



Our expertise,  
your peace of mind

---

# ISO 27001 and ISO 27002

---

Transitioning to  
the 2022 standards



[www.itgovernance.co.uk](http://www.itgovernance.co.uk)



+44 (0)333 800 7000

## Contents

Introduction	3
Timeline	3
About this green paper	3
A quick overview of the Standards	3
The structure of ISO management system standards	3
The structure of ISO 27001	3
How ISO 27002 fits into ISO 27001	3
The rest of the ISO 27000 family	3
Certification benefits	3
Comparing the 2013 and 2022 editions of ISO 27001	4
High-level changes to Annex A and ISO 27002	6
The ISO 27002 attributes	7
Attribute presentation	8
Creating your own attributes	8
Using and creating views	8
New controls	9
Noteworthy merged controls	11
Transitioning checklist	12
Conclusion	12
Certified ISO 27001:2022 ISMS Foundation Training Course	14
Useful ISO 27001 resources	15
More free green papers	16
IT Governance solutions	17

# Introduction

In 2022, the international standard for information security management, [ISO 27001](#), and its companion standard, [ISO 27002](#), were [updated](#) for the first time in nearly a decade. In that decade, the cyber security landscape has seen significant changes, with further changes on the horizon: at the time of writing, technologies like AI and quantum computing are rapidly improving and being adopted, both of which will introduce new opportunities for organisations – but for criminals too.

Over the last decade, organisations have also changed the way they work, particularly in terms of:

- [Mobile device](#) usage – especially in terms of bring your own device (BYOD), with the global BYOD market growing from \$76 billion<sup>1</sup> to \$401 billion<sup>2</sup> (£59 billion to £311 billion) between 2013 and 2022;
- [Cloud](#) uptake – between 2013 and 2022, heavy Cloud users grew from 26%<sup>3</sup> to 63%<sup>4</sup>; and
- More recently, remote working – in January and February 2020, 5.7% of UK workers worked exclusively at home; by April 2020 (the first COVID-19 lockdown), this rose to 43.1%.<sup>5</sup> Even by June 2020, after that lockdown was eased, that figure remained high at 36.5% (in other words, a 640% increase in under six months). In February 2022, when ISO 27002:2022 was published, 84% of UK workers who worked from home during the pandemic planned to continue hybrid working.<sup>6</sup>

All three require organisations to extend their boundaries, thereby making their security more permeable. This introduces the need for new security measures, which ISO 27001:2022 and ISO 27002:2022 account for. Other good-practice security frameworks that published updates in 2022 also account for these changes, including version 4.0 of the [Payment Card Industry Data Security Standard \(PCI DSS\)](#) and version 3.0 of [Cyber Essentials](#) (updated to v3.1 in 2023).

## Timeline

Organisations already certified to ISO 27001:2013 have until 31 October 2025 to transition to ISO 27001:2022.<sup>7</sup> However, certification bodies will stop offering (re)certification to ISO 27001:2013 by 29 April 2024, so you may well have to transition before the 31 October 2025 deadline if your current certificate expires after 29 April 2024.

If you certify against ISO 27001:2013 by 29 April 2024, that certificate will expire or be withdrawn on 31 October 2025, even if three years (the normal duration of an ISO management system certificate) have not passed.

## About this green paper

This green paper is intended to help organisations already familiar with the 2013 editions of ISO 27001 and ISO 27002 transition to or adopt the 2022 editions. The paper provides an overview of the key changes to both ISO 27001 and ISO 27002, followed by a transitioning checklist and our concluding thoughts on the new Standards.

## A quick overview of the Standards

This section lays out some key high-level points in relation to ISO 27001, ISO 27002 and ISO management system standards to help you follow the rest of the paper if you need a refresher.

### The structure of ISO management system standards

Both the 2013 and 2022 versions of ISO 27001 follow the common structure used for all recent ISO management system standards, irrespective of their domain of application. As such, even if you are new to ISO 27001 and information security management, areas of the Standard will feel familiar if your organisation has already implemented, for example, [ISO 9001](#) or [ISO 14001](#).

This familiarity goes beyond structure: some parts of ISO management system standards even have identical text. This text is defined in Annex SL, which was updated in 2021 (which ISO 27001:2022 accounts for).<sup>8</sup> As such, management systems in different fields share many terms and definitions, plus have similar requirements (for example, they must all have support from top management and be continually improved), giving organisations the option to use their resources more efficiently by operating an [integrated management system](#).

### The structure of ISO 27001

The main structure of ISO 27001 remains unchanged, with Clauses 4–10 laying out requirements for the ISMS, and each clause covering the same areas as before. For both editions, Annex A provides a list of controls and their descriptions, though the structure of the annex itself has completely changed in 2022, in line with the overhauled ISO 27002 (discussed later in this paper).

### How ISO 27002 fits into ISO 27001

Both the 2013 and 2022 editions of ISO 27002 elaborate on the Annex A controls, explaining them in more detail and providing implementation guidance. As with the 2013 editions, organisations cannot achieve certification against ISO 27002:2022, only ISO 27001:2022.

### The rest of the ISO 27000 family

[ISO 27005](#), which provides guidance on how to manage information security risks, was also updated in 2022; the other standards in the [ISO 27000 family](#) will be updated in due course. However, we do not expect to see the role of each standard within the family change – for instance, [ISO 27000](#) will continue to provide the definitions used in the rest of the family, and ISO 27001 will continue to be the only standard organisations can certify their ISMS against.

### Certification benefits

Naturally, organisations can implement ISO 27001 without achieving certification. However, doing so would deny you the opportunity to demonstrate to stakeholders, such as customers and regulators, how committed to security you are, as well as cause you to lose out on any contracts or other business opportunities that demand ISO 27001 certification as a prerequisite.

# Comparing the 2013 and 2022 editions of ISO 27001

Fundamentally, ISO 27001:2022 is the same as ISO 27001:2013 – the 2022 edition is very much a set of tweaks and refinements rather than an overhaul. For example, ISO 27001 now refers to itself as “this document” rather than “this International Standard”. It has also changed its title from *Information technology — Security techniques — Information security management systems — Requirements to Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, reflecting today’s areas of focus for an effective ISMS that truly keeps the information held and processed by the organisation secure.

ISO 27001:2022 also introduces minor changes to the main ISMS requirements outlined in Clauses 4–10, of which the noteworthy ones are outlined in Table 1 below. As you will see, most of these changes simply align ISO 27001 to the latest Annex SL and, by extension, other recent ISO management systems.

