ISO/IEC 27031

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27031:2025 — Cybersecurity — **Information and communication technology readiness for business continuity** *(second edition)*

Abstract

"ISO/IEC 27031 provides guidance on ensuring that information and communication technology (ICT) is prepared to support business continuity. It outlines a framework for ICT readiness that aligns with broader business continuity objectives, ***helping organizations to prevent, respond to and recover from ICT-related disruptions that could impact critical operations.***

In today's digital world, organizations rely heavily on ICT systems to operate, deliver services and maintain trust with stakeholders. Disruptions to these systems — from cyberattacks to system failures — can have severe consequences. ISO/IEC 27031 helps organizations build ICT resilience by integrating readiness planning into business continuity and information security practices. It ensures that ICT services can be restored within agreed timeframes, protecting operations, reputation and customer trust. This readiness is not only about internal systems but also extends to dependencies on third-party services such as cloud providers.

Benefits:

- *Supports uninterrupted business operations during ICT disruptions*
- *Strengthens alignment between ICT, security and continuity strategies*
- *Reduces recovery time and data loss after incidents*
- *Enhances organisational resilience and stakeholder confidence*
- *Integrates smoothly with ISO/IEC 27001 and ISO 22301 practices"*

[Source: ISO.org summary page]

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

Introduction

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of **I**nformation and **C**ommunication **T**echnology in ensuring business continuity.

The standard:

- Suggests a structure or framework (a coherent set or suite of methods and processes) for any organisation – 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 organisation's ISMS, helping to ensure business continuity;
- Enables an organisation to measure its ICT continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

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 **R**eadiness for **B**usiness **C**ontinuity [a general term for the processes described in the standard] supports **B**usiness **C**ontinuity **M**anagement "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 organisation."

ICT readiness is important for business continuity because ICT is prevalent and vital: many organisations' critical business processes (including those involved in managing incidents plus the related business continuity, disaster and emergency responses) are highly dependent on ICT. Therefore, BCM would be incomplete without adequately considering the need to protect availability and continuity of the ICT.

ICT readiness encompasses:

- Preparing the organisation'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 organisation.

The standard incorporates the cyclical **P**lan-**D**o-**C**heck-**A**ct Deming-style approach, extending the conventional business continuity planning process to take greater account of ICT. It incorporates 'failure scenario assessment methods' such as **F**ailure **M**odes and **E**ffects **A**nalysis, 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.

Status of the standard

The *first* edition was published in **2011**.

The revision project ran into trouble and was cancelled in 2020, then rebooted. The standard was revised to cover the need for ICT support for business continuity arising from *both* deliberate *and* accidental incidents.

The *second* edition was published in May **2025**.

Personal comments

The value of this standard is unclear, given that ISO 22301 does such a good job in this general area while ISO/IEC 24762 covers ICT **D**isaster **R**ecovery specifically.

I wish the standard jad been extended beyond the ICT domain since:

- The ISO27k standards concern risk and security to information, not just "ICT" (a clumsy and unnecessary amplification of good old "IT" which in common usage has included comms for, oh at least 50 years); and
- **O**perational **T**echnology (such as **I**ndustrial **C**ontrol **S**ystems running manufacturing plant, and assorted facilities management systems providing power, cooling *etc*.) is not mentioned, not even once - neither

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

included nor excluded, just completely ignored.

However, the second edition, like the first, remains stubbornly focused on ICT.

Furthermore, to avoid any hint of overlap/conflict with the ISO 22300 standards, ISO/IEC 27031 does *not* replace a **B**usiness **C**ontinuity **M**anagement **S**ystem. That said, the standard orbits around "IRBC" (**I**CT **R**eadiness for **B**usiness **C**ontinuity) ... which is essentially a systematic way to manage the IT elements of business continuity, supplementing the BCMS as a whole.

Although the issued standard mentions ICT *resilience to* - as well as *recovery from* - disastrous situations, the coverage on resilience is limited.

Contingency planning involves developing the organisation's flexibility, capability, resources and dogged determination to cope with whatever situations actually eventuate, preparing for the uncertainties and challenges ahead. What will actually happen following an incident is contingent on the situation that occurs, its significance (reflecting its scale, nature, timing, implications for the business *etc*.) and the resources available (surviving!) at that point. The standard only refers once to 'contingency', as a convoluted, badly-phrased note to the definition of [ICT] readiness.

< Previous standard ^ Up a level ^ Next standard >