PECB Magazine

ANNIVERSARY ISSUE

PECB Magazine Celebrates 50 Editions

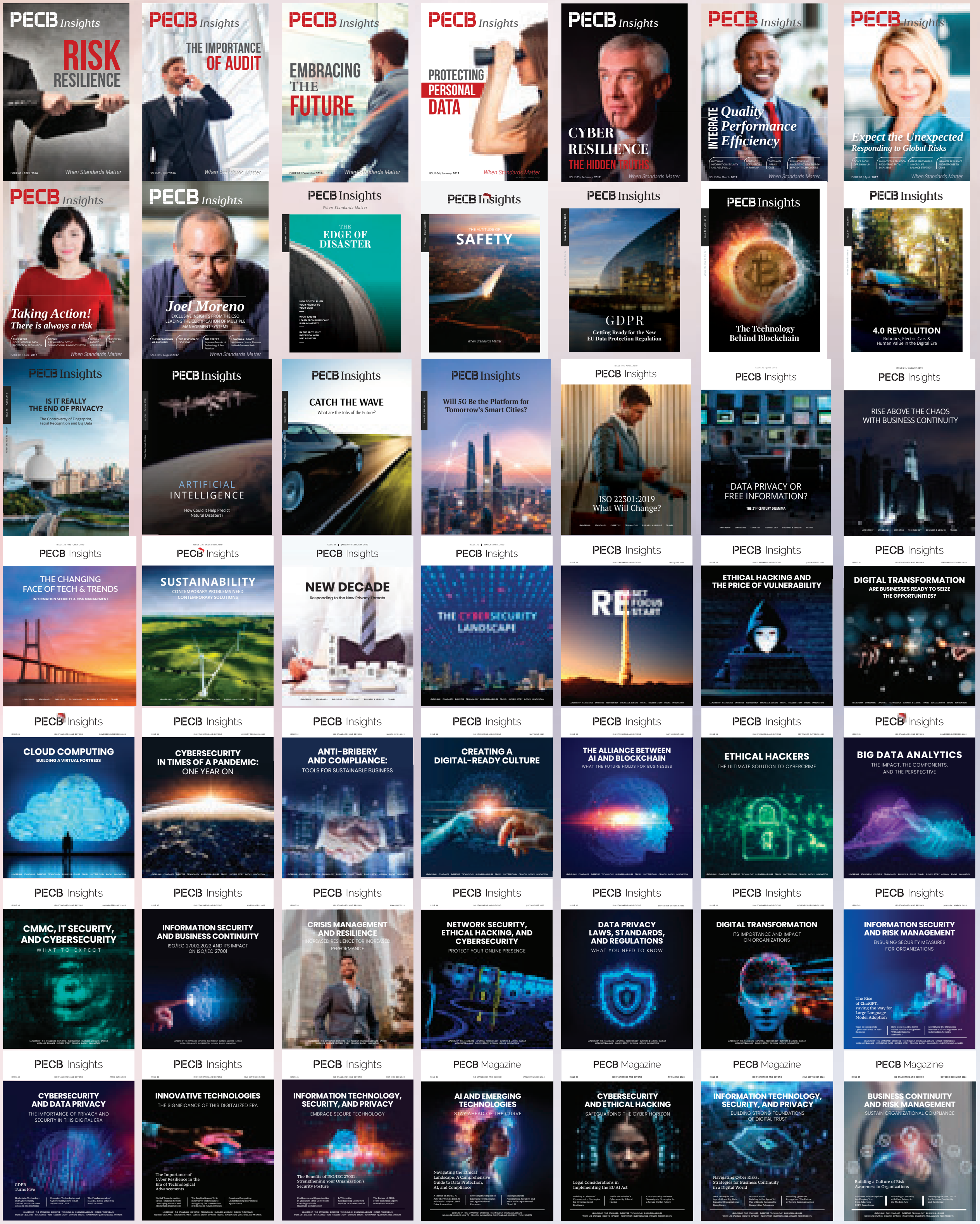
In 2016, PECB Magazine embarked on a mission to deliver cutting-edge insights into the world of standards, compliance, and technology.

Each edition has showcased thought leaders across diverse industries, covering a broad spectrum of topics, from cybersecurity and risk management to information security and digital transformation. This commitment to excellence has made PECB Magazine a trusted resource for professionals seeking to navigate the complexities of modern business environments.

The 50th edition marks a significant milestone, reflecting on the publication's journey while looking ahead to the future. This special issue celebrates the collective contributions of authors, industry pioneers, and readers who have shaped its success. It is a testament to the magazine's ongoing dedication to delivering high-quality content that informs, inspires, and empowers.

As PECB Magazine continues to evolve, its core mission remains unchanged: to be a beacon of knowledge and a catalyst for positive change. With each new edition, the magazine reaffirms its commitment to providing thought-provoking content that drives professional growth and industry advancement.

