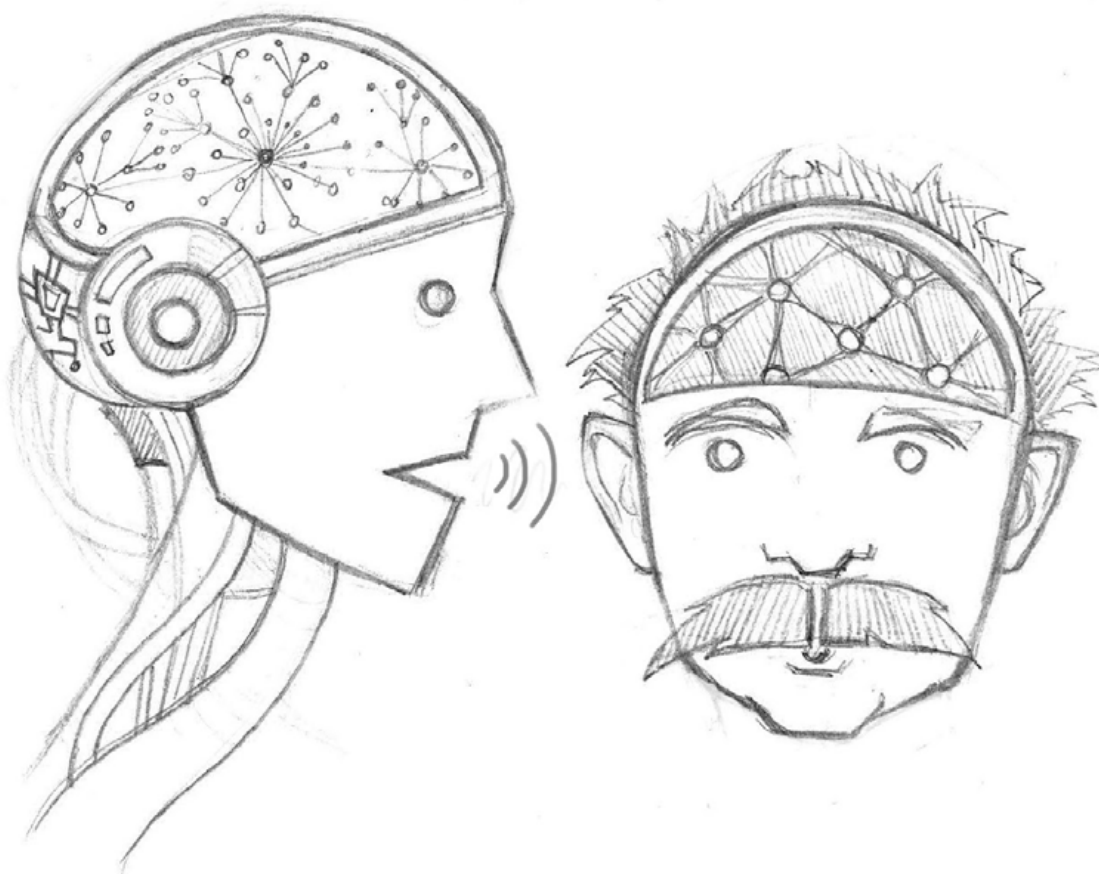
How did AI affect common data protection practices?

AI algorithms are ubiquitous these days. State-of-the-art techniques can be found under the hood on most of the common online platforms of tech giants, such as; Google, Facebook, Booking, Spotify, Amazon, YouTube, etc.

The goal of such algorithms is to increase the efficiency of these systems regarding a previously defined business goal.

From the business perspective, the best strategy should lead to a win-win situation, which means that the AI should be applied in a way that is attractive, both for the service providers and also for the users. This principle should make the business work.

However, there are different voices also out there. Looking at the problem in black and white, the application of AI algorithms can be treated from two different perspectives: AI can be malicious or good. One can say that malicious companies use their data to calmly calculate incentives for a higher consumption rate, they are interested only in profit. On the other hand, the application of AI in Information Retrieval (IR) can be treated as a purposeful Intelligent Augmentation (IA) tool, which provides value to the online users. In general, the task of IR is to process a huge set of items. By huge we mean that it cannot be processed one by one, by humans because of time and capacity limitations. IR algorithms help users to find relevant items in this set. This relevance can be calculated related to a search query or to a specific user. In the first case, we talk about web search engines, as Google, Bing, etc. In the latter case, we talk about personalization. In most cases, web search comes in hand with personalization.





From the business perspective, organizations equipped with AI can provide a better service as users tend to find the relevant products/services easier. This is true for search results, advertisements, audio tracks, travel destinations, videos, etc. In general, better service leads to a higher engagement and a higher profit in the end.

AI algorithms are trained with examples, so-called datasets. It means that a relatively massive amount of examples should be presented to the actual AI algorithm. Based on its modeling ability, the algorithm then learns the interdependencies in data with a certain accuracy. The essence of algorithm development is to find the right algorithm for the right task. If the algorithm is too simple, it will not be able to fulfill its task at all. If the algorithm is too powerful, it will memorize the training data instead of learning its interdependencies. In general, it means that the AI algorithms are eager on training data. The quality of the data strongly determines the quality of the algorithm. The organization that manages to acquire sufficient and high-quality data will be able to develop high-quality algorithms and will hopefully be able to convert the algorithm into a revenue stream. This paradigm is often mentioned as data is the new oil. Those organizations have the chance for a higher profit that manage to gather relevant and high-quality data.

