SPECTRE

ADVISORY

ISO/IEC 27002:2022

The new era of security controls?

Introduction

When implementing an Information Seucrity Management System based on ISO/IEC 27001:2013, one of the most important choices to make is which risk mitigating measures are the most applicable for the organization. Throughout the information security industry, there are many standards a company can try to implement as control framework but only a few of them are as controversial as ISO/IEC 27002. Where the technical cyber defense specialists state that this "old" standard is not adequate for the current challenges, the standard is so well known amongst information security specialists that most of them know it by heart. The new version of ISO27002 will rock the industry and we will try to briefly clarify the new structure already.

ISO27002:2022

The last major update of the ISO/IEC 27002 standard dates from October 2013 when the previous version of 2005 was withdrawn. (ISO.org, 2013) We have seen small updates in 2014 and 2015 but these didn't have a serious impact on the content of the standard and were published as corrigenda within the official 2013 standard. This means that the latest version is already 8 years old. With the cyber- and information security landscape evolving so rapidly, it was time to provide a new and heavily modernized version of the ISO control framework to provide information security professionals with adequate tools to tackle the modern challenges. Recent vulnerability outbreaks like Log4J have proven that a flexible control framework, including amongst others incident response and patch management, is necessary for a comprehensive security approach. The biggest change in the new version is that the new ISO/IEC 27002:2022 provides organizations with the freedom to develop their own and risk-based security management guidelines.

The current publishing date for the ISO/IEC 27002:2022 version is 02/22 based on ISO.org.

How Spectre Advisory can help?

Starting or changing the setup of an ISO implementation to achieve a higher security maturity level or even certification might seem a daunting task that will put a lot of stress on your security team. Spectre Advisory is able to assist you in the different aspects of a certification track.

Whether it is providing guidance or executing tasks, together with your team we can get you and your organization on track for certification. Spectre Advisory will:

- Help you with the design and scoping of your security management system;
- Reduce the time spent on documentation and certification preparation tasks;
- train your team to increase their overall knowledge of information security;
- act as a Center of Excellence that you can contact when in doubt.
- Setup the necessary security awareness training and testing to increase the resilience of all employees, including the management board.

Don't hesitate to contact us if you have any questions. Our experts will gladly advice you on the certification cycle and how we can help you in your specific situation.

What will change in the 2022 version?

To provide you with the most important changes, we summarized these in a few bullets:

- Change in overall setup from a “code of practice” to an “Information Security Control overview”
- Less restrictive but more as guidance to allow risk-based decision making
- Addition of attributes that allow easy filtering and referencing
- 14 clauses are changed into 4 main themes
- Decrease in amount of controls from 114 to 93
    - 1 control removed (removal of assets)
    - 11 new controls
- Clear and documented link to other frameworks

The ISO/IEC 27000 family

This short introduction on the rest of the ISO/IEC 27000 family is necessary to provide some context when writing on the new ISO/IEC 27002 standard. The ISO/IEC 27000 series are a set of public standards detailing the industry good practices for organizations to improve their information security. All of the standards in the 27000 series are based on the implementation of an Information Security Management System as described in the ISO/IEC27001 standard. The implementation of an ISMS and the different steps that are to be taken are described in detail in the other standards. Due to the specific nature of some sectors, sector-specific guidelines were developed and published.

As there are over 45 standards in the 27000 series, we only included a brief summary of the most important ones divided in their respective categories. Overall, there are four types of standards within the 27000 series:

- Standards **describing an overview** and terminology
- Standards **specifying requirements**
- Standards describing **general guidelines**
- Standards describing **sector-specific guidelines**

Describing an overview and terminology

ISO/IEC 27000:2018

Introduces Information Security and the ISO27000 series including an overview of the different standards and serves as a glossary for the entire ISO27000 series.

Standards specifying requirements

ISO/IEC 27001:2013

Contains the requirements to which an organization must adhere when implementing an Information Security Management System. These requirements will be checked by the external auditor when applying for a certification. [This is the only standard (for regular organizations) that allows for certification]

ISO/IEC 27006:

Contains the requirements for organizations that act as accredited audit and certification bodies for Information Security Management System implementations.

