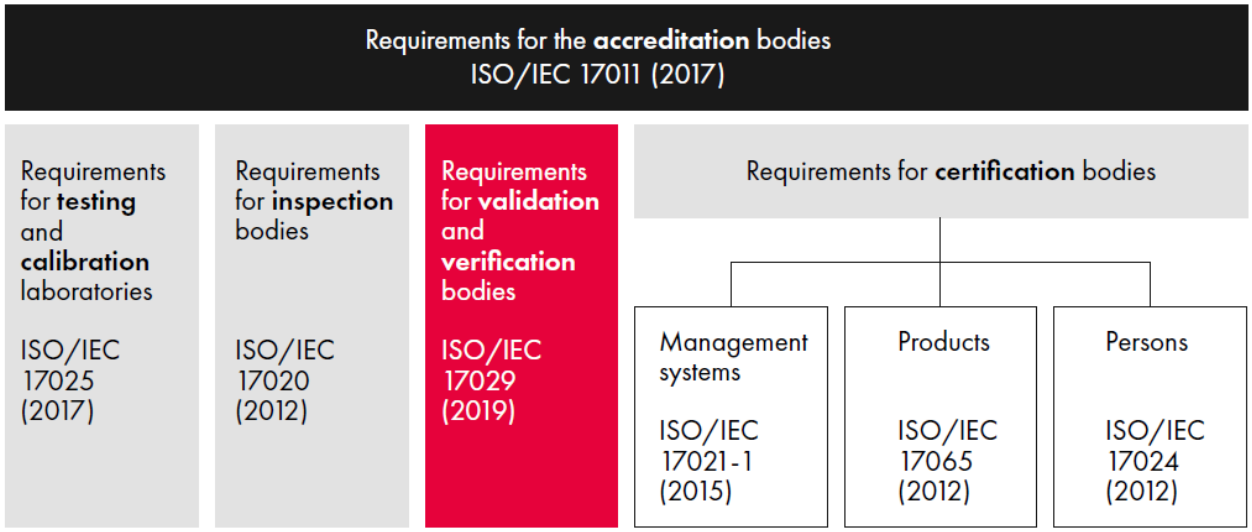
MASTERING DIGITAL ASSURANCE IN THE AGE OF AI

A closer look at key digital governance standards recently published or under development

CPAs can now provide assurance services for the validation of digital governance standards under a new international accreditation standard. The recently published ISO/IEC 17029 standard entitled «Requirements for validation and verification bodies» provides a pathway for auditors to conduct assurance engagements with organizations to verify and validate compliance to national and international digital governance standards.



Source: Committee on Conformity Assessment (2019, 7).

1. **Privacy -** A growing number of international standards have been developed to support compliance to privacy legislation. Here are examples of ISO/IEC standards that organizations can use to facilitate compliance to the EU's General Data Privacy Regulation (GDPR).

Table 1: ISO/IEC Standards Facilitating Compliance with the GDPR

No.	Title	Context
ISO/IEC 15944-5:2008	Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints	Facilitates the creation of an electronic business architecture reflecting external requirements and restrictions such as jurisdictional domain. Will help organizations adopt the GDPR in their practices.
ISO/IEC 15944-12:2020	Information technology — Business operational view — Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)	Provides a framework to identify external requirements and restrictions related to personal data for recorded information in business transactions.
ISO/IEC 19944-1:2020	Cloud computing — Cloud services and devices: data flow, data categories and data use — Part 1: Fundamentals	Creates a foundation for categorizing data that crosses between customers and cloud providers. Includes categories such as health data where the GDPR is applicable.
ISO/IEC 19944-2:2022	Cloud computing and distributed platforms — Data flow, data categories and data use — Part 2: Guidance on application and extensibility	Provides guidance on how to apply 19944-1 and includes privacy-related examples.
ISO/IEC 20546: 2019	Information technology — Big data — Overview and vocabulary	Establishes clear terms and definitions to facilitate the understanding of concepts around big data.
ISO/IEC 20889: 2018	Privacy enhancing data de-identification terminology and classification of techniques	Elaborates on the use of de-identification. In line with privacy principles found in ISO/IEC 29100, its use can enhance the protection of personal data.
ISO/IEC 22624: 2020	Information technology — Cloud computing — Taxonomy based data handling for cloud services	Incorporates further data classification and geolocation information. Highlights where the GDPR needs to be considered.
ISO/IEC 22678: 2019	Information technology — Cloud computing — Guidance for policy development	Highlights that existing policies may need to be changed and interpretations around the GDPR might be required to demonstrate due diligence.
ISO/IEC 23751: 2022	Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA)	Explores how data-sharing agreements can be established. This permitted sharing concept can impact how the GDPR is applied.
ISO/IEC 27001: 2013	Information technology — Security techniques — Information security management systems — Requirements	Provides a framework for the creation of an information security management system to help prevent data breaches and facilitate GDPR compliance.
ISO/IEC 27002: 2013	Information technology — Security techniques — Code of practice for information security controls	Provides guidance on how to apply 27001. Helps in selecting the right controls for the establishment of an ISMS.

