ISO/IEC 27017

ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — **Code of practice for information security controls based on ISO/IEC 27002 for cloud services** *(first edition)*

Abstract

"ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: additional implementation guidance for relevant controls specified in ISO/IEC 27002; additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers."

[Source: ISO/IEC 27017:2015/ITU-T X.1631]

Introduction

This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of **cloud-specific information security controls** supplementing the guidance in ISO/IEC 27002:2013 and other ISO27k standards.

Scope and purpose

The code of practice provides additional information security controls implementation advice beyond that provided in ISO/IEC 27002:2013, in the cloud computing context.

The standard advises *both* cloud service customers *and* cloud service providers, with the primary guidance laid out side-by-side in each section. For instance, section 6.1.1 on information security roles and responsibilities says, in addition to section 6.1.1 of ISO/IEC 27002:2013:

Cloud service customer	Cloud service provider
The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service	The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

provider.	

Other information for cloud computing

Even when responsibilities are determined within and between the parties, the cloud service customer is accountable for the decision to use the service. That decision should be made according to the roles and responsibilities determined within the cloud service customer's organisation. The cloud service provider is accountable for the information security stated as part of the cloud service agreement. The information security implementation and provisioning ... *[read the standard for the full text!]*

Normative standards

The standard cites ISO/IEC 27000 and ISO/IEC 27002:2013, of course, plus ISO/IEC 17788 (Cloud computing - Overview and vocabulary) and ISO/IEC 17789 (Cloud computing - Reference architecture). Curiously, although ISO/IEC 27001 is noted in the bibliography, it is not considered 'normative' *i.e.* essential reading: although unusual, it is possible to adopt the information security controls recommended by ISO/IEC 27002 without also having an ISMS.

Status of the standard

The current *first* edition was published in **2015**. Having been developed jointly by ISO/IEC and ITU-T, the standard is dual-numbered *ISO/IEC 27017* and *ITU-T X.1631* with identical content.

Work on a *second* edition started in 2022. It will be updated to "capture a full set of guidance for information security controls applicable to cloud services, both from the third [2022] edition of ISO/IEC 27002 and any additional controls specific related specifically to cloud services."

ISO/IEC SC 27 and SC 38, ITU-T SG17 and the Cloud Security Alliance are collaborating on the revision, requiring careful scheduling to coordinate several parallel activities.

Substantial changes are coming in the second edition of this standard, not least a complete reorganisation of the controls as per ISO/IEC 27002:2022.

The title will become "*Information security, cybersecurity and privacy protection - Information security controls based on ISO/IEC 27002 for cloud services*". It is at **D**raft **I**nternational **S**tandard stage, and will hopefully receive comments from ITU-T SG17 before completion and publication as ISO/IEC 27017 and X.1631 - maybe late 2025, possibly 2026.

Personal comments

In my opinion, ISO/IEC 27017:2015 takes an unrealistically simplistic view of cloud service provider and customer relationships as individual one-to-one interactions. In reality, cloud services are often provided by multiple suppliers to multiple clients in different organisations, and nothing remains static for long. In practice, inter-organisational business relationships often extend through complex cloud supply chains or supply networks, with multiple parties involved in collaborating to assemble, deliver and manage cloud services (*e.g.* network, data centre, physical servers, virtual servers, operating systems, DBMSs and other layered software, applications, and all the associated services). Consequently, there are *numerous* supplier-customer relationship risks to manage, such as organisational interdependence, contracting and subcontracting, complexity, dynamics and compliance. There are risk visibility and trust issues, resourcing challenges, commercial angles, technological challenges and more to contend with. Cloud-related information risks are cloudy!

Risk treatments for cloud and other information risks may include risk sharing, avoidance and acceptance - not just risk mitigation using security controls. Neither ISO/IEC 27017:2015 nor ISO/IEC 27002 pay sufficient attention to risk treatments other than mitigation using security controls.

Particularly for small or immature organisations, cloud services providing email, file storage and office apps *etc*. may be treated as mere commodities, procured without adequate consideration of information risk, security, privacy *etc*. However, some cloud services may be critical for core business, and cloud generally increases the organisation's attack surface. [This issue may be more relevant to ISO/IEC 27005 and ISO/IEC 27036.]

Cloud services have widely proven their value for resilience and flexible working through COVID. Whereas the COVID crisis is nearly over, there are general principles and lessons here that can help organisations be better prepared to cope with future widespread/global challenges such as further pandemics, wars, Internet connectivity issues *etc.* Our challenge now is to draw them out, consider and embed them where appropriate - possibly in this standard.

The standard has widespread support from ISO/IEC JTC 1/SC 27, ITU-T SG17, national standards bodies and CSA among others. However, aligning disparate perspectives and objectives while remaining within the defined scope of the current update project is tricky.

SC 27 decided *not* to progress a separate cloud information security management system specification standard, judging that ISO/IEC 27001 is sufficient and given pressure from ISO not to proliferate Management Systems Standards 'unnecessarily'. Therefore, **SC 27 does not intend to develop a formal requirements specification standard against which to certify the security of cloud service providers** specifically. Providers can

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

however be certified against ISO/IEC 27001, ISO/IEC 27701 and other standards in the usual way, while there are non-ISO cloud security assessment and certification, classification, benchmarking or assurance schemes such as CSA STAR.

< Previous standard ^ Up a level ^ Next standard >