Table 1: Overview of noteworthy changes to Clauses 4–10 of ISO 27001:2022 compared to Clauses 4–10 of ISO 27001:2013

Clause	Subclause	Change description	ISO 27001:2013	ISO 27001:2022	Commentary
4. Context of the organization	4.2	Organisations must now identify “relevant requirements” of interested parties – a slight change in focus.	“the requirements of these interested parties relevant to information security”	“the relevant requirements of these interested parties”	This slight change in focus, in line with the most recent Annex SL, recognises that it is possible for an interested party to have a relevant requirement that is not addressed through the ISMS. For example, the requirement may relate to information security, but does not apply to the interested party’s relationship with the organisation.
		Organisations must now identify which “relevant requirements” will be addressed through their ISMS.	–	“which of these requirements will be addressed through the [ISMS]”	
	4.4	The ISMS must now explicitly include “the processes needed and their interactions”.	“establish, implement, maintain and continually improve an [ISMS]”	“establish, implement, maintain and continually improve an [ISMS], including the processes needed and their interactions”	
5. Leadership	5.1	New note clarifying how the term ‘business’, when used in the Standard, may be interpreted.	–	“Reference to ‘business’ in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization’s existence.”	Another addition that aligns ISO 27001 with the most recent Annex SL. ISO 27001 uses the term ‘business’ relatively little compared to other ISO standards, but including it allows for easier integration with them.
6. Planning	6.2	Information security objectives must now be monitored.	–	“be monitored”	These additions come straight from the latest Annex SL. None of the old requirements relating to objectives have been removed, including the one on retaining documented information on the objectives.
		Information security objectives must now be available as documented information.	–	“be available as documented information”	
	6.3	New subclause that requires changes to the ISMS to be planned.	–	“When the organization determines the need for changes to the [ISMS], the changes shall be carried out in a planned manner.”	
7. Support	7.4	The communication requirements have been slightly simplified.	“d) who shall communicate; and e) the processes by which communication shall be effected.”	“d) how to communicate.”	This phrasing aligns ISO 27001 with the most recent Annex SL, but also makes this requirement simpler and clearer.

8. Operation	8.1	The requirement to plan how to achieve information security objectives has been replaced with a more expansive requirement.	“the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.”	“the processes needed to meet requirements, and to implement the actions determined in Clause 6, by: — establishing criteria for the processes; — implementing control of the processes in accordance with the criteria.”	Once again, these changes align ISO 27001 with the latest Annex SL. They also add value in their own right, respectively making the requirements clearer by being more precise about what is expected of the organisation, and clearly showing that products and services can be outsourced, as well as processes. The latter is especially important in today’s security landscape.	
		Externally provided products and services as well as processes (relevant to the ISMS) must now be controlled.	“outsourced processes are determined and controlled”	“externally provided processes, products or services that are relevant to the [ISMS] are controlled”		
9. Performance evaluation	9.1	Ensuring methods of monitoring, measuring, analysing and evaluating the effectiveness of the ISMS are comparable and reproducible has now been added to the main body of the Standard. This was previously only a note.	“b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; NOTE The methods selected should produce comparable and reproducible results to be considered valid.”	“b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;”	Only the location of this note has changed – not its wording, including use of the word ‘should’ (rather than ‘shall’), making it a recommendation rather than a requirement. This is, in fact, the only ‘should’ in the main body of any clause in the Standard. This change – which does <u>not</u> come from Annex SL – is likely to give more weight to the recommendation.	
	9.2	This clause has been split into two subclauses, but otherwise does not introduce any new or changed requirements.	9.2 Internal audit	9.2 Internal audit 9.2.1 General 9.2.2 Internal audit programme	There are slight changes in phrasing, in addition to the structural changes, that align ISO 27001 to the most recent Annex SL. However, there are no changes in the actual requirements in this clause.	
	9.3	This clause has been split into three subclauses, but introduces no changed requirements and only one new requirement (see below).	9.3 Management review	9.3 Management review 9.3.1 General 9.3.2 Management review inputs 9.3.3 Management review results	Like Clause 9.2, the slight changes in phrasing as well as the structural changes align to the most recent Annex SL. However, this clause also has one new requirement, which again comes directly from the latest Annex SL, but also simply makes sense.	Particularly where the health of the relationship with the interested party directly impacts the organisation’s prosperity, it should be a matter for management.
		Management review must now also consider changes in needs and expectations of interested parties.	–	“changes in needs and expectations of interested parties that are relevant to the [ISMS];”		
10. Continual improvement	10.1 and 10.2	The subclauses have been reordered, but their substance has not changed.	10.1 Nonconformity and corrective action 10.2 Continual improvement	10.1 Continual improvement 10.2 Nonconformity and corrective action	This reordering, and some minor phrasing changes, align ISO 27001 to the latest Annex SL but, again, also just make sense. Continual improvement is something that should always be happening, whereas nonconformities should be the exception.	

The Standard itself describes its main changes as having aligned its text with:

1. “the harmonized structure for management system standards”; and
2. “ISO/IEC 27002:2022”.

The first point has been addressed in Table 1 above, showing that almost all changes simply align the latest edition of ISO 27001 to the most recent Annex SL. Let us progress to the second point.

## High-level changes to Annex A and ISO 27002

Unlike the ISMS requirements themselves, ISO 27002 – and therefore Annex A of ISO 27001, as they are aligned – has been overhauled. Table 2 below sets out the high-level changes.

