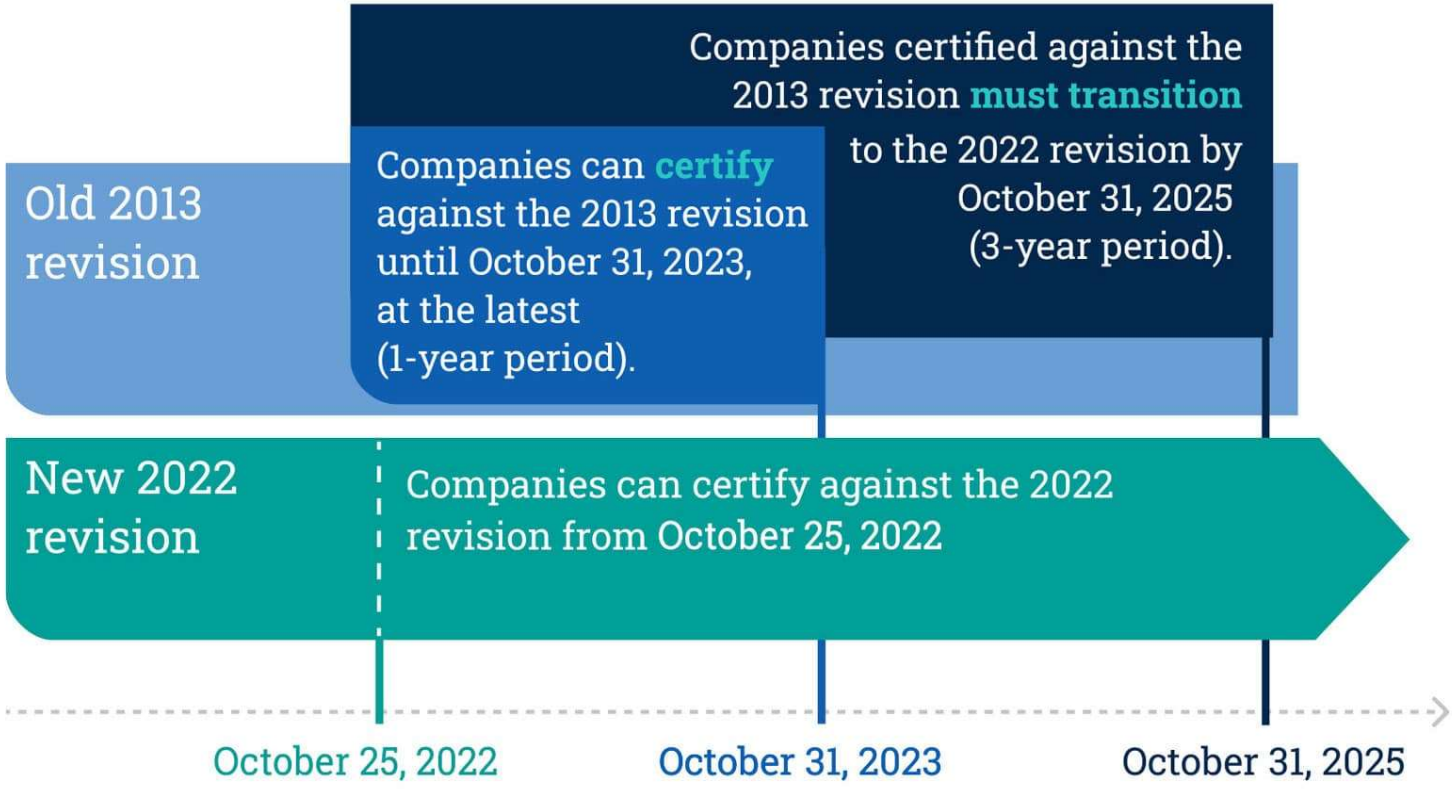
ISO / IEC 27001: 2022 Transition Programme

Main changes in the ISO 27001 2022 revision:

- The main part of ISO 27001, i.e., clauses 4 to 10, has changed only slightly.
- The changes in Annex A security controls are moderate.
- The number of controls has decreased from 114 to 93.
- The controls are placed into 4 sections, instead of the previous 14.
- There are 11 new controls, while none of the controls were deleted, and many controls were merged.

