PECB Magazine

JULY - SEPTEMBER
2025

ISSUE 52

Information Technology, Security, and Privacy

Prepare for the Future of Tech

Translating Frameworks into Impact: Turning ISO, NIST, and SOC 2 into Actionable Business Outcomes

Strengthening Data Foundations for the Future of AI

Blockchain for Privacy: Beyond Cryptocurrency into Verified Consent

From Model to Market: The Role of Trust in AI Product Development

ISO STANDARDS AND BEYOND

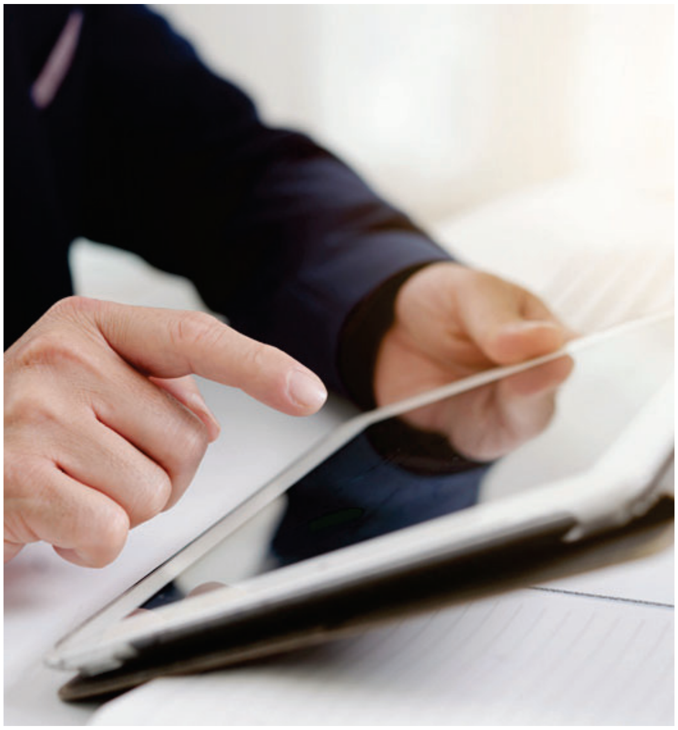
Translating Frameworks into Impact: Turning ISO, NIST, and SOC 2 into Actionable Business Outcomes

The business digital landscape continues to be shaped by digital transformation, where technologies such as Artificial Intelligence (AI), Cloud Computing, Big Data and Data Analytics, Blockchain, Internet of Things (IoT), 5G, and emerging digital infrastructures constantly transform how companies manage, operate, and deliver products and services.

These advancements aim to improve efficiency and profitability, build trust among investors and stakeholders, and enhance the overall customer experience.

However, the digital threat landscape for businesses also expands, bringing numerous **digital risks**, including emerging ones that can threaten the vision and mission of organizations. Such risks can be unacceptable in highly competitive markets and environments, potentially leading to operational losses that impact vendors, the public, and, in some cases, public safety.

Therefore, as global regulatory and legal requirements evolve and expand to protect national security, investors' and stakeholders' well-being, and including customer trust, the reality of compliance risk for companies grows, even becoming an emerging risk as they operate within their sector or industry, across international borders, and in cross-border contexts.



Compliance: Enforcing Good Governance

Regulations and legislation are two significant components that can be tedious for companies, regardless of the sector or industry in which they operate. However, due to digital risks to national security and the well-being of stakeholders, the regulatory and legislative environment continues to expand. This evolving expansion is leading companies to manage an increasingly complex compliance landscape through implemented compliance programs as part of their due diligence. This ensures compliance risk reduction for the company, minimizing legal, financial, and reputational risks, which can result from non-compliance. But on a positive note, this evolving compliance landscape aims to ensure confidentiality, integrity, availability, and privacy for all stakeholders; fostering and ensuring digital trust and safety from compliant companies as they conduct their business across sectors or industries, international borders, and cross-border.

It certifies their commitment to due diligence and care in their business practices. In other words, its aim is to ensure responsible business conduct by requiring the implementation of good corporate governance in companies, through the implementation, operation, management, and continuous improvement of their compliance programs. This allows companies to achieve compliance and promote corporate societal well-being to all stakeholders.

Transforming Compliance, Enabling Digital Trust Excellence (DTE)

Industries and sectors that have undergone digital transformation face inherent risks related to threats against their digital infrastructure and services, as well as critical challenges regarding data protection and privacy strategies. As highlighted earlier, compliance aims to ensure that companies safeguard the interests of all stakeholders by mandating the development and operation of DTE programs (in essence) for compliance. This involves implementing actionable and auditable compliance frameworks.

Key pillars of DTE are:

- Security and Resilience
- Privacy and Data Protection
- Transparency and Explainability
- Accountability and Governance
- Ethics and Responsibility
- Compliance and Auditability
- Quality and Reliability

These key pillars align well when corporate governance is mature and well-established; a global requirement for all companies to mitigate business risk and act as social partners in global human development. Therefore, companies should view compliance as a tool to enhance and strengthen their strategic leadership and responsibility towards the community by effectively implementing DTE programs, rather than perceiving it as an obstacle to their business operations, mission, and profit margins.