Table 2: Overview of high-level changes to ISO 27002:2022 compared to ISO 27002:2013

Area of change	ISO 27002:2013	ISO 27002:2022	Commentary
Title	<i>Information technology — Security techniques — Code of practice for information security controls.</i>	<i>Information security, cybersecurity and privacy protection — Information security controls.</i>	‘Code of practice’ has been removed from the title to better reflect the Standard’s purpose as a reference set of information security controls. The first part of the title reflects the new ISO 27001 title.
Size	94 pages.	164 pages.	The size of the 2022 edition has increased by 74% (in terms of page count). This is largely because the Standard now provides more extensive guidance for most controls, each control has a table that sets out its attributes (see below), and there are two new annexes.
Number of controls	114 controls.	93 controls.	Since the 2022 Standard is considerably longer than the 2013 edition, it can appear confusing that it contains fewer controls. This is due to the large number of merged controls: 56 controls from ISO 27002:2013 were merged into 24 controls in ISO 27002:2022 (the noteworthy ones are discussed on page 11) – the natural result of the structural change discussed below. Consequently, from an implementation (and audit) point of view, organisations have got more work to do.
Control grouping	14 clauses that each reflect a concrete area of security, e.g. information security policies, HR security, asset management, access control, cryptography, etc.	4 ‘themes’ that categorise the controls by the broad area of security they concern: ‘organizational’, ‘people’, ‘physical’ and ‘technology’ controls.	The broader approach taken in the 2022 edition of ISO 27002 reflects the simpler structure taken for the controls now, as shown in the next row.
Structuring of controls	Three levels: 1. Security control clause (14) 2. Main security category (35) 3. Control or subcategory (114)	Two levels: 1. Theme (4) 2. Control (93)	The control structure has been flattened from three to two levels, necessitating the dramatic increase of the second level. However, the introduction of ‘attributes’ (see next row), which can be used to filter controls, helps ensure this two-tiered approach does not become overly unwieldy.
Attributes	No attributes, just the extra structural level discussed in the previous row.	Five attributes – discussed further on page 7 – have been introduced: control type, information security properties, cybersecurity concepts, operational capabilities and security domains. These are different ways of categorising controls, independently from the four themes.	As ISO 27002:2022 explains in Clause 4.2, “Attributes can be used to filter, sort or present controls in different views”. Because you can create many different views via the attributes (see page 8), changing to a simpler, two-level structure makes a lot of sense. The attributes should also help simplify the process of choosing appropriate controls, or validate a control selection on a larger scale.
Control layout	Category name and objective (covering multiple controls). Control name, control description, implementation guidance, and other information (e.g. legal considerations and references to other standards).	Control name, attribute table, control description, purpose of the control, implementation guidance, and other information (additional explanations or references to related documents).	The 2022 Standard provides more information for each control, though the only truly new element is the attribute table. Since there is no equivalent for the categories now, the category names have been removed. The objectives have been incorporated into the 2022 Standard as the ‘purpose’ section for each control. The implementation guidance itself is also significantly more detailed for most controls.
Annexes	None.	Two.	The first new annex explains how to use the attributes. The second new annex maps the 2022 controls against the 2013 set.

Table 3 on page 7 goes into more depth on the attributes introduced by ISO 27002:2022, explaining what each of them is and what their values are, after which we discuss ways to use the attributes.

# The ISO 27002 attributes

Table 3: Overview of the ISO 27002:2022 attributes and attribute values

Attribute	Attribute description	Attribute values		Value description
Control type	How the control modifies the risk with respect to security incidents.	1	Preventive	Tries to prevent information security incidents.
		2	Detective	Identifies possible information security incidents.
		3	Corrective	Acts after an information security incident occurs.
Information security properties	The information security characteristic(s) the control aims to preserve.	1	Confidentiality	“property that information is not made available or disclosed to unauthorized individuals, entities, or processes” (Clause 3.10 of ISO 27000:2018).
		2	Integrity	“property of accuracy and completeness” (Clause 3.36 of ISO 27000:2018).
		3	Availability	“property of being accessible and usable on demand by an authorized entity” (Clause 3.7 of ISO 27000:2018).
Cybersecurity concepts	Under what cyber security concept(s), as defined in ISO/IEC TS 27110:2021, the control falls. These concepts also align to the five stages of defence in depth or cyber resilience used widely, including by the <a href="#">NIST Cybersecurity Framework (CSF)</a> .	1	Identify	Identifying the assets to protect.
		2	Protect	Protecting assets from misuse, intentional or unintentional.
		3	Detect	Identifying when assets might be, or have been, misused (i.e. identifying incidents).
		4	Respond	Containing and mitigating a detected incident.
		5	Recover	Restoring impaired capabilities or services following incident resolution.
Operational capabilities	Closely aligned to the security control clauses from ISO 27002:2013, though new topics have been added while others are now absent, this attribute indicates to practitioners what the control’s information security capabilities are. This is by far the largest set of attributes.	1	Governance	Requiring oversight from top management.
		2	Asset_management	Managing assets by tracking them and controlling their use.
		3	Information_protection	Protecting sensitive and/or confidential information.
		4	Human_resource_security	HR-related (and therefore people-related) security measures, like providing <a href="#">training</a> .
		5	Physical_security	Relating to physical information security, like mitigating environmental threats.
		6	System_and_network_security	Securing systems and networks that hold or access information, or affect its security.
		7	Application_security	Securing applications that hold or access information, or affect its security.
		8	Secure_configuration	Configuring software, etc. in line with the need-to-know and least privilege principles.
		9	Identity_and_access_management	Controlling access to information and information systems to authorised individuals only, and having them prove that they are who they claim to be.
		10	Threat_and_vulnerability_management	Keeping up with threats and vulnerabilities, and mitigating them appropriately.
		11	Continuity	Ensuring critical business functions can continue to operate at an acceptable level during a security incident.
		12	Supplier_relationships_security	Securing the supply chain to mitigate third-party risks to your information.
		13	Legal_and_compliance	Security matters affecting legal, statutory, regulatory and contractual requirements.
		14	Information_security_event_management	Managing information security events (such as logging them) to help identify and investigate security incidents.
		15	Information_security_assurance	Reviewing security measures to give assurance.
Security domains	A means of classifying the control in line with broad security and governance categories.	1	Governance_and_Ecosystem	Addresses general governance of security and risk management.
		2	Protection	Addresses areas like IT security architecture and maintenance, identity and access management, and so on.
		3	Defence	Concerns detective and incident management activities.
		4	Resilience	Addresses areas like continuity of operations and crisis management.

## Attribute presentation

For each control, the Standard presents the attributes in a table such as Table 4:

Table 4: Example attribute table in ISO 27002:2022

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and _Ecosystem #Resilience

Note that each attribute value is preceded by a hashtag to make them searchable, and that any given control can have more than one value.

The Standard also makes clear that organisations are free to disregard any of the attributes it provides. Ultimately, the attributes and their values are classifications intended to improve ease of use – they will not be audited and play no role in achieving ISO 27001:2022 certification. As such, each practitioner (and organisation) is free to adopt and interpret the attributes as is useful to them. The fact that most of the attribute values lack formal definitions reinforces this stance.