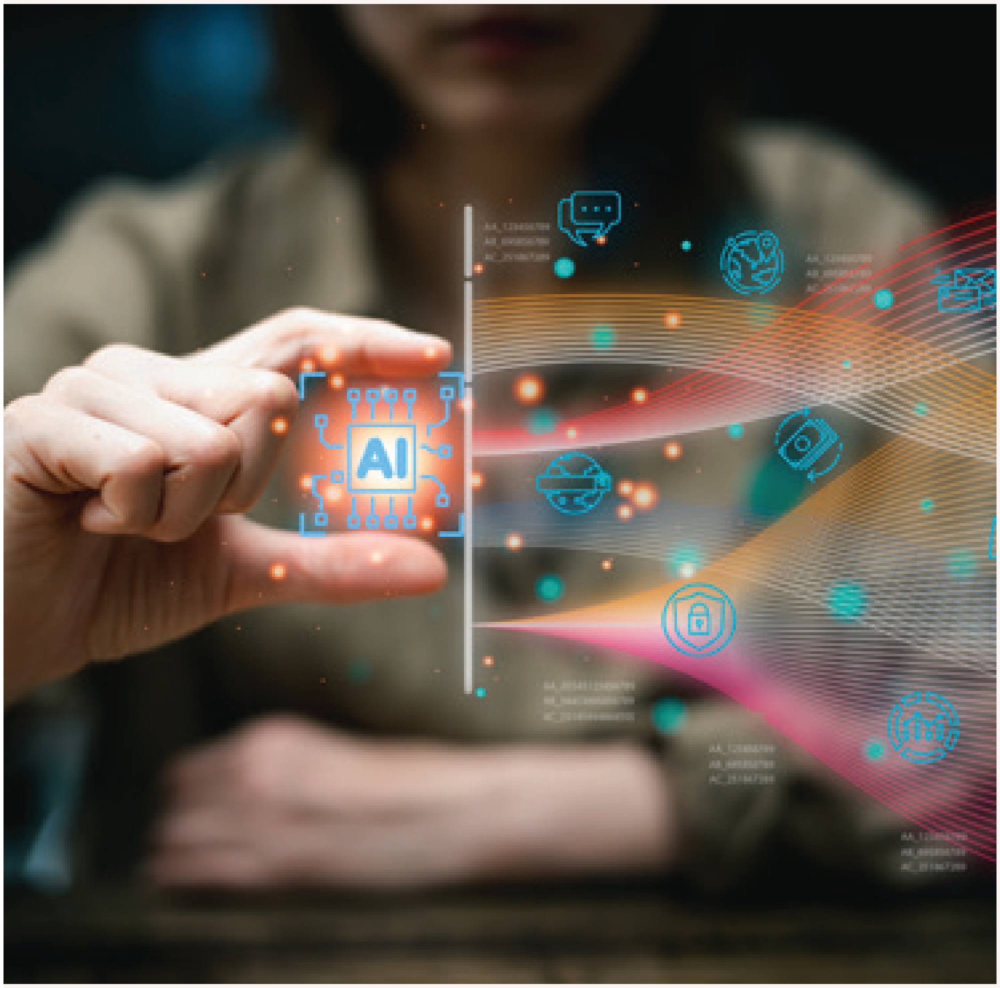
Here's to 50 editions—and many more to come.


PECB Insights
RISK RESILIENCE
When Standards Matter
THE IMPORTANCE OF AUDIT
EMBRACING THE FUTURE
PROTECTING PERSONAL DATA
CYBER RESILIENCE
THE HIDDEN TRUTHS
INTEGRATE Quality Performance Efficiency
Expect the Unexpected
Responding to Global Risks
Taking Action!
There is always a risk
Joel Moreno
THE EDGE OF DISASTER
THE ALTITUDE OF SAFETY
GDPR
Getting Ready for the New EU Data Protection Regulation
The Technology Behind Blockchain
4.0 REVOLUTION
Robotics, Electric Cars & Human Value in the Digital Era
IS IT REALLY THE END OF PRIVACY?
The Controversy of Fingerprint, Facial Recognition and Big Data
ARTIFICIAL INTELLIGENCE
How Could It Help Predict Natural Disasters?
CATCH THE WAVE
What are the Jobs of the Future?
Will 5G Be the Platform for Tomorrow's Smart Cities?
ISO 22301:2019
What Will Change?
DATA PRIVACY OR FREE INFORMATION?
THE 21ST CENTURY DILEMMA
RISE ABOVE THE CHAOS WITH BUSINESS CONTINUITY
THE CHANGING FACE OF TECH & TRENDS
INFORMATION SECURITY & RISK MANAGEMENT
SUSTAINABILITY
CONTEMPORARY PROBLEMS NEED CONTEMPORARY SOLUTIONS
NEW DECADE
Responding to the New Privacy Threats
THE CYBERSECURITY LANDSCAPE
RESET REFOCUS RESTART
ETHICAL HACKING AND THE PRICE OF VULNERABILITY
DIGITAL TRANSFORMATION
ARE BUSINESSES READY TO SEIZE THE OPPORTUNITIES?
CLOUD COMPUTING
BUILDING A VIRTUAL FORTRESS
CYBERSECURITY IN TIMES OF A PANDEMIC: ONE YEAR ON
ANTI-BRIBERY AND COMPLIANCE:
TOOLS FOR SUSTAINABLE BUSINESS
CREATING A DIGITAL-READY CULTURE
THE ALLIANCE BETWEEN AI AND BLOCKCHAIN
WHAT THE FUTURE HOLDS FOR BUSINESSES
ETHICAL HACKERS
THE ULTIMATE SOLUTION TO CYBERCRIME
BIG DATA ANALYTICS
THE IMPACT, THE COMPONENTS, AND THE PERSPECTIVE
CMMC, IT SECURITY, AND CYBERSECURITY
WHAT TO EXPECT
INFORMATION SECURITY AND BUSINESS CONTINUITY
ISO/IEC 27002:2022 AND ITS IMPACT ON ISO/IEC 27001
CRISIS MANAGEMENT AND RESILIENCE
INCREASED RESILIENCE FOR INCREASED PERFORMANCE
NETWORK SECURITY, ETHICAL HACKING, AND CYBERSECURITY
PROTECT YOUR ONLINE PRESENCE
DATA PRIVACY LAWS, STANDARDS, AND REGULATIONS
WHAT YOU NEED TO KNOW
DIGITAL TRANSFORMATION
ITS IMPORTANCE AND IMPACT ON ORGANIZATIONS
INFORMATION SECURITY AND RISK MANAGEMENT
ENSURING SECURITY MEASURES FOR ORGANIZATIONS
CYBERSECURITY AND DATA PRIVACY
THE IMPORTANCE OF PRIVACY AND SECURITY IN THIS DIGITAL ERA
INNOVATIVE TECHNOLOGIES
THE SIGNIFICANCE OF THIS DIGITALIZED ERA
INFORMATION TECHNOLOGY, SECURITY, AND PRIVACY
EMBRACE SECURE TECHNOLOGY
PECB Magazine
AI AND EMERGING TECHNOLOGIES
STAY AHEAD OF THE CURVE
CYBERSECURITY AND ETHICAL HACKING
SAFEGUARDING THE CYBER HORIZON
INFORMATION TECHNOLOGY, SECURITY, AND PRIVACY
BUILDING STRONG FOUNDATIONS OF DIGITAL TRUST
BUSINESS CONTINUITY AND RISK MANAGEMENT
SUSTAIN ORGANIZATIONAL COMPLIANCE