There were times when the acquaintances of any user and also other sensitive data could be queried from Facebook without any significant restriction. Back then, it was culturally accepted and also unregulated. The first moves to data protection have been conducted by the organizations themselves to protect their own database, their own business. The popularization of search engines, social media platforms, massive content providers, and the expansion of applied AI algorithms attracted the spotlight to this sector. Spotlight and revenue typically come with regulations sooner or later, thus it happened. We call it GDPR or MDR in the medical world. Data collection became regulated.

The primary message bound to GDPR is data protection, which leads basically to a positive attitude for the average citizen and is basically a noble goal. The question lies more in the implementation of the principles of the regulation. In practice, data protection is conducted with administrative/bureaucratic techniques. It means the definition of several dedicated working hours for legal, economical, and IT professionals to elaborate the IT workflows that operate according to the principles described in GDPR.

It means that the costs of data collection has increased.

Does GDPR prevent the citizens? The answer could be: In some cases yes and in some cases not.

I still receive phone calls from a broker I have never seen to transfer them my money and who recommends me to buy high-performance stocks. I already asked the broker to remove me from their database, without any effect. I still receive emails from a “bank in the Netherlands” about billions of euros that will be transferred to my account as soon as I pay the transaction fee. I still receive a lot of spam from companies I have never heard of. It means that GDPR had a short attenuation effect on the spamming/scamming activity but it is gone. Basically, it reflects the efficiency of law enforcement techniques applied currently.

Various business models appeared in the online world to acquire data. In the case of tech giants, data can be found directly in the online system. Some software libraries/devkits provide AI algorithms and also help the developers with data acquisition and dashboards to manage data collection user settings. I guess that most of the users use the default settings by just clicking the ‘ok’ button and are more or less immune to the terms and conditions and also to the GDPR settings.

I think that the economic effects of GDPR are also not communicated clearly and are also not sufficiently visible. In general, from the economical side, regulations like MDR, GDPR, and Standard Essential Patents (SEP) typically help big companies and hinder small ones, as such regulations increase the costs to enter and operate on the market. Furthermore, big companies have more resources, more routine in lobby activities, and better access to legislation procedures. Such mechanisms can be involved to conduct market cleaning, which process has its advantages and disadvantages.

AI capable IoT applications are gaining more and more attention these days. As it has already been mentioned, the first step of developing an AI algorithm is data collection. Fortunately, this type of data does not involve personal information and can be collected in a less regulated manner.

It means that there is a significant pool of AI algorithms that can be developed without asking permission from the users.

Finally, privacy is a key issue in the case of AI algorithm development. Even if the training data is properly anonymized, leaking algorithm design can lead to the violation of privacy. An example can be presented from the world of recommender systems, personalization algorithms. Such algorithms typically calculate the user preferences, the recommended items based on user interaction, namely: who purchased what.

In the case of common items, when there are a lot of purchase items available, the recommendations are driven by the statistics, for example, which items are purchased by similar users. In extreme cases, when there are rarely purchased items in the context, the identity of the person can be revealed.

To summarize this article, AI has several direct and indirect effects on data protection and authentication. In the first part of this article (first two questions), the more technical aspects have been discussed. It focuses directly on the application and practical issues. The last question discusses the effect more from the societal perspective. It brings up questions and reflects on mechanisms related to this topic.



László Grad-Gyenge
Artificial Intelligence Expert,
Researcher and Lecturer

László is the owner and managing director of Creo, a software development company. The company mainly does business software for multiple platforms as web development and app development. Creo has a special interest in the MedTech sector.

In his daily work, László focuses on applied AI projects. He works in various domains, such as recommender systems, natural language processing, digital signal processing, computer vision, and autonomous vehicles. His goal is to apply his AI algorithms in the software products developed by his company.





EXPLORING PARADISE ON EARTH

Bali is one of the most famous islands in the Indonesian archipelago. The island is home to an ancient culture that is known for its warm hospitality. Over the years, the grace and charm of Bali and its people have earned this tiny Indonesian island numerous epithets of praise and homage, with many referring to it as; Island of the Gods, The Last Paradise, Land of a Thousand Temples, and Morning of the World.

This island has a lot to offer to its visitors with its varied landscape of hills and mountains, rugged coastlines and sandy beaches, lush rice terraces, and barren volcanic hillsides all providing a picturesque backdrop to its colorful, deeply spiritual, and unique culture, stakes a serious claim to be paradise on earth.

With something to offer to a very broad market of visitors from young backpackers, right through to the wealthy, Bali packs multiple adventures with world-class surfing and diving, a large number of cultural, historical palaces set against stunning natural sceneries are some of its top attractions that make Bali one of the world's top destinations. Bali also offers plenty for adventure-seekers. From white water rafting, diving, volcano hiking, jungle trekking, water sports, cycling, and much more.

The island is blessed with fertile land, lush green forests, and beautiful beaches. The ultimate tourist destination is located at the southern tip of the island, near Denpasar, the capital of the island. Kuta, Nusa Dua, and Sanur are just some internationally popular beaches along its southern coast.