## Creating your own attributes

You can apply the attributes defined by ISO 27002:2022 to self-developed controls if you find it useful. The Standard also states that organisations may create their own attributes and attribute values, suggesting the following four-step approach in Clause A.2:

1. Determine what attribute(s) would be useful to your organisation; for example, maturity level, priority or assets involved.
2. Determine appropriate attribute values. For example, for maturity, you could use the values from the ISO/IEC 33000 series.
3. Copy the ISO 27002 control names and identifiers into a spreadsheet or database, and add the appropriate attribute values to each control.
4. Sort the spreadsheet (or query the database) to extract the required information. In effect, this creates your own views.

## Using and creating views

Views – whereby you put all controls and their attribute values into a spreadsheet or database, then filter or sort by attribute – are a useful way of simplifying the control selection process. For instance, you might be considering treatment options for a particular risk, and know that you need detective controls, which you can filter for under the ‘control type’ attribute as in Table 5:

Table 5: Top two rows if you filtered for ‘#Detective’ under ‘control type’, using the default attributes

No.	Control	Control type	Information security properties	Cyber-security concepts	Operational capabilities	Security domains
5.7	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and _vulnerability _management	#Defence #Resilience
5.25	Assessment and decision on information security events	#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information _security_ event_ management	#Defence

Alternatively, you may feel that a particular asset needs its integrity protected, in which case you can filter for that under ‘information security properties’, or that your overall security lacks measures for efficient recovery after an incident, which you can filter for under ‘cybersecurity concepts’.

The attributes can also be used to validate your control selection on a larger scale by adding the selection in a format like Table 5 to, for example, a spreadsheet, then checking that you have accounted for all control types, information security properties, cybersecurity concepts, and so on. You can also check that you have not over- or underrepresented any areas.



## New controls

ISO 27002:2022 introduces 11 completely new controls, which are outlined in Table 6 below. However, as you will see, if you have already implemented the 2013 control set, you are likely already performing much of the below (though possibly not yet to the level required). Nevertheless, there is good reason for treating these activities as separate controls, mostly to draw more attention to them due to their growing importance in today's security landscape. There are also a few controls that are truly new, having not been covered at all by ISO 27002:2013.

Table 6 below discusses the controls individually in more detail, including what links there are to the previous Standard, if any.

Table 6: Overview of the new controls introduced in ISO 27002:2022

Control		ISO 27002 control description	Commentary
5.7	Threat intelligence	"Information relating to information security threats should be collected and analysed to produce threat intelligence."	Threat intelligence is an effective means of keeping up with the threat environment and informing your mitigation actions, but has only become more mainstream in recent years – thus only being introduced in this latest edition of the Standard.  The control's main subtopics are types of threat intelligence, intelligence selection and how to use obtained intelligence.
5.23	Information security for use of cloud services	"Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements."	The need for this control is fairly obvious: organisations rely on <a href="#">Cloud services</a> more than ever before. Moreover, securing information in the Cloud comes with unique risks and challenges. Having said that, Cloud security also has plenty of overlap with securing other IT infrastructures. As such, ISO 27002:2013 indirectly covered much of this control's guidance, including defining all relevant information security requirements (14.1.1 from 2013) and defining relevant roles and responsibilities (6.1.1).  This control's guidance discusses various points to define (like the two examples above), and what to check for in Cloud service agreements.
5.30	ICT readiness for business continuity	"ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements."	This control focuses on availability – a property of security and, as such, arguably a subset of 5.29 of the 2022 control set (information security during disruption) or 17.1 of the 2013 set (information security continuity). However, this control (5.30) <i>only</i> focuses on the availability of information and associated assets in the event of a disruption – uninterruptible power supplies, for example – so the organisation can continue to meet its objectives, regardless of the circumstances. ISO likely made this a separate control to emphasise the importance of considering availability separately – and in addition to – preserving the overall security of your assets during a disruption.  ISO 27002:2022 recommends establishing your continuity requirements by conducting a <a href="#">business impact assessment (BIA)</a> .
7.4	Physical security monitoring	"Premises should be continuously monitored for unauthorized physical access."	ISO 27002:2013 briefly covered some of the guidance this control offers, like in 11.1.1.f (installing intruder detection systems), but this really is essentially a new control.  The points covered include installing video monitoring systems and intruder alarms, and preventing them from being disabled remotely.
8.9	Configuration management	"Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed."	Secure configuration is a basic yet vital means of keeping information secure. ISO 27002:2013 did account for this, mostly via 12.1.1 (documented operating procedures) and 12.5.1 (installation of software on operational systems), but only to a very limited extent – nothing like the depth this new control requires. Making this a separate control also aligns ISO 27002 to other good-practice frameworks such as the PCI DSS and Cyber Essentials.  The new control's main subtopics are defining secure configuration templates, configuration management and monitoring configurations.
8.10	Information deletion	"Information stored in information systems, devices or in any other storage media should be deleted when no longer required."	Information deletion is a topic touched on by various controls in the 2013 set, including 8.1.1 (inventory of assets), 8.1.2 (ownership of assets) and 11.2.7 (secure disposal or reuse of equipment, though this is also a separate control (7.14) in the 2022 set). However, since 2013, deleting data and information when no longer required has received a lot more attention as a best-practice security and privacy activity in its own right – the <a href="#">General Data Protection Regulation</a> (GDPR, published 2016), for example, stipulates 'storage limitation' as one of just six key data processing principles. By including information deletion as a separate control, ISO 27002:2022 aligns itself to today's security best practices.  This control mainly offers guidance on selecting an appropriate deletion method and collecting evidence of the deletion.

