PECB Magazine

ISSUE 48 ISO STANDARDS AND BEYOND JULY-SEPTEMBER 2024

INFORMATION TECHNOLOGY, SECURITY, AND PRIVACY

BUILDING STRONG FOUNDATIONS OF DIGITAL TRUST

Navigating Cyber Risks: Strategies for Business Continuity in a Digital World

Data Privacy in the Age of AI and Big Data: Ensuring Organizational Compliance

Personal Brand Building in the Age of AI: The Ultimate Sustainable Competitive Advantage

Decoding Quantum Encryption: The Future of Secure Communication

LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISURE
WORK-LIFE BALANCE HOW TO OPINION INNOVATION QUESTIONS AND ANSWERS TECH PROJECTS

PECB Magazine

Check out the previous edition

Issue
47
PECB Magazine
ISO STANDARDS AND BEYOND
APRIL-JUNE 2024
CYBERSECURITY AND ETHICAL HACKING
SAFEGUARDING THE CYBER HORIZON
Legal Considerations in Implementing the EU AI Act
Building a Culture of Cybersecurity: Strategies for Organizational Resilience
Inside the Mind of a Cybersecurity Ethical Hacker
Cloud Security Sovereignty: S a Secure Digita
LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISU
WORK-LIFE BALANCE HOW TO OPINION INNOVATION QUESTIONS AND ANSWERS

Subscribe & find out more at

www.insights.pecb.com

The Emerging Risk Artificial Intelligence

BY EDWARD MILLINGTON

The capitalization of business opportunities and securing markets imply agile creativity and innovation. It involves meeting and exceeding stakeholders' expectations, delivering products and services on time, and enhancing partners, clients, and customers' experience. By utilizing emerging technologies like artificial intelligence (AI), organizations can rapidly achieve their mission and strategic goals, enabling them to navigate an expanding and evolving business landscape in a diverse and efficient manner. In fact, according to McKinsey's research, 70% of organizations are projected to use AI in some capacity by 2030.

Emerging Risk

While the goal for any organization is to be profitable, gain greater market share, and exceed stakeholders' expectations, developing, deploying, and utilizing AI in the organization is increasingly becoming a key strategy to attain these strategic business objectives. However, this also creates many (emerging) challenges that must be addressed.

Therefore, organizations must gain a comprehensive understanding of the emerging risks associated with AI. These risks, which can lead to digital liabilities and other business risks, including data privacy losses, intellectual property losses, potential breaches of data protection laws, and the potential to impact human social and cultural norms, must be fully understood. However, with a thorough understanding of these emerging risks, organizations can navigate the use of AI in a responsible and informed manner, ensuring they are prepared for the future.

The ISO/TC 262 Technical Committee on “ISO 31050 – Guidance for managing emerging risks to enhance resilience” defines emerging risks as those risks that are characterized by their newness, insufficient data, and a lack of verifiable information and knowledge needed for decision-making related to them.

These risks can pose the most significant challenges to resilience, safety, and operational and business continuity

Emerging risk has three types of categorization (internal, strategic, and external), as suggested by the International Risk Governance Council (IRGC).

- High uncertainty and a lack of knowledge about potential impacts and interactions with risk-absorbing systems.

- Increasing complexity, emerging interactions, and systemic dependencies that can lead to non-linear impacts and surprises.
- Changes in context (for example, social and behavioral trends, organizational settings, regulations, and natural environments) that may alter the nature, probability, and magnitude of expected impacts.

AI, a data-driven system, must have the following essential certifiable principles throughout its lifecycle:

- Fairness
- Trustworthiness
- Transparency
- Accountability
- Responsibility
- Reliability and Safety
- Privacy and Security
- Ethical Value
- Human Control
- Shared Benefit

Therefore, **AI risks can encompass all three categories of emerging risk throughout its lifecycle**, thus, emphasizing the importance of proactive emerging risk governance.

Artificial Intelligence Management System (AIMS)

Operating, monitoring, and continually improving AI to meet these general principles throughout its lifecycle requires a strategic approach to AI governance, risk, and compliance. This will allow the organization to effectively and efficiently utilize the emerging technology within its context, safely and responsibly. Implementing and operating a Management System will allow an organization to achieve this strategic objective.

> **A management system is a set of interrelated or interacting elements of an organization that establish policies and objectives, as well as processes to achieve those objectives.**

To uphold AI principles and ensure responsible development, deployment, and use of AI, an Artificial Intelligence Management System (AIMS) should be implemented based on the ISO/IEC 42001 standard.