LEADERSHIP

The Intersection of AI and Cybersecurity: Governance and Risk Management in the Age of Intelligent Systems

Our human evolutionary path continues to merge phenomenally with artificial intelligence (AI).



As 2030 approaches, AI integration is expected to exceed well over 80% in all sectors, according to the World Economic Forum, highlighting the need to ensure that the risks associated with the development, deployment, and use of AI are well understood and managed responsibly for trustworthiness.

AI trustworthiness based on the ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology is highlighted as:

- Meet stakeholders' expectations
- AI robustness
- AI reliability
- AI resilience
- AI controllability
- AI explainability
- AI predictability
- AI transparency
- AI bias and fairness

These requirements emphasize the need for **good governance and risk awareness**, **risk management**, **continuous monitoring, and improvement** as integration becomes evident (transparently) through everyday human enhancements and activities, automation, functions, and processes. With the expansion of the business threat landscape due to digital transformation and the subsequent strengthening of cybersecurity to mitigate cyber risks, cybercriminals are utilizing the power of AI, creating and expanding further cyber risks through the enhancements of 1) vishing, phishing and social engineering campaigns, 2) specialized automated tools, and 3) tactics and techniques to attack, compromise and breach organizations.

Furthermore, cybercriminals' threat to AI operations is of critical importance since the development and deployment of AI are still largely ungoverned (due to competitive innovation at the state level) and operationally non-transparent to the operator or user.

Further to the World Economic Forum's Global Cybersecurity Outlook 2025 Report, 68% of organizations do not have processes to assess AI security before deployment. **This inadequate governing vulnerability can create emerging risks** that can negatively affect government institutions, organizations and their clients, stakeholders, and customers, thereby, creating public safety issues (in healthcare, power generation, supply chain, water and waste management, etc.), including unexpected circumstances and outcomes, whether political, economic, social, or cultural. Such societal risks at scale can become underlying national security issues if AI is not risk-assessed, monitored, and governed responsibly.

The global cost of cybercrime is expected to reach approximately U.S. $10.5 trillion in 2025 and U.S. $19.7 trillion by 2030. According to the World Economic Forum's Global Cybersecurity Outlook 2025 Report, the risk surrounding cybercrime with organized crime becomes a very concerning and critical matter.

For example, we have seen attacks on critical national infrastructures (CNI), such as healthcare, oil pipelines, and water management systems, resulting in public safety issues. These types of attacks are increasing public awareness and safety concerns surrounding CNI and its cybersecurity posture. The new face of cybercrime and its utilization of AI to achieve its criminal objectives has become a national security concern. Therefore, AI can become a national security risk if not responsibly governed, developed, deployed, and utilized.

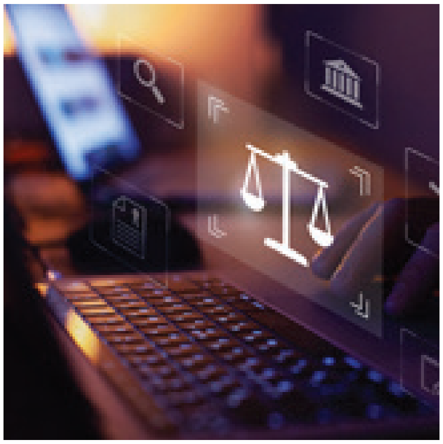
AI and Cybersecurity

The Tactics, Techniques, and Procedures (TTPs) of the highly structured and organized cybercriminal syndicate (criminal enterprise) are becoming more sophisticated and complex. With the use of generative AI, the efficacy of those TTPs is becoming more predominant, highly developed, and advanced, as seen through the sophistication of malware, deepfake audio, pictures and videos, vishing, social engineering, and phishing attacks. Some AI tools used by cybercriminals to commit cybercrime are:

- WormGPT
- FraudGPT
- GhostGPT
- Google Gemini
- HackerGPT

Understanding the necessity to defend against these advanced persistent threats (APTs), cyber defense strategies require AI-integrated cybersecurity tools to be highly efficacious and efficient in detecting and responding to these dangerous threats, which are highly sophisticated and complex, reducing the risks resulting from such attacks. That is, **fight criminal AI with good AI!**

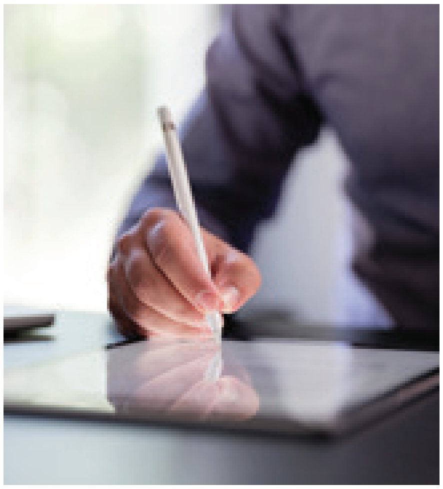
For the last seven years or so, we have seen companies such as Palo Alto Networks, Darktrace, CrowdStrike, and Check Point utilizing AI throughout their ecosystem of cybersecurity tools and services to remediate and mitigate cyber threats. Being one step ahead of cybercriminals is crucial in reducing cyber risks to the business that can cause public safety issues, digital liabilities, breaches, operational losses, etc. These are some of the varying business risks that affect the mission, board strategic direction and governance, and business well-being.