8.11	Data masking	“Data masking should be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.”	<p>Data masking – such as pseudonymisation and anonymisation techniques (which are the main focus of this new control) – are commonly used for personally identifiable information (PII), but can be used to protect other types of sensitive data too, including payment card data. Since the 2013 Standard did not cover such techniques at all, this can be considered a truly new control, likely introduced as these techniques have become more widespread in recent years, mainly due to privacy legislation like the GDPR.</p> <p>Besides providing guidance on the actual masking techniques, the control also offers guidance on using those techniques in accordance with your access control policies: some people should have access to the unmasked data, others to the obfuscated data only. Data masking is an effective security technique, but not a one-size-fits-all solution.</p>
8.12	Data leakage prevention	“Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.”	<p>ISO 27002:2013 briefly mentioned preventing information leakage as part of a few controls, such as 8.3.2 (disposal of media), but did not cover this topic in any depth despite its obvious importance in an information security context, and as such more than worthy of being a control in its own right.</p> <p>The control’s guidance covers points to consider for preventing data leakage, and how to use tools designed for this purpose. It also covers behaviours to teach staff to prevent data leakages.</p>
8.16	Monitoring activities	“Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.”	<p>The 2013 Standard recommended organisations produce, keep and regularly review event logs in control 12.4.1 (event logging), which came under the ‘logging and monitoring’ security category. Logging and monitoring are, of course, linked; however, they are separate activities that require separate guidance, and as such have been split into two lengthy controls in the 2022 Standard: 8.15 (logging) and 8.16 (monitoring activities), taking up nearly five full pages combined. It is also worth noting that the guidance on monitoring in the 2013 control set was extremely limited, and as such can easily be regarded as a truly new control.</p> <p>The new 8.16 guidance discusses what to consider for your monitoring system, including that it should establish what ‘normal’ behaviour is to have a baseline to monitor against, involve automated software and communicate abnormal events to relevant parties. The monitoring system can also be informed by threat intelligence (5.7).</p>
8.23	Web filtering	“Access to external websites should be managed to reduce exposure to malicious content.”	<p>This control is, in effect, an expansion on 12.2.1.c from ISO 27002:2013, which said to consider “implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting)”. However, this new control is not just a subset of 8.7 from 2022 and 12.2 from 2013 (protection against/from malware), as it also addresses other (potentially) malicious content types, like websites sharing illegal content, and “undesirable or inappropriate websites and web-based applications” in general, which were not covered in the previous Standard.</p> <p>The guidance mostly provides a list of website types to consider blocking, and discusses establishing rules and providing staff training for using online resources appropriately.</p>
8.28	Secure coding	“Secure coding principles should be applied to software development.”	<p>With software development far more prevalent now than in 2013 – and continuing to be a growing market, particularly with the rise of AI – there is a clear need for this new control, whose topics were only briefly touched on in 14.2.1 (secure development policy) of the 2013 Standard. Ensuring that secure coding principles are being applied in the development process itself ensures that fewer vulnerabilities end up in the software to begin with, which does not just mitigate the risks but also makes managing the software’s security further down the line easier and cheaper.</p> <p>The control’s guidance addresses general points like establishing relevant processes and monitoring real-world threats and vulnerabilities, then details the principles themselves, breaking them up into three sections: before, during and after coding.</p>

## Noteworthy merged controls

In total, 56 controls from ISO 27002:2013 have been merged into 24 controls in ISO 27002:2022. Most of these are very straightforward mergers, which are unlikely to confuse those preparing to transition. With that in mind, Table 7 below only covers the merged controls we believe are more prone to causing confusion (mostly by wondering where certain controls have disappeared to) if you are more familiar with the control set from 2013.

Table 7: Overview of the noteworthy merged controls from the 2013 to the 2022 editions of ISO 27002

ISO 27002:2013 controls		ISO 27002:2022 control		ISO 27002:2022 control description	Commentary
6.1.5	Information security in project management	5.8	Information security in project management	"Information security should be integrated into project management."	The new control description strongly reflects the description of 'information security in project management' (6.1.5) from the 2013 set, but now simply regards the old 'information security requirements analysis and specification' control (14.1.1) as a subset. In other words, new or enhanced information systems are also considered projects.
14.1.1	Information security requirements analysis and specification				
18.1.1	Identification of applicable legislation and contractual requirements	5.31	Legal, statutory, regulatory and contractual requirements	"Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date."	The 2022 control description is very similar to the description for 'identification of applicable legislation and contractual requirements' (18.1.1) from the 2013 set. However, unlike ISO 27002:2013, the updated Standard considers meeting such requirements in terms of using cryptography (the old 'regulation of cryptographic controls' (18.1.5)) being a subset of that.
18.1.5	Regulation of cryptographic controls				
8.3.1	Management of removable media	7.10	Storage media	"Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements."	ISO 27002:2013 essentially split the various stages of the media life cycle into separate controls, whereas the 2022 Standard combines them into one control. It also groups 'removable media', 'media' and 'equipment, information or software' under the single term of 'storage media'.
8.3.2	Disposal of media				
8.3.3	Physical media transfer				
11.2.5	Removal of assets				
6.2.1	Mobile device policy	8.1	User end point devices	"Information stored on, processed by or accessible via user endpoint devices should be protected."	Controls 6.2.1 and 11.2.8 from the old Standard refer to 'mobile devices' and 'unattended equipment' respectively; ISO 27002:2022 combines these into 'user endpoint devices', and simply requires accessible information on them to "be protected".
11.2.8	Unattended user equipment				
12.6.1	Management of technical vulnerabilities	8.8	Management of technical vulnerabilities	"Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken."	The 2022 control description is very close to the description for 'management of technical vulnerabilities' (12.6.1) from 2013; however, the updated Standard considers the old 'technical compliance review' control a subset of that, for both seek to mitigate technical vulnerabilities in information systems.
18.2.3	Technical compliance review				
12.4.1	Event logging	8.15	Logging	"Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed."	While this control merger may appear straightforward, there is an important change in the new control 8.15 compared to the 2013 set: logs must now be "analysed", not merely "regularly reviewed". This is evident not just from the control descriptions, but also from the control guidance itself. The old guidance mainly focused on what logs to collect and how to protect them, whereas control 8.15 (from the 2022 Standard) provides detailed guidance on log analysis, too.
12.4.2	Protection of log information				
12.4.3	Administrator and operator logs				

## Transitioning checklist

---

So, what ground should organisations cover to transition effectively? Here is a high-level checklist:

- **Conduct a gap analysis**  
Compare your current measures against both the main clauses and Annex A from ISO 27001:2022 to identify any shortcomings. Table 1 in this green paper should help with this for Clauses 4–10, and Annex B in ISO 27002:2022, which maps the 2022 against the 2013 set, should help with the controls. Conducting this type of [gap analysis](#) will tell you where you need to focus your efforts and inform your transition project plan.
- **Conduct a new risk assessment**  
When your next risk assessment is due, look at the 2022 control set as you consider your risk responses.
- **Produce a revised risk treatment plan**  
Following a new risk assessment, as per ISO 27001's requirements, you need to revise your risk treatment plan.
- **Issue a revised Statement of Applicability (SoA)**  
As usual after a new risk assessment and treatment plan, you will need to issue a revised SoA. If you are working against the 2022 control set and due to be audited before you are able to achieve certification against the new Standard, like with any other non-Annex A control set, you will need to compare those controls against the old Annex A. However, this is a very straightforward process thanks to the new Annex B in ISO 27002. The new attributes should also speed up the control validation process.
- **Update documentation where necessary**  
Where you are implementing changes to your controls, even if they are only small ones, your [documentation](#) – policies, procedures, records, and so on – will need to reflect them, so be sure to review and update it where necessary.
- **Arrange for a transition audit**  
Finally, when your next audit is due (or if you are new to the Standard, when you are ready for your first audit), arrange a date with your certification body. For organisations new to ISO 27001, and that have not chosen a certification body yet, be sure to choose one listed on the United Kingdom Accreditation Service (UKAS) website.<sup>10</sup>

Again, this checklist is very broad – organisations should only use it as a starting point for developing their own checklist and/or action plan, taking into account their individual circumstances, including the status of their current ISMS or ISO 27001 implementation project.