The international standard outlines the requirements for creating, implementing, maintaining, and continuously improving an AI Management System tailored to the organization's context. It is the only international standard that provides a comprehensive approach to AIMS implementation, auditing, and certification. Therefore, the standard provides the following benefits to organizations developing, deploying, and utilizing AI:

- Accountability and Responsibility
- Improved Decision-Making
- Continuous Learning
- Commitment to Trustworthiness

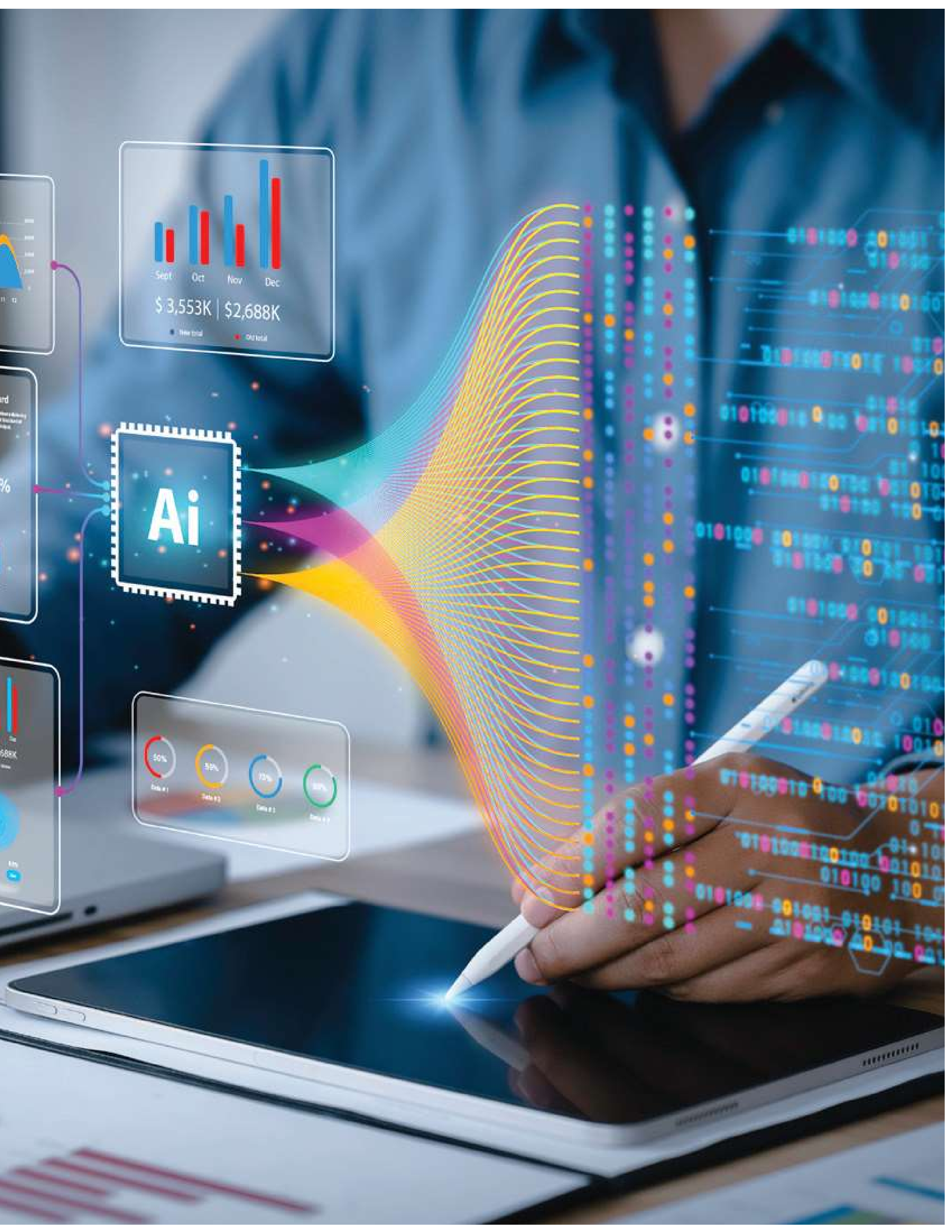
The AIMS, by design, provides an integrated approach to managing AI projects throughout their lifecycles. This is achieved through the involvement of top-level executive and their support, AI policy development, AI risk management, selection and design of controls, implementation of controls, management of documented information, communication, competence and awareness, management of AI operations, monitoring, measurement, analysis, and evaluation, internal audit, management review, treatment of non-conformities, and continual improvement - to name a few of the activities involved.

The ISO/IEC 42001 structure surrounds:

- 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

AI Governance

Managing emerging risks resulting from using AI is crucial for any organization’s well-being and limiting potential risk exposure. The inability to maintain and demonstrate AI principles throughout its lifecycle can create risk for all stakeholders, exposing the organization to unknown risks.


Sept
Oct
Nov
Dec
$ 3,553K | $2,688K
New total
Old total
Ai
50%
59%
73%
Data # 1
Data # 2
Data # 3
Data # 4

Risk management can become challenging if risk governance is not flexible and adaptable. Therefore, the realization of AI governance necessitates that organizational risk management of AI-enabled emerging technologies is effective and efficient, whether in development, deployment, or utilization. Compliance with the ISO/IEC 42001 AIMS standard implies that all clauses (4-10) activities and processes foster good AI governance at the international level, thereby, demonstrating the organization's responsibility for the safe use and development of AI in achieving its strategic goals and objectives.

