INFORMATION SECURITY MANAGEMENT SYSTEM

ISO 27001:2022

TRANSITION Q&A

ACI®

Highlights of several crucial dates on Transition:

- The issue date of ISO 27001:2022: **25th October 2022.**
- The transition period: **25th October 2022 – 30th October 2025 (36 months).**
- The expiry date of ISO 27001:2013 Certificates: **31st October 2025.**
- ACI deadline for accepting ISO27001:2013 Certification application: **30th April 2024.**

Highlights of ACI services to facilitate the Transition:

- Preliminary Gap Analysis
- Gap Assessment: A professional review of clients' ISMS against ISO27001:2022 requirements
- Professional Customer Services team ready for answering enquiries from the clients regarding the transition
- (TIS1) ISO27001:2022 Introduction & Conversion training to provide a generic introduction of the ISO27001:2022 requirements;
- (TIS2) ISO27001:2022 Effective Application training;
- (TIS3) ISO27001:2022 Implementation & Documentation Training;
- (TIS4) ISO27001:2022 Internal Auditor Training;

ACI®

General

Q1 When is the ISO27001:2022 issued?

ISO27001:2022 was issued on 25th October 2022.

Q2 What are the major differences between ISO27001:2022 & ISO27001:2013?

- 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.

Q3 What are the core concepts of ISO27001:2022?

- Process Approach
- Plan-Do-Check-Act Cycle
- Risk Assessment and treatment
- Safeguard Implementation

Q4 We have got ISO27001:2013 Certificate already. What is the impact of the new standard on us?

According to the resolution of International Accreditation Forum (IAF MD26:2022), there is a 36-month transition period from the issue date of ISO27001:2022 for all the existing ISO27001:2013 Certificates to transit to ISO27001:2022 Certificates.

Therefore, all ISO27001:2013 Certificates will be expired on 31st October 2025. (i.e. the ISO27001:2013 certificates will have lost validity 31st October 2025).

ACI®

Q5 We are going to implement a Information Security management system (ISMS) for certification. What should we do?

There are two options:
i) You can directly implement the ISMS in accordance with ISO27001:2022 and apply for the certification of ISO27001:2022;

ii) Alternatively, if you have already begun to set up the ISMS based on ISO27001:2013, you can go ahead to obtain the ISO27001:2013 certificate first on or before 30 April 2024 and later do the transition to ISO27001:2022 on or before 30 Jul 2025.

Q6 Is there any deadline for the application for ISO27001:2013 Certification?

ACI welcomes ISO27001:2013 Certification application made during the Transition Period provided that such application should be on or before 30 April 2024.

The reason for setting this deadline is to ensure sufficient time for the certified clients to prepare the transition after being certified for ISO27001:2013.

Q7 When should we do the transition?

During the Transition Period, the ISO27001:2013 certified clients can choose to transit at any time provided that the deadline of successful transition is 30th October 2025* . The clients can decide their schedule for transition.

However, it is highly recommended for the clients to complete the transition as early as possible

i) to avoid the transition peak;

ii)to leave enough time for the submission of plans of correction and corrective actions and the arrangement of any follow up visits if there were non-conformities (NCs) raised in the Transition Audit(s).
(* Remark : ACI's deadline for Transition Audit(s) is 30th October 2025.)

Q8 How should we start for the transition?

i) Review ISO27001:2022;

ii) Implement the ISMS in accordance with the ISO27001:2022;

iii) Plan the transition;

iv) Discuss with ACI the plan and reserve the date(s) for Transition Audit(s).

ACI®

Q9 What is the transition process?

For ACI, all ISO 27001:2013 certified clients seeking ISO27001:2022 transition shall undergo a Transition Audit(s). Normally, there are two types of Transition Audit: one-off audit or staged audit.

i) For One-Off Transition Audit, the audit will be a one time audit in which the fulfillment of the clients' ISMS against all the ISO27001:2022 requirements will be evaluated within the same audit. It can be carried out together with the normal scheduled audits such as Surveillance Visit (SV) or Renewal Audit or a single independent audit.

ii) For staged type, the evaluation of the fulfillment of the clients' ISMS against the ISO27001:2022 requirements will be conducted in several planned audits provided that the accumulative results of these audits can prove the full fulfillment of the client's ISMS with ISO27001:2022.
Each audit of Transition Audits in such case can be carried out together with the normal scheduled audits such as Surveillance Visit (SV) or Renewal Audit or a single independent audit.

Point to note:
For the staged type, during each audit of the Transition Audits, as the ISMS is not or has not been evaluated to be fully complied with ISO27001:2022, the normal audit for ISO27001:2013 will be still carried out. Please make sure to maintain effectively the ISMS of ISO27001:2013 before the completion and success of the transition.