Not only is AI used in cybercrime and other organized criminal activities, but cybercriminals are attacking AI tools and services utilized by all business sectors. This poses the greatest threat to AI systems that lack adequate security controls, affecting their operations and trustworthiness. Threats to AI take on the following forms shown below (complete list on Mitre ATLAS):

- Machine Learning (ML) supply chain compromised
- Tampering (poisoning) of data used in AI training
- Attacks on the Large Language Models (LLM) (indirect prompt injection, jailbreaks)
- AI availability
- Access and exfiltration of confidential and private data utilized by AI

The evolution of AI combined with the competitive nature of getting to market first has seen grave risks to AI trustworthiness due to vulnerabilities in its development and deployment, which cybercriminals can exploit (Threat actors jailbreak DeepSeek, Qwen AI models to generate 'malicious' content: Report, 2025). Such exploitations create serious risks for all sectors, especially CNI, such as financial institutions, governments, education, healthcare, etc. For example, the exploitation of the generative AI DeepSeek highlights the risks associated with AI and its vulnerabilities.



Due to these high-level risks, as highlighted in the OECD "Framework for the Classification of AI Systems" report and the EU AI Act, risks surrounding AI must be governed and risk-managed well, thereby reducing risk to public safety, organizations, systems, democracies, etc.

> Managing risks surrounding AI requires governance and risk awareness, risk management, and continuous monitoring and improvement in the AI Management System (AIMS) program to uphold AI Principles, as noted in the OECD Framework for the Classification of AI Systems

- Inclusive growth, sustainable development, and well-being
- Human-centered values and fairness
- Transparency and explainability
- Robustness, security, and safety
- Accountability

Such an AI Management System (AIMS) program can be based on the auditable ISO/IEC 42001 standard.

- The ISO-standardized AIMS was created to:
- Reduce risks surrounding the development, deployment, and utilization of AI
- Enable the responsible and ethical use of AI
- Develop, deploy, and utilize AI in a trustworthy manner
- Develop, deploy, and utilize AI in the context of the organization, institution, etc.

Consequently, building a responsible and trustworthy AI System, as highlighted by the European Commission High-Level Expert Group on AI (AI HLEG) Ethics Guidelines for Trustworthy AI, will require thorough strategic support that a holistic standard, such as the ISO/IEC 42001 AIMS, can provide through guidelines and directions, including the ability to be internationally audited as a management system.

Managing Risk Surrounding AI

As highlighted in the previous paragraphs, the risks surrounding AI are critical as its evolution and integration continue to merge into intricate and non-transparent operations. Mediating risks to AI and mitigating AI risks in designing, deploying, and utilizing AI is crucial in creating a responsible and trustworthy AI system. Stating it differently, a risk-based approach to each phase of the AI lifecycle makes AI trustworthy. Organizations, governments, and non-governmental organizations implementing an AIMS based on the ISO/IEC 42001 standard will be able to achieve AI strategic goals through governance, risk management, and continuous monitoring and improvement of controls. The ISO/IEC 42001:2023 AIMS standard structure is as follows:

- Clause 4 – The Organizational Context
- Clause 5 – Leadership
- Clause 6 – Planning
- Clause 7 – Support
- Clause 8 – Operation
- Clause 9 – Performance Evaluation
- Clause 10 – Improvement

- Annex A (Normative) – Reference control objectives and controls
- Annex B (Normative) – Implementation guidance for AI controls
- Annex C (Informative) – Potential AI-related organizational objectives and risk sources
- Annex D (Informative) – Use of the AI Management system across domains and sectors

The following standards and regulatory frameworks surrounding AI Systems enrich the ISO/IEC 42001:2023 Information Technology — Artificial Intelligence — Management System Standard:

- ISO/IEC FDIS 42005 Information technology — Artificial intelligence — AI system impact assessment
- ISO/IEC FDIS 42006 Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems
- ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
- ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management
- ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- NIST Artificial Intelligence Risk Management Framework (AI RMF)
- EU AI Act

Governance

Tackling the risks surrounding AI must be governed and managed holistically, through:

Governmental national AI strategies, policies, laws, and regulations—OECD AI Principle—Recommendations for Policymakers—Principle 2.3

Corporations' adherence to policies in compliance with laws and regulations, in addition to boards supporting programs throughout the organization, enhances compliance further with policies, which can initiate necessary cultural changes.

Public-private partnership (PPP) collaboration to support innovation, expertise capacities, technology change and evolution awareness, and aid in the timely creation of fair legal frameworks—OECD AI Principle—Recommendations for Policymakers—Principle 2.5.

International partnerships to further collaborate and acquire additional expertise, allowing for comprehensive and fully documented activities and processes in creating global policy frameworks to responsibly develop, deploy, and use AI, upholding AI principles—OECD AI Principle—Recommendations for Policymakers—Principle 2.5.

