A Breakdown of Key ISO 2022 Updates and What They Mean For You

Everything you need to know about the ISO 2022 changes and how they affect your current program.

DRATA

drata.com

DRATA

A Breakdown of Key ISO 2022 Updates and What They Mean For You

After ISO published its 2022 updates, our team received countless questions on whether or not this influenced our customers' current work towards their audits. Fortunately, all certified organizations have until Oct. 31, 2025 to transition to the new 2022 revision. But new certification applicants may continue to be audited against the 2013 revision only until Oct. 31, 2023. In this guide, our team highlights a few key changes to help you update your program as you pursue or maintain compliance.

This guide was put together by compliance and cybersecurity risk management experts with extensive experience helping customers achieve ISO certification.

Here's what we'll cover:

DRATA

Meet the Experts

Troy Fine

Troy Fine is a 10-year former auditor, now Senior Manager of Cybersecurity Risk Management and Compliance at Drata. He advises customers on building sound cybersecurity risk management programs that meet security compliance requirements.

Troy is a CPA, CISA, CISSP, and CMMC Provisional Assessor. His areas of expertise include, GRC, SOC 2 audits, SOC 2+ examinations, CMMC, NIST 800-171, NIST 800-53, Sarbanes-Oxley Section 404 compliance, HITRUST, HIPAA, ISO 27001, and third-party risk management assessments.

Anthony Gagliardi

Anthony Gagliardi is Manager of Compliance at Drata. He advises customers on building sound cybersecurity risk management programs that meet security compliance requirements.

Anthony is a CPA, CISA, CISSP, and CMMC Provisional Assessor. His areas of expertise include, GRC, SOC 2 audits, SOC 2+ examinations, CMMC, NIST 800-171, NIST 800-53, Sarbanes-Oxley Section 404 compliance, HITRUST, HIPAA, ISO 27001, and third-party risk management assessments.

Richard Stevenson

Richard Stevenson is Manager of Cybersecurity Risk Management and Compliance at Drata. He advises customers on building sound cybersecurity risk management programs and security policies that meet security compliance requirements.

Richard is an AWS Certified Cloud Practitioner, CompTIA CySA+, and Shared Assessment Certified Third-Party Risk Assessor specializing in SOC 2, ISO 27001, NIST 800-53, NIST 800-171, SOX, HIPAA, third-party risk management, and enterprise risk management.

DRATA

What's New in ISO 27001:2022?

At first glance, the recently published ISO 27001:2022 looks like an entirely new standard which can feel overwhelming. Even just glancing through the table of contents, you'll see a change in formatting when compared to ISO 27001:2013.

While the International Organization for Standardization (ISO) did shift its focus and requires you to think differently about your ISO 27001 program, the fundamental difference is the standard's organization. Once you understand what's new in ISO 27001:2022, you'll realize that most of your current compliance program remains intact.

First, What Is ISO 27001:2022?

ISO 27001:2022 is the framework specifying the requirements an organization should use when establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

Intended to be applicable to companies of all sizes and across all industry verticals, the generic requirements include the information security risk assessment and treatment.

DRATA

Understanding the New Mindset

If you're an organization that's been following the ISO standard, a few quick notes here will help you understand the primary shift.

First, the standardization body no longer refers to ISO 27001 as a "standard," it consistently changes the word to "document." While this seems like a minor change, it's actually part of the larger refocus. The first place you see this change is in Note 2 under Subsection 6.1.3:

> **Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.**

In the 2013 publication, Note 1 reads:

> **Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.**

These two major mindset changes for ISO 27001:2022 are:

- Recognizing that information security is dynamic.
- Moving away from the "control objectives" language.

ISO considers 27001:2022 to create minimum baseline controls rather than a closed, comprehensive list.

Additionally, by removing the phrase “control objectives” from the entire document, ISO is moving away from the future focused “we hope that this control works as intended.” The controls are now focused on “this is what we actually have in place, and this is why we did this.”