Q10 How should we choose between one-off type and staged type Transition Audit(s)?

The choice for one-off type or staged type Transition Audit(s) may have impact in terms of clients' internal manpower arrangement or business plan. Clients are advised to have a comprehensive consideration before making decision and discuss with ACI if necessary.

ACI®

Q11 How does ACI begin the transition for the clients?

ACI auditors will conduct a Gap Assessment for every ACI certified client of ISO27001:2013 (upon request) in the occasions of the normal scheduled audit such as Surveillance Visits (SVs) and Renewal Audit (REAs). The purpose of this Gap Assessment is for ACI:

- to know the clients' preliminary plan of transition;
- to have a general picture on the readiness of the clients' management system for the transition;
- to discuss any issues of the transition, if any or necessary, which may be more preferable to be discussed in clients' certified sites.

Q12 What does ACI do to assist certified clients for the transition?

Besides, the abovementioned Preliminary Gap Analysis, in order to get our clients more familiar with the ISO27001:2022 requirements and facilitate our clients' preparation for the transition, ACI with pleasure provides the following services:

- (TIS1) ISO27001:2022 Introduction & Conversion training to provide a generic introduction of the ISO27001:2022 requirements;
- (TIS2) ISO27001:2022 Effective Application training;
- (TIS3) ISO27001:2022 Implementation & Documentation Training;
- (TIS4) ISO27001:2022 Internal Audit Training;
- Upon request, ACI auditors can come to the client's office to perform a comprehensive Gap Assessment by going through every requirement of the ISO27001:2022 with the client in order to check whether the client's existing ISMS fulfill the requirements and if not, what the discrepancies are;
- Professional customer support to answer enquiries on the transition including the quotation for the Transition Audit(s) and reservation of dates for Transition Audit(s).

ACI®

Q13 What should be prepared for the transition audit?

The transition audit shall not only rely on the document review, especially for reviewing the technological information security controls.

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.

Q14 What is the duration of the transition audit? How about the expiry date of the Certification?

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.

資訊安全管理系統認證

ISO 27001:2022 轉版 Q&A

ACI®

轉版的關鍵日期:

- ISO27001:2022生效日期:
  2022年10月25日
- 過渡期:
  2022年10月25日 – 2025年10月30日
  (36個月)
- ISO27001:2013證書有效至:
  2025年10月31日
- ACI截止接受ISO27001:2013 認證申請日期:
  2024年4月30日

ACI轉版服務的好處:

- 初步差距分析
- 差異評估: 專業評核員根據ISO27001:2022的要求檢視客戶的管理體系，並提交評估報告。
- 專業的客戶服務團隊隨時準備回答客戶有關轉版的查詢
- (TIS1) ISO27001:2022 介紹 & 轉版課程;
- (TIS2) ISO27001:2022 有效應用課程;
- (TIS3) ISO27001:2022 執行與文件處理課程;
- (TIS4) ISO27001:2022 內部審核員課程;

ACI®

常見問題

Q1 ISO27001:2022 何時生效?

ISO27001:2022 於2022年10月25日開始生效

Q2 ISO27001:2022 和 ISO27001:2013 之間的主要區別?

- ISO 27001 的主要部分，即第 4 至 10 條僅略有變化。
- 附件 A 安全控制的變化是適度的。
- 控制數量從 114 個減少到 93 個。
- 控件分為 4 個部分，而不是之前的 14 個。
- 新增了 11 個控件，但沒有一個控件被刪除，許多控件被合併。

Q3 ISO27001:2022有什麼核心概念?

- 過程方法 (Process Approach)
- Plan-Do-Check-Act
- 風險評估和處理
- 保障執行

Q4 我們已經獲得ISO 27001:2013認證。新標準對我們有什麼影響?

國際認證論壇（IAF MD26:2022）宣佈一個為期36個月的過渡期讓所有現有的ISO27001:2013版證書轉版至ISO27001:2022版證書。

因此，所有的ISO 27001:2013證書將於2025年10月31日到期(注: 所有的ISO 27001:2013證書將會從2025年10月31日開始失效)。

Q5 我們正準備實施質量管理體系並申請認證（ISMS）。我們應該怎樣做?

這裡有兩個選擇：

i) 你可以直接按照ISO27001:2022實施ISMS，並申請ISO27001:2022證書;

ii) 另外，如果你已經開始根據ISO27001:2013的要求建立ISMS，您可以在2024年4月30日前依舊申請ISO27001:2013證書， 並於上述的截止日期前轉版至ISO27001:2022版本。

Q6 ISO27001:2013 證書設有截止申請日期嗎?