Compliance: Enabling DTE Frameworks, Building Business Resilience

As regulatory and legislative requirements for digital-transformed businesses expand, meeting compliance and reducing compliance risks necessitate the implementation of frameworks that foster positive outcomes with regulators and the law. Moreover, companies are legally obliged to adhere to data protection and privacy regulations and laws due to either: 1) their global clients' database, or 2) the geolocations where their services and operations are conducted.

Digital technologies in operations and services that drive the business serviceability and profitability have inherent digital risks! Therefore, to enable DTE and reduce compliance risk, companies can implement frameworks based on the International Standards Organization (ISO) ISO/IEC 27001 and ISO/IEC 27701, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the National Institute of Standards and Technology Privacy Framework (NIST PF) and the American Institute of Certified Public Accountants (AICPA) SOC 2 to achieve this goal. Below are the benefits of international standards and frameworks:

ISO/IEC 27001 – Information Security Management System (ISMS)

Benefits: Provides a globally recognized framework for establishing, implementing, and maintaining an Information Security Management System (ISMS) that aligns with legal, regulatory, and contractual requirements. It helps companies and organizations systematically identify and manage information security risks, ensuring that appropriate controls are in place to protect sensitive data.

By meeting the standard's requirements, businesses can demonstrate due diligence to regulators, clients, and partners, reducing the risk of non-compliance penalties. Additionally, ISO/IEC 27001's structured approach facilitates ongoing monitoring, continuous improvement, and readiness for audits, making it easier to adapt to evolving data protection laws and industry-specific regulations.

ISO/IEC 27701 – Privacy Information Management System (PIMS)

Benefits: Provides a structured framework for managing privacy risks through a Privacy Information Management System (PIMS). As an extension of ISO/IEC 27001, it helps organizations align with global data protection regulations such as GDPR, CCPA, and LGPD, reducing the complexity of meeting diverse legal requirements. By integrating privacy controls into existing information security systems, ISO/IEC 27701 enables organizations to generate clear documentation of how personal data is processed, which can serve as evidence of compliance during audits. This not only enhances regulatory assurance but also builds trust with stakeholders by demonstrating a strong commitment to protecting personal information.

NIST CSF

Benefits: Provides a flexible, risk-based framework that helps organizations efficiently meet multiple regulatory requirements (like HIPAA or FISMA) through a common cybersecurity language. It enables proactive gap identification, prioritization of resources, and continuous improvement, reducing audit costs and building trust with regulators and customers. By integrating governance with business objectives, it also future-proofs organizations against evolving cyber threats and regulations.

NIST PF

Benefits: It is a strategic risk management tool designed to enhance privacy engineering and embed privacy-by-design principles into organizational practices. It helps companies and organizations to build trust by guiding ethical decisions that balance data use with individual and societal privacy protection.

Additionally, it supports compliance with current regulations and prepares businesses for future changes in technology and policy.

The framework also promotes clear communication about privacy practices with stakeholders such as customers, partners, regulators, and assessors.

SOC 2 – AICPA Trust Services Criteria for Security, Availability, Processing, Integrity, Confidentiality, and Privacy

Benefits: Provides a rigorous, standardized framework for managing and protecting customer data in line with the five Trust Service Principles—security, availability, processing integrity, confidentiality, and privacy.

Achieving SOC 2 demonstrates to regulators, clients, and partners that robust controls are in place, helping meet legal and industry-specific requirements while reducing the risk of data breaches and non-compliance penalties.

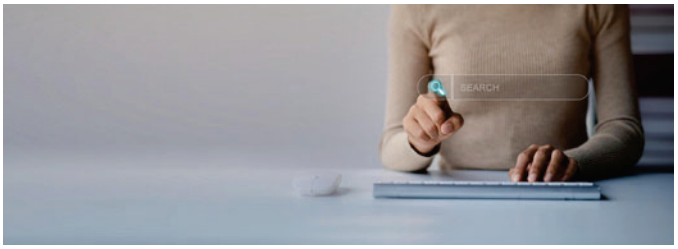
The audit process also drives operational improvements by identifying vulnerabilities and strengthening internal processes, which enhances risk management and audit readiness. Ultimately, SOC 2 compliance builds marketplace trust and offers a competitive edge by signaling a strong, verifiable commitment to data protection.

Compliance: A Business Function

Regulatory and legislative requirements are a way of life from the time of creation. Therefore, compliance should not be viewed as an intrusive parasite in the business ecosystem, but as an integrated business function to achieve and develop the company beyond its current limits.

Compliance should be viewed as a business goal of operational excellence and the board's strategic excellence in its oversight of achieving its vision and corporate societal responsibility to communities, serving as a partner in the protection and security of all stakeholders. For compliance to be a true business function and enabler, it must be established as a management system.