## Conclusion

---

To summarise, both ISO 27001 and ISO 27002 had new editions published in 2022, though only ISO 27002 received a true overhaul – ISO 27001 was mostly a case of aligning it to the latest Annex SL.

ISO 27002, on the other hand, has been dramatically changed, introducing a completely new structure; a new way of grouping controls; several new controls, on top of some significant control mergers; and attributes. Perhaps more importantly still, the Standard now offers far more extensive guidance for each control.

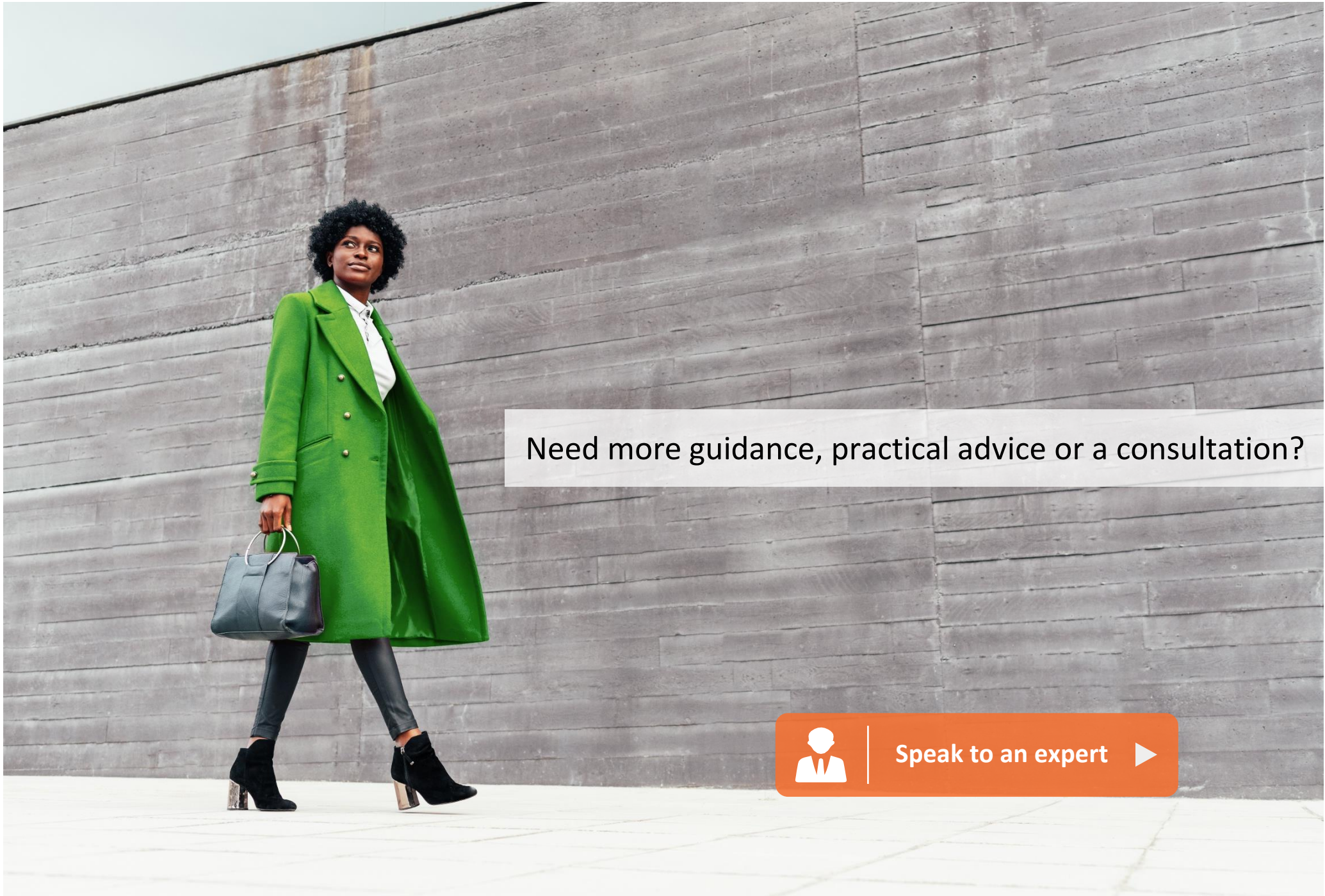
Here at IT Governance, we feel that both 2022 Standards are an improvement on their 2013 editions:

- ISO 27001 is now better aligned to other recent ISO management system standards, which makes it easier to combine implementation projects and/or manage an integrated management system.
- ISO 27002 is much more comprehensive now and provides clearer guidance on control selection and implementation. This is in part thanks to the revised control layout, which separates out the purpose of each control, helping practitioners and organisations better gauge whether that control is likely to be an effective means of mitigating a particular risk. The implementation guidance itself is also more detailed now, making it easier to implement the Standard, particularly for first-time adopters. Finally, the attributes are another useful addition for the control selection and validation processes.


Regardless of when your first ISO 27001:2022 audit is due, we *strongly* recommend starting your transition sooner rather than later. This is not just for the usual reasons of avoiding the stress typically associated with rushed projects, but also because – as outlined in the bullets above – we feel that the 2022 Standards improve on the previous editions.

Particularly if you lack experience or confidence when it comes to implementing an ISMS, the improved guidance in ISO 27002:2022 will make the process significantly easier. Meanwhile, more seasoned practitioners will benefit from the new and updated controls from the new set, which, understandably, are much better suited to today's security landscape than the 2013 set.

Anything cyber moves at an exceptionally fast pace. Organisations must adapt accordingly to thrive and survive.