A High-Level View of the Table of Contents

If you’re just opening up the new publication, the table of contents might seem like it’s adding several new sections under:

- Planning
- Support
- Performance Evaluation

Once you start digging into the standard and comparing the two side by side, the reality is that these changes just serve to highlight pre-existing content, making them more obvious and indicating that ISO believes they should be considered on their own.

What Do These Changes Mean for Your Compliance?

For the most part, ISO 27001:2022 changes very little. Only a few new controls have been added. However, it’s important to highlight one fundamental change surrounding compliance documentation.

DRATA

Everywhere that ISO 27001:2022 mentions documentation, the language now requires that: documented information shall be available.

The original 2013 language focus required that organizations: shall keep documented information.

The use of the word “availability” implies that companies should have the ability to provide the information when someone asks for it rather than just keeping it stored.

The Reorganization of ISO 27001:2022 Annex A

ISO 27001:2022’s changes don’t exist in a vacuum. ISO released 27001:2022, 27002:2022, and 27005:2022 all at the same time because they’re highly interconnected. The reorganization of 27001:2022’s Annex A corresponds directly to the reorganization of 27002:2022.

Instead of 14 categories of controls, 27002:2022 and 27001:2022 are now grouped into four categories, which ISO refers to as “themes”:

- Organizational Controls
- People Controls
- Physical Controls
- Technological Controls

DRATA

Organizational Controls

The organizational controls are defined first within the ISO 27002:2022. This section defines the higher level, governance-focused controls of the ISO 27001 framework. These set the stage for the more actionable controls defined within the other three themes.

When you sift through and compare the two documents, you'll notice that Organizational Controls aggregates the following under one heading:

- Management direction for information security
- Asset management
- Information classification
- Supplier relationships
- Access control
- Incident management
- Business continuity management
- Compliance with legal and contractual requirements

So what's new in ISO 27001:2022?

Although ISO rewrote many controls so that they would better align with its new mindset, it did add a few new controls:

- 5.7 Threat intelligence
- 5.23 Information security for use of cloud services
- 5.30 ICT readiness for business continuity

DRATA

Physical Controls

ISO categorizes controls as physical if they concern physical objects.

The Physical Controls section aggregates:

- Physical and environmental security
- Equipment

Only one new physical control was added, “7.4 Physical security monitoring.” All the other controls are exactly the same as in the 2013 publication.

Technological Controls

According to ISO, Technological Controls are the ones that concern technology. The Technological Controls section aggregates:

- System and application access control
- Operational procedures
- Redundancies
- Protection from malware
- Test data
- Technical vulnerability management
- Security in development and support processes
- Backup
- System and application access control
- Cryptography
- Technical vulnerability management

The changes to previous controls and all new controls really respond to the risks arising from digital transformation, cloud-based environments, and new privacy laws.

The new Technological Controls are:

- 8.9 Configuration management
- 8.10 Information deletion
- 8.11 Data masking
- 8.12 Data leakage prevention
- 8.16 Monitoring activities
- 8.23 Web filtering
- 8.28 Secure coding

Lastly, a few rewrites should also be highlighted.

For example:

- **8.16 Monitoring activities:** “anomalous behavior” responds to cloud risks
- **8.19 Installation of software on operational systems:** old “restrictions on software installation” more aligned to remote work and mobile devices
- **8.30 Outsourced development:** “direct” and “review” responds to third-party risks

DRATA

What's New in ISO 27002:2022?

> Clocking in at 152 pages, ISO 27002:2022 reads and feels like an entirely different document than ISO 27002:2013. ISO 27002:2022's changes highlight the International Organization for Standardization's (ISO's) shifting mindset.
>
> While most of the controls themselves remain the same, the document's organization and explanations highlight ISO's shifting mindset around the way companies should view security. Here's a peek at the changes between ISO 27002:2002 and ISO 27002:2013.

First, What Is ISO 27002:2022?

