transcendent group GOVERNANCE RISK COMPLIANCE

TRANSCENDENT GROUP INSIGHT

UPDATES TO ISO/IEC 27002 – WHAT YOU NEED TO KNOW

ISO recently published a draft version for the final balloting of the soon to be updated ISO/IEC 27002 standard.

In short, the updated version consolidates the security controls of the standard in four new categories; (1) organizational controls, (2) people controls, (3) physical controls and (3) technological controls.

Also, a set of new controls are introduced, and a couple are modified or merged – all with the objective of supporting organizations to adapt to the everchanging risk landscape of the modern information security environment.

Despite the document being labelled as a draft; it has been reviewed and commented on by the national bodies in several review rounds and is thus unlikely to receive any major changes. The current ballot round is due in the end of April and the target release date for the final version is late 2021.

In the following sections we are going to be focusing on the most significant changes and how your organization should be preparing for them.

What is ISO/IEC 27002?

ISO/IEC 27002 is one of the most well-known standards and guidelines for organizations of all types and sizes to be used as a best practice reference for identifying and implementing information security controls to manage information security risk.

The standard guides an organization to identify and design the right type and number of controls for an optimized level of protection. As always, the security posture and the required resources and investments shall be based on the business value to protect.

Simplified, there are two main sources for the identification of security controls:

a) risk assessments based on the organization’s information assets, and strategic goals

b) legal, statutory, regulatory, and contractual requirements

What has changed?

Before the update, there were 14 categories (number 5-18) of the security controls in the standard. Now, the controls have been consolidated into four categories; organizational controls, people controls, physical controls and technological controls. Some controls have been merged, some have been modified and several new controls have been introduced. In addition to this, the amount of controls have been reduced from a total of 114 controls to 93, including the following 11 new controls:

1. Threat Intelligence
2. Information security for the use of cloud services
3. ICT readiness for business continuity
4. Physical security monitoring
5. Configuration management
6. Information deletion
7. Data masking
8. Data leakage prevention
9. Monitoring activities
10. Web filtering
11. Secure coding

While some of the new controls seem practically mandatory (cloud security, configuration management) some might not be necessary for all organizations (secure coding).

The controls have also been assigned different attributes for easier classification and management:

- **Control type:** #Preventive, #Detective, #Corrective
- **Information security properties**: #Confidentiality, #Integrity, #Availability
- **Cybersecurity concepts**: #Identify, #Protect, #Detect, #Respond, #Recover
- **Operational capabilities**: e.g. #Continuity, #Physical security, #Information security event management
- **Security domains:** #Governance_and_Ecosystem, #Protection, #Defence, #Resilience

The standard is now also enabled to allow for controls from other standards, e.g. NIST, OWASP, etc. to have organizations an optimal fit of prioritized controls.

A new privacy aspect

While the current version of the ISO/IEC 27002 standard focuses almost exclusively on information security the update has introduced a few privacy-related controls, such as:

- Data masking (Control 8.11)
- Information deletion (Control 8.10)

All organizations process personal data and these new controls will support the GDPR regulatory controls to implement an effective protection of personally identifiable data.

How will this impact ISO/IEC 27001:2013?

Since ISO/IEC 27001:2013 is derived from the controls of the current ISO/IEC 27002, the ISO/IEC 27001 is due for an update. A decision of the revision of ISO/IEC 27001:2013 has not yet been made but might be in the near future.

What your organization should be doing?

As always, organization’s should through risk assessments identify the risks and corresponding controls.

We have split up the major tasks as follows:

1. Review the new 27002 draft and all the 93 controls. Compare current control implementation with new control descriptions. Evaluate need for new controls or control modification. Do not forget the privacy-related controls.

2. Create a development plan: prioritize risks and controls, identify necessary resources and other dependencies. Create actionable development plan.

3. Implement the development plan: get an early start by implementing the necessary controls and updating your Statement of Applicability (SoA).

Seeing that the new ISO/IEC 27002 is still in draft state and unlikely to change getting a head start might be a good idea.

Concluding reflections

The changes to the ISO/IEC 27002 standard require businesses to further investigate their current security measures to understand how to remain compliant and keep managing their risk exposure. The updates to ISO/IEC 27002 have been implemented to modernize and simplify the guidelines for running an efficient and effective information security management system (ISMS) and now also integrate privacy to some extent. The new updates also allow organizations to design and implement security controls based on different standards to get a more optimized level of protection.

The business incentives for acquiring a certification have increased over the past couple of years since the demand from customers and regulatory organs have grown. These new updates intends to support modern organizations in creating a security control framework with less amount of categories and controls for a more direct framework of governance. Whether you are already ISO 27001 certified or still working towards it, we highly recommend getting a head start and incorporating the upcoming changes into your management system.

While it is certain to create quite a bit of work and long hours for information security management professionals it is certainly a step in the right direction.

Plan for protecting your business tomorrow. Contact us today.

Please reach out

Alex Fagerström

Senior Information Security Consultant

alex.fagerstrom@transcendentgroup.com

+35 84 067 92 624

Pontus Lilliequist

Senior Information Security Consultant

pontus.lilliequist@transcendentgroup.com

+46 72 181 93 11

Bendik Mjaaland

Head of IT Governance and Security, Norway

bendik.mjaaland@transcendentgroup.com

+47 93 873 600