Organizations implementing an AIMS based on the ISO/IEC 42001 standard will, by default, utilize the ISO/IEC 38507:2022 Information Technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations – helping them adapt their overall governance and policies for using AI.

The standard helps governance committees, boards, CEOs, varying executives, stakeholders, and interested parties with the structural guidance on defining responsibility and assigning accountability to using or developing AI. In addition, it provides risk awareness of the implications of data and data governance through the AI system lifecycle. It also shows how an effective AI governance framework can offer valuable insights and a higher return on investment.

Finally, the AI policy resulting from the actions and activities of the governance board should be guided by the ISO/IEC 42001 Annex B.2.2 AI Policy statement guidance. Finalizing all of the AI governance activities and processes is the Statement of Applicability (SoA).

The SoA, as highlighted by the ISO/IEC 42001, clause 3.26 Statement of Applicability, is a documented statement listing the controls that are relevant and applicable to the AIMS. It contains the justification for the inclusion and exclusion of Annex A controls and is the key document external auditors review and analyze during the certification audit process. The SoA document must have management validation and approval before initiating the AIMS operations.

AI Risks

There are four risk categories in which an AI system can be classified according to the EU AI Act. There are; unacceptable-risk AI systems, high-risk AI systems, low-risk AI systems, and minimal-risk AI systems.

The EU AI Act requires high-risk systems providers to manage the AI system's lifecycle thoroughly, ensuring safety and good governance, upholding AI principles, and meeting regulatory compliance concerning AI in its development, deployment, and utilization.

For organizations to specifically risk-manage AI risks, the ISO/IEC 42001-based AIMS recommends utilizing the ISO/IEC 23894:2023 Information Technology – Artificial Intelligence Guidance on risk management standard to efficiently and effectively address AI risk. The new standard adapts and develops the guidelines and general principles of risk management defined in ISO 31000:2018, which aids organizations of any size or sector to comprehensively understand risk in its entirety, develop strategic decision-making processes, provide operational excellence through risk awareness while developing proactive approaches to managing risks and building stakeholder confidence.

Organizations using the ISO/IEC 23894 standard to manage AI risks will develop, deploy, and safely utilize AI technology – upholding all AI principles while meeting the organization's contextual strategic goals and values.

The standard, through its Annex C, provides a non-exhaustive list of organizational objectives and risk sources that can be considered in the risk management process. It guides the organization in strategically managing AI risks, aligning it with organizational core values and compliance with laws, regulations, and industry standards. The following are some of the objectives that can be considered:

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

AI Controls

Once AI risks are understood in the context of the organization and the comprehensive analysis of the organization's AI landscape (understanding AI applications, assessing data usage and flow, and evaluating AI integration) has been carried out, organizations can use

Annex A of ISO/IEC 42001, which includes reference control objectives and controls to manage AI risk and achieve business objectives. Some examples of controls can be:

- AI policy
- AI roles and responsibilities
- Report of concerns
- Data resources
- Tooling resources
- AI systems impact the assessment process
- Objectives for responsible development of AI system
- AI system verification and validation
- AI System operation and monitoring

Conclusion

Organizations seeking to manage AI emerging risks should utilize the ISO/IEC 42001 AIMS standard. It is a comprehensive, certifiable standard referencing many international ISO standards in its implementation and operations to reduce AI risks and enhance AI governance.

The standard allows organizations the ability to explore and exploit opportunities associated with AI while reducing business risks, building innovative reputations, and exceeding stakeholders', clients', and customers' expectations.

Standards and Frameworks to note when discussing emerging risks:

- ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system
- ISO/TS 31050:2023 Risk management — Guidelines for managing an emerging risk to enhance resilience
- 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)
- ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO 31000:2018 Risk management — Guidelines
- NIST Artificial Intelligence Risk Management Framework

Edward Millington
Founder and Managing Director of CariSec Global Inc.

Edward (BSc, CISO, CISSP, ISO/IEC 27005, ISSA, MCIIS, MIET), a Chief Information Security Officer, a Principal Security Consultant, and an ISO/IEC 27005 Information Security Senior Lead Risk Manager and an ISO/IEC 42001 AI Management System Senior Lead Implementer, is the Founder and Managing Director of CariSec Global Inc., a company standing at the forefront of Next-Generation Managed Service Providers, offering Risk-Integrated Cybersecurity and ICT Managed Strategic Services in varying sectors: financial, government, health, manufacturing, private, retail, and energy and utilities.

Edward's leadership is a cornerstone of his success. With a wealth of experience spanning close to three decades in the fields of information systems security, information and communications technology, and telecommunications, he has successfully guided numerous organizations 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 specialized areas like governance, risk, and compliance, instills confidence in his ability to lead, guide, and advice.

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 and is a full member of the Royal Chartered Institute of Information Security (CIISec) and a candidate assessor; a Professional Evaluation and Certification Board (PECB) Trainer; a member of the PECB Focus 15 group; an EU CyberNet Expert Pool Member; and a member of the International Information Systems Security Association (ISSA).

Edward's expertise is not only extensive but also globally recognized. He has been featured in several security magazines and has spoken at multiple global and regional conferences.