ISO 27002:2022 provides a set of generic information security controls that organizations use when establishing and maintaining an ISMS. Since the information security controls are based on internationally recognized best practices, organizations can implement them as listed or use them to develop organization-specific information security management controls.

Similarly, organizations can choose to use a completely different control set when implementing ISO 27001:2022 rather than using or customizing the controls listed in ISO 27002:2022.

DRATA

A High-Level View of the Table of Contents

The table of contents and the introduction help you understand the goals ISO has within the larger changes.

Before you even get into the meat of ISO 27002:2022, you notice a fundamental change within the table of contents. Whereas ISO 27002:2013 consisted of 14 control categories referred to as “domains,” ISO 27002:2022 streamlines this into four buckets, called “themes.”

↗ Themes:

- **Organizational:** everything not concerning people, physical, or technological controls
- **People:** concerning individuals
- **Physical:** concerning physical objects
- **Technical:** concerning technology

Introduction

While a large portion of the Introduction remains the same, you can start to see where ISO’s going by looking at some of the language changes:

- **Background and context:** Focus on the risk treatment requiring careful planning and attention rather than just the controls themselves.
- **Controls:** A new section defining a control as, “a measure that modified or maintains risk,” with an example that a policy maintains while compliance to a policy modifies.
- **Determining controls:** Greater focus on risk assessment and the need to balance resources/ investments with a control’s business impact.

Unlike the 2013 publication, ISO 27002:2022 highlights that organizations need to focus their attention on risk mitigation and management.

DRATA

Understanding the New ISO 27002:2022 Control Format

By focusing on control themes and attributes, ISO enables organizations to look at the same controls through multiple lenses.

Control Attributes

ISO associates each control with five attributes:

- **Control type:** Focused on when and how it modifies risk across Preventive, Detective, and Corrective.
- **Information security properties:** Defined by information characteristic(s) that it preserves across Confidentiality, Integrity, and Availability.
- **Cybersecurity concepts:** Aligned to the ISO TS 27110 cybersecurity framework across Identify, Protect, Detect, Respond, and Recover.
- **Operational capabilities:** Based on the practitioner's perspective of information security capabilities.
- **Security domains:** Viewed from the four information security domains across Governance and Ecosystem, Protection, Defense, and Resilience.

Control Layout

Based on the changes to the organization, ISO also created a new layout for each control consisting of:

- **Control title:** Control's short name
- **Attribute table:** Values for a control's assigned attributes
- **Control:** What the control is
- **Purpose:** Why the control matters
- **Guidance:** How to implement the control
- **Other information:** Additional text or references to related documents

The primary change that shows ISO's shifting mindset is that ISO 27002:2022 focuses on a control's "purpose" rather than outlining a "control objective."

An “objective” is an aim, something toward which you direct effort. Meanwhile, a “purpose” is the reason something exists or a goal to be obtained. By switching this language, ISO focuses on achieving and implementing a control for a reason rather than just something you put effort into or hope to do in the future.

What Are the New Controls Listed in ISO 27002:2022?

While there is significant overlap between the 2013 version and the 2022 version, ISO added 11 net new controls to the publication, mostly ones that respond to digital transformation and the evolving landscape of privacy regulations.

Organizational Controls

The new controls that ISO added are:

- **5.7 Threat intelligence:** Collecting and analyzing information related to information security threats.
- **5.23 Information security for use of cloud services:** Establishing processes for the acquisition, use, management, and exit from cloud services.
- **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.

Physical Controls

The new controls ISO included is:

- **7.4 Physical security monitoring:** Continuously monitoring for unauthorized physical premises access.

