ISO 27002 DIS

Its Significance & What to Expect

The adoption of ISO 27001 certification has continued to grow over the years, both nationally and internationally. As management system standards go, ISO 27001 is unique in that it includes a control set for organizations implementing or maintaining an information security management system (ISMS) to consider when addressing their information security risk. That control set, known as Annex A of ISO 27001 and expanded upon in ISO 27002, is about to change.

schellman
Quality, above all. | WHITEPAPER

When did the process start?

Two years ago, the ISO/IEC JTC 1 / SC 27 committee was tasked with initiating and undertaking the revision to ISO/IEC 27002 (ISO 27002). Subject matter experts from around the globe, as well as national delegations, have since participated in this multi-year endeavor—one that has demanded a particularly rigorous effort due to the importance of ISO 27002.

What is available now & when will the final version be published?

In early 2021, the draft international standard (DIS) was published for final review and comment—it can currently be purchased at the ISO Standards Store. Though this is not the final version, which is expected to be formally published later this year—or early next year at the very latest—it is expected and assumed that most of the content in this DIS will find its way into what will be the new, formal standard for ISO 27002. When this new version is in fact published, the 2013 version of ISO 27002 will thusly be replaced and then cancelled.

What has changed between the 2013 version & the DIS?

Title

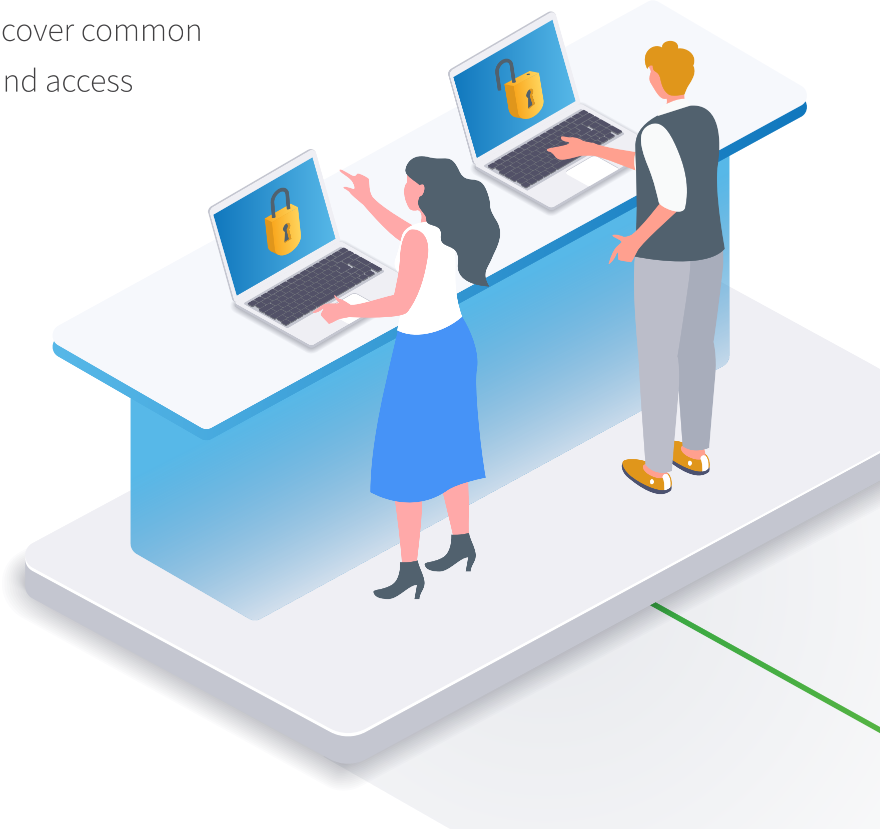
Perhaps the foremost change, the phrase “Code of Practice” has been removed from the title of the DIS to better reflect its purpose as a reference set of information security controls. The intention of ISO 27002 has always been to help organizations ensure that no necessary control has been overlooked when designing and implementing an information security management system (ISMS). This purpose is the same irrespective of the intended usage of this document, and the guidance given for individual controls is based on internationally recognized best practice.

> The intention of ISO 27002 has always been to help organizations ensure that no necessary control has been overlooked when designing and implementing an information security management system (ISMS).

What has changed between the 2013 version & the DIS? (cont.)

