ISO Spaghetti: A Practical Guide to the Standards That Govern Risk, Resilience and Security

Helen Molyneux, Director | Cambridge Risk Solutions | June 2026

If you have ever tried to specify which ISO standard your organisation needs — or been on the receiving end of a procurement tender asking for several of them at once — you will know the feeling. It is not quite confusion, and it is not quite confidence. It is somewhere in the middle, wondering whether the person who wrote the specification actually knows what they are asking for.

This guide is an attempt to cut through that. Five standards appear regularly in the resilience, risk and security space: ISO 22301, ISO 27001, ISO 22361, ISO 31000 and ISO 22316. They are not interchangeable. They do not cover the same ground. And stacking them all into a procurement specification does not make an organisation more resilient — it just creates more paperwork.

What follows is a plain-English explanation of what each standard actually does, where they overlap, where they diverge, and how to think about which ones are genuinely relevant to your organisation.

First, a word about the difference between certifiable and guidance standards

Before going any further, it is worth drawing a distinction that is frequently glossed over.

ISO 22301 and ISO 27001 are certifiable management system standards. This means that an organisation can be independently audited against them by an accredited certification body and, if they pass, awarded a certificate. That certificate is issued for a specific scope, is subject to surveillance audits, and expires if not renewed. It represents a third-party assurance that the management system meets the requirements of the standard.

ISO 22361, ISO 31000 and ISO 22316 are guidance standards. They contain no requirements against which an organisation can be audited. There is no certification, no audit, and no certificate. They exist to inform practice rather than to mandate it.

> *This matters because a tender document that asks for 'ISO 31000 certification' is asking for something that does not exist. ISO 31000 cannot be certified to. The same applies to ISO 22361 and ISO 22316. If you see this in a specification, it is a signal that the requirement has not been thought through carefully.*

Cambridge Risk Solutions Ltd
Registered Office: Whitehough Cottage, Whitehough, High Peak, SK23 6BX
Company Number: 05534745 VAT Number: 872 5569 85
0800 035 1231 info@cambridge-risk.com www.cambridge-risk.com

ISO 22301 — Business Continuity Management

ISO 22301 is the international standard for Business Continuity Management Systems (BCMS). It requires organisations to establish, implement, maintain and continually improve their ability to continue operating during and after a disruptive incident.

In practice, this means conducting a Business Impact Analysis to understand which activities are critical and how quickly they need to be restored; developing business continuity strategies and plans; and, critically, testing those plans through exercises. An ISO 22301 audit will assess whether the management system is functioning and whether the plans are realistic — not simply whether they exist.

ISO 22301 is often described as the standard that ensures an organisation can keep going when things go wrong. That is broadly accurate, but the detail matters. It is principally about operational continuity — maintaining services, protecting supply chains, recovering functions. It is not primarily about crisis communications, or reputational management, or the leadership behaviours required during a prolonged emergency. Those are addressed elsewhere.

Who typically needs it?

Organisations with explicit continuity obligations tend to pursue ISO 22301 certification: those in the supply chains of Category 1 responders under the Civil Contingencies Act 2004, organisations in critical national infrastructure, and those whose clients demand it through contractual requirements. It is also increasingly relevant for any organisation that takes its supply chain risk seriously, given the direction of travel in both regulation and procurement.

> *ISO 27001 (2022 revision) includes control 5.30, which requires information security continuity to be planned and implemented. This creates an overlap with ISO 22301, but it is not a substitute for it. Control 5.30 addresses the continuity of information security specifically — not the broader operational continuity that ISO 22301 requires.*

ISO 27001 — Information Security Management

ISO 27001 is the international standard for Information Security Management Systems (ISMS). It requires organisations to identify their information assets, assess the risks to those assets, and implement a set of controls drawn from Annex A of the standard.

The 2022 revision of ISO 27001 updated the control structure significantly — moving from 114 controls across 14 domains to 93 controls across four themes: Organisational, People, Physical and Technological. Business continuity, previously addressed under Annex A.17, is now captured in control 5.30. The change is more than cosmetic: the 2022 revision reflects a matured understanding of information security as something that requires cultural and organisational embedding, not just technical controls.