ISO/IEC 27701

This standard is an extension to the ISO/IEC 27001:2013 standard containing the requirements for organizations to setup a Privacy Management System in order to methodically comply with the relevant privacy-based regulations.

Standards describing general guidelines

ISO/IEC 27002

Details the Code of practice for information security controls containing the expected information security control framework for organizations pursuing an ISO/IEC 27001:2013 certification.

ISO/IEC 27005

Describes how to setup and conduct an information security risk assessment in accordance with the requirements of the ISO/IEC 27001:2013 standard. This also includes the complete Information security risk management process.

ISO/IEC 27100

Describes cybersecurity and other relevant concepts, linking cybersecurity to information security, in the context of an Information Security Management System, finally bridging the gap between the technical and non-technical domain of security.

Standards describing sector-specific guidelines

ISO/IEC 27011

Defines guidelines supporting the implementation of information security controls in telecommunications organizations.

ISO/IEC 27017

Defines guidelines for the implementation of information security controls applicable to the provision and use of cloud services by providing additional controls (including guidance) and additional implementation guidance for relevant ISO/IEC 27002:2013 based controls.

Many of the standards in the ISO27000 series rely on the ISO/IEC 27002:2013 standard so they will need changing and some of these are already started development. The most important one to change is the ISO/IEC 27001:2013 that will also get a new version based on the new ISO/IEC27002:2022. The requirements for an ISMS are not expected to change drastically but all the references to the control framework will definitely need an update. This update to the standard is expected to follow the publishing of the new ISO/IEC 27002:2022 standard.

The new themes

The old ISO/IEC 27002:2013 standard was created based on 14 clauses that contained the specific controls when implementing an ISO/IEC 27001:2013 based Information Security Management System (ISMS). The new ISO/IEC 27002:2022 standard is split up in four themes that handle people-based, physical-based, technological-based, and organizational-based controls.

ISO/IEC 27002:2013			
A5. Information security policies (02)	A6. Organization of information security (07)	A7. Human resource security (06)	A8. Asset management (10)
A9. Access control (14)	A10. Cryptography (02)	A11. Physical and environmental security (15)	A12. Operations security (14)
A13. Communications security (07)	A14. System acquisition, development and maintenance (13)	A15. Supplier relationships (05)	A16. Information security incident management (07)
A17. Information security aspects of business continuity management (04)	A18. Compliance (08)		

ISO/IEC 27002:2022			
5. organizational controls (37)	6. People controls (08)	7. Physical controls (14)	8. Technological controls (34)

Where the 2013 version contained 114 controls, the 2022 version only contains 93. This doesn't mean that some requirements were left out but many of the very general controls in the 2013 version are merged into one control and 11 new controls were added. These controls are added as they represent the new developments in the cyber- and Information security industry. Due to the holistic nature of the standard and the fact that the new manner of describing the controls leaves the organization the possibility to define their own proper control implementations, this new ISO/IEC 27002:2022 standard is able to easily adapt to changing operational situations.

The new ISO/IEC 27002:2022 controls are comprised of:

5.7 Threat intelligence
To provide awareness of the threat environment that can impact the organization so that the organization can take appropriate mitigation actions.

5.23 Information security for use of cloud services
To specify and manage information security for the use of cloud services.

5.30 ICT readiness for business continuity
To ensure the availability of the organization's information and other associated assets in the event of a disruption.

7.4 Physical security monitoring
To detect and deter unauthorized physical access.

8.9 Configuration management
To ensure hardware, software, services, and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

8.10 Information deletion
To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory, and contractual requirements for data deletion.

8.11 Data masking
To limit the exposure of sensitive data including personally identifiable information, and to comply with legal, statutory, regulatory, and contractual requirements.