Structure

Aside from the name change, one large material difference seen in the DIS regards the structure of the control set within ISO 27002—a change likely most critical to those with an existing or planned ISMS. While the 2013 version features 14 control domains that cover common information security areas like incident response, operations security, and access control, the DIS instead names just four control categories that include Organizational (Clause 5), People (Clause 6), Physical (Clause 7), and Technological (Clause 8).



What has changed between the 2013 version & the DIS? (cont.)

Note the differences in the tables below, where control counts are included in parentheses:

ISO/IEC 27002:2013			
5 Information security policies (2)	9 Access control (14)	13 Communications security (7)	16 Information security incident management (7)
6 Organization of information security (7)	10 Cryptography (2)	14 System acquisition, development and maintenance (13)	17 Information security aspects of business continuity management (4)
7 Human resources security (6)	11 Physical and environmental security (15)		
8 Asset management (10)	12 Operations security (14)	15 Supplier relationships (5)	18 Compliance (8)

ISO/IEC 27002 DIS			
5 Organizational (37)	6 People (8)	7 Physical (14)	8 Technological (34)

What has changed between the 2013 version & the DIS? (cont.)

Moreover, the DIS introduces the concept of themes, i.e., those four clauses above. The categorization approach is as follows:

- People if they concern individual people
- Physical if they concern physical objects
- Technological if they concern technology
- Organizational if not included in any theme above

What has changed between the 2013 version & the DIS? (cont.)

The DIS also includes the concept of views and attributes to differentiate controls based on different perspectives—e.g., control type (attribute) as preventive or detective (view). Further details on this approach can be found in Annex A of the DIS, which organizations can use to improve the application of these controls and enhance their risk assessment results. As this organizational structure demonstrated in the DIS allows for association to common control concepts, this new method should avoid any duplication that may have been present in the 2013 version, given that with the multiple control domains, common controls can be associated to different domains.

Control Set

The DIS also makes a significant change regarding the total control count, which decreases from the 114 in the 2013 version to 93. Though that seems like a 21-control swing, only one control was actually deleted from the 2013 set, per the mapping in the DIS to the 2013 version—instead, multiple controls from the 2013 version were consolidated into one control in the DIS. 11 new controls were also introduced to bring the total to 93; generally, these controls are based on changes in the technological landscape that have occurred since the 2013 publication.

What has changed between the 2013 version & the DIS? (cont.)

High Level Comparison			
Consolidated Controls			
5.1 – Policies for information security	**5.1.1, 5.1.2**	6.8 – Information security event reporting	**16.1.2, 16.1.3**
5.8 – Information security in project management	**6.1.5, 14.1.1**	7.2 – Physical entry controls	**11.1.2, 11.1.6**
5.9 – Inventory of information and other associated assets	**8.1.1, 8.1.2**	7.10 – Storage media	**8.3.1, 8.3.2, 8.3.3**
5.10 – Acceptable use of information and other associated assets	**8.1.3, 8.2.3**	8.1 – User endpoint devices	**6.2.1, 11.2.8**
5.14 – Information transfer	**13.2.1, 13.2.2, 13.2.3**	8.8 – Management of technical vulnerabilities	**12.6.1, 18.2.3**
5.15 – Access control	**9.1.1, 9.1.2**	8.15 – Logging	**12.4.1, 12.4.2, 12.4.3**

What has changed between the 2013 version & the DIS? (cont.)

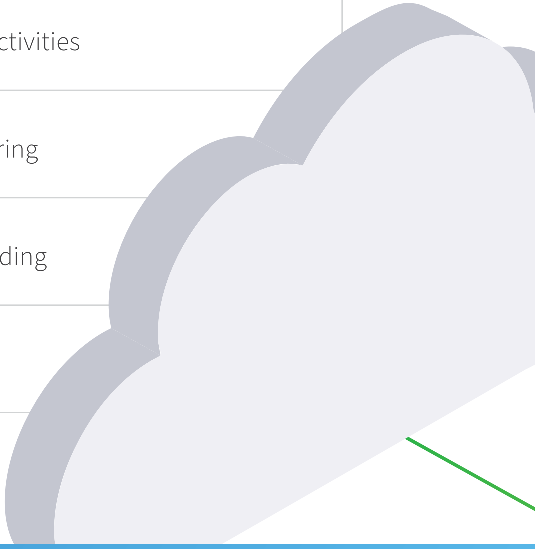
High Level Comparison

Consolidated Controls (cont.)