Need more guidance, practical advice or a consultation?

 | [Speak to an expert](#) ▶

# Certified ISO 27001:2022 ISMS Foundation Training Course

Get a comprehensive introduction to the features and benefits of ISO 27001:2022 in this one-day accredited course, developed by industry-leading experts and delivered by an experienced practitioner.

## Topics covered

- An overview of ISO 27001:2022 and its application.
- The core elements of an ISMS and the benefits of ISMS certification.
- Key elements of ISMS implementation project planning.
- The key steps involved in an ISO 27001 risk assessment.
- An overview of the ISO 27001 Annex A controls.
- An overview of available standards and management system documentation.

## Why choose us for your training needs?


- We are internationally recognised as the authority on ISO 27001 – our team led the world’s first ISO 27001 certification project, and since then we have trained more than 8,000 professionals on ISMS implementation and audit.
- Train with industry experts – our trainers are working consultants with years of practical, hands-on experience.
- Learn from anywhere – we fully embrace flexible and remote working, and have adjusted our delivery methods to allow you to learn from anywhere.
- Access your training anywhere – all course materials are provided as digital copies, allowing you to access them anywhere and at any time.
- We have trained more than 28,000 people, and we are confident that you will pass with us first time. If you do not, we will train you again for free.<sup>11</sup>
- Choose the delivery method that suits you – we offer classroom, instructor-led Live Online, self-paced online and in-house training, as well as a range of [elearning options](#).

Find out more ▶




# Useful ISO 27001 resources

IT Governance offers a unique range of ISO 27001 products and services, including standards, gap analysis tools, documentation toolkits and training courses.




### ISO/IEC 27001:2022 Standard

Download the 2022 edition of ISO/IEC 27001 (*Information security, cybersecurity and privacy protection — Information security management systems — Requirements*), the international standard for information security management that provides the specification for a best-practice ISMS.




### ISO/IEC 27002:2022 Standard

Download the 2022 edition of ISO/IEC 27002 (*Information security, cybersecurity and privacy protection — Information security controls*), providing detailed implementation guidance for all Annex A controls. This Standard includes a mapping of the 2022 control set against the 2013 set.



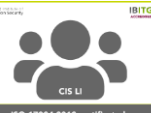
### ISO 27001:2022 Gap Analysis Tool

Identify to what extent your organisation is compliant with Clauses 4–10 and Annex A of ISO 27001:2022 with this Excel-based gap analysis tool. Quickly and easily map your current information security measures against the Standard’s requirements and controls by answering simple yes–no questions, so you can clearly establish areas for development, and plan and prioritise your project effectively.




### ISO 27001 Toolkit

Save hours of work in your ISMS implementation project with more than 140 customisable, ISO 27001-compliant documentation templates and expert guidance. You can further accelerate your project with the included gap analysis tools, which will help you understand what needs to be done to achieve ISO 27001 certification. This toolkit is hosted on our Cloud-based DocumentKits platform, allowing for easy collaboration.




### Certified ISO 27001:2022 ISMS Lead Implementer Training Course

Gain the skills to lead and manage an ISO 27001:2022-compliant ISMS implementation project. This three-day course teaches the nine critical steps involved in planning, implementing and maintaining an effective ISMS, how to structure and manage your ISO 27001 project, and more. Learn in person, or choose from Live Online or self-paced online formats.



### Certified ISO 27001:2022 ISMS Internal Auditor Training Course

Learn how to drive continual improvement within your organisation’s ISMS, and find out how to identify opportunities for improvement and take corrective action to maintain ISO 27001:2022 compliance in this two-day course. Learn in person, or choose from Live Online or self-paced online formats.



### Certified ISO 27001:2022 ISMS Lead Auditor Training Course

Gain the skills to deliver second-party (supplier) and third-party (external and certification) audits against ISO 27001:2022. Learn how to lead a team of auditors and competently manage an ISMS audit programme, best-practice audit methodology, and more in this five-day course. Learn in person, or choose from Live Online or self-paced online formats.

[View more](#) 

## More free green papers

IT Governance publishes numerous free green papers – as well as many other resources, including webinars, infographics and case studies – on a wide range of topics. Here are two you might be interested in:



**Mobile Device Security**  
Adapting to flexible working

Protect • Comply • Thrive

**Mobile Device Security – Adapting to flexible working**

For all their benefits, relying on mobile devices such as smartphones and laptops does come with security risks. Want to learn more about how to mitigate them? This green paper discusses some of the most common mobile device security risks, and highlights a range of measures that can help you mitigate them.



**Cloud Security**  
Who is responsible?

Our Expertise, Your Peace of Mind

**Cloud Security – Who is responsible?**

Cloud computing is another technology that provides incredible opportunities but comes with risks. Want to learn more about them and where your responsibilities lie? This green paper helps you better understand the Cloud provider–customer relationship and your legal and contractual requirements. It also outlines a practical approach to meeting your obligations.

### About IT Governance green papers

The concept of “Our expertise, your peace of mind” informs everything we do – sharing our knowledge and experience to ensure our customers’ IT governance, risk management and compliance (GRC) projects go smoothly and are successful.

Our green papers draw on our specialists’ experience and expertise to give you the guidance you need to move your projects forward, whether you need expert advice on compliance, a concise guide to a tricky process or tips for implementing management systems.

IT Governance green papers: the green light at the start of your IT GRC journey.

[Visit our resource hub](#)



# IT Governance solutions

---

IT Governance is your one-stop shop for cyber security and IT GRC information, books, documentation toolkits, training, consultancy, penetration testing, software tools, and more. Our products and services work harmoniously together so you can use them individually or combine different elements depending on your needs.

## Books

Our sister company IT Governance Publishing (ITGP) is the world's only niche IT governance publisher, collaborating with industry experts to produce high-quality publications about best-practice frameworks, compliance and technical subjects.

Our books cover a wide range of GRC topics, including cyber security and resilience, data privacy and business continuity. They also come in a range of formats, including softcover, PDF, ePub, Kindle and audiobook.

Visit [www.itgovernance.co.uk/shop/category/itgp-books](http://www.itgovernance.co.uk/shop/category/itgp-books) to view our full catalogue.

## Toolkits

Created by expert practitioners and used by more than 17,000 organisations worldwide, our toolkits contain fully customisable documentation templates designed to help you meet your compliance obligations, ranging from ISO 27001 to the GDPR, the PCI DSS, Cyber Essentials, ISO 22301, and more.