But Bali is more than just white beaches in Badung and Denpasar. This Land of Gods is rich in cultural heritage as reflected in many colorful ceremonies and art crafts. It also boasts the best hotels and accommodations on the planet. Here are some destinations you can expect in Bali;

The Beautiful Beaches Along the Coastline

Amazing beach luxury resorts in any of Bali's famous areas leave little to the imagination a few of which, such as: Kuta, Jimbaran, Seminyak, Tanjung Benoa, Candidasa, Lovina, Sanur and, Nusa Dua, where most of the great hotels and villas are right on the beach, are not unfamiliar names to those who love traveling.

As previously said, Kuta, Sanur, Nusa Dua, and several other beaches do not need an introduction at all. But there is more to this island than just white sandy beaches with a magnificent view. There are beaches with caves as Gunung Payung and Uluwatu, beaches with black sand, such as Soka and Amed, as well as, extremely private beaches like Karma Kandara, and many more different kinds of beaches; some rocky, some with green hills, and some are the most ideal for watching sunsets. Whatever you are looking for in a beach vacation, be sure that Bali has it all.



The Rich Cultural and Religious Heritage

Bali is also known as the Island of Hinduism as most of the residents are Hindu, leading to lots of religious monuments dotted all around the Island. And it is not only shrines and temples, Balinese life is closely connected to nature, so the preference to preserve most of natural wonders around them is evident.

Shrines, for instance as: Pura Besakih, Pura Luhur Uluwatu, or Pura Tanah Lot are already popular among tourists. Also worth visiting are religious palace and parks, such as; Istana Tirta Gangga, Desa Penglipuran, or Taman Air Suasada. Balinese also do many ceremonies almost daily.



The Parks and Recreations

Due to its natural beautiful landscapes, Bali cannot stop growing as a tourist destination. Lots of parks and monuments are being built around the island, as man-made attractions which range from exotic parks to huge monuments. You can find zoos, petting zoos, bird parks, cultural parks, and many other similar attractions in many places. Some of the monuments worth noting are: Puputan Monument, Bali Bomb Memorial, and the new Garuda Wisnu Kencana.



The Lively Diving Spots

Diving is probably an underrated attraction here. It is true that Bali's underwater is not as rich as Indonesia's coral wonders, but they are great if you are already on the island. Menjangan Island offers a spectacular shallow coral reef under its calm waters, ideal for snorkeling. Nusa Penida dan Lembongan is where you go to watch Mola-mola, Manta Rays, and other migratory fish. Tulamben is a unique diving spot where you can see coral reefs flourishing on the USAT Liberty shipwreck.



How to Get There and What to Do in Bali

Easiest way to get to Bali is of course by air. Ngurah Rai International Airport connects Bali with many countries around the world. Bali is accessible via land from Java, although, the car should take a ferry at Banyuwangi. By sea, you can reach Bali from Java and Lombok.

Once you get there, there are many options of transportations you can pick. You can ask a travel agency for a tour package or you can simply rent a car or motorcycle to get around. Be aware that the traffic congestion in Bali can be pretty bad during certain periods of the year.

Best Time to Visit Bali

The best time to visit Bali depends mainly on the weather and what locals refer to as high and low seasons, which do affect the overall price for accommodation.

The high season is during the months of July and August, during Easter Holidays, and Christmas / New Year (December until the 1st week of January), making these Bali's busiest times.

However, for many reasons, the best time to come to Bali is April, May, June, and September. October is not too bad either, still less rainy than November, just before and just after high season. It is still dry season, it is slightly less humid, and room prices and villa rentals can be much cheaper than during high season.

Many shops offer sales and promotional offers, restaurants are less crowded in those mid-season months, and in general Bali is a bit more relaxed.



During these periods is also the best time for water sport activities, such as; scuba diving, surfing, snorkeling, etc. Waters are clear and it does not get too crowded. Also, worth mentioning are major activities and attractions such as; the family parks and entertaining things to do (Bali Zoo, Bali Bird Park, Marine & Safari Park, Waterbom, White Water Rafting, Monkey Forest, etc) have fewer visitors which can make the experience far more enjoyable.

If you wish to explore the island and visit the main sightseeing spots, temples, or go for a day trip and tour, then these months are ideal for you. And not to forget, in general, the traffic and business on the roads is more bearable. Especially in Kuta, Legian, and sometimes even Seminyak the narrow streets are packed during certain times in the day with cars and motorcycles. Some tourists love it that way and could not imagine a holiday otherwise, but if you prefer a more quiet vacation, then Kuta and Legian during high season might not be the best choice.



What to Expect From Bali

Whatever your expectations and desires, they all can be more than fulfilled. Bali is regularly rated as one of the Top 10 tropical holiday destinations of the world.

However, Bali is not simply that. It is diverse, complex, and sometimes unpredictable and falls short of your expectations if you do not know some basic rules.

The island is a vibrant, dynamic organism which is home to many Indonesians and a few thousand expats living and making a living here. Although one can find the most luxurious resorts, pristine beaches, best cuisines, and coconut trees on Bali, for many it is simply home.

Partnership with PECB

Through a partnership with PECB, we have achieved great success in becoming the market leader for training services in Indonesia and South East Asia. This success has been facilitated with great support from the team at PECB, who have been accessible and ready to assist at all times, permitting us access to required documents or additional information as required. Despite our organizations operating in different time zones, we have managed to handle communication well.

