CERTIFICATION EUROPE™

ISO/IEC 27001:2022 TRANSITION POLICY

Certification Europe ISO/IEC 27001:2022 Transition Policy (INAB)

ISO/IEC 27001:2022 has been released and is replacing the existing Information Security Management System ISO/IEC 27001:2013.

A mandatory document has been released by The International Accreditation Forum (IAF) in conjunction with the standard to support the transition deadline requirements from ISO/IEC 27001:2013 to ISO/IEC 27001:2022.

Certification Europe has created this policy document to help clarify the certification process for current and future clients.

There are two key deadline dates detailed within the IAF mandatory document:

Deadline 1 – 30th April 2024

Clients obtaining ISO/IEC 27001 for the first time, will be allowed to achieve ISO/IEC 27001:2013 Certification up until 30th April 2024. These clients can then transition at a later date before the final transition deadline (detailed below).

All initial certifications after 30th April 2024 must be done to ISO/IEC 27001:2022 version of the standard only

Existing Clients who already hold certification can recertify their ISO/IEC 27001:2013 compliant system up until 30th April 2024 and transition at a later date before the final transition deadline.

All clients who are required to meet this deadline will need to have completed their assessments no later than 29th February 2024. This is to ensure that enough time to address any non-conformances if they arise during the assessment and for the certification decision to be made.

Deadline 2 – 31st October 2025

Existing clients who have ISO/IEC 27001:2013, who do not fall within the Deadline 1 criteria, will be required to complete their transition and receive their certification   to ISO/IEC 27001:2022 no later than 31st October 2025.

To ensure that this deadline is met, all transition assessments must be completed by 29th August 2025. This is to ensure that enough time is provided to the clients to address any non-conformances if they arise during the assessment and for the transition decision to be made.

Once clients successfully transition their existing ISO/IEC 27001:2013 certification, the expiry date of their ISO/IEC 27001:2022 certificate will be in-line with their current 3-year certification so no certification time will be lost.

Questions & Answers

While ISO/IEC 27001:2022 is similar in parts to ISO/IEC 27001:2013 there are some additional requirements that clients will have to meet before their Information Security Management System can be deemed to be compliant with the ISO/IEC 27001:2022 standard.

As we want to make the ISO/IEC 27001:2022 certification process clear and smooth for current and future clients, we have developed a simple policy with the common questions and answers we have received.

What if we are an existing Certification Europe client with ISO/IEC 27001:2013 whose certificate expires before 30th April 2024?

For existing clients, currently certified to ISO/IEC 27001:2013 with expiry dates on certificates before 30th April 2024, Certification Europe will continue to conduct assessment against ISO/IEC 27001:2013 as per the planned surveillance / recertification assessment schedule. Reference will only be made to the ISO/IEC 27001:2013 standard when reporting assessment findings.

During the surveillance / recertification assessments, the assessor will agree with the client a date in the future to carry out a transition assessment of their Information Security Management System against the requirements of ISO/IEC 27001:2022. The time and number of additional days required will be agreed with each client for the transition assessment to take place.

Following the recertification, surveillance assessments will continue to be conducted against the ISO/IEC 27001:2013 version of the standard until the client is in a position to carry out their transition assessment. Transition assessments must be completed by 29th August 2025

At the end of the transition assessment, if the assessor is of the opinion that the Information Security Management System is compliant with the additional requirements of the ISO/IEC 27001:2022 standard then a recommendation for transition of certification may be made, at the assessor's discretion, based upon the evidence observed during the assessment. Findings from this transition assessment will be recorded in the assessment report and will be subject to an independent technical review prior to a final decision being made.

If the assessor is not in a position to recommend transition of certification, then a further assessment may be required depending on the nature of the issues requiring action. Any required action would be agreed between the assessor and client representative at the assessment closing meeting.

If transition to ISO/IEC 27001:2022 is not approved prior to the end of the transition period on 31st October 2025 the client's Information Security Management System will not be certified to either ISO/IEC 27001:2022 or ISO/IEC 27001:2013. The client will need to start the certification process again, with a stage 1 & 2 assessment to have their system certified to ISO/IEC 27001:2022..

What if we are an existing Certification Europe client with ISO/IEC 27001:2013 whose certificate expires after 30th April 2024

For existing clients currently certified to ISO/IEC 27001:2013 with expiry dates on certificates after 30th April 2024, Certification Europe will continue to conduct surveillance assessments against ISO/IEC 27001:2013 as per the planned surveillance schedule, however when conducting their recertification, clients will be required to transition to ISO/IEC 27001:2022 at this assessment. Reference will only be made to the ISO/IEC 27001:2022 standard when reporting assessment findings at the recertification assessment.

Recertification/Transition assessments must be completed eight weeks before the transition deadline meaning they are required to be completed by 29th August 2025

Following the recertification, surveillance assessments will be conducted against the ISO/IEC 27001:2022 version of the standard.

At the end of the recertification/transition assessment, if the assessor is of the opinion that the Information Security Management System is compliant with the additional requirements of the ISO/IEC 27001:2022 standard then a recommendation for transition of certification may be made, at the assessor's discretion, based upon the evidence observed during the assessment. Findings from this assessment will be recorded in the recertification/transition assessment report and will be subject to an independent technical review prior to a final decision being made.

If the assessor is not in a position to recommend transition of certification, then a further assessment may be required depending on the nature of the issues requiring action. Any required action would be agreed between the assessor and client representative at the assessment closing meeting.

If transition to ISO/IEC 27001:2022 is not approved prior to the end of the transition period on 31st October 2025 the client's Information Security Management System will not be certified to either ISO/IEC 27001:2022 or ISO/IEC 27001:2013. The client will need to start the certification process again, with a stage 1 & 2 assessment to have their system certified to ISO/IEC 27001:2022.

What if we are an organisation wishing to achieve ISO/IEC 27001 for the first time?

For organisations that have developed an Information Security Management System with a view to obtaining ISO/IEC 27001:2013 certification, stage 1 and stage 2 assessments must complete by 29th February 2024, eight weeks before Deadline 1 on 30th April 2024. The client will then have until 29th August 2025, eight weeks before Deadline 2, to conduct their ISO/IEC 27001:2022 transition assessment.

All initial certification assessments after 30th April 2024, will be conducted against the ISO/IEC 27001:2022 version of the standard.

Any further enquiries should be directed to our Customer Services Team via e-mail at **customerservices@certificationeurope.com**.