In this context, for DTE, it should be based on ISO/IEC 27001 Information Security Management System or ISO/IEC 27001 Privacy Information Management System.



> A management system is a structured framework of policies, processes, and procedures that enables an organization to achieve its objectives, manage risks, and continually improve performance. It ensures it can achieve its specific goals consistently and effectively.

Compliance: Turning Frameworks into Actionable Outcomes

Through frameworks to achieve DTE, compliance can:

1. **Enhance Customer Trust** through the implementation, management, operation, and continuous development of information security management systems to achieve cyber and information security excellence. A company that is ISO/IEC 27001 and ISO/IEC 27701 certified demonstrates, through this excellence, its corporate due diligence to security, data protection and privacy, in addition to safeguarding operational infrastructures for public safety and well-being. This is highly marketable, building societal trust with current and future customers, in addition to all other stakeholders. Companies attaining SOC 2 Compliant certification also demonstrate full commitment to digital operational trust, especially to North American (NA) stakeholders. SMEs that use the NIST CSF & PF and are audited demonstrate due diligence and their aim in achieving DTE.
2. **Ensure Operational Resilience** through the utilization of frameworks like ISO/IEC 27001, NIST CSF, and SOC 2. Within the NA market, the NIST CSF can become the champion for the detection, response and recovery from incidents, while being SOC 2 compliant, demonstrating to all stakeholders of the company's commitment to service high availability, data security, and privacy.. These characteristics can secure lucrative contracts, improve SLAs and guarantee excellence in uptimes.
3. **Achieve Mature Regulatory** and Contractual Readiness by utilizing all frameworks, companies will demonstrate, by certified audits, the institution of risk management programs to address cyber and information security risks. That is, compliance with data protection and privacy laws, third-party and supply chain risk management, monitoring and logging, and incident response management. This aligns well with regulatory and legal requirements, including minimizing risk and enhancing contractual language for security due diligence.
4. **Attain Cost Optimization** through the implementation of management systems based on the frameworks to reduce redundant risk controls, streamline risk management activities and processes, and continuously improve controls, all in the context of the business. Additionally, doing so strategically at the enterprise risk management level demonstrates a company's due diligence in operational efficiencies and cost reduction, thereby improving product and service quality and delivery efficiencies. This responsible characteristic can build the company's reputation in all markets for all stakeholders, with the added advantage of securing more investors and improving market shares and dividends.

Conclusion

In view of the World Economic Forum Global Risks Report 2025, besides cyber espionage and warfare, vulnerabilities in digital strategies can all create and enhance the global top ten risks in that report, whether for the short or long term.

With the continued integration of digital systems globally with varying vulnerabilities and capabilities and the exponential rate of digital transformation in every sector and industry, regulations and laws, which have always followed slowly behind, will likely expand with increasing rates, possibly aggressively, to minimize the risk to humanity.

Reiterating, risks from various sources, such as cybercrime, nation-state threats, hacktivists, and rogue governments, are too great; therefore, compliance and human well-being go hand in hand. It is required to ensure good corporate governance, and should be integrated into the strategic, tactical, and operational functions, processes, and procedures of the company.

Companies that embrace compliance demonstrate Digital Trust Excellence (DTE) and their corporate social responsibility to the global community through trust, stewardship, and safety, while also gaining profitability, enhancing stakeholder offerings, and building economic resilience.

Edward Millington

Founder and Managing Director
of CariSec Global Inc.

Edward Millington (BSc, CISSP, CISO, SOC 2, ISO, FCIIS, CCCF, MIET) is a Strategic Board Advisor, Principal Security Consultant, and Senior Lead Risk Manager, serving as Founder and Managing Director of CariSec Global Inc. With nearly three decades of expertise across information systems security, ICT, and telecommunications, he has partnered with boards, chairpersons, and executives to embed resilience, digital trust, and ethical technology governance into organizational culture.

His leadership is widely regarded as a cornerstone of organizational transformation, guiding enterprises across multiple sectors to achieve strategic goals, regulatory alignment, and operational resilience. Edward's hallmark is translating complex frameworks, such as ISO/IEC 27001, NIST CSF, SOC 2, and ISO/IEC 42001, into actionable, board-level strategies that deliver measurable impact. He is recognized for strategic foresight in AI governance, Digital Operational Resilience, and Cyber Risk Management, seamlessly bridging policy insight with technical depth.

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 Fellow member of the Royal Chartered Institute of Information Security (CIISec) and a CIISec Assessor; a Professional Evaluation and Certification Board (PECB) Trainer; a member of the PECB Focus 15 group; a Commonwealth Caribbean Cyber Fellow (CCCF) and Co-Chair; an EU CyberNet Expert Pool Member; and a member of the International Information Systems Security Association (ISSA).

A globally recognized advocate, he champions the integration of cyber risk into enterprise risk management, advising boards and executives on cyber governance, digital transformation, and AI security. His thought leadership continues to shape global cybersecurity strategies.