PECB grants compact and innovative modules, making the training services we offer easily accommodating for all interested. Promotional support by the team at PECB, as well as the tools offered in that regard, make for very powerful advancements in selling training services.



NA Putra
CEO at NQA Indonesia

in

NA Putra background includes the founding, development, and portfolio management of enterprises in: The Certification Business, Training Services, Assessment Services, Productivity, Business Improvement & Innovation Sector, and affinity sectors in the Asia Pacific Region.

Specializing in: Third-Party Certification, Training Services, Assessment Services, Improving & Innovating, and Affinity Services, Productivity and Business Improvement Services, Business Transformation Services, and Anti Bribery, Compliance & Anti-Corruption. He is also a PECB Approved Trainer for ISO 37001 & ISO 45001.





A Deeper Look Into Our Technology Advanced Era

We are living in a modernized technology-forward world. Technology has been playing a big role in our lives, making everything more efficient in our personal lives, as well as our organizations much faster and more effective in performance. However, knowing how to keep up with information and making sure that you are staying secure in this fast-evolving field, is just as important.

If you are interested in learning more about information security, cybersecurity, or business continuity, here is a list of books that will help you expand your knowledge.

1. ISO 22301:2019 Auditing Guide and ISO 22301:2019 Implementation Guide



If you wish to personally understand and learn more about business continuity, you can do so from the comfort of your own home.

ISO 22301:2019 Auditing Guide eBook provides the elementary audit concepts, principles, and phases in the audit of a business continuity management system in compliance with ISO 19011 and ISO/IEC 17021-1. It gives readers an understanding of the role of an auditor in; planning, leading, and following an audit.

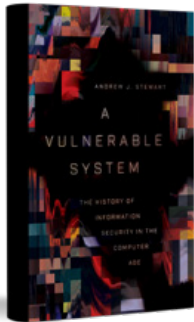
ISO 22301:2019 Implementation Guide eBook defines the fundamentals of business continuity, as well as the necessary steps of implementing a business continuity management system based on ISO 22301. This book can function as a tool, helping an organization experience the advantages of a properly functioning BCMS.

2. Cyber Security: Issues and Current Trends by Emil Pricop



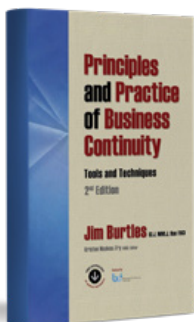
The book imparts a solitude of various issues and challenges of cybersecurity that offers readers a deeper understanding and awareness about it. Multiple tools and techniques used by cyber attackers to exploit a system are carefully analyzed throughout the book. It also delves into the concept of privacy and anonymity through different topics around anonymous services, which are practically discussed to the reader. In later chapters, the author explains the importance of preventive measures such as intrusion detection system (IDS). Since cyberattacks have become more prominent, digital forensics is a must for crime investigation and in taking the needed measures so these attacks do not become an occurrence. Through the book, there is a collection of evidence from the victim's devices and the systems that have importance in an investigation. The purpose of the book is to help its readers who use electronic gadgets in their daily lives.

3. A Vulnerable System: The History of Information Security in the Computer Age by Andrew J. Stewart



Information Security threats penetrate our everyday life, this book demonstrates how despite the demand for information security increasing, the needs are not being met. This book provides a wonderful blend of history, business, and technical understanding. For anyone involved in information security, it provides a great read since it is a very compelling book from start to finish. The author, as a historian, gives the reader a comprehensive understanding of people, events, and contexts from the last 70 years of information security. Even though the history of information security includes a lot of gloomy days, which the book showcases, the author writes of what is needed to turn it around, he explains that there needs to be a concerted effort to understand how complexity affects information security and how it can be managed.

4. Principles and Practice of Business Continuity: Tools and Techniques 2nd Edition by Jim Burtles



This book provides a very practical and easy-to-understand approach for beginners. It offers a very resourceful read, exploring frameworks and guides worth adapting, and on developing and maintaining a good Business Continuity Management program in your organization. In order to deliver information on the practical front of business continuity, the author explains six main scenarios. To quote Burtles – “If you and your organization are prepared to deal with these six generic risks, you will be able to recover from any business disaster”. He walks the reader through the tools and techniques on; bringing people together to win executive support, organize response teams, create a Business Continuity Plan, and recover from the disruption. The author's way of explaining step-by-step, real-world scenarios, will give you a sense of security in performing your duties.

Top Five High-Paying Job Positions You Can Pursue with an ISO 22301 Certification

As the world becomes more and more unpredictable, the frequency and severity of disruptions, be them natural or human-caused, increases drastically. Considering these circumstances, it is essential for organizations to ensure the continuity of their business operations and processes.

The importance of business continuity and resiliency has increased the demand for professionals certified against ISO 22301. This certification helps business leaders identify potential disruptions and evaluate their impact on an organization. It also helps them make effective and accurate decisions, deploy effective responses, and minimize the overall impact of unexpected events.

The business continuity management solutions market is expected to grow. This directly increases the creation of new business continuity roles in different organizations.

The knowledge and skills needed to perform tasks related to business continuity are very specific and essential to individuals performing such roles. One of the best forms of demonstrating such skills and knowledge is by holding an ISO 22301 certification.