ISO 27001:2022 TRANSITION TIMELINE



ISO 27001 & ISO 27002 history

- The first version of ISO 27001 was published way back in 1999 under the name of BS 7799-2, and it has gone through several changes since then.
- ISO 27001 should not be confused with ISO 27002 – the former one is the main standard against which you can certify your company, while the latter one is the supporting standard that provides guidelines on the implementation of security controls. The most important difference is that ISO 27002 is not mandatory for ISO 27001 certification, and a company cannot get certified against ISO 27002.
- ISO 27002 was first published in 1995 under the name of BS 7799-1, and in February this year the ISO 27002:2022 revision was published with the new structure of 93 controls – this exact same structure of controls was adopted by ISO 27001:2022, as explained below.

Comparison

- Overall, when compared to the 2013 revision, the changes in the ISO 27001:2022 revision are small to moderate. The main part of the standard remains with 11 clauses, and the changes in this part of the standard are small.
- At first glance, Annex A has changed a lot – the number of controls has dropped from 114 to 93, and it is organized into only four sections versus the 14 sections in the 2013 revision. However, after a closer look, it becomes obvious that the changes in Annex A are only moderate.

Changes in the management system

- The text of the mandatory clauses 4 through 10 has changed only slightly, mainly to align with ISO 9001, ISO 14001, and other ISO management standards, and with Annex SL.

- Here's a brief overview of the changes in ISO 27001:2022:

- In clause 4.2 (Understanding the needs and expectations of interested parties), item (c) was added requiring an analysis of which of the interested party requirements must be addressed through the ISMS.

- In clause 4.4 (Information security management system), a phrase was added requiring planning for processes and their interactions as part of the ISMS.

- In clause 5.3 (Organizational roles, responsibilities and authorities), a phrase was added to clarify that communication of roles is done internally within the organization.

•In clause 6.2 (Information security objectives and planning to achieve them), item (d) was added that requires objectives to be monitored.

•Clause 6.3 (Planning of changes) was added, requiring that any change in the ISMS needs to be done in a planned manner.

•In clause 7.4 (Communication), item (e) was deleted, which required setting up processes for communication.

•In clause 8.1 (Operational planning and control), new requirements were added for establishing criteria for security processes, and for implementing processes according to those criteria. In the same clause, the requirement to implement plans for achieving objectives was deleted.

