ISO, CSA STAR, & International Equivalent

In today's evolving threat landscape, protecting digital information is a priority – and in some cases, a requirement. Complying with industry regulations, though, can be complicated. You need a partner that understands your security, privacy, and resiliency obligations for new and emerging technologies.

Tevora IS that partner. Our consultants have extensive knowledge and experience in security, privacy, and resiliency. Our team can help with the creation of necessary documentation and implementation of controls to meet the various requirements.

Organizations are increasingly adopting cloud or hybrid services for its applications due to its benefits such as cost savings, reliability and scalability. As the number of companies utilizing these services increases, so does security, privacy, and resiliency risks. The International Organization for Standardization (ISO) develops global standards for everything from data to management systems. Below is a list of the most common and critical standards for organizations to consider:

ISO Standards:

- ISO 27001 - Information Security Management System (ISMS)
  - STAR Cloud Security Standards
- ISO 27017 - Cloud Services Code of Practice
- ISO 27018 - Privacy Code of Practice
- ISO 27701 - Privacy Information Management System (PIMS)
- ISO 22301 - Business Continuity Management System (BCMS)
- ISO 42001 - Artificial Intelligence Management System (AIMS)

How Tevora Helps You

Achieve ISO Certification

Readiness Assessment:

- Determine environment scope
- Define control applicability
- Conduct interviews and evidence analysis
- Identify compliance gaps and the impact of gaps on ISO standards
- Recommend information security control objectives and the controls necessary to meet ISO standards.

Consulting Support:

- Develop a Policy (e.g., ISMS, PIMS, etc.)
- Develop a Statement of Applicability (SoA)
- Assist in the development and alignment of necessary security documentations
- Provide guidance on the implementation of security controls

Internal Audit and Risk Assessment

- Conduct an internal audit of the management system and associated documentation. Note: Tevora Lead Auditors can integrate the ISO control set in a unified approach to cover one or more standards (e.g., ISO 27001, 27017, and 27018).
- Perform a risk assessment of the new management system to identify organizational risk.

Audit Day Support

- Provide support during the accredited third-party ISO certification audit to ensure success.

Feature/Standard	ISO 27001 - ISMS	ISO 27017 - Cloud	ISO 27018 - Privacy	ISO 27701 (PIMS)	ISO 22301 (BCMS)	ISO 42001 (AIMS)
Title	Information Security Management Systems (ISMS)	Code of practice for information security controls for cloud services	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	Privacy Information Management Systems (PIMS)	Business Continuity Management Systems (BCMS	Artificial Intelligence Management System (AIMS)
Scope	Generic information security management	Specific guidance on applying ISO 27001/27002 controls, plus additional controls, to cloud services	Specific guidance on protecting personal data in the cloud, aligned with ISO 27002 controls	Extends ISO 27001 to manage privacy information effectively	Establishing, implementing, and maintaining business continuity	Establishing, implementing, and maintaining artificial intelligence effectively
Objective	To provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS	To give guidelines for information security controls applicable to the provision and use of cloud services	To establish guidelines for protecting personal data in the cloud in accordance with privacy principles	Enhance privacy protection and comply with privacy regulations	Ensure resilience and continuity of operations	Enhance artificial intelligence implementation, and protection, and comply with regulations
Primary Focus	Overall Information Security Management	Cloud service provider and customer security responsibilities	Privacy and protection of personally identifiable information (PII) in the cloud	Privacy and data protection compliance	Business resilience against disruptions	Artificial intelligence implementation and protection
Key Features	• Risk assessment and treatment • Security policy • Organization of information security • Human resource security • Asset management • Access control • Cryptography • Physical and environmental security • Operations Security • Communications Security • System acquisition, development, and maintenance • Supplier relationships • Information security incident management • Information security aspects of business continuity management • Compliance	• Extended security control set for cloud services • Cloud-specific risk management • Segregation in virtual computing environments • Virtual machine hardening • Data encryption • Operations security specific to the cloud • Shared roles and responsibilities between providers and customers	• Consent and choice • Accountability • Data processing agreement requirements • Stronger access control to PII • Encryption of PII • Transparency and compliance • Data integrity and availability • Right to audit and compliance with privacy policies	• Risk Assessment and Treatment • Privacy Impact Assessment • Data processing and consent management • Privacy by Design and Default • Data subject rights • Information Security and Privacy Controls • Privacy Policy and Procedures • Training and Awareness • Third-party Management and Due-Diligence • Record Keeping and Monitoring	• Business Continuity Policy • Risk Assessment & Business Impact Analysis (BIA) • Business Continuity Strategies & Solution • Incident Response Structure • Business Continuity Plans & Procedures • Training & Awareness • Exercising & Testing • Performance Evaluation • -Recovery Plans and Strategies • Improvement • Documentation & Record Keeping	• Policies related to AI • Internal Organization • Resources for AI System • Assessing the impacts of AI systems • AI system life cycle • Data for AI system • Information for interested parties of AI systems • Use of AI system • Third-party and customer relationships
Applicability	All types of organizations	Organizations using cloud services (providers and customers)	Public cloud computing services acting as PII processors	Organizations that are PII controllers or processors	All organizations at risk of operational disruptions	All types of organizations involved in developing, providing, or using AI-based products or services
Certification	Yes, organizations can be certified to ISO 27001 demonstrating they have implemented the standard	No separate certification; ISO 27017 controls can be integrated into an ISO 27001 audit	No separate certification; ISO 27018 controls can be integrated into an ISO 27001 audit	Yes, as an extension to ISO 27001 certification	Yes, separate and independent certification	Yes, separate and independent certification

International ISO Equivalent Standards:

Given the evolving threat landscape globally, countries are developing new laws, regulations, and standards that may be mandated for compliance. Non-compliance with such laws, regulations, and standards could potentially result in fines and penalties. As of the date of this data sheet, here are a few key regulations and standards mandated by countries and a comparison against the ISO 27001 requirements. Please note, this is not an extensive list, so if you have questions about a specific regulation not mentioned, reach out to our team for support.

