EXPERT VIEW – MARCH 2021

Author:
Wolfgang Schwab
Head of Cyber Security
wschwab@teknowlogy.com

Co-author:
Ollie O'Donoghue
Senior Analyst
odonoghue@teknowlogy.com

a teknowlogy group company

The most important cloud compliance standards to comply with and require providers to meet

The Covid-19 pandemic has plunged society into one of the greatest crises in recent history. Besides all the negative impacts, however, this pandemic is also driving developments that had previously been tackled rather half-heartedly. Cloud adoption is a good example of this dynamic. The fast deployment of cloud services raises questions about what cloud compliance standards companies can and should comply with internally for private clouds as well as for public cloud deployment. In this Expert View, we focus on the most important organizations that develop cloud compliance standards, i.e. organizations a company should follow, and on widely used cloud compliance standards, i.e. standards a company might want to comply with, and require its service providers to comply with, too.

Expert View level: Strategic
Sectors concerned: All
Topics covered: Infrastructure & cloud computing, cyber security
Priority: ●●●

OPERATIONAL
STRATEGIC
FORWARD-LOOKING

Organizations that set cloud compliance standards

Several professional and technical organizations address different aspects of cloud technology, providing their own standards, recommendations, and guidelines for successful cloud implementation.

The most important organizations include:

- **Cloud Standards Customer Council (CSCC)** is an end-user support group focused on the adoption of cloud technology and on examining cloud standards, security, and interoperability issues.
- **DMTF** supports the management of existing and new technologies, e.g. cloud, by defining appropriate standards. Its working groups, e.g. Open Cloud Standards Incubator, Cloud Management Working Group, and Cloud Auditing Data Federation Working Group, address cloud issues in detail.
- **Open Grid Forum (OGF)** develops standards for grid computing, cloud, and advanced digital networking and distributed computing technologies.
- **Organization for the Advancement of Structured Information Standards (OASIS) –** This nonprofit organization develops open standards for security, cloud technology, IoT, content technologies, and emergency management.
- **TM Forum Cloud Services Initiative** is a consortium of technology firms that provides a platform to address technology challenges. Its Cloud Services Initiative provides a resource for defining cloud standards to be used by technology firms and user organizations.

The importance of cloud compliance standards and the most important standards

Compliance auditors love certifications as they prove that a company or its service providers follow at least the basic rules in service fulfillment. Therefore, buyers should keep track of developments in existing and new certifications and require potential service providers to meet certain cloud compliance standards in order to make audits easier and ensure that service fulfillment is compliant.

The most important standards are briefly described in the following paragraphs.

NIST

The National Institute of Standards and Technology (NIST) is a physical science laboratory and a non-regulatory agency of the United States Department of Commerce. NIST develops and distributes standards largely for US government use, but which are also widely used by private organizations in the US and abroad:

- **NIST SP 500-291 (2011)** provides a set of current standards on cloud computing, analyzes standards priorities, and identifies gaps in existing standards.
- **NIST SP 500-293 (2011)** provides a framework for cloud computing infrastructures, incl. technical specifications for service level agreements and cloud service metrics.
- **NIST SP 800-144 (2011)** provides an overview of the security and privacy challenges facing public cloud computing and makes recommendations on what to

consider when outsourcing data, applications, and infrastructure to a public cloud environment.

- **NIST SP 800-145 (2011) –** The definition of cloud computing lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, elasticity, and measured service. It serves as a benchmark for comparing cloud services and deployment strategies.

ISO

The International Organization for Standardization (ISO) is an international standard-setting body composed of representatives from various national standards organizations. It develops standards for different kinds of technologies and systems, including the following:

- **ISO/IEC 17789:2014 –** This standard defines cloud computing roles (cloud provider, cloud user, cloud broker, and cloud auditor), activities, and functional components, as well as interactions.
- **ISO/IEC 17826:2016 –** This standard is intended for application developers who are implementing or using cloud storage. It defines how to access cloud storage and manage the data stored there.
- **ISO/IEC 18384:2016** establishes terminology, guidelines, and general technical principles underlying service-oriented architectures (SOA), including principles related to functional design, performance, development, deployment, and management.
- **ISO/IEC 19086-1:2016** seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud service level agreements (SLAs).
- **ISO/IEC 19941:2017** specifies types of cloud computing interoperability and portability, the relationship and interactions between these two cross-cutting aspects of cloud computing, and common terminology and concepts used to discuss interoperability and portability, particularly relating to cloud services.
- **ISO/IEC 19944-1:2020** describes the various types of data flowing within the devices and cloud computing ecosystem, the impact of connected devices on the data that flows within the cloud computing ecosystem, and flows of data between cloud services, cloud service customers, and cloud service users; provides foundational concepts, including a data taxonomy; and identifies the categories of data that flow across cloud service customer devices and cloud services.
- **ISO/IEC Technical Report 22678:2019** provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in organizations.
- **ISO/IEC Technical Specification 23167:2020** provides a description of a set of common technologies and techniques used in conjunction with cloud computing, such as virtual machines (VMs) and hypervisors; containers and container management systems (CMSs); serverless computing; microservices architecture; automation; platform-as-a-service systems and architecture; storage services; as well as security, scalability, and networking as applied to the above cloud computing technologies.
- **ISO/IEC 27017:2015** provides guidance on the information security aspects of cloud computing, making recommendations and assisting with the implementation of cloud-specific information security controls, supplementing the guidance in ISO/IEC 27002.
- **ISO/IEC 27018:2019** intends to be a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or a guidance document for organizations for implementing commonly accepted PII protection controls.

Key takeaways

- Cloud compliance standards are important for service provider selection and internal usage.
- There are many organizations that develop cloud compliance standards; the most important are Cloud Standards Customer Council, DMTF, Open Grid Forum, Organization for the Advancement of Structured Information Standards, and the TM Forum Cloud Services Initiative.
- The most important cloud compliance standard-issuing bodies are NIST and ISO, providing numerous standards that help public and private-sector organizations to use cloud computing in a secure and compliant way.

Recommended further reading

Expert View: The most important personnel cyber security certifications
Expert View: What are the most important (cyber) security certifications I should ask providers for?

THE INDEPENDENT EUROPEAN RESEARCH AND CONSULTING FIRM FOR SOFTWARE AND IT SERVICES IN THE CONTEXT OF CORPORATE DIGITAL TRANSFORMATION

For more information, please contact us at contact@teknowlogy.com.

PAC
a teknowlogy group company