Table 1: ISO/IEC Standards Facilitating Compliance with the GDPR (continued)

No.	Title	Context
ISO/IEC 27018: 2019	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Establishes a framework to protect PII in public cloud computing. This enhanced protection for PII can help improve the protection of personal data, an essential element of the GDPR.
ISO/IEC 27701: 2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines	Addition to ISO/IEC27001 and ISO/IEC27002. Provides additional guidance to maintain a privacy information management system.
ISO/IEC 29100: 2011	Information technology — Security techniques — Privacy framework	Provides a PII security framework for ICT to improve the handling of personal data. Offers additional support for the GDPR compliance process.
ISO/IEC 29151: 2017	Information technology — Security techniques — Code of practice for personally identifiable information protection	Highlights guidance for the application of controls to limit exposure to data breaches, a key objective of the GDPR.
ISO/IEC 29184: 2020	Information technology — Online privacy notices and consent	Provides a foundation for informed customer consent of data usage and closely aligns with GDPR requirements.
ISO 31700: 2023	Consumer protection — Privacy by design for consumer goods and services	Provides a road map for organizations to design and implement privacy features and controls into their products. It addresses privacy issues raised by the GDPR.
ISO/IEC 38500: 2015	Information technology — Governance of IT for the organization	Provides a governance model to establish an efficient IT infrastructure, which can facilitate the transition toward a GDPR-compliant model.
ISO/IEC 38505-1:2017	Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data	Provides guidance for organizations on how to apply ISO/IEC 38500.

Source: SCC (2020b)

2. **Artificial Intelligence** – On December 11th, 2023, the European Union adopted its new AI legislation. EU standards bodies CEN and CENELEC have been tasked with the development of a series of new standards to facilitate compliance to the new legislation.

Table 1: List of European standards and/or European standardisation deliverables to be drafted and deadlines for their adoption

Reference information		Deadline for the adoption by CEN and CENELEC
1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems	31/01/2025
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems	31/01/2025
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems	31/01/2025
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems	31/01/2025
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems	31/01/2025
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems	31/01/2025
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems	31/01/2025
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems	31/01/2025
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process	31/01/2025
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems	31/01/2025

3. **Digital Governance Standards Institute (DGSI)** – The DGSI is a Canadian standards development organization accredited by the Standards Council of Canada. Its standards are used by both industry and governments nationally and internationally.