1. Head of Business Continuity Planning

Based on the information provided by PayScale, Zippia, and ZipRecruiter, the average salary of a head of business continuity planning is \$123,981 per year.

2. Global Business Continuity Manager

Based on the information provided by PayScale, Salarycom, and ZipRecruiter, the average salary of a global business continuity manager is \$121,346 per year.

3. Business Continuity Consultant

Based on the information provided by PayScale, Glassdoor, and ZipRecruiter, the average salary of a business continuity consultant is \$94,879 per year.



4. Disaster Recovery Analyst

Based on the information provided by PayScale, Glassdoor, and ZipRecruiter, the average salary of a disaster recovery analyst is \$91,465 per year.

5. Business Continuity Specialist

Based on the information provided by PayScale, Salarycom, and ZipRecruiter, the average salary of a business continuity specialist is \$81,601 per year.

A business continuity management system (BCMS) based on the requirements of ISO 22301 ensures the continuity and resilience of an organization's business and processes before, during, and after unexpected interruptions. An ISO 22301 certification can pave the way for new job opportunities that are fundamental to having a BCMS in place that serves as the backbone of any organization.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

[Click here to see how PECB can help](#)



ISO 22301 Lead Auditor eLearning Training Course in English Available Now!

Take advantage of the opportunity to become a PECB certified auditor by attending the PECB ISO 22301 Lead Auditor eLearning training course and open a new gate of opportunities.

Each eLearning training course is delivered by several experienced Trainers from all around the world, who will help you master audit techniques, manage an audit program, audit team, communicate with customers, and resolve conflict.

CHECK THE BROCHURE!

To learn more about our other eLearning training courses, please click [here](#).





WEBINAR **LIVE**

TAKE A LOOK AT PECB'S LATEST WEBINARS

Following the continuous evolvement in the industry, PECB's Webinars are always up-to-date with discussions on current trending topics.

Learn more about the latest developments in Information Security from experts in the field.



[PECB WEBINARS](#)

Business Continuity and the Impact on HR Leaders



RAJKUMAR SHARMA

Before the pandemic, business continuity was defined based on how organizations can run their operations without impacting their overall productivity/deliverables. When there were any natural calamities or outages such as network or infrastructure, most organizations would be prepared with a plan for it and would conduct mock drills regularly. Then comes 2020, COVID-19 pandemic hits us and most of the organizations quickly switch to work-from-home, which was part of the business continuity plan, and in cases where it was not possible, explored ways to manage their operations.

While it looked like organizations were running smoothly during the pandemic, there were a few elements which, due to the unanticipated situation, for many organizations were not pre-thought:

1. **Employee Well-being:** Along with taking care of health during the pandemic, everyone grappled with high levels of stress, anxiety, feeling of helplessness when they or their loved ones were having health struggles. This resulted in employees looking for extended leaves or breaks from work and in most cases, not all organizations were prepared for it.
2. **Growth or Transformation:** At the start of the pandemic, organizations did experience some slowness, since there was uncertainty on how the situation would evolve and how it would impact the business; however, after the lull for 1 or 2 quarters, organizations started to experience growth or transformation in most cases. Almost all industries/sectors experienced growth or they had to accelerate their transformation journey, such as digital transformation, and for this to happen the demand for talent increased rapidly, including the need to have skilled talent in different areas.
3. **Talent Mobility:** If one would think of a side effect to an efficient business continuity plan, it would be talent mobility. During the pandemic, most of the talent moved places, in order to be closer to loved ones, or where it felt that they are closer to their



passion and now they are looking to continue with the same model as a long-term plan. Also, another facet of talent mobility is the attrition, last year we did see how every second or third employee of an organization was looking for a change irrespective of their tenure.

4. **Talent Burnout:** In most cases, organizations were able to run operations as per the plan, maintaining their productivity/deliverables; however, all of that did come at a price. Employees experienced burnout, and eventually, it started impacting the overall productivity and quality of deliverables.

HR leaders were tasked to put together approaches to address the above-listed points, despite that, it has not been addressed completely yet.

The pandemic did highlight the need to consider aspects from the consumers' standpoint as part of any business continuity plan proactively. As I reflect on my two decades of experience, in most cases, HR leaders are pulled-in to address the consumers' aspects as an after-effect.

I reckon this is the best time for HR leaders to get in the fore-front and help their leadership look at the following aspects proactively:

1. **Talent Planning:** HR leaders should collaborate in the overall talent planning process and consider the following aspects:
 - a. How future business growth plans are considered while looking at the overall demand? This is one area that has been a challenge for all HR leaders, since the talent demand is like a moving target.
 - b. How could there be a balance between the number of employees working in office and remotely? In the new normal, everyone is looking forward to flexibility, all the while being connected with their colleagues.
 - c. How do you upskill or reskill talent to meet the evolving business requirements? The last 15-months have highlighted that acquiring talent is not that easy, in comparison to the past, it is important that HR leaders put together a comprehensive plan to upskill or reskill the talent within the firm.
 - d. How to integrate new talent so they are able to effectively contribute quickly? Integration of new hires has been challenging during these times, since the business demand is growing, and the stress to help integrate the new hires is falling on the existing talent in the firm, who also have to continue to work on their deliverables.