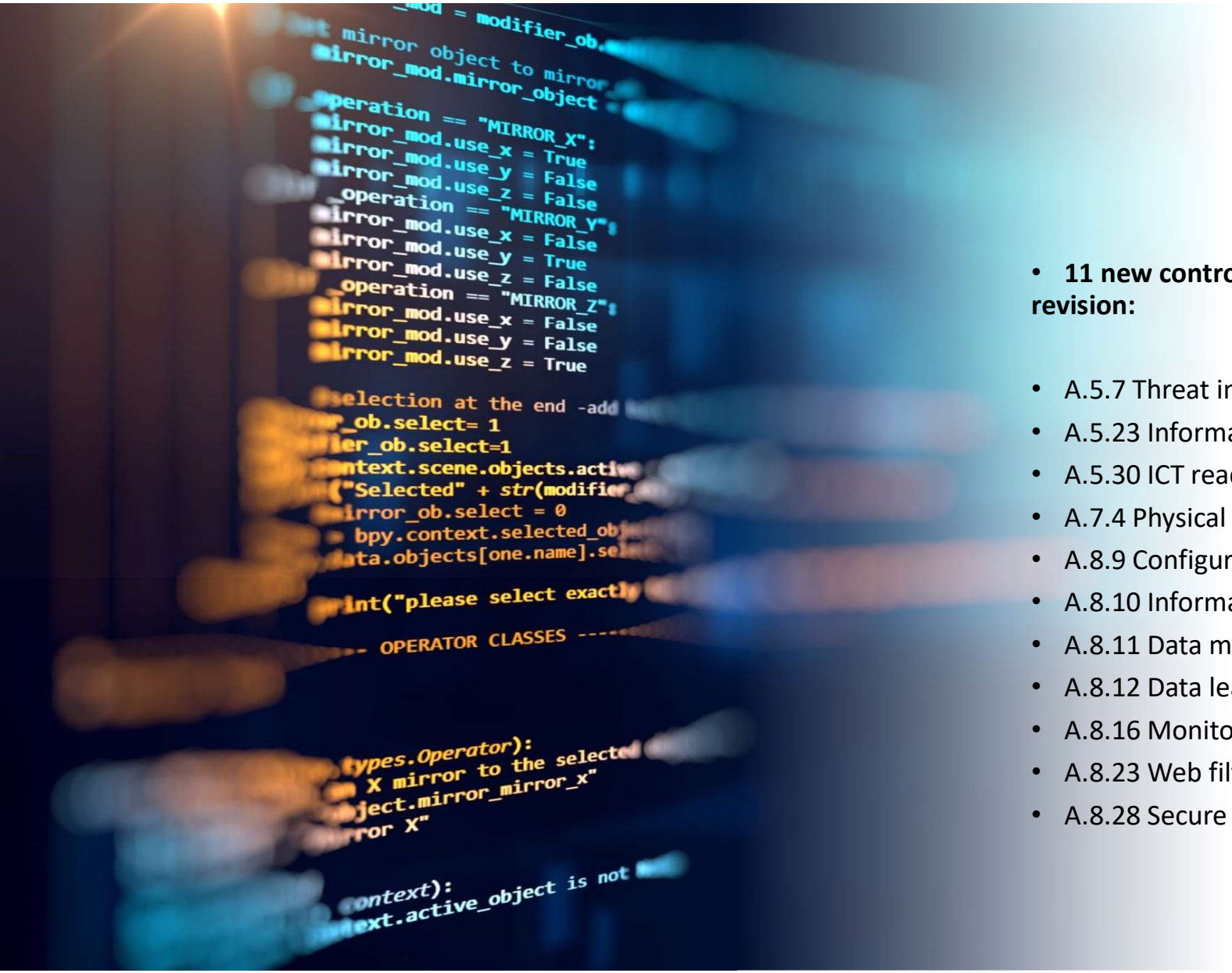
•In clause 9.3 (Management review), the new item 9.3.2 c) was added that clarifies that inputs from interested parties need to be about their needs and expectations, and relevant to the ISMS.

•In clause 10 (Improvement), the subclauses have changed places, so the first one is Continual improvement (10.1), and the second one is Nonconformity and corrective action (10.2), while the text of those clauses has not changed.

- **CHANGES IN ANNEX A SECURITY CONTROLS**

- In reality, the changes in Annex A are only moderate because most of the controls have either stayed the same (35 of them) or have only been renamed (23). Another 57 controls were merged, which has reduced the number of controls, but the requirements within those controls remained almost the same. Finally, one control was split into two separate controls, while the requirements stayed the same.


A.5.7 Threat intelligence
A.5.30 ICT readiness for business continuity
A.8.9 Configuration management
A.8.11 Data masking
A.8.16 Monitoring activities
A.8.28 Secure coding
Information security for use of cloud services A.5.23
Physical security monitoring A.7.4
Information deletion A.8.10
Data leakage prevention A.8.12
Web filtering A.8.23
11 new controls introduced in the ISO 27001 2022 revision



- **11 new controls introduced in the ISO 27001 2022 revision:**

- 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

A.5.7 Threat intelligence

Description. This control requires you to gather information about threats and analyze them, in order to take appropriate mitigation actions. This information could be about particular attacks, about methods and technologies the attackers are using, and/or about attack trends. You should gather this information internally, as well as from external sources like vendor reports, government agency announcements, etc.

Technology. Smaller companies probably do not need any new technology related to this control; rather, they will have to figure out how to extract the threat information from their existing systems. If they do not have one already, larger companies will need to acquire a system that will alert them to new threats (as well as to vulnerabilities and incidents). Companies of any size will have to use threat information to harden their systems.

Organization/processes. You should set the processes for how to gather and use the threat information to introduce preventive controls in your IT systems, to improve your risk assessment, and to introduce new methods for security testing.