The success of any program must be driven at the highest level, whether in government or an organization, to achieve its strategic objectives and cultural changes through mature development. Therefore, if the ISO/IEC 42001, Clause 5 directive for leadership is applied, leadership commitment to the AIMS, the establishment of AI policy, and support for human resources can be realized.

The implementation of governance committees with responsibility and accountability for the AIMS program will allow the development of AI risk-aware policies, supporting AI trustworthiness and responsible development, deployment, and utilization.

In addition to the general AI Policy (guided by the ISO/IEC 42001, Annex A/B.2.2 AI Policy statement guidance), the following sub-related policies will exist: AI ethics policy, data governance policy, privacy policy, AI human-resources policy, AI transparency policy, responsible AI deployment policy, etc. Governance committees understanding the factors that can impact AI trustworthiness through the ISO/IEC TR 24028:2020 technical report will be better equipped to develop, implement, and operate AI governance structures and systems based on the ISO/IEC 38507:2024 standard. Moreover, this enhanced AI governance through leadership and being directed by the ISO/IEC 42001 Clauses 4 – 10 will support the structures and mechanisms to achieve AI trustworthiness and responsible use.

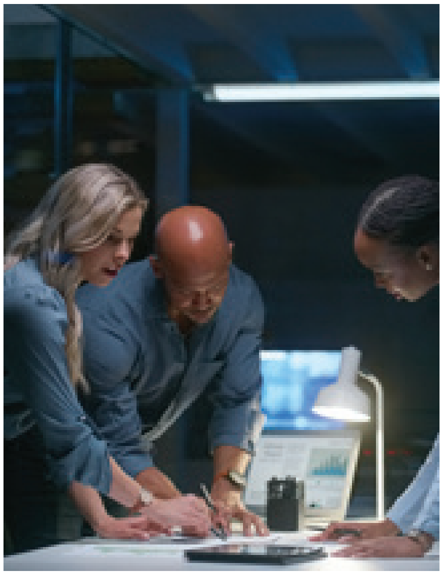
Risk Management

Creating trustworthy AI systems implies having the correct risk-based controls to uphold AI principles in developing, deploying, and using AI. Implementing the risk management activities and processes as directed by ISO/IEC 38507:2024, clause 6.7.2, and undertaken by the ISO/IEC 23894:2023 risk management guidance will determine the documented controls needed—an activity driven by ISO/IEC 42001, clause 6.1.

For governments and organizations wanting to use the NIST AI Risk Management Framework 1.0 (NIST AI RMF 1.0), please see:

- Crosswalk AI RMF (1.0) and ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management
- (NIST AI Risk Management Framework to ISO/IEC-42001 Crosswalk, n.d.)

The AI Systems Impact Assessment, as specified in ISO/IEC 42001, clause 6.1.4, starts the process of assessing the impact of AI systems in their development, deployment, and utilization on people, organizations, and ecosystems (NIST AI RMF 1.0).



Once completed, the ISO/IEC 23894:2023 risk management approach, which models the ISO/IEC 31000:2018 risk management framework, customized for AI systems risk management, is undertaken to treat the risks surrounding AI as highlighted in Table 1.

The Statement of Applicability, identified in ISO/IEC 42001, clause 3.26, and required by clause 6.1.3 for AI risk treatment, is the controls justification accounting document for auditing. It demonstrates the organization's due diligence in creating and deploying a responsible and trustworthy AI system that will uphold public safety, organization, and ecosystem security and potentially seek ISO/IEC 42001:2023 certification.

‣ Accountability ‣ AI Expertise ‣ Availability and quality of training and test data ‣ Environmental impact ‣ Fairness	‣ Maintainability ‣ Privacy ‣ Robustness ‣ Safety ‣ Security ‣ Transparency and explainability

Table 1: Organizational Objectives and Risk Sources

By understanding the potential AI-related organizational objectives and risk sources described in the ISO/IEC 42001, Annex C (Informative), shown in Table 1, government policymakers and organizations' risk managers can directly address the objectives to create a responsible and trustworthy AI system. Once the risks have been identified, assessed, and evaluated, it is time for risk treatment. This involves determining possible controls, as highlighted in Table 2, to treat the risks identified in the risk management activities, guided by the ISO/IEC 23894:2023 standard or the NIST AI RMF.