Technological Control

The new technological controls primarily respond to new privacy law requirements and risks arising from new types of technologies:

- **8.9 Configuration management:** Configurations, including security configurations, of hardware, software, services, and networks should be established, documented, implemented, monitored, and reviewed.
- **8.10 Information deletion:** Deleting information stored in information systems, devices, or other storage media when it's no longer needed.
- **8.11 Data masking:** Masking data according to access control and other topic-specific policies and business requirements while considering all applicable legislation.
- **8.12 Data leakage prevention:** Applying prevention measures to all systems, networks, and any other devices that process, store, or transmit sensitive information.
- **8.16 Monitoring activities:** Networks, systems, and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.
- **8.23 Web filtering:** Reducing exposure to malicious content by managing access to external websites.
- **8.28 Secure coding:** Applying secure coding principles to software development.

DRATA

ISO 27001:2022 vs. ISO 27002:2022

Compliance almost always feels like one of those alphabet soups that you ate when you were sick. You needed to eat, but it wasn't exactly what you wanted to eat regularly. If you're a business that needs to comply with the International Organization for Standardization (ISO) 27000-series, the different numbers and acronyms feels like that nourishing yet unexciting alphabet soup.

Understanding the critical differences between ISO 27001:2022 and ISO 27002:2022 helps you align your business objectives to your compliance goals.

DRATA

5 Critical Differences Between ISO 27001:2022 and ISO 27002:2022

Although the two documents work together, they have several significant differences.

Purpose

ISO 27001 outlines the foundational qualities that start by:

- Understanding your organization and its context.
- Understanding the needs and expectations of different internal and external stakeholders.
- Determining the ISMS's scope.

ISO 27002 supplements by outlining and detailing the controls that you will implement to support the way your ISMS addresses your information security risk. Additionally, it provides guidance around how to implement these controls.

Contents

As the purpose of each document drives the content, the information each one contains differs.

ISO 27001 defines seven clauses, which are broken into subclauses. The first three sections of the ISO 27001 are administrative information such as scope, definitions, and similar items and are not actionable by an organization implementing ISO 27001. The remaining clauses and their subclauses focus on how to establish, implement, and maintain an internal program based on processes, including:

- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Meanwhile, ISO 27002 contains the controls that support the processes outlined in ISO 27001. The document details the 93 controls that it separates according to four themes:

- Organizational
- People
- Physical
- Technological

Level of Detail About Controls

Although both documents discuss the information security controls, ISO 27001 only provides a very high level list in its Appendix A. ISO 27002 goes into far more detail, providing the following for each control:

- Short name for the control
- A table outlining the control's attributes
- What the control is
- Why you should implement the control
- How you should implement the control
- Additional explanations or references to other related documents

Applicability

When establishing an ISMS, every organization needs to incorporate ISO 27001's requirements. The document specifically explains under Scope:

> **Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.**

However, the fundamental basis of your ISO 27001 implementation is your organization's risk assessment and treatment.

Based on how your organization defines risk and chooses to treat risk, you may not need to implement every single ISO 27002 control. ISO 27002:2022's Annex A exists to show organizations how they can use attributes so that they can create different views of controls. In section Annex A, section A.2, ISO notes:

> **Organizations can discard the examples of attributes proposed in this document and create their own attributes with different values to address specific needs in the organization. In addition, the values assigned to each attribute can differ between organizations.**

While organizations need to have all the components of an ISMS listed in ISO 27001, they can implement controls based on ISO 27002:2022 in a way that makes sense for their unique business and security needs.

Certification

ISO certifications only apply to an organization's ability to conform to ISO 27001.

To achieve an ISO 27001 certification, you need to:

- Create a project plan that defines responsibilities, oversight, and milestone management.
- Define the ISMS's scope by determining whether it will encompass the entire organization or focus on a single department/system.
- Perform a risk assessment that focuses on identifying risks applicable to the scope you defined in step 2 and how to mitigate those risks.
- Engage in a gap assessment that identifies current controls and determines additional controls needed to fully mitigate risk.
- Design, implement, and document policies and controls.
- Document and collect evidence proving that policies and controls function as intended.

ISO 27002 doesn't have a certification because it's just a list of optional controls. However, most organizations will use ISO 27002 for steps four through six of the certification process.