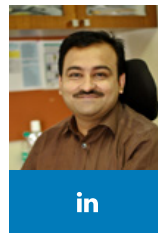


- a. How are other aspects from onboarding accounted for, such as IT assets getting delivered to new joiners on time? If the need is to have the new joiners get productive quickly, then getting some of the required infrastructures to them on time is going to be the key.
 - b. How aspects of employee well-being are accounted for in the overall planning? This is going to be an evolving and important area. Employee wellness programs need to consider aspects for every individual, for instance, what is their requirement or what type of support are they looking forward to. This is one of the most critical ones, since it has a direct impact on the overall productivity, deliverables, and in turn the revenue and margins of any organization.
1. Talent Management: While attrition will continue to be a challenge for some more time, we need to focus on employee engagement and retain their needs to be the primary focus going forward. We all know that the way we manage our talent has a direct impact on productivity and deliverables and there is enough research available to prove this point. Few considerations in this area:
 - a. What are the primary reasons for employees leaving organizations? Everyone has their reason or need to leave any organization and it is important to focus on the themes emerging from the various exit discussions. In some cases, employees are looking forward to understanding the purpose of their role and how it translates to impact on business and society. While for many recognition is an important aspect, for example, acknowledging contributions or monetary recognition, there are few who would like to create a balance between their professional and personal priorities.
 - b. What are the external factors which could influence talent within the organization and trigger attrition? An interesting trend that emerged during this 'Great Resignation' period is that most of the attrition has been in the space of passive talent. They were not actively looking for jobs; however, when they were reached out, they did not decline as to further explore the opportunity. This is also the talent that could be in the zone of either being highly engaged or disengaged and get influenced based on what they see or hear from others. It is important that as HR leaders we think of ways to connect and understand the needs of this talent segment and move them towards being more engaged and continuing to contribute with high impact.
 - c. What are the other factors which could influence employee well-being? When we thought we were getting a better handle of the pandemic, a new geopolitical situation emerged, which is impacting the talent, since they might have friends, family, or they might not be comfortable with this notion of conflict for power. Most of the time, these are very sensitive topics and could create division; however, the current talent does expect a point of view from their organization.
 2. Agility: We do not know when the next pandemic or situation could occur; nonetheless, I feel as HR leaders we need to be agile and quickly adapt as per situations and recommend solutions and approaches. There will not be any perfect or complete business continuity plan for future unpredictable situations.

As HR leaders, we need to think of business continuity as part of our core role and help the leaders of the organization and our team members to think through their processes and systems, if they are designed to meet any unexpected demand or situation, and how they can scale-up quickly to evolving business needs.

Taking into consideration the above-mentioned points, ISO 22301 allows you to respond effectively and promptly based on the procedures that apply before, during, and after the event. ISO 22301 shares the ability to secure data backups, minimize major losses, and maximize the recovery time of critical functions to your organization.

With a Business Continuity Management System, your organization is prepared to detect and prevent threats, assuring that you will continue to operate without any major impacts or losses.



Rajkumar Sharma
Strategic HR Leader

is a Human Resources Leader with 20 years of proven track record in partnering with business leaders on key people dimensions, organization transformation programs, driving talent attraction,

engagement & management, and development initiatives, such as leadership development program, designing & implementing competency model for high-performance environment, career management framework, expanding talent sourcing channels, structured & agile onboarding curriculum, learning roadmaps, focused coaching interventions for diverse profiles spread across different geographies, which ensures that they are delivering impact where it matters most.



THE UPDATED VERSION OF ISO/IEC 27002 IS HERE!

ISO/IEC 27002 provides guidelines for organizational information security standards, management, implementation, and maintenance.

It aims to make individuals capable of assisting organizations sustain confidentiality, integrity, and availability of information.

[PURCHASE HERE](#) ►

ISO/IEC 27001 Training Courses Are Now Updated!

Following the update of ISO/IEC 27002, the latest changes will be reflected in ISO/IEC 27001.

PECB ISO/IEC 27001 Lead Implementer and Lead Auditor training courses have been updated based on the latest version of the ISO/IEC 27002 standard.

You can now get certified to the updated PECB ISO/IEC 27001 Lead Auditor and Lead Implementer training courses.

BOOK YOUR SEAT ►

To learn more about ISO/IEC 27002, ISO/IEC 27001, and other courses, contact us at marketing@pecb.com

Customer Centricity through the implementation of Business Continuity – ISO 22301



**BARBARA FARISAI CHINZUNZA,
EXECUTIVE MBA IN INFORMATION SECURITY MANAGEMENT**

The coming of Covid-19 two years ago presented a severe and increasingly complicated challenge that confronted the survival of most businesses. The urgency and relevance of business continuity management (BCM) to alleviate potential risks, quicken recovery, and provision of customer needs became very relevant and important for any company despite their size. BCM is a framework that helps in identifying an organization's risk of exposure to internal and external threats. The goal of BCM is to provide the organization with the ability to effectively respond to threats such as pandemics, natural disasters, or data breaches and protect the business interests of the organization. BCM includes disaster recovery, business recovery, crisis management, incident management, emergency management, and contingency planning.