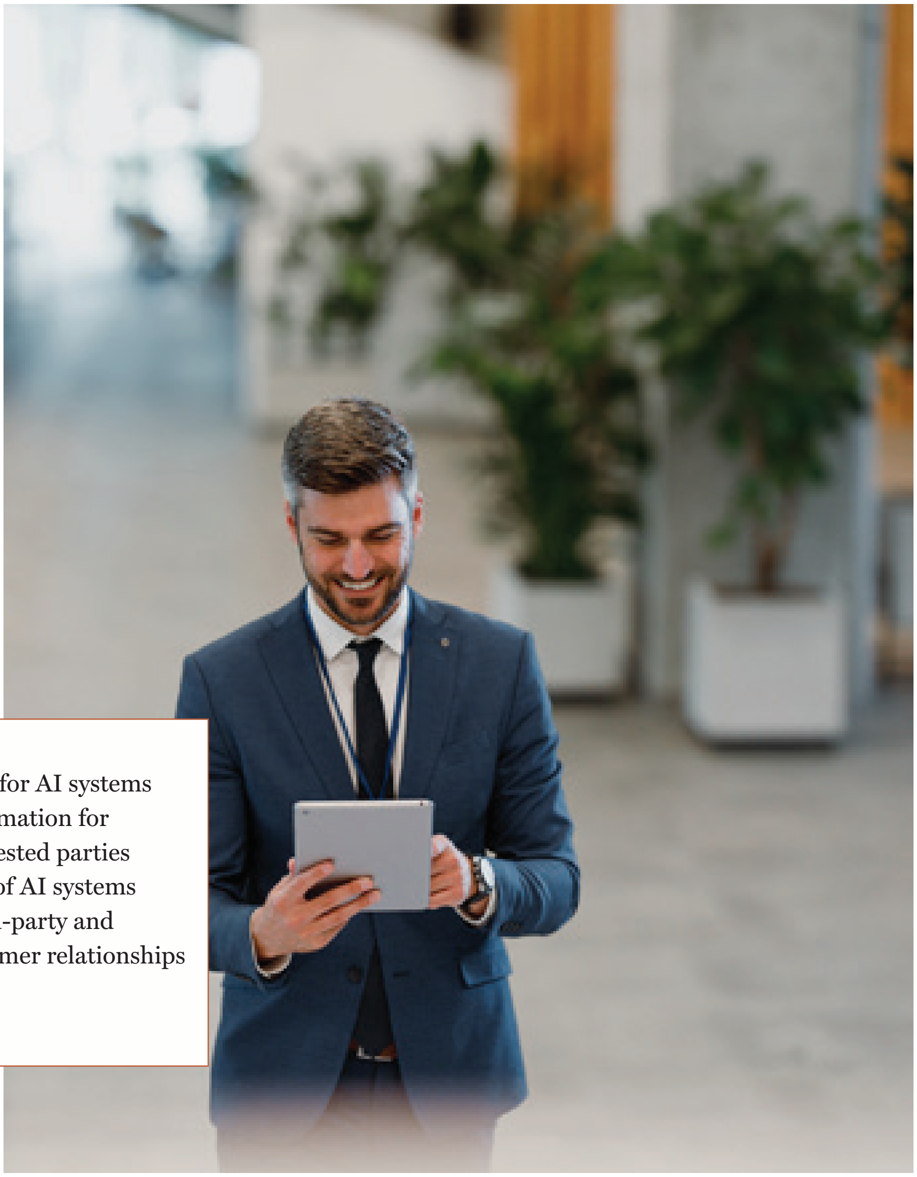
‣ Policies Related to AI ‣ Internal organization ‣ Resources for AI Systems ‣ Assessing impacts of AI systems ‣ AI system life cycle	‣ Data for AI systems ‣ Information for Interested parties ‣ Use of AI systems ‣ Third-party and customer relationships

Table 2

Continuous Monitoring and Improvement

Once the controls are implemented, continuous monitoring is needed to determine the efficacy and efficiency of the AI system's controls for its trustworthiness. Risk communication and consulting, recording and reporting, and monitoring and reviewing are all crucial activities and processes of the AI Risk Management Framework in creating a trustworthy and responsible AI system.

These activities and processes continually improve the risk management program and continue throughout the ISO/IEC 42001:2023 AIMS program lifecycle through clauses 7 – 10.



Conclusion

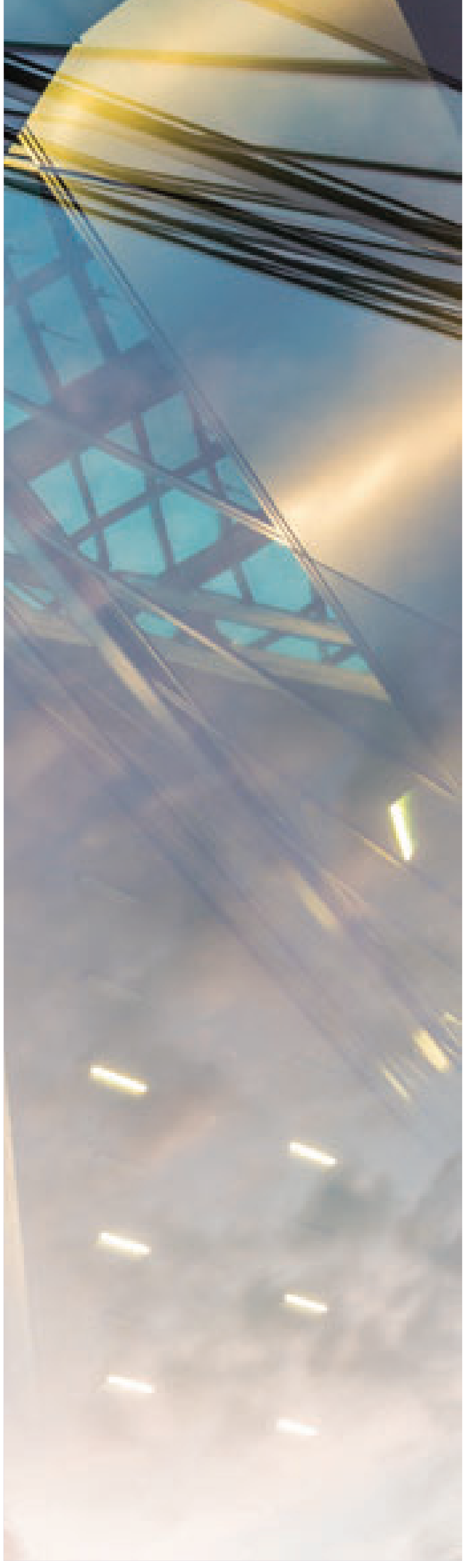
AI integration in our everyday lives, ecosystems, and organizations will continue to persist, and as such, we must develop, deploy, and use AI responsibly. The risk to people, organizations, and ecosystems is too significant to ignore AI risks. In other words, **AI must be trustworthy!**

Additionally, the threat of cybercrime against AI, exploiting its vulnerabilities and using it to attack CNI, is a national security concern. We must take a strategic approach to managing AI Risks by instituting international frameworks and standards like the NIST AI RMF and the ISO/IEC 42001:2023 standard to create, protect, and preserve trustworthy AI systems.