People. Make employees aware of the importance of sending threat notifications, and train them on how and to whom these threats are to be communicated.

Documentation. No documentation is required by ISO 27001; however, you might include rules about threat intelligence in the following documents:

•Supplier Security Policy – Define how the information about threats is communicated between the company and its suppliers and partners.

•Incident Management Procedure – Define how the information about threats is communicated internally in the company.

•Security Operating Procedures – Define how to gather and process information about the threats.

A.5.23 Information security for use of cloud services

- **Description**. This control requires you to set security requirements for cloud services in order to have better protection of your information in the cloud. This includes purchasing, using, managing, and terminating the use of cloud services.
- **Technology**. In most cases, new technology will not be needed, because the majority of cloud services already have security features. In some cases, you might need to upgrade your service to a more secure one, while in some rare cases you will need to change the cloud provider if it does not have security features. For the most part, the only change required will be using existing cloud security features in a more thorough way.
- **Organization/processes**. You should set up a process to determine security requirements for cloud services and for determining the criteria for selecting a cloud provider; further, you should define a process for determining acceptable use of the cloud, and also the security requirements when cancelling the use of a cloud service.
- **People**. Make employees aware of the security risks of using cloud services, and train them on how to use the security features of cloud services.
- **Documentation**. No documentation is required by ISO 27001; however, if you are a smaller company, you might include rules about cloud services in the Supplier Security Policy. Larger companies might develop a separate policy that would focus specifically on security for cloud services.

A.5.30 ICT readiness for business continuity

Description. This control requires your information and communication technology to be ready for potential disruptions so that required information and assets are available when needed. This includes readiness planning, implementation, maintenance, and testing.

Technology. If you did not invest in solutions that enable resilience and redundancy of your systems, you might need to introduce such technology – this might range from data backup to redundant communication links. These solutions need to be planned based on your risk assessment and how quickly you need your data and your systems to be recovered.

Organization/processes. Besides the planning process, which needs to take into account the risks and business needs for recovery, you should also set up the maintenance process for your technology, and the testing process for your disaster recovery and/or business continuity plans.

People. Make employees aware of potential disruptions that could happen, and train them on how to maintain IT and communication technology so that it is ready for a disruption.

Documentation. No documentation is required by ISO 27001; however, if you are a smaller company, you might include the ICT readiness in the following documents:

•Disaster Recovery Plan – readiness planning, implementation, and maintenance

•Internal Audit Report – readiness testing

If you are a larger organization, or if you implemented **ISO 22301**, then you should document readiness through the Business Impact Analysis, Business Continuity Strategy, Business Continuity Plan, and Business Continuity Testing Plan & Report.

A.7.4 Physical security monitoring

- **Description**. This control requires you to monitor sensitive areas in order to enable only authorized people to access them. This might include your offices, production facilities, warehouses, and other premises.
- **Technology**. Depending on your risks, you might need to implement alarm systems or video monitoring; you might also decide to implement a non-tech solution like a person observing the area (e.g., a guard).
- **Organization/processes**. You should define who is in charge of the monitoring of sensitive areas, and what communication channels to use to report an incident.
- **People**. Make employees aware of the risks of unauthorized physical entry into sensitive areas, and train them how to use the monitoring technology.
- **Documentation**. No documentation is required by ISO 27001; however, you might include physical security monitoring in the following documents:
- Procedures that Regulate Physical Security – what is monitored, and who is in charge of monitoring
- Incident Management Procedure – how to report and handle a physical security incident

A.8.9 Configuration management

Description. This control requires you to manage the whole cycle of security configuration for your technology to ensure a proper level of security and to avoid any unauthorized changes. This includes configuration definition, implementation, monitoring, and review.

Technology. The technology whose configuration needs to be managed could include software, hardware, services, or networks. Smaller companies will probably be able to handle configuration management without any additional tools, whereas larger companies probably need some software that enforces defined configurations.

Organization/processes. You should set up a process for proposing, reviewing, and approving security configurations, as well as the processes for managing and monitoring the configurations.

People. Make employees aware of why strict control of security configuration is needed, and train them on how to define and implement security configurations.

