GRAHAM HILL

CONSULTING

NEW REVISION of ISO 27001:2022 RELEASED!

Introduction

Graham Hill Consulting is pleased to offer this white paper, which provides an overview of the newly released 3rd edition of the ISO 27001 standard for information security management systems. ISO 27001 is the globally-recognized management system standard constructed to secure an organization's information assets. In 2021, an ISO Survey reported that there were 58,687 total valid ISO 27001 certificates applying to 99,755 sites.

ISO/IEC 27001:2013 → ISO/IEC 27001:2022

ISO/IEC 27001:2022 [Information security, cybersecurity and privacy protection – Information Security Management Systems – Requirements] was published on October 25th, 2022 and the ISO/ISO 27002:2022 [Information security, cybersecurity and privacy protection — Information security controls] was released in February 2022.

ISO 27002 is a critically import reference document that describes the information security controls outlined in ISO 27001, Annex A. We'll discuss this document a little more in the transition 'Transition Plan' section below.

The International Accreditation Forum (IAF) has outlined the requirements for a 3-year controlled transition period for all organizations currently certified to ISO 27001:2013. As with previous ISO transitions, both the out-going and the in-coming standards will be valid during that time, but certified organizations must complete their transitioning to the new standard before the end of 3-year Transition Period.

The major update to ISO 27001:2022 and consequently ISO 27002:2022 is the complete reorganization of the structure of Annex A. Minor updates were also made to the standard itself.

What changed?

- Minor changes within the body of the ISO 27001 standard have been made to better align with the harmonized structure for management system standards (i.e. Annex SL). Of note, very minor changes have been made in the following requirements:
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.4 Information security management system
  - 6.2 Information security objectives and planning to achieve them
  - 6.3 Planning of changes
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.3.2 Management review inputs
- The Annex A controls have been reorganized from 14 control objectives to 4 broad themes that include: Organizational, People, Physical, and Technological Controls
- The number of controls within Annex A stands at 93 controls compared to the 114 controls in the previous edition
- Several previous controls have been combined into broader new controls; and 11 new controls have been added, including:
  - A.5.7 Threat intelligence
  - A.5.23 Information security for use of cloud services
  - A.5.30 ICT readiness for business continuity
  - A.7.4 Physical security monitoring
  - A.8.9 Configuration management
  - A.8.10 Information deletion
  - A.8.11 Data masking
  - A.8.12 Data leakage prevention
  - A.8.16 Monitoring activities
  - A.8.23 Web filtering
  - A.8.28 Secure coding

(416)-884-3989 info@ghill.ca www.ghill.ca

Transition plan

Graham Hill Consulting has created a clear transition path that is easy for our clients to integrate and apply within their ISMS. Our goal is to provide organizations with the guidance and tools necessary to make the transition from ISO 27001:2013 to ISO 27001:2022 as smooth as possible.

The International Accreditation Forum (IAF) has stated in IAD MD 26:2022 that organizations will have approximately 3 years from the date of the standard's publication to transition their ISO 27001 management system and become compliant to the new standard.

In order to ensure that organizations are successful with their transition they should adhere to the following guidelines:

Transition guidelines - ISO /IEC 27001:2022

October 25, 2022

- ISO/IEC 27001:2022 3rd edition - Release date
- Transition period begins

October 31, 2022

- All existing certificates to ISO 27001:2013 will expire 36 months
- All registrars will need to be assessed and authorized by ANAB to perform ISO 27001:2022 audits
- Graham Hill Consulting currently expects this process to occur in early 2023; as such we expect that commencement of ISO 27001:2022 audits of organizations will begin in Q1/Q2 2023

April 1, 2024

- All initial (new) certifications should be to the 27001:2022 edition after this date and all recertification audits are recommended to utilize the 27001:2022 edition after this date
- Registrars should continue to accept applications for certification and issue new certificates against the 27001:2013 standard until this date

August 31, 2025

- All transition audits should be conducted by this date
- This gives registrars have two months to issue ISO27001:2022 certificates

October 31, 2025

- Transition period ends
- Certificates for ISO/IEC 27001:2013 will no longer be valid after this date

(416)-884-3989 info@ghill.ca www.ghill.ca

Transition process

Transition tip! Certified clients should plan to transition in combination with recertification audits. A full recertification audit will be required to the new standard even if you are in a surveillance year.

Preparing for transition

- Organizations must update their information security management system in accordance with the requirements of ISO 27001:2022 before the transition audit is conducted.
- Organizations should incorporate the guidance contained in the new ISO 27002:2022 standard which categorizes the Annex A controls into 5 control attributes. Attributes include: Control Type, Information Security Properties, Cybersecurity Concepts, Operational Capabilities, Security Domains. ISO 27002:2022 also specifies a purpose for each individual control to better explain the intent of each control.
- Training on the new requirements of ISO27001 and ISO27002 is highly recommended prior to any revisions or implementation.
- A full internal audit to the ISO27001:2022 requirements must be completed and any nonconformances to the new requirements must be corrected before the transition audit. Don't forget to train your auditors to the new standard prior to the audit!
- A full management review in accordance with the requirements of the new standard prior to the transition audit being conducted is also required.

Transition audit

- We expect that registrars will commence offering transition audits as early as Q1 2023.
- If the transition audit is combined with periodic surveillance, the audit will probably require additional audit time to cover the existing requirements and the new requirements/concepts introduced by ISO 27001:2022.
- If the transition audit is in a recertification year, the audit will probably not require additional audit time. This is this is the most cost-effective option.
- Organizations may also transition via a special stand-alone audit carried out expressly for the purpose of transition however, this is the most costly option.

ISO 27001:2022 certification

Registrars will issue updated certification documents following successful transition audits and disposition of any applicable findings.

- ○ Where the transition is conducted in combination with a surveillance or via a special audit, the expiration of the existing certificate shall be retained (since these are not full re-assessment audits).
- ○ Where the transition is conducted in combination with a recertification audit, the certificate will be re-issued for a renewed three year period.

Additional support

The **Graham Hill Consulting** team is here to support you and your organization throughout the transition process. We offer training and consulting customized to your specific needs. Services include:

- ISO27001:2022 Awareness Training
- ISO27002:2022 Awareness Training
- ISO27001:2022 Internal Auditor Training
- ISO27001:2022 Internal Audit Support
- ISO27001:2022 Transition Implementation Consulting and Support

Call now for a free, no obligation, consultation and quotation!