When done right, BCM can prove to be a competitive advantage for any organization. This is especially true if a disruption impacts an entire group segment where you are able to respond or recover more quickly than the others, minimizing the disruption to your customers. When it becomes clear that you excel in dealing with operation disruptions, trust and assurance will be established in your brand, allowing you to leverage this to be a preferred choice for your customers and even bolster confidence and increase your shareholder value.

ISO 22301 is a standard that specifies the need to implement, maintain and improve a business continuity management system with an emphasis on understanding continuity and preparedness requirements, establishing business continuity management policies and objectives,

implementing and operating controls and measures for managing an organization's overall continuity risks and continual improvement based on objective measurements. The standard is customer-centric and emphasizes the need to meet and surpass customer expectations to ensure business sustainability, as well as revenue growth.

Understanding continuity and preparedness

The most important aspect in the development of a BCM is to clearly articulate the stakeholder needs, therefore, specific focus must be given to customers because they are key to the success of the organization. Focusing on customer needs will also allow the BCM to be fit for its purpose and provide the organization with a sound overview of the process criticality, hence, as long as you design and implement the business continuity plan starting with a customer's perspective, to drive the business impact analysis, you can expect positive results. Understanding your customer needs is key in identifying where you create value for them, allowing you to prioritize and discern how much downtime is manageable in different areas before impacting your organization and how fast you should be up and running again. Impacts can focus on opportunity costs, loss of customers, and customer dissatisfaction.

Establishing business continuity management policies and objectives

This is done to ensure that the S.M.A.R.T objectives are set and aligned with the requirements that are customer-oriented. Policies and objectives are designed through



identifying internal and external dependencies that may have the biggest influence on an organizations' customers. Good customer objectives are more than just meeting the needs of customers, it aims at exceeding their expectations. Hence, offering top-notch quality customer objectives is something every organization should ensure. That establishment is to secure customer retention, brand image, and ultimately an increase in revenue.

Implementing operating controls and measures for managing an organization's overall continuity risks

Having identified customers' needs, established policies and objectives that are critical for the organization, the next step will be to put in controls that address and mitigate the risks that have been identified. Threat and changes are inevitable within the environment that our organization operates within, so, a deliberate approach to put up controls to mitigate the threats is mandatory. These controls include; setting up disaster recovery sites, business continuity plans, and business continuity procedures. Lack of these will ultimately mean that a business will fail to continue, leaving its customers with no option besides to migrate to competition that will be having better options.

Continual improvement

A continual improvement process (CIP), is an ongoing effort to improve products, services, or processes. Processes are constantly evaluated and improved in the light of their efficiency, effectiveness, and flexibility to the

ever-changing customer needs and business environments. There are various methodologies that organizations use to bring structure to the process of identifying and acting upon opportunities for improvement. Some common methodologies are: Six Sigma, Kaizen, Lean, and Toyota Production System. Although these methodologies differ, the foundation of each of them is the continuous improvement model and the principles which are based on:

- › Improvements, which stem from small changes rather than major paradigm shifts or new inventions
- › Employee ideas are valuable
- › Incremental improvements are typically inexpensive to implement
- › Employees take ownership and are involved in the improvement
- › Improvement is reflective

Conclusion

Every business will resonate with the fact that customers act as the lifeblood of every organization. Therefore, their satisfaction is of utmost significance for the success of the organization, which can be ensured by offering top-notch quality customer service. Implementing ISO 22301 has been proven to improve customer satisfaction, brand image, and revenue growth. In this age of unpredictability, ISO 22301 is essential and organizations are encouraged to implement it to ensure business stability and sufficiency for the ever-evolving customer requirements.

Explore New Opportunities for Growth and Success

As an institute of higher education, PECB University aims to offer top-quality business education.

Excel in your chosen field with a University Degree, with our new program structure on:

- Executive MBA in Cybersecurity
- Executive MBA in Business Continuity Management
- Executive MBA in Governance, Risk, and Compliance

Visit the PECB University Website to get more information or contact the PECB University counselor at university.studentaffairs@pecb.com





SEIZE THE OPPORTUNITY, LIGHTEN YOUR PATH

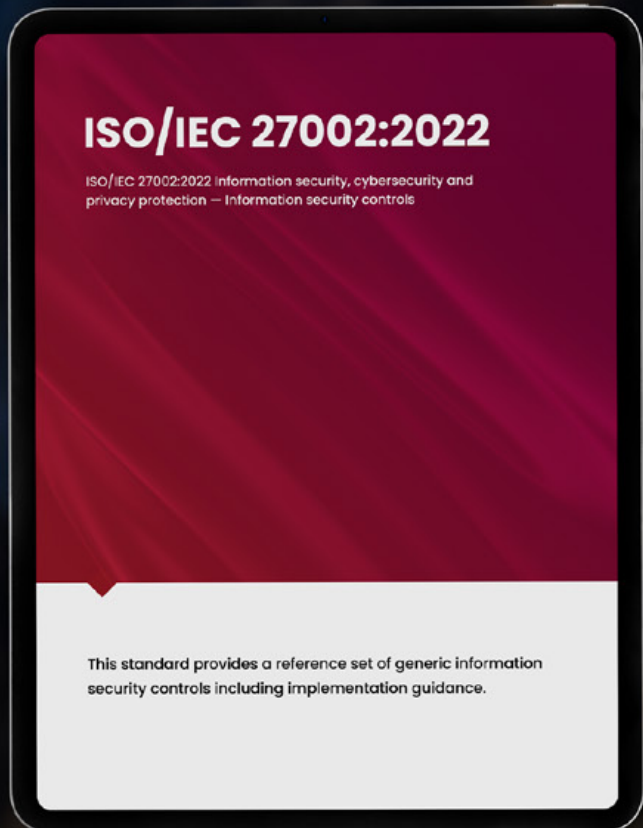
Take advantage of PECB's new and updated training courses!
Contact us at marketing@pecb.com or visit our [website](#) for more details.