DRATA

How Do ISO 27002:2022 Controls Support ISO 27001 Compliance?

Understanding how the documents work together is easier when you have a concrete example.

ISO 27001 ISMS Requirement

Within Clause 6 Planning, Subsection 6.2 states:

When planning how to achieve its security objectives, the organization shall determine:

- What will be done.
- What resources will be required.
- Who will be responsible.
- When it will be completed.
- How the results will be evaluated.

This section is about planning the control implementations that mitigate risk as determined within the risk assessment. To determine the controls, you look at ISO 27001's Annex A.

Within Annex A, you'll find the following control:

> **5.9 Inventory of information and other associated assets: An inventory of information and other associated assets, including owners, shall be developed and maintained.**

DRATA

ISO 27002:2022

All the details about control 5.9 are outlined in ISO 27002.

27002 defines the purpose as:

> **To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.**

The Guidance section provides additional information including:

- Identifying assets
- Categorizing them by importance based on the type of data associated with them
- Keeping the inventory accurate and updated
- Conducting regular reviews
- Automatically enforcing updates when installing, changing, or removing an asset
- Detailing the asset owner duties

Control Implementation

An example of the control implementation would be an asset inventory that contains a list of all assets listed as high, medium, and low risk based on the data they process, manage, or store complete with the person responsible for managing and updating it, the date of the most recent entry, and the operating system/ software/firmware version.

DRATA

What's New in ISO 27005:2022?

The changes that the International Organization for Standardization (ISO) made in its recently published ISO 27001:2022 created a ripple effect across the 27000-series. Since ISO 27001:2022 is the foundation upon which ISO 27002:2022 and ISO 27005:2022 rest, ISO updated these publications to reflect its evolving approach to evaluating and managing information security risk.

Although the primary underpinnings of risk analysis and treatment remain the same, you should understand a few key differences between ISO 27005:2018 and ISO 27005:2022.

First, What is ISO 27005:2022?

The ISO 27005 publication assists organizations who seek to comply with ISO 27001:2022 by providing guidance about how to perform information security risk management activities. Specifically, ISO 27005 enables organizations of all types, sizes, and industry verticals to engage in the information security risk assessment and treatment process.

What Are the Primary Differences Between ISO 27005:2018 and ISO 27005:2022?

A quick glance at the publication's table of contents gives you insight into the changes. Although 10 pages longer than its predecessor, ISO 27005:2022 is divided into 10 clauses and one annex compared to the 27005:2018's 12 clauses and six annexes.

Most of the changes focus on aligning ISO 27005's terminology, structure, and guidance text to the updated ISO 27001:2022 document. However, if you've been through the ISO compliance process in the past, you should note the following larger changes:

- Introduction of risk scenario concepts
- Difference between event-based and asset-based risk identification approaches

What Is a Risk Scenario?

ISO 27005:2022 defines a risk scenario as a sequence or combination of events that lead from an initial cause to an unwanted consequence.

An event is an occurrence or change to a set of circumstances that can:

- Be expected and but not happen.
- Be unexpected and does happen.
- Have more than one occurrence, cause, or consequence.

A consequence is the outcome of an event, affecting objectives that can:

- Be certain or uncertain.
- Have positive or negative effects.
- Directly or indirectly affect objectives.
- Be expressed qualitatively or quantitatively.
- Escalate through cascading and cumulative effects.

DRATA

What Are Event-Based and Asset-Based Risk Identification Processes?

Although ISO 27005:2022 discusses the two risk identification approaches, it also points out that they complement each other.

Event-Based Risk Identification

An event-based risk identification approach evaluates events and consequences by:

- Identifying strategic scenarios.
- Considering risk sources.
- Reviewing how risk sources use or impact interested parties.
- Understanding how interested parties reach their objectives.

