ISO/IEC 27031

ISO/IEC 27031:2011 — Information technology — Security techniques — **Guidelines for information and communications technology readiness for business continuity**

Introduction

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology (ICT) in ensuring business continuity.

The standard:

- Suggests a structure or framework (a coherent set or suite of methods and processes) for any organization – private, governmental, and non-governmental;
- Identifies and specifies all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization's ISMS, helping to ensure business continuity;
- Enables an organization to measure its ICT continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC 27022
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035
ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039

Scope and purpose

The standard encompasses all events and incidents (not just information security related) that could have an impact on ICT infrastructure and systems. It therefore extends the practices of information security incident handling and management, ICT readiness planning and services.

ICT Readiness for Business Continuity (IRBC) [a general term for the processes described in the standard] supports Business Continuity Management (BCM) "by ensuring that the ICT services are as resilient as appropriate and can be recovered to pre-determined levels within timescales required and agreed by the organization."

ICT readiness is important for business continuity purposes because:

- ICT is prevalent and many organizations are highly dependent on ICT supporting critical business processes;
- ICT also supports incident, business continuity, disaster and emergency response, and related management processes;
- Business continuity planning is incomplete without adequately considering and protecting ICT availability and continuity.

ICT readiness encompasses:

- Preparing the organization's ICT (*i.e.* the IT infrastructure, operations and applications), plus the associated processes and people, against unforeseeable events that could change the risk environment and impact ICT and business continuity;
- Leveraging and streamlining resources among business continuity, disaster recovery, emergency response and ICT security incident response and management activities.

ICT readiness should of course reduce the impact (meaning the extent, duration and/or consequences) of information security incidents on the organization.

The standard incorporates the cyclical PDCA approach, extending the conventional business continuity planning process to take greater account of ICT. It incorporates 'failure scenario assessment methods' such as FMEA (Failure Modes and Effects Analysis), with a focus on identifying 'triggering events' that could precipitate more or less serious incidents.

The SC 27 team responsible for ISO/IEC 27031 liaised with ISO Technical Committee 233 on business continuity, to ensure alignment and avoid overlap or conflict. The FCD advised: "If an organization is using ISO/IEC 27001 to establish Information Security Management System (ISMS), and/or using ISO 2239PAS or ISO 23301 to establish Business Continuity Management System (BCMS), the establishment of IRBC should preferably take into consideration existing or

ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27101
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC TS 27570

intended processes linked to these standards. This linkage may support the establishment of IRBC and also avoid any dual processes for the organization."

Status of the standard

ISO/IEC 27031 was originally intended to be a multi-part standard but this was changed to two parts (a formal *specification* plus a *guideline*) and finally reduced to a single part (just the *guideline*) which was **published in 2011**.

The standard is currently being revised. The title will become "Guidelines for information and communication technology *resilience* for business continuity." It is *due* to be published by the end of 2019 ... but looks likely to slip into 2020 and might even be cancelled since it is still in the **W**orking **D**raft stage (6th WD!).

Personal comments

It is unclear how valuable this standard is, given that ISO 22301 does such a good job in this general area, while ISO/IEC 24762:2008 covers ICT Disaster Recovery. If it is to remain a part of ISO27k, it at least ought to be properly aligned with ISO 22301, and ideally extended beyond the ICT domain since ISO27k is about *information* risk and security, not just "ICT" (a clumsy and unnecesary refinement of good old "IT").

Despite its length (41 pages), there are several gaps in the WD text awaiting inputs, and numerous grammatical and technical issues.

Although this standard mentions *resilience to* as well as *recovery from* disastrous situations (and it will be part of the title at the next release), the coverage on resilience is quite light, perhaps because of the strange definition: "Resilience: ability to transform, renew, and recover, in timely response to events". That's just odd! Resilience in the information risk and security context is about the organization being able to bend rather than break. It's about toughness and determination, keeping the essential core business activities going despite adversity. Common examples for high-availability IT systems are load balancing between redundant servers and comms links, and automated failover. Sound engineering concepts such as redundancy, robustness and flexibility ensure that vital business operations are not materially degraded or halted by most incidents.

ISO 22300:2018 defines resilience as "ability to absorb and adapt in a changing environment." That's still not quite right, as far as I'm concerned, too vague and off-topic but it sure beats "ability to transform, renew, and recover, in timely response to events".

PS ISO 22301 is about to be updated: it is at FDIS stage.

< Previous standard ^ Up a level ^ Next standard >