Documentation. ISO 27001 requires this control to be documented. If you are a small company, you can document the configuration rules in your Security Operating Procedures. Larger companies will typically have a separate procedure that defines the configuration process.

You will usually have separate specifications that define security configurations for each of your systems, in order to avoid frequent updates of the documents mentioned in the previous paragraph. Further, all changes to configurations need to be logged to enable an audit trail.

A.8.10 Information deletion

Description. This control requires you to delete data when no longer required, in order to avoid leakage of sensitive information and to enable compliance with privacy and other requirements. This could include deletion in your IT systems, removable media, or cloud services.

Technology. You should be using tools for secure deletion, according to regulatory or contractual requirements, or in line with your risk assessment.

Organization/processes. You should set up a process that will define which data need to be deleted and when, and define responsibilities and methods for deletion.

People. Make employees aware of why deleting sensitive information is important, and train them on how to do this properly.

Documentation. No documentation is required by ISO 27001; however, you might include rules about information deletion in the following documents:

•Disposal and Destruction Policy – how the information on removable media is deleted

•Acceptable Use Policy – how regular users need to delete the sensitive information on their computers and mobile devices

•Security Operating Procedures – how system administrators need to delete the sensitive information on servers and networks

Larger organizations might also have a Data Retention Policy that defines how long each type of information is needed, and when it needs to be deleted.

A.8.11 Data masking

Description. This control requires you to use data masking together with access control in order to limit the exposure of sensitive information. This primarily means personal data, because they are heavily regulated through privacy regulations, but it could also include other categories of sensitive data.
Technology. Companies can use tools for pseudonymization or anonymization in order to mask data if this is required by privacy or other regulations. Other methods like encryption or obfuscation can also be used.
Organization/processes. You should set up processes that will determine which data need to be masked, who can access which type of data, and which methods will be used to mask the data.
People. Make employees aware of why masking data is important, and train them on which data need to be masked and how.
Documentation. No documentation is required by ISO 27001; however, you might include rules on data masking in the following documents:
•Information Classification Policy – determine which data are sensitive and what categories of data need to be masked
•Access Control Policy – defines who can access what type of masked or unmasked data
•Secure Development Policy – defines the technology of masking the data
Larger companies, or companies that need to be compliant with the European Union General Data Protection Regulation (EU GDPR) and similar privacy regulations, should also have the following documents:
•Privacy Policy / Personal Data Protection Policy – overall responsibilities for data masking
•Anonymization and Pseudonymization Policy – details on how data masking is implemented in the context of a privacy regulation

A.8.12 Data leakage prevention

Description. This control requires you to apply various data leakage measures in order to avoid unauthorized disclosure of sensitive information, and if such incidents happen, to detect them in a timely manner. This includes information in IT systems, networks, or any devices.

Technology. For this purpose, you could use systems to monitor potential leakage channels, including emails, removable storage devices, mobile devices, etc., and systems that prevent information from leaking – e.g., disabling download to removable storage, email quarantine, restricting copy and paste of data, restricting upload of data to external systems, encryption, etc.

Organization/processes. You should set up processes that determine the sensitivity of data, assess the risks of various technologies (e.g., risks of taking photos of sensitive information with a smartphone), monitor channels with the potential of data leakage, and define which technology to use to block the exposure of sensitive data.

People. Make employees aware of what kind of sensitive data is handled in the company and why it is important to prevent leakages, and train them on what is and what isn't allowed when handling sensitive data.

Documentation. No documentation is required by ISO 27001; however, you might include rules on data leakage prevention in the following documents:

- Information Classification Policy – the more sensitive the data are, the more prevention needs to be applied
- Security Operating Procedures – which systems for monitoring and prevention should be used by administrators
- Policy on Acceptable Use – what is and what isn't allowed for regular users

A.8.16 Monitoring activities

Description. This control requires you to monitor your systems in order to recognize unusual activities and, if needed, to activate the appropriate incident response. This includes monitoring of your IT systems, networks, and applications.

Technology. For your networks, systems, and applications, you could monitor the following: security tool logs, event logs, who is accessing what, activities of your main administrators, inbound and outbound traffic, proper execution of the code, and how the system resources are performing.