Finally, cybersecurity businesses developing AI-driven cybersecurity defense tools must understand the risks surrounding AI and create highly efficient and practical tools to fight adversary AI-driven attacks that can cause substantial operational and financial losses to governments and businesses, public safety issues, and risks to democracies.

Edward Millington

BSc, CISO, SOC 2, CCCF, CISSP,
ISO, ISSA, MCIIS, MIET



Principal Security Consultant, is the Founder and Managing Director of CariSec Global Inc., a company at the forefront of Next-Generation Managed Security Service Providers, providing Risk-Integrated Cybersecurity and ICT-managed strategic services in varying sectors: financial, government, health, manufacturing, private, retail, and energy and utilities.

Mr Millington's leadership is a cornerstone of his success. With a wealth of experience spanning close to three (3) decades in the fields of information systems security, information and communications technology, and telecommunications, he has successfully guided numerous organisations to achieve their strategic goals and objectives. His exceptional approach to strategic planning, design, and solutions direction, leveraging his unparalleled expertise and innovation in varying specialised areas like governance, risk and compliance, instils confidence in his ability to lead, guide and advise.

He holds a Bachelor of Science Degree in Electronics and is a member of The Institute of Engineering and Technology (IET). He is a Certified Information Security Professional (CISSP), a PECB Certified – Chief Information Security Officer, Senior Lead SOC 2 Analyst, ISO/IEC 27005 Information Security Senior Lead Risk Manager, ISO/IEC 27035 Information Security Senior Lead Incident Manager, ISO/IEC 42001 AI Management System Senior Lead Implementer – and is a full member of the Royal Chartered Institute of Information Security (CIISec) and a candidate assessor and interviewer; a Professional Evaluation and Certification Board (PECB) Trainer; a member of the PECB Focus 15 group; a Commonwealth Caribbean Cyber Fellow and Co-Chair; an EU CyberNet Expert Pool Member; and a member of the International Information Systems Security Association (ISSA).

Mr Millington's expertise is not only extensive but also globally recognised. He has been featured in several security magazines and has spoken at multiple global and regional conferences. His insights are also regularly shared in newspaper articles and on television, focusing on cyber and information security risk, cyber resilience, and enterprise risk management. His advocacy communications centre on integrating cyber risks into the overall organisation's risk management program, a testament to his global influence in the field.

SPECIAL T

TITANIUM

EduGroupe Accompagner pour réussir

FIREBRAND

orsys FORMATION

SMATICA Training & Consulting

KOENIG step forward

ib cegos

schellman Quality, above all.

Igp Innovación Gestión Buenas Prácticas

PLATINUM

DAR AL-HEKMA UNIVERSITY

CYNTHUS THE EXCELLENCE EFFECT

TSTC ICT en Security Trainingen

safeshield

Senti

KRUCEK

SGS

PINK

skillsoft global knowledge. SAUDI ARABIA

E-WORK

1st CAR

SPARTAN

FEDERATED MANAGEMENT INSTITUTE

DS DANSK STANDARD

DATASEC 10

CRMS

RESTREP

GOLD PA

protiviti

aac aswar akka consultancy

READYNEZ IT's easy when you're Ready

ACG Cybersecurity

IBEFORO PRIVATE LIMITED

de-dsb

consultIT

BS.

QPLUS

smart-TEC

parker SOLUTIONS GROUP

alc TRAINING

LGMS

GRVA TECH

CS CONSULTING

L3RN

inlexso INNOVATIVE LEGAL SOLUTIONS

Tecnofor by DIGULAR

CoesCR

KPMG GHANA

devforma

plb

MAXPERT

mobiliza ACADEMY

INTI.Q SOLUTIONS

Elfash

QMC since 2002

NCS Security Solutions

Note that PECB Partners are listed as per the credentials

HANKS TO

PARTNERS

- A
- Oo2 Formations & Consulting
- glasspaper
- m2i Formation
- Digital Jewels Africa
- art Skills
- skillsoft global knowledge FRANCE
- Digital Encode
- ABILENE ACADEMY
- sustain