ACI於過渡期間仍歡迎ISO27001:2013的認證申請，直至2024年4月30日。

之所以設定上述期限， 是為了確保客戶通過ISO27001:2013認證後有足夠時間準備轉版。

Q7 我們應該什麼時候做轉版?

在過渡期間，在ISO 27001:2013的認證客戶可以選擇於2025年10月30日 * 或之前的任何時候轉版，客戶可決定 其轉版時間表。

但我們強烈建議客戶應儘早完成轉版。

i) 以避免轉版高峰期;

ii) 以預留足夠時間提交糾正計劃和糾正措施及安排後續跟進行動， 若客戶於轉版審核期間被提出不符合項(NCs) 。

Q8 我們應該如何開始轉版?

i) 覆核 ISO27001:2022;

ii) 根據ISO27001:2022實施ISMS;

iii) 規劃轉版;

iv) 與ACI商討規劃和預約日期進行 轉版審核。

ACI®

Q9 有什麼轉版流程?

在ACI，所有ISO27001:2013證書客戶都會經歷轉版審核，以獲得ISO27001:2022版證書。

在一般情況下共有兩種類型的轉版審核可供客戶選擇：一次性審核或分階段審核。

i) 一次性審核 – 客戶的質量管理體系是否符合ISO27001:2022的要求，將在這一次性審核裡作評估。它可與其他審核 如監督審核（SV）或再認證審核一併進行，或作單一獨立審核。

ii) 分階段審核 – 將會於數次審核中進行，由累計結果證明客戶的質量管理體系(ISMS）已全面符合ISO27001:2022版之要求。

上述情況下，每一次轉版審核都可以與其他例行審核一同進行，例如監督審核（SV），覆審或作單一獨立審核。

注意:

於轉版審核其間，由於質量管理體系（ISMS）未或尚未完全通過ISO27001:2022版的評審，例行審核依然需要按照ISO27001:2013執行。請務必在轉版審核完成和通過前持續執行管理體系滿足ISO27001:2013。

Q10 一次性審核或分階段審核，我們應如何選擇?

選擇一次性審核還是分階段審核，可能會影響客戶的內部人手安排或商業計劃。所以客戶於作出決定前需要綜合考慮各種因素，必要時請與ACI商討

Q11

ACI會怎樣開始為客戶進行轉版?

ACI審核員將會為每位ACI認證客戶於例行審核， 例如監督審核(SV) 或再認證審核(REA)期間進行初步差距分析(根據客戶要求)。

進行差距分析的原因如下:

- 了解客戶轉版的初步方案
- 讓ACI了解各客戶對轉版的準備
- 在有需要時，與客戶商討任何關於轉版 的事宜。 因為有些時候在客戶的認證地點商討轉版事宜更為合適。

Q12

ACI會為客戶提供什麼協助進行轉版?

除了上述的初步差距分析， 為了令我們的客戶對ISO27001:2022的要求更熟悉， 同時便於準備轉版， ACI有幸為各位提供以下服務:

- (TIS1) ISO27001:2022 介紹 & 轉版課程– 簡短介紹ISO27001:2022的要求;
- (TIS2) ISO27001:2022 有效應用課程;
- (TIS3) ISO27001:2022 執行與文件處理課程;
- (TIS4) ISO27001:2022 內部審核員課程;
- ACI審核員可按客戶要求， 到客戶的認證地點， 跟據ISO27001:2022版的每項要求為客戶的質量管理體系作全面差距評估， 分析其體系的符合性與差距。
- 專業支援服務 - 解答客戶關於轉版的問題，包括轉版審核報價及審核排期。

ACI®

Q13 轉版審核需要準備什麼?

轉版審計不能僅依靠文件審查，特別是對技術資訊安全控制的審查。

轉版審核應包括但不限於下列內容：

- **ISO/IEC 27001:2022** 的差距分析，以及更改客戶 **ISMS** 的需求。
- 更新適用性聲明**(SoA)**。
- 如適用，更新風險處理計畫。
- 客戶選擇的新或更改的資訊安全控制措施的實施和有效性。

Q14 轉版審核需要多少時間? 認證的有效期限會改變嗎?

1) 與再認證審核一起進行時，轉版審核至少需要 **0.5** 人天。
2) 當與監督審核一起或作為單獨審核進行時，轉版審核至少需要 **1.0** 人天。

當客戶因僅成功完成轉版審核而更新認證文件時，其目前認證週期的到期時間不會改變。

所有基於 **ISO/IEC 27001:2013** 的認證應在過渡期結束時過期或撤銷。

轉版問題查詢
Email: enquiry@aci-limited.com Phone: 39778988