



PECB Insights Magazine

A Full Year of Insightful Articles

Let Us Take a Look at What 2022 Had to Offer

PECB Insights Magazines 2022

2022 has been a year full of collaborations, insights, and various discussed themes, such as CMMC, Information Security, Business Continuity, Crisis Management and Resilience, Network Security, Ethical Hacking, Cybersecurity, Data Privacy, as well as Digital Transformation.



January - February 2022

CMMC, IT Security, and Cybersecurity - In this issue of PECB Insights magazine, experts explained the impacts, changes, and expectations on these matters, such as the direction CMMC is headed in, the benefits of 5G and the potential cybersecurity risks, and much more.



March - April 2022

Information Security and Business Continuity - One thing that stays evident for the economy, is for organizations to remain running and unaffected. However, changes and disruptions are continuous so learning how to manage and face these challenges has become a necessity. To continue delivering high-quality products and services as organizations, we need to create systems of prevention and recovery to deal with potential threats.



May - June 2022

Crisis Management and Resilience - When the world was faced with the global crisis of a pandemic, organizations faced supply chain disruptions, continuous threats to operations, and new strains of the virus that devastated several industries. What lessons have you learned and how prepared is your organization for the years ahead? For more insights on these matters, read this edition of the magazine.



July – August 2022

Network Security, Ethical Hacking, and Cybersecurity – In recent years, organizations and individuals alike, have started realizing the importance of a safe space online, this has led to the need of ensuring safety as one of the main priorities for every organization. However, the increasing magnitude and sophistication of threats have made it very challenging and this realization has also led to fields such as; Cybersecurity, Network Security, and Ethical Hacking being on the rise.



September – October 2022

Data Privacy Laws, Standards, and Regulations – The constantly growing use of technological advances has led to a great amount of data circulating online, from daily life to organizational data, presenting a threat to unauthorized access or being targeted by malicious actors. For organizations, this has brought higher expectations from consumers to ensure that the entrusted data is handled responsibly. Learn more in this edition of the magazine.



November – December 2022

Digital Transformation – In a time where all processes are moving constantly towards digitalization, the importance of understanding the value of its implementation within an organization has become prominent, considering that all organizations share a common goal – bringing value and delivering significant services to customers. In this issue, we cover the most innovative topics on Digital Transformation, where experts in the field were able to share their insights on topics such as; AI and the Metaverse, IoT and Blockchain, Data Privacy in Digital Transformation, Cloud Security, IoT and Edge Computing, and much more.

Top Three Issues of 2022

PECB Insights

ISSUE 36

ISO STANDARDS AND BEYOND

JANUARY-FEBRUARY 2022

CMMC, IT SECURITY, AND CYBERSECURITY

WHAT TO EXPECT

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

CMMC, IT Security, and Cybersecurity

PECB Insights

ISSUE 38

ISO STANDARDS AND BEYOND

MAY-JUNE 2022

CRISIS MANAGEMENT AND RESILIENCE

INCREASED RESILIENCE FOR INCREASED
PERFORMANCE

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

Crisis Management and Resilience

PECB Insights

ISSUE 41

ISO STANDARDS AND BEYOND

NOVEMBER-DECEMBER 2022

DIGITAL TRANSFORMATION

ITS IMPORTANCE AND IMPACT
ON ORGANIZATIONS

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

Digital Transformation

Top Three Articles of 2022

OPINION

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

BY PETER GELLEN

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.

TECHNOLOGY

Security Considerations for 5G Technology Enablers

BY LUC SAMSON

In order to completely fulfill the business needs driving the development of 5G by the 3GPP standard organization, 5G uses and introduces technology enablers that transform 5G networks into cloud-based, programmable, software-driven, service-based, and holistically-managed infrastructures, utilizing enablers such as cloud technologies, Artificial Intelligence, open APIs, and Multi-access Edge Computing.

Although 3GPP standard specifications have increased the security of 5G relative to 4G, the use of those enablers, some of which are not in the scope of 3GPP, have introduced new security threats and vulnerabilities that cannot be addressed solely by the 3GPP security framework. With such a diversity of technology enablers composing the 5G solution eco-system, the overall 5G security framework looks fragmented.

This article presents the technology enablers introduced or used by 5G, with their respective security vulnerabilities. It also presents the contribution of key organizations, government, and industry groups that work on securing 5G enablers via security standards, vulnerability analysis, and best practice recommendations.

1.0 5G Business Drivers

Four generations of cellular technologies were all about connecting people, whereas 5G is about connecting people and everything else.

In line with this vision, the 5G business objectives are:

- **Enhancing Service Offerings** - relative to 4G with improved network performance, a wider range of types of devices supported, and more vertical segments being better served
- **Creating New Business Models** - beyond connectivity provider by fostering an open and agile ecosystem of partners and allowing customers to self-manage their services

➤ **Improving Operational Efficiency** - by shortening the time-to-market and time-to-customer of new services, by simplifying network operations, and reducing the cost of services

Taken together, those objectives will accelerate the digital transformation of digital economic sectors.

2.0 5G Enablers

This figure shows the dependency between the 5G business drivers and the 5G technology enablers.

TECHNOLOGY

Building An Effective Crisis Management Team

BY GEARY SIKICH

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

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

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

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

Security Considerations for 5G Technology Enablers

LEADERSHIP

Building An Effective Crisis Management Team

BY GEARY SIKICH

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

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

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

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

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

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

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

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

Your next biggest challenge:

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

Klein gives five reasons why Crisis Management Teams fail to react and begin to function in Crisis Mode.

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

Crisis Management Team (CMT)

```
graph TD; TC[Team Competencies TC] --> TM[Team Metacognition TM]; TI[Team Identity TI] --> TM; TC_I[Team Cognition TC-I] --> TM; TM --> TC; TM --> TI; TM --> TC_I;
```

Team Competencies (TC)
How good are the team's competencies and how they will engage with tasks presented?


Team Identity (TI)
Does everyone know who does what? Is everyone clear on their role? Is anyone from "management" in charge? Do they get on well for "them" and "the thing they're doing"?

Team Cognition (TC-I)
Is the CMT heading for the same goal? Does everyone know what the team's purpose is? Are they communicating in a consistent manner? Do they get on well for "themselves"?

Team Metacognition (TM)
Who's taking responsibility? Is everyone clear on their role? Is anyone from "management" in charge? Do they get on well for "them" and "the thing they're doing"?

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

Building An Effective Crisis Management Team



Thank you for your continuous support!
We look forward to what's ahead.

PECB Insights Magazine