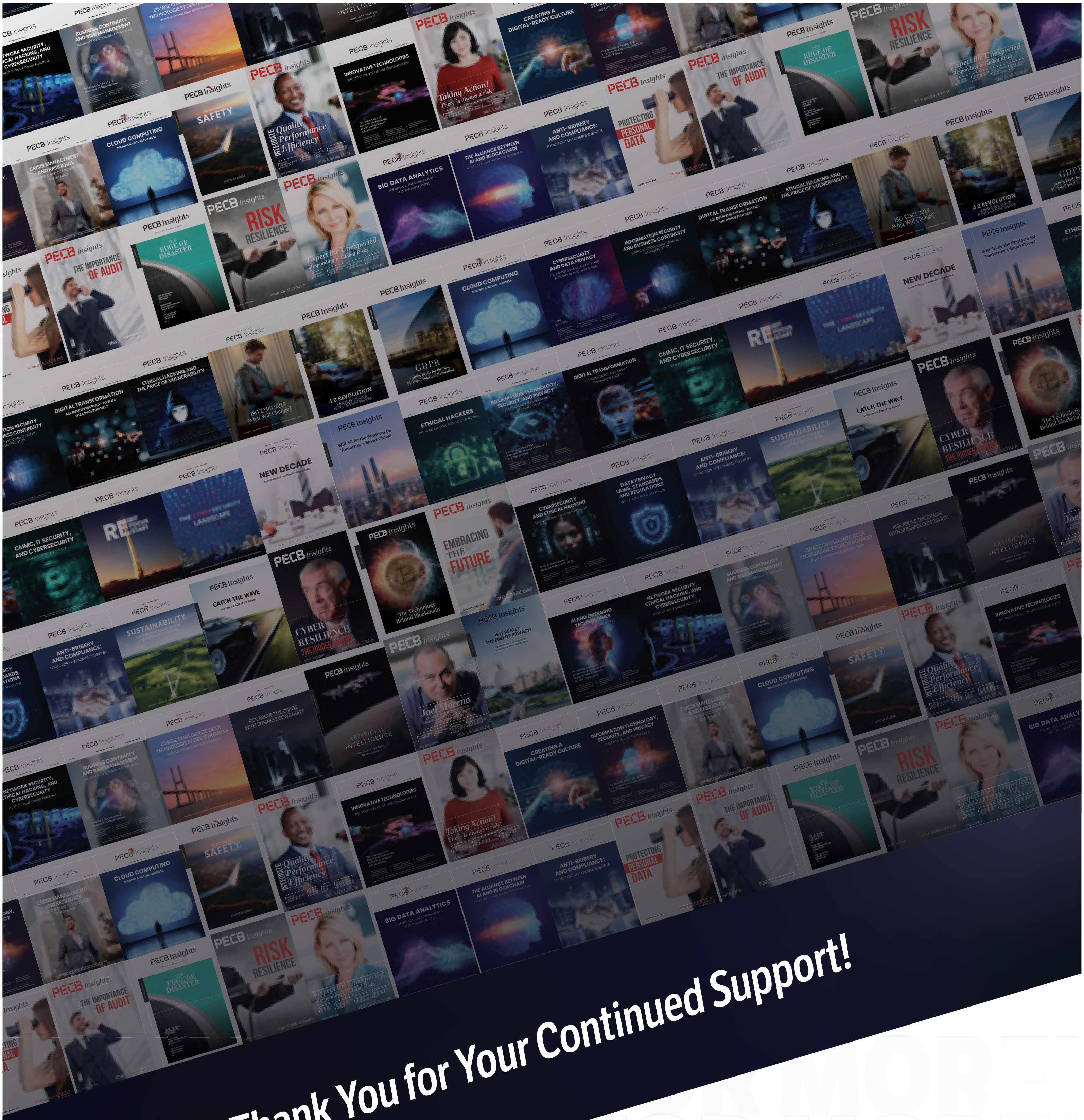
PARTNERS

- nel Africa
- Deloitte. NIGERIA
- skillsoft global knowledge NETHERLANDS
- CERTyou
- NEOSECURE
- CYBER MINUTE
- REER
- pwc
- BDO
- CYBERSTRAT
- RISKPROFS
- EGYBYTE Inspiring Minds
- RAMAS
- BIT
- iCERTWORKS TRAINING & CERTIFICATION
- New Horizons
- CAA Crest Advisory Africa
- MKUTANO TRAINING SOLUTION

ARTNERS

- Bureau of Standards Jamaica
- Behaviour Brasil
- analytix
- Acute
- devUp
- digicomp
- INTELLIGENT security
- Tenol Alpha
- KPMG NORWAY
- INFOTEC
- eimf
- formind
- Training Heights
- LAM
- LUMIFY work
- msdd.neT
- BDO Chapelle
- JK MANAGEMENT
- Linqs
- GREAT LEARNING
- KMC
- bsi.
- CIRECOM
- Deloitte. FRANCE
- CSB .school
- RiskOff
- IDESP
- InfoAssure Limited.
- global Success Systems

acquired from January 1, 2024, to December 31, 2024.


PECB Insights
PECB Magazine
RISK RESILIENCE
Expect the Unexpected
THE IMPORTANCE OF AUDIT
EDGE OF DISASTER
PROTECTING PERSONAL DATA
Taking Action! There is always a risk
INTEGRATE Quality Performance Efficiency
SAFETY
CLOUD COMPUTING
CRISIS MANAGEMENT AND RESILIENCE
BIG DATA ANALYTICS
THE ALLIANCE BETWEEN AI AND BLOCKCHAIN
ANTI-BRIBERY AND COMPLIANCE
CREATING A DIGITAL-READY CULTURE
INNOVATIVE TECHNOLOGIES
NETWORK SECURITY, ETHICAL HACKING, AND CYBERSECURITY
BUSINESS CONTINUITY AND RISK MANAGEMENT
DIGITAL TRANSFORMATION
ETHICAL HACKING AND THE PRICE OF VULNERABILITY
ISO 22301:2019 What Will Change?
4.0 REVOLUTION
GDPR
NEW DECADE
CMMC, IT SECURITY, AND CYBERSECURITY
CATCH THE WAVE
SUSTAINABILITY
CYBER RESILIENCE
EMBRACING THE FUTURE
The Technology Behind Blockchain
ETHICAL HACKERS
DATA PRIVACY LAWS, STANDARDS, AND REGULATIONS
CYBERSECURITY AND ETHICAL HACKING
ARTIFICIAL INTELLIGENCE
RISE ABOVE THE CHAOS WITH BUSINESS CONTINUITY
Joel Moreno
IS IT REALLY THE END OF PRIVACY?
AI AND EMERGING TECHNOLOGIES
INFORMATION TECHNOLOGY, SECURITY, AND PRIVACY
CYBERSECURITY AND DATA PRIVACY
INFORMATION SECURITY AND BUSINESS CONTINUITY
Will 5G Be the Platform for Tomorrow's Smart Cities?
L'IMAGE CHANGEANTE DE LA TECHNOLOGIE ET DES TENDANCES

Thank You for Your Continued Support!

STAY TUNED FOR MORE!