Asset-Based Risk Identification

An asset-based approach evaluates operational scenarios by inspecting assets, threats, and vulnerabilities to identify and assess risks by considering:

- Primary assets by type and priority.
- Supporting assets by type and priority.
- Dependencies between primary and supporting assess.
- Interactions between assets, their risk sources, and the organization's interested parties

Combining Event-Based and Asset-Based Processes

The different risk identification processes focus on different basic requirements for the interested parties. Interested parties are defined as internal or external people who perform or are involved in information security risk management, including information security management system (ISMS) professionals and risk owners.

Organizations can use both approaches to describe the same risk scenario from different perspectives. Consider a risk scenario where malicious actors gain access to personally identifiable information using a stolen password.

- **Event-based approach:** reviews at a high level, the consequences the scenario would have on the internal and external interested parties.
- **Asset-based approach:** reviews the steps the malicious actors take from obtaining the password through lateral movement to gaining access to the data.

Whereas an event-based risk identification approach focuses on the management level objectives and impact, the asset-based approach follows the actor's attack path through interconnected assets.

Where Does ISO 27005:2022 Fit Into an Organization's ISO Compliance Program?

Like most compliance publications, ISO 27005:2022 is one of several documents that you need to understand when putting together your compliance program.

DRATA

Although the documents detail different aspects of your compliance posture, they all reference one another:

- ISO 27001:2022 defines the processes and controls required for an ISMS.
- ISO 27002:2022 provides implementation guidance for the information security controls listed in ISO 27001:2022's Annex A.
- ISO 27005:2022 details how you define and apply ISO 27001:2022's information security risk assessment process in Clause 6.1.2 that treats information security risks as required by Clause 6.1.3.

In addition to the documents listed above, ISO also publishes additional supplementary guidance within the same family. ISO 27003 covers additional guidance for implementing the ISMS and required processes defined within ISO 27001, ISO 27004 provides guidance on monitoring and measuring the performance of the ISMS, and ISO 27006 provides guidance for certification bodies performing ISO 27001 audits.

Not all of these documents have been updated to reflect the changes in ISO 27001:2022, but ISO is currently working to create the new versions. While these documents are not required, they can assist with implementing certain portions of the ISMS, like ISO 27005:2022 does with Clauses 6.1.2 and 6.1.3.

Documenting the ISO 27005 Risk Treatment Process

All three updated documents focus more heavily on documentation than their predecessors did. While ISO 27005:2018 often implied certain documentation, the 2022 publication formally outlines documentation requirements in the implementation guidance sections of Clause 10.4.2 "Documented information about processes" and Clause 10.4.3 "Documented information about results."

Documented information about the risk treatment process should contain:

- The method used to select appropriate information security risk treatment options.
- The method used to determine necessary controls.
- How ISO 27001:2022 Annex A was used to determine no necessary controls were accidentally overlooked.
- How the risk treatment plan was produced.
- How risk owners provide approval.

Additionally, the updated publication formalizes the internal or external audit function's risk treatment plan review in Clause 10.7 "Corrective action," noting that audits may detect nonconformities that require you to revise the risk treatment plan.

DRATA

Automation and Continuous Monitoring for ISO Certification

While the changes appear dramatic, the number of new controls in these updates is limited. ISO's reorganization and repositioning are the underlying changes. Whether you're being audited against the 2022 updates or their predecessors, Drata enables you to accelerate your audit readiness by providing controls pre-mapped across multiple frameworks, giving you the speed and agility needed for a robust ISO compliance program.

With our automated asset inventory, pre-built risk self-assessments, endpoint monitoring tool, and built-in security training you can streamline and document all your ISO compliance activities, reducing costs and time by eliminating manual tasks.

Our platform continuously monitors your environment, giving you real-time visibility into your compliance posture. Using our single source of audit documentation, you have on-demand access to everything you need, including formal documentation, employee acceptance, version history, evidence collection, asset and personnel tracking, and access control workflow automation.

If you're struggling to determine what controls you should implement, you can access our compliance experts who will answer the questions that get you compliant and help you stay compliant.

Book a demo today and start achieving your ISO compliance goals.