Each toolkit is hosted on our Cloud-based DocumentKits platform, enabling us to regularly update them and making it easier for you to collaborate. The toolkits also come with unlimited support for account setup and assistance to help you customise and use the templates.

Visit [www.itgovernance.co.uk/documentation-toolkits](http://www.itgovernance.co.uk/documentation-toolkits) to view all our toolkits.

## Training

We provide a wide range of training courses, covering areas including data privacy, information security and ISO 27001, cyber security, ethical hacking, and professional certification courses such as CISA®, CISM®, CGEIT® and CRISC®. To date, we have trained more than 28,000 individuals.

Our courses range from introductory to advanced training, and are available as classroom, Live Online and self-paced online courses. Visit [www.itgovernance.co.uk/training](http://www.itgovernance.co.uk/training) for more information.

More interested in short awareness courses that deliver a consistent, interactive and comprehensive message to all your staff? Visit [www.itgovernance.co.uk/staff-awareness-e-learning-courses](http://www.itgovernance.co.uk/staff-awareness-e-learning-courses) for more information.

## Consultancy

Whatever your IT GRC needs and budget, we have consultancy options to suit you. From fixed-price packaged solutions to bespoke and corporate consultancy services, we can help you meet your objectives efficiently and cost-effectively.

Our unique combination of technical expertise and practical experience managing hundreds of projects around the world means we can deliver a complete solution, managing your project from start to finish. Join the more than 5,000 organisations we have already helped, and let us offer you cost-saving and risk-reducing solutions based on international best practice and frameworks.

Visit [www.itgovernance.co.uk/consulting](http://www.itgovernance.co.uk/consulting) for more information.

## Penetration testing

Identify and mitigate your vulnerabilities before criminal hackers can exploit them. Our CREST-accredited penetration testing solutions can support your organisation's security by identifying vulnerabilities in your infrastructure, applications, wireless networks and people through our fixed-price penetration testing packages.

At the end of each engagement, you will receive a comprehensive report that clearly explains any issues we have identified from both technical and non-technical perspectives, how those issues affect your organisation, and recommendations for remediating them.

Visit [www.itgovernance.co.uk/penetration-testing-services](http://www.itgovernance.co.uk/penetration-testing-services) for more information.

## Software

Our sister company Vigilant Software develops industry-leading software tools designed to make meeting your security obligations and complying with privacy laws simple and affordable.

The CyberComply platform comprises six Cloud-based tools: Compliance Manager, the Data Flow Mapping Tool, the Data Protection Impact Assessment (DPIA) Tool, GDPR Manager, Incident Manager and vsRisk.

Visit [www.itgovernance.co.uk/shop/category/software](http://www.itgovernance.co.uk/shop/category/software) for more information.

## Endnotes


- <sup>1</sup> Grand View Research, “Bring Your Own Device Market Size, Share & Trends Analysis Report By Device (Smartphones, Tablets, Laptops), By End-Use (Mid-To-Large Sized Businesses, Small Businesses) And Segment Forecasts, 2012 - 2020”, <https://www.grandviewresearch.com/industry-analysis/bring-your-own-device-market>.
- <sup>2</sup> Industry Research, “Global Bring-Your-Own-Device (BYOD) Industry Research Report, In-Depth Analysis Of Current Status And Outlook Of Key Countries 2023-2028”, March 2023, <https://www.industryresearch.biz/global-bring-your-own-device-byod-industry-23044218>.
- <sup>3</sup> RightScale (acquired by Flexera in 2018), “RightScale State of the Cloud Report 2013”, July 2013, <https://www.slideshare.net/arms8586/rightscale-state-of-the-cloud-report-2013>.
- <sup>4</sup> Flexera, “Flexera 2022 State of the Cloud Report”, March 2022, <https://m3comva1.frb.io/uploads/docs/Flexera-State-of-the-Cloud-Report-2022.pdf>.
- <sup>5</sup> Alan Felstead and Darja Reuschke, “Homeworking in the UK: Before and During the 2020 Lockdown”, August 2020, <https://wiserd.ac.uk/publication/homeworking-in-the-uk-before-and-during-the-2020-lockdown/>.
- <sup>6</sup> Office for National Statistics (ONS), “Is hybrid working here to stay?”, May 2022, <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/ishybridworkingheretostay/2022-05-23>.
- <sup>7</sup> IAF, “IAF MD 26:2023 – Transition Requirements for ISO/IEC 27001:2022”, February 2023, [https://iaf.nu/iaf\\_system/uploads/documents/IAF\\_MD26\\_Issue\\_2\\_15012023.pdf](https://iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf).
- <sup>8</sup> International Organization for Standardization (ISO)/Technical Management Board (TMBG), “Annex SL Guidance documents”, October 2022, [https://www.iso.org/committee/54996.html?t=-Duqtv8H-DoUiDQTNcPLN0UhREpjaZ130Orwm4\\_WLY97n2yln9bsl\\_OpNRJZCit&view=documents#section-isodocuments-top](https://www.iso.org/committee/54996.html?t=-Duqtv8H-DoUiDQTNcPLN0UhREpjaZ130Orwm4_WLY97n2yln9bsl_OpNRJZCit&view=documents#section-isodocuments-top).
- <sup>9</sup> 3.4 of Annex SL defines a ‘management system’ as a “set of interrelated or interacting elements of an organization (3.1) to establish policies (3.5) and objectives (3.6), as well as processes (3.8) to achieve those objectives”. From “Annex SL Guidance documents”.
- <sup>10</sup> UKAS, “Who’s Accredited?”, accessed July 2023, <https://www.ukas.com/find-an-organisation/browse-by-category/?cat=2572>.
- <sup>11</sup> Terms and conditions apply, available at: <https://www.itgovernance.co.uk/training-faq-7>.







## IT Governance Ltd


---

 Unit 3, Clive Court, Bartholomew's Walk  
Cambridgeshire Business Park, Ely  
Cams., CB7 4EA, United Kingdom

 [www.itgovernance.co.uk](http://www.itgovernance.co.uk)

 +44 (0)333 800 7000

 [servicecentre@itgovernance.co.uk](mailto:servicecentre@itgovernance.co.uk)

 [/it-governance](https://www.linkedin.com/company/it-governance)

 [@ITGovernance](https://twitter.com/ITGovernance)

 [/ITGovernanceLtd](https://www.facebook.com/ITGovernanceLtd)