5.17 – Authentication information	**9.2.4, 9.3.1, 9.4.3**	8.19 – Installation of software on operational systems	**12.5.1, 12.6.2**
5.18 – Access rights	**9.2.2, 9.2.5, 9.2.6**	8.24 – Use of cryptography	**10.1.1, 10.1.2**
5.22 – Monitoring, review and change management of supplier services	**15.2.1, 15.2.2**	8.26 – Application security requirements	**14.1.2, 14.1.3**
5.29 – Information security during disruption	**17.1.1, 17.1.2, 17.1.3**	8.29 – Security testing in development and acceptance	**14.2.8, 14.2.9**
5.31 – Identification of legal, statutory, regulatory and contractual requirements	**18.1.1, 18.1.5**	8.31 – Separation of development, test and production environments	**12.1.4, 14.2.6**
5.36 – Compliance with policies and standards for information security	**18.2.2, 18.2.3**	8.32 – Change management	**12.1.2, 14.2.2, 14.2.3, 14.2.4**

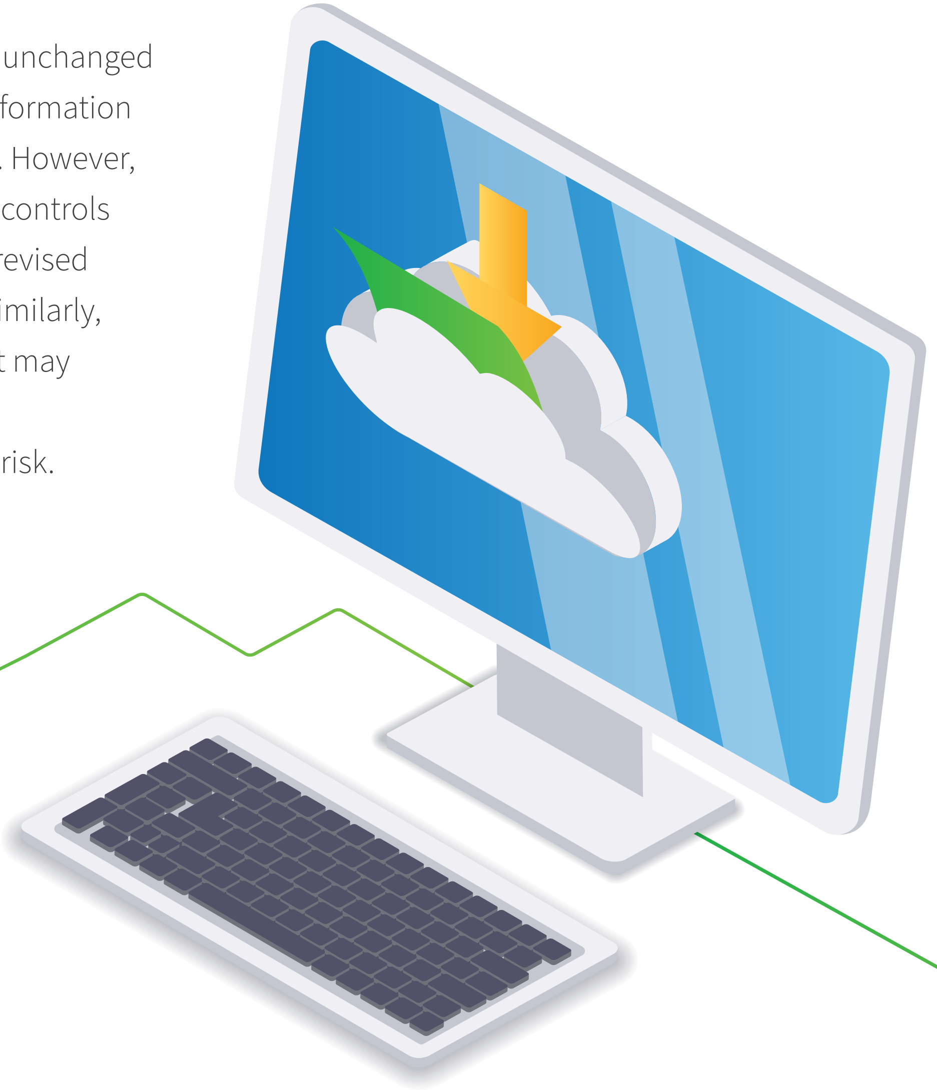
What has changed between the 2013 version & the DIS? (cont.)