ISO 27001 is often the first standard that organisations in professional services, technology and data-handling sectors pursue, because client contracts and GDPR compliance pressures make it a visible and commercially relevant credential. But it is worth being clear about what it does and does not cover.

What ISO 27001 does not do

ISO 27001 includes a substantive set of incident management controls — covering planning, response, learning and evidence — but these are scoped to information security incidents. Operational continuity across the wider business, including non-IT functions, is a different question, and one that ISO 22301 is built to answer.

Having ISO 27001 certification is meaningful and increasingly expected. It is not, by itself, evidence that an organisation is resilient.

ISO 22361 — Crisis Management

ISO 22361 was published in 2022 and addresses crisis management at the leadership level. It is a guidance standard — not certifiable — and it fills a gap that ISO 22301 deliberately does not cover.

Where ISO 22301 is about keeping the organisation running, ISO 22361 is about how leadership responds when the situation is genuinely novel, fast-moving and reputationally significant. It covers crisis leadership, decision-making under uncertainty, crisis communications, and the behaviours and structures that enable an organisation to navigate a serious incident rather than merely survive it.

The distinction matters in practice. A business continuity plan tells people what to do when a known disruptive scenario unfolds. A crisis management framework addresses what happens when the scenario is not in the plan — when the incident is evolving, when the media are involved, when stakeholder trust is at stake, and when the chief executive needs to make decisions without full information.

Who typically needs it?

Any organisation with a high public profile, complex stakeholder relationships, or significant reputational exposure will benefit from ISO 22361 as a reference framework for crisis management. It is particularly relevant for organisations in regulated sectors, those that interface directly with the public, and those whose response to a serious incident would be subject to external scrutiny.

> *Because ISO 22361 is a guidance standard, organisations cannot be certified to it. What they can do is use it as the basis for developing crisis management capability — which should then be tested through exercises that go beyond the operational scenarios covered by ISO 22301.*

ISO 31000 — Risk Management

ISO 31000 provides principles and guidelines for risk management. It is deliberately broad, applicable to any organisation regardless of sector, size or type of risk, and it is not certifiable.

Its value lies in providing a coherent framework and common language for risk management: defining risk appetite, establishing a risk assessment methodology, and embedding risk management into organisational governance and decision-making. It is the standard that underpins good practice across all the other standards in this space — ISO 22301 requires a risk assessment, ISO 27001 requires a risk assessment, and ISO 22361 assumes that risk management thinking informs crisis preparedness. ISO 31000 describes how to do risk management well.

In that sense, it sits slightly apart from the others. Rather than being an alternative to ISO 22301 or ISO 27001, it is the foundation on which both should be built.

The certification trap

Because ISO 31000 is a guidance standard, any tender specification asking for 'ISO 31000 certification' reflects a misunderstanding of what the standard is. If an organisation wants to demonstrate that it manages risk systematically, the mechanism for that is typically ISO 9001 (quality management), ISO 27001, or ISO 22301 — all of which embed risk management as a core requirement, drawing on the principles of ISO 31000 without making it a separate certification requirement.

ISO 22316 — Organisational Resilience

ISO 22316 is perhaps the least well known of the five standards covered here, and it is also the most conceptual. Published in 2017, it provides guidance on the principles and attributes of organisational resilience — the capacity to absorb disruption, adapt, and continue to achieve objectives in the face of change. This standard is currently under revision, with ISO/DIS 22316 expected to be released shortly.

It does not provide a management system, a set of controls, or a certifiable framework. What it offers is a way of thinking about resilience as something broader than any individual standard: the intersection of business continuity, crisis management, risk management, leadership culture, and adaptive capacity.

In practice, ISO 22316 tends to be most useful for larger organisations that have already implemented ISO 22301 and ISO 27001 and are looking to build a more integrated and strategic understanding of resilience. For smaller organisations earlier in their resilience journey, it is background reading rather than a starting point.