Training Course	Language	Status	
ISO 9001 Lead Auditor	English	Updated	→
ISO 45001 Lead Implementer	English	Updated	→
ISO/IEC 27001 Foundation	English	Updated	→
ISO 22301 Foundation	English	Updated	→
ISO/IEC 20000 Foundation	English	Updated	→
ISO/IEC 20000 Introduction	English	Updated	→
ISO 31000 Risk Manager	French	Updated	→
ISO 37301 Introduction	English	New!	→
ISO 37301 Foundation	Spanish	New!	→

Explore the Benefits of ISO/IEC 27002:2022

PECB Store always offers the latest published or updated Information Security and Business Continuity Standards, available for your purchase.

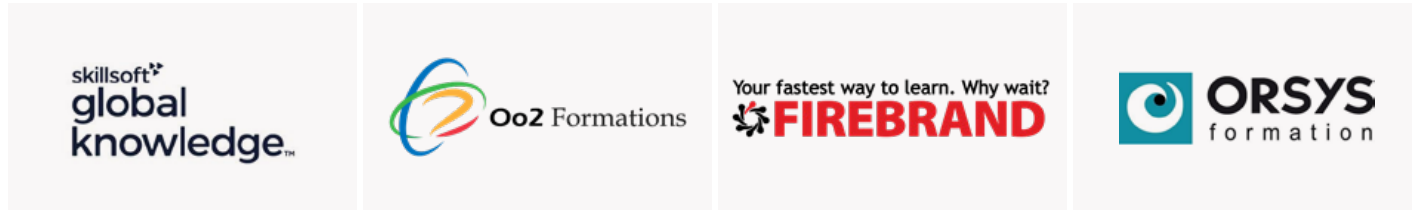
Invest in your future, starting with ISO/IEC 27002:2022, and understand security concepts, maintenance, management, and implementing an information security management system within your organization.



SHOP NOW! ►

SPECIAL T

TITANIUM



GOLD PA



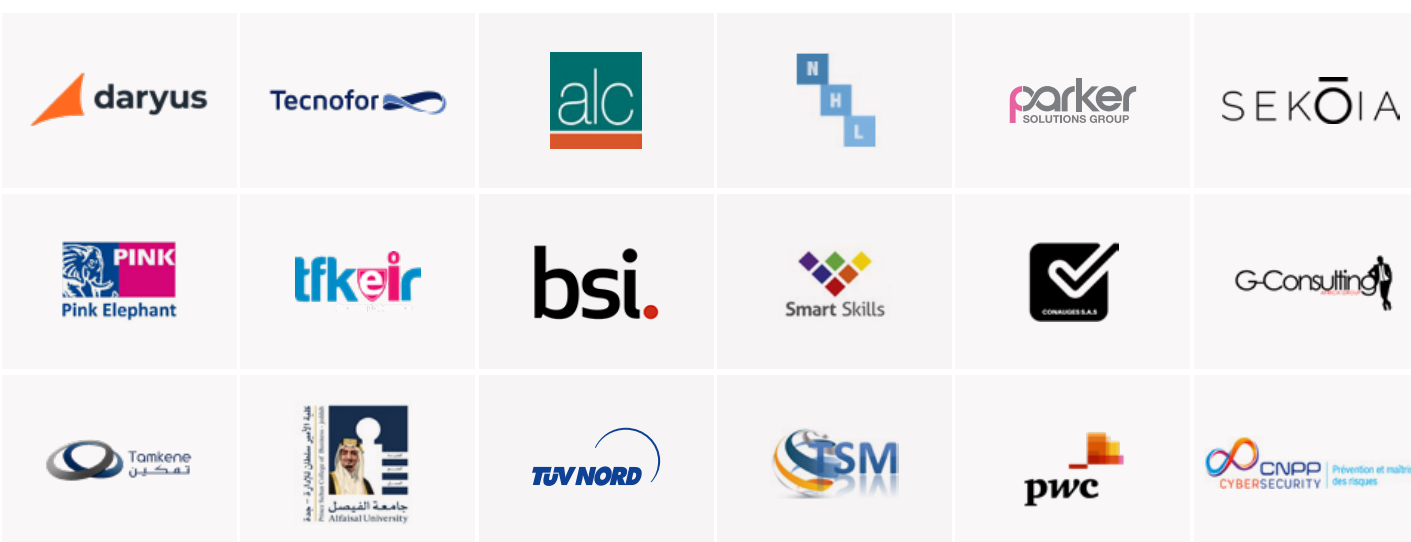
Note that PECB Partners are listed as per the credits

HANKS TO

PARTNERS



PARTNERS



ENHANCE YOUR ORGANIZATION'S PERFORMANCE

THROUGH INFORMATION SECURITY
AND BUSINESS CONTINUITY