High Level Comparison	
Removed Controls	
11.2.5 – Removal of assets	
New Controls	
5.7 – Threat intelligence	8.11 – Data masking
5.23 – Information security for use of cloud services	8.12 – Data leakage prevention
5.30 – ICT readiness for business continuity	8.16 – Monitoring activities
7.4 – Physical security monitoring	8.22 – Web filtering
8.9 – Configuration management	8.28 – Secure coding
8.10 – Information deletion	



What hasn't changed?

Despite these major differences, a number of controls remain unchanged from their 2013 versions within the DIS, including those like information backup, clock synchronization, and outsourced development. However, it is important to note that while the general concept of these controls may be the same, the actual control wording may have been revised to reflect what the best practice is for that control presently. Similarly, the implementation guidance relevant to that control concept may have been updated as well, in order to ensure that the control implementation considers current technological and process risk.



Will the new revision of ISO 27002 impact ISO 27001?

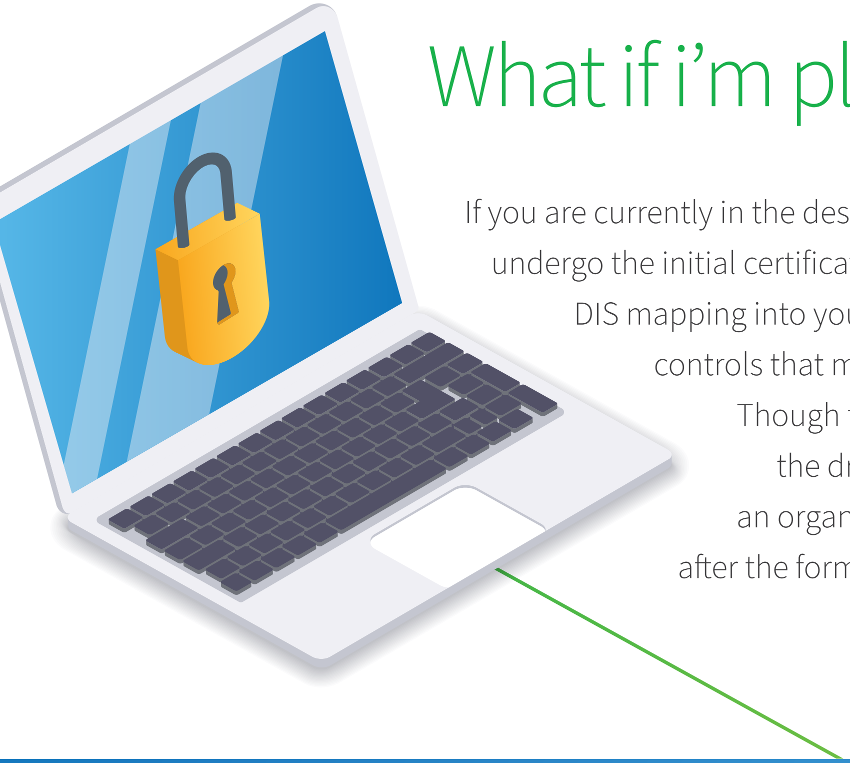
Organizations familiar with ISO 27001 understand that Annex A of the current version of ISO 27001 is essentially the control set from ISO 27002. But as the upcoming revision of ISO 27002 will replace and cancel the previous 2013 version—including its related control set—this will also in effect render Annex A of ISO 27001 obsolete as well. Due to such implications, it is very likely that, upon formal publication of the new ISO 27002, Annex A of ISO 27001 will also be amended to again mirror this new control set in order to avoid having a discrepancy between the two standards.

In fact, ISO is in the process of forming a specific team to assess the impact of this upcoming change on ISO 27001-certified organizations. ISO is very aware that all such organizations are interested parties regarding the ISO 27002 revision, and the governing body remains dedicated to ensuring that the market impact is minimal. As such, the expectation is that a formal communication will be issued by ISO noting the changes and how they will incorporate into an ISMS, along with potential timeline impacts and other supporting guidance.