At a glance: the five standards compared

	ISO 22301	ISO 27001	ISO 22361	ISO 31000	ISO 22316
Focus	Business continuity	Information security	Crisis management	Risk management	Organisational resilience
Certifiable?	Yes	Yes	No — guidance only	No — guidance only	No — guidance only
Management system?	Yes (BCMS)	Yes (ISMS)	No	No	No
Requires audit?	Yes	Yes	No	No	No
Key output	BC plans & procedures tested via exercises	Information security controls & ISMS	Crisis leadership & decision-making frameworks	Risk appetite, assessment & treatment framework	Adaptive capacity & culture

	ISO 22301	ISO 27001	ISO 22361	ISO 31000	ISO 22316
Overlaps with...	ISO 27001 (A5.30 and incident management), ISO 22361	ISO 22301, ISO 22361 (information security incident management bleeding into crisis territory at scale)	ISO 22301 (incident management), ISO 27001 (major security incidents), ISO 22316	ISO 27001, ISO 22301, ISO 22316	ISO 22301 and ISO 22361 (resilience as the umbrella concept)
Underpinned by...	ISO 31000	ISO 31000	ISO 31000		ISO 31000
Who typically needs it?	Organisations with continuity obligations or supply chain requirements	Organisations handling personal data, sensitive info, or with cyber risk exposure	Organisations with complex stakeholder environments or high public profile	Any organisation embedding structured risk management	Larger organisations building long-term resilience maturity

Which standards does your organisation actually need?

The honest answer is that it depends on your sector, your risk profile, your client requirements, and your stage of maturity. The following questions are a starting point.

Start here: what are your external obligations?

If you have contractual or regulatory requirements to hold a specific certification — ISO 27001 is increasingly specified in public sector contracts, and ISO 22301 is common in supply chain requirements for critical infrastructure — that is your starting point. Do not second-guess a contractual requirement; meet it, and then consider what else is warranted.

Do you handle personal data or sensitive information at scale?

If yes, ISO 27001 should be a priority. It provides a structured and auditable approach to information security that addresses GDPR obligations, client assurance requirements, and cyber risk in a way that no other single standard matches.

Do you have operational continuity obligations?

If your clients depend on you to continue operating during a disruptive event — or if disruption to your services would have significant downstream consequences — ISO 22301 is the appropriate standard. ISO 27001 alone is not sufficient for this.

Do you have significant public exposure or reputational risk?

If a serious incident could result in media coverage, public scrutiny, or political attention, then crisis management capability matters as much as business continuity planning. ISO 22361 is the reference framework for this. It cannot be certified to, but it can be used to structure a genuine crisis management capability that goes beyond a document on a shelf.

Is risk management embedded in your governance?

ISO 31000 is worth reading as a framework even if you never reference it publicly. If your board-level risk management is currently a quarterly conversation about a colour-coded spreadsheet, there is something useful in ISO 31000's approach to risk appetite, context, and integration with strategic decision-making.

Are you thinking about resilience strategically?

If you have ticked the boxes on ISO 22301 and ISO 27001 and are now asking what good looks like beyond certification, ISO 22316 is the place to look. It will not give you a checklist. It will give you a more sophisticated way of thinking about what it means for an organisation to genuinely be resilient.

A final thought on the spaghetti

The proliferation of standards in this space is not a conspiracy. Each of the five standards described here exists because it addresses something real. The problem arises when they are treated as interchangeable, or when certification to one is assumed to confer the benefits of another.

The organisations that manage disruption well are rarely those with the most certificates. They are the ones that have thought carefully about which frameworks are genuinely relevant to their context, implemented them with substance rather than for optics, and tested them before they needed them.

If you are trying to work out where to start — or whether what you have in place is actually fit for purpose — that is a conversation worth having.

About Cambridge Risk Solutions

Cambridge Risk Solutions is an award-winning independent consultancy specialising in business continuity, crisis management and information security. Founded in 2008, we work across public and private sectors, holding Lead Auditor certifications for both ISO 22301 and ISO 27001.

www.cambridge-risk.com