Feature/Standard	ISO 27001	France HDS	Netherlands NEN-7510	Spanish ENS	Japan ISMAP	Australia IRAP
Title	Information Security Management Systems	Health Data Hosting (Hébergeurs de Données de Santé)	Information Security in Healthcare (Norm NEN 7510)	National Security Framework (Esquema Nacional de Seguridad)	Information Security Management for Information Systems and Personal Information	Information Security Registered Assessors Program
Scope	Generic information security management	Healthcare sector data hosting	Information security in healthcare	National security framework	Information systems and personal information	Information security assessments for Australian Government
Objective	Establish, implement, maintain, and continually improve an ISMS	Secure hosting of health data and patient information	Secure handling of healthcare information	Establish a national security framework	Ensure information security and personal information protection	Assess and certify information security products and services
Primary Focus	General information security management	Healthcare data hosting and processing	Healthcare information security	National security and critical infrastructure protection	Information systems and personal information protection	Information security assessments for the Australian Government
Key Features	• Risk management • Security policy • Access control • Incident response • Continual improvement	• Specific focus on healthcare data protection • Strong encryption requirements • Patient consent requirements • Secure communication requirements • Physical security requirements	• Healthcare information security controls • Access controls for healthcare data • Identity and access management controls • Secure software development and- Secure software development and maintenance • Incident response planning and testing	• Risk management and incident response • Incident response and reporting • Legal and regulatory compliance • Continuous improvement • Continuous monitoring and auditing	• Protection of personal information • Consent and choice • Data integrity and availability • International standards alignment	• Security risk management • Compliance with the Australian Government Information Security Manual (ISM) • Certification and accreditation process
Certification	Organizations can obtain ISO 27001 certification	HDS certification required for healthcare data hosting	Certification process for compliance with NEN 7510	Organizations can obtain ENS certification	Certification process for compliance with ISMAP standards	Organizations can obtain IRAP certification
Applicability	All organizations and sectors	Healthcare organizations and data hosting providers	Healthcare organizations and service providers	Government agencies and critical infrastructure providers	All organizations handling personal information	Organizations providing products and services to the Australian Government
Regulatory Body	International Organization for Standardization (ISO)	Ministry of Health in France	NEN in the Netherlands	Spanish National Cybersecurity Institute (INCIBE)	Japan Information Security Management Association (ISMA)	Australian Cyber Security Centre (ACSC)
Legal Framework	Voluntary standard	Mandatory for healthcare data hosting in France	Mandatory for healthcare organizations in the Netherlands	Mandatory for certain government and critical infrastructure entities	Guidelines with some legal backing	Part of the Australian Government's protective security policy framework

CSA STAR Overview:

STAR leverages the Cloud Security Alliance series of controls to ensure the cloud environment meets security industry best practices and augments the ISO 27001 standard. Organizations must be ISO 27001 certified by an accredited Certification Body to apply for the STAR Certification, or you can get the ISO 27001 certification and STAR together. CSA STAR certifications are issued for three years and have the same expiration date as the underlying ISO 27001 certificate.

Details	Level 1 (Self-Assessment)	Level 2 (STAR Certification)	Level 3 (STAR Continuous)
Applicability	Designed for low-risk/maturity environments	Designed for medium-risk/maturity environments	Designed for high-risk/maturity environments
Regulatory Body	Requires companies to complete a Consensus Assessments Initiative Questionnaire (CAIQ) self-assessment for security, privacy, or both.	Requires companies to complete a CAIQ self-assessment along with being audited by an independent third-party certification body.	Requires companies to complete a CAIQ self-assessment along with continuous automated monitoring.
Legal Framework	Must annually review and update CAIQ self-assessment	• Must annually review and update CAIQ self-assessment • Must have an annual internal audit completed by an independent third party (e.g., Tevora) • Must have an annual external audit completed by an authorized independent certification body (e.g., BSI or Schellman)	• Must review and update CAIQ self-assessment continuous • Must have automated monitoring tools to validate requirements continuously

ACHIEVED ACCREDITATIONS:

AUTHORIZED ASSESSOR:

PCI DSS QSA
PCI PA-DSS QSA
3DS ASSESSOR

TEVORA Compromise Elsewhere.

Tevora is a global leader in enterprise cybersecurity, risk, and compliance services. Founded in 2003, Tevora's team of expert consultants is devoted to supporting the CISO in protecting their organizations from digital threats, creating more secure and compliant business operations. With 20 years of consistent growth, Tevora has accumulated numerous awards and recognitions for growth and industry leadership

Go forward. **We've got your back.**

Go forward. We've got your back.

We live in a digital world, and your customers trust you to keep their information safe. We make it our responsibility to equip you with the information, tools, and guidance you need to stay out of the headlines [and get back to business].

Eyes on the future.

Tevora takes a long-term outlook and proactive approach to every engagement. We combine our technical knowledge with practical business acumen to produce and execute strategies that fortify your organization's assets and build a foundation for the future.

Audit Standards

Our MBAs and CISSPs can help your organization assess and test against PCI DSS, PA-DSS, SSF, HITRUST, ISO 27001, STAR, SOC I, SOC II, MPAA and more.