Still, there will be a necessary effort on the part of each organization to ensure that a revised SOA, based on the new version of ISO 27002, is suitable to support the ISMS; however, with the mapping of the DIS to the 2013 version of ISO 27002, the exercise should not be seen as starting from scratch.

What does this mean for organizations currently certified against ISO 27001?

If you currently maintain a certified ISMS, you are not required to do anything at this time. As noted above, the DIS is the draft version of what will eventually be the final version once issued, and further modifications are still possible prior to formal publication. Still, acquiring a copy of the current DIS and including any possible impact and related migration effort into your project management process would be recommended.



What if i'm planning for initial certification?

If you are currently in the design or implementation phase of your ISMS and are looking to undergo the initial certification later in 2021 or early 2022, you may want to incorporate the DIS mapping into your SOA. It would also be prudent to take into consideration any new controls that may be introduced as a component of the revision to ISO 27002. Though the DIS is not the final version of what will be published, utilizing the draft control set and related mapping to 2013 will only better prepare an organization for certification if their external audit is planned to occur after the formal publication of the revised ISO 27002 standard.

How will this impact extended standards like ISO 27017, ISO 27018, ISO 27701, & others that rely upon ISO 27002?

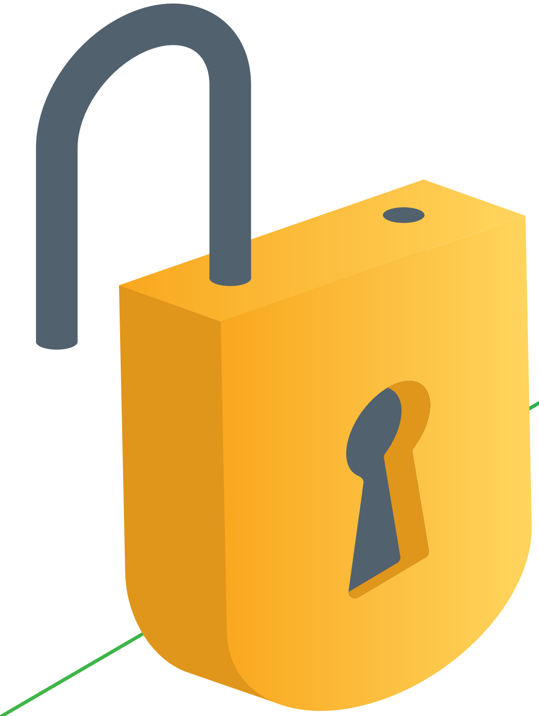
Currently, extended standards like ISO 27017, ISO 27018, and ISO 27701 have not been formally discussed with regard to the ISO 27002 revision. Each of these standards includes additional implementation guidance based on controls within the 2013 version of ISO 27002, and that implementation guidance will likely remain unchanged; however, the association to the ISO 27002 control will be materially impacted, specifically if the control has been consolidated with other controls. And in the case of ISO 27017, which includes extended controls within the current control domain structure of the 2013 version of ISO 27002, those previous control domains will no longer exist, requiring—at minimum—a new structure for ISO 27017.

It's important to note that the intent of these extensions would still remain relevant, and assessments against them will continue. Though it may possibly mean a more complex mapping—e.g., ISO 27017 to ISO 27002:2013 to ISO 27002:2021 to ISO 27017—to ensure that all implementation guidance and additional controls are considered and implemented, the revision to ISO 27002 will not, or should not, prevent an organization that currently or plans to include these extended standards from being assessed against them.

Where does the situation stand right now?

ISO/IEC JTC 1 / SC 27 is planning on conducting additional meetings between now and the eventual publication date of the revision to ISO 27002. With any international standard revision, there are specific protocols that have to be performed, including required additional assessments and approval per the proper authoritative chain. The expectation is that the revised ISO 27002 standard will be issued in Q4 of 2021, and, once published, it will be part of any external audit assessment for an ISMS that includes ISO 27002 as its control set.

Planning and preparation are key to any management system, and Schellman encourages all currently certified organizations or those implementing an ISMS to start this phase as soon as possible—that includes performing gap analysis, incorporating the transition into the project and risk management processes, as well as ensuring management themselves has transparency into this transition as part of the review process.



Over the next several months, as additional information becomes public, Schellman will be sure to provide updates and communicate relevant information to our clients and the market.

CLICK FOR MORE INFO

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000
Outside of the United States, please dial: +1.813.288.8833