Organization/processes. You should set up a process that defines which systems will be monitored; how the responsibilities for monitoring are determined; and the methods of monitoring, establishing a baseline for unusual activities, and reporting events and incidents.

People. Make employees aware that their activities will be monitored, and explain what is and what is not considered normal behavior. Train IT administrators to use monitoring tools.

Documentation. No documentation is required by ISO 27001; however, if you are a smaller company, you might include rules about monitoring in the Security Operating Procedures. Larger companies might develop a separate procedure that would describe how to monitor their systems.

On top of this, it would be useful to keep records of monitoring activities.

A.8.23 Web filtering

Description. This control requires you to manage which websites your users are accessing, in order to protect your IT systems. This way, you can prevent your systems from being compromised by malicious code, and also prevent users from using illegal materials from the Internet.

Technology. You could use tools that block access to particular IP addresses, which could include the usage of anti-malware software. You could also use non-tech methods like developing a list of forbidden websites and asking users not to visit them.

Organization/processes. You should set up processes that determine which types of websites are not allowed, and how the web filtering tools are maintained.

People. Make employees aware of the dangers of using the Internet and where to find guidelines for safe use, and train your system administrators on how to perform web filtering.

Documentation. No documentation is required by ISO 27001; however if you are a smaller company, you might include rules about web filtering in the following documents:

•Security Operating Procedures – Define rules for system administrators on how to implement web filtering.

•Acceptable Use Policy – Define rules for all users on what is acceptable usage of Internet.

Larger companies might develop a separate procedure that would describe how the web filtering is performed.

A.8.28 Secure coding

Description. This control requires you to establish secure coding principles and apply them to your software development in order to reduce security vulnerabilities in the software. This could include activities before, during, and after the coding.

Technology. You might be using tools for maintaining an inventory of libraries, for protecting the source code from tampering, for logging errors and attacks, and for testing; you could also use security components like authentication, encryption, etc.

Organization/processes. You should set up a process for defining the minimum baseline of secure coding – both for internal software development and for software components from third parties, a process for monitoring emerging threats and advice on secure coding, a process for deciding which external tools and libraries can be used, and a process that defines activities done before the coding, during the coding, after the coding (review and maintenance), and for software modification.

People. Make your software developers aware of the importance of using secure coding principles, and train them on methods and tools for secure coding.

Documentation. No documentation is required by ISO 27001; however if you are a smaller company, you might include rules about secure coding in the Secure Development Policy. Larger companies might develop separate procedures for secure coding for each of their software development projects.

KingCert Transition Process

a) Organizations that will be certified by KingCert for the first time

- The first certification applications made according to ISO/IEC 27001:2013 will be accepted until 31.07.2023, and as of 01.08.2023, the first certification applications made according to ISO/IEC 27001:2022 will start to be accepted. Inspections will be carried out according to ISO/IEC 27001:2022 for all applications made after 01.08.2023.

- However, KingCert will be able to issue an accredited certificate after the ISO7IEC 27001:2022 updated accreditation is published after 09.2023.

- 1)KingCert may conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit.
- 2) The transition audit shall not only rely on the document review, especially for reviewing the technological information security controls.
- 3) The transition audit shall include, but not be limited to the following:
- • The gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS.
- • The updating of the statement of applicability (SoA).
- • If applicable, the updating of the risk treatment plan.
- • The implementation and effectiveness of the new or changed information security controls chosen by the clients.
- 1) Minimum of 0.5 auditor day for the transition audit when it is carried out in conjunction with a recertification audit.
- 2) Minimum of 1.0 auditor day for the transition audit when it is carried out in conjunction with a surveillance audit or as a separate audit.
- When the certification document is updated because the client successfully completed only the transition audit, the expiration of its current certification cycle will not be changed.
- All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period.

KING CERT INTERNATIONAL CERTIFICATION LTD.

Tsarigradsko Shose Blvd. No:133, Bic Izot Fl.6., Office No:603, 1784 Sofia Bulgaria

Telefon: +359 878 398 622

E-Mail: info@KingCert.com

KING®
CERT