a. Published Standards

DGSI Standard	Title
Automated Decision Systems (AI)	CAN/CIOSC 101, Ethical Design and Use of Automated Decision Systems
	DGSI /WA 126, Baseline Requirements for Vendors Offering AI/ML Lifecycle Solutions to Financial Institutions
Blockchain	CIOSC/TS 114, Technical Specification for Agricultural Blockchain – Traceability of Canola Through the Canadian Supply Chain
Connected Cities	CAN/CIOSC 106-1, Connected Cities – Part 1: Discovery of Digital Twins for Built Environments
Cybersecurity	CAN/CIOSC 104, Baseline Cyber Security Controls for Small and Medium Organizations
	CAN/CIOSC 105, Cybersecurity of Industrial Internet of Things (IIoT) Devices
	CAN/DGSI 118: Cyber Resiliency in Healthcare
Data Governance	CAN/DGSI 100-1, Data Governance – Part 1: Data Centric Security
	CAN/CIOSC 100-2, Data Governance – Part 2: Third-Party Access to Data
	CAN/CIOSC 100-4, Data Governance – Part 4: Scalable Remote Access Infrastructure
	CAN/CIOSC 100-6, Data Governance – Part 6: The Responsible Use of Digital Contact Tracing,
Monitoring Data in the Workplace	CAN/DGSI 100-7, Data Governance – Part 7: Operating model for responsible data stewardship
	CAN/DGSI 100-8: Data Governance – Part 8 – Framework for Geo-Residency and Sovereignty
	CAN/CIOSC 100-9, Data Governance - Part 9: Zero-Copy Integration
	CAN/DGSI 117, English-French Lexicon for Digital Governance and Technologies

Digital Credentials	DGSI/TS 115, Technical Specification for Digital Credentials and Digital Trust Services
Digital Skills	CAN/DGSI 112, National Occupational Standard for Cybersecurity
Digital Trust & Identity	CAN/DGSI 103-1, Digital Trust & Identity – Part 1: Fundamentals
	CAN/DGSI 103-2, Data Trust & Identity – Part 2: Delivery of Healthcare Services
Health Data & Information	CAN/DGSI 100-5, Data Governance – Part 5: Health Data and Information Capability Framework
Modern Procurement	CAN/DGSI 108, Agile and open procurement of digital solutions
Open Finance	CAN/CIOSC 110-1, Open Finance – Part 1: Customer Experience
Privacy & Access Control	CAN/CIOSC 109-1, Privacy – Part 1: Qualification and Proficiency of Access-to-Information, Privacy, and Data Protection Professionals

b. Standards in development

DGSI Standards No.	Title	Technical Committee
CAN/DGSI 100-3	Data governance -- Part 3: Privacy enhancing data de-identification framework	TC 01: Data Governance
CAN/DGSI 103-0	Digital Trust and Identity - Code of Practice	TC 04: Digital Trust and Identity
CAN/DGSI 103-3	Digital trust and identity -- Part 3: Digital credentials	TC 04: Digital Trust and Identity
CAN/DGSI 103-4	Digital trust and identity -- Part 4: Digital wallets	TC 04: Digital Trust and Identity
CAN/DGSI 106	Series of standards for the discovery and management of digital twins for built environments	TC 06: Connected Cities

CAN/DGSI 108	Agile and open procurement of digital solutions	TC 08: Modern Procurement
CAN/DGSI 109-2	Canadian Information Privacy Protection Framework	TC 09: Privacy and Access Control
CAN/DGSI 111	Series of standards supporting the implementation of online electoral voting in Canada	TC 11: Online Electoral Voting
CAN/DGSI 123	Design, Use and Evaluation of a Regulatory Sandbox	TC 16: Regulatory Sandbox
CAN/DGSI 116	Health Data and Information Lexicon	TC 13: Health Data and Information
CAN/DGSI 100-11	Data governance for the delivery of community and human services	TC 01: Data Governance
CAN/DGSI 100-0	Data Governance – Techniques – Code of Practice	TC 01: Data Governance
DGSI 119-1	Election and Voting Technologies – Part 1: Vote Tabulators	TC 14: Electoral Voting Technologies
DGSI 119-2	Election and Voting Technologies - Part 2: Electronic Poll Books	TC 14: Electoral Voting Technologies
CAN/DGSI 120	Guidance for Authentication of Remote Biometrics	TC 15: Biometrics
CAN/DGSI 121	Sharing of urban dataset meta-data	TC 06: Connected Cities
HRSO 300.03 / CAN/DGSI 100-10	Data Governance in Human Research	TC 01 : Data Governance
DGSI 124	Terminology: Municipal land use planning applications	TC 17: Land Use Planning & Development
DGSI 125	Common data fields for use in municipal planning application forms.	TC 17: Land Use Planning & Development