8.12 Data leakage prevention
To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

8.16 Monitoring activities
To detect anomalous behavior and potential information security incidents.

8.22 Web filtering
To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

8.28 Secure coding
To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

ISO/IEC 27002:2022 attributes

The second biggest change, next to the rework of the clauses, is the definition of attributes to every control that can be used by organizations to create a multitude of views of the different controls. In the implementation of a control framework, it is important to be able to provide a clear overview to all stakeholders and to be able to balance out the implementation efforts.

There are five categories of attributes that are defined for each of the controls.

Overview of ISO/IEC 27002:2022 attributes	
Attribute	**Elements**
Control types	Preventive, detective, corrective
Information security properties	Confidentiality, integrity, availability
Cybersecurity concepts	Identify, protect, detect, respond, recover
Operational capabilities	Governance, Asset management, Information protection, Human resource security, physical security, system and network security, application security, secure configuration, identity and access management, threat and vulnerability management, continuity, supplier

	relationship security, legal and compliance, information security event management, security assurance
Security domains	governance_and_ecosystem, protection, Defence, Resilience

The full matrix of the attributes connected to the controls is also included in the ISO/IEC 27002:2022 standard as an overview to allow easy filtering or sorting of the controls.

What to do next?

The most important thing to do is to get as much information as possible on this new standard to analyze the impact of the new ISO27002:2022 standard on your organization. With this overview document, you already have an initial view on the new standard but this does not provide enough insight to perform a holistic analysis. You can wait for the new standard to be published or already buy the draft standard (DIS 27002) from your accreditation body.

It is nevertheless important to take into account that the requirements for an existing ISMS will not change overnight but that under normal circumstances a transition period is granted depending on your certification cycle. This means that you will get 2 to 3 years to adapt to the new standard when you have an active Information Security management system.

We recommend to adopt the new standard as soon as possible as this will give you an adequate amount of time to transition into the new reporting but will also prove to your customers that you are keeping track of new developments in the information security industry.

Below you can find a basic overview of the steps that you will need to take to adopt the new ISO/IEC 27002:2022 standard based on the ISO27001 requirements. This list is neither mandatory nor limiting and only aims to provide you with a general guidance.

Steps to take when transitioning to the new standard		
Clause	**Attention point**	
4. Context of the organization	(4.3)	Maybe this is a good time to review the scope of your ISMS?
5. Leadership	(5.2) (27002)	Update your Information Security Policy Update the different policies to include the references to the correct standard
6. Planning	(6.2) (6.1.3)	Update the risk treatment methodology to incorporate the new information security control references Update the Statement of Applicability
7. Support	(7.3) (7.5.2)	Update the security awareness training and provide a communication to you employees on the changes in documentation Update the references in other related documentation to ensure no broken links
8. Operation	(8.2)	Review your risk assessment tooling if specific controls are used
9. Performance evaluation	(9.2)	Update the internal audit plan in accordance to the new standard
10. Improvement	The adoption of the new ISO/IEC 27002:2022 standard can be used as proof of continual improvement towards both the internal and external auditor.	

The road to success

Changing the security control framework, being voluntary or mandatory, will have a serious impact on your team on an operational level. Updating all the mandatory documentation, in combination with the assessment of current state maturity of the newly documented controls, will take a lot of time. Spectre Advisory can support you in transitioning between the different standards using proven tools and techniques.

Why work with Spectre Advisory?

Through the expertise of our experts in implementing and auditing ISO/IEC 27001:2013 based Information Security Management Systems, we are able to offer you and your organization the advice and operational support with the implementation or optimization of your ISMS. We can provide you with an effective and efficient approach that is specific to your company based on its industry, size and business objectives. We will assist and guide you through the entire process of the implementation and help you to integrate information security governance into the DNA of you company.

Don’t hesitate to contact us with any questions and we will happily provide you with a made-to-measure solution.

SPECTRE
ADVISORY

Nick Van den Bergh
Managing Director

nick.vandenbergh@spectre-advisory.com

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Spectre Advisory product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Spectre Advisory, suppliers or licensors. Spectre Advisory services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Spectre Advisory to its customers are controlled by Spectre Advisory agreements, and this document is not part of, nor does it modify, any agreement between Spectre Advisory and its customers.