# 

# 

**ISO 27001:2022 Client Transition**

**Checklist**

for

Date completed on

© Centre for Assessment Ltd 2023

This report remains the property of Centre for Assessment

Centre for Assessment Ltd.

Lee House, 90 Great Bridgewater Street, Manchester, M1 5JW

Tel: +44 (0) 161 237 4080

e-mail: iso@centreforassessment.co.uk

web: www.centreforassessment.co.uk

**IMPORTANT NOTES**

This checklist is a guide and aide memoir only. Successful completion of this plan does not guarantee being successful at your transition audit, which will also require objective evidence of compliance with new and changed requirements.

The checklist is structured in 3 parts as follows:

* **Part 1** covers the changes and additions to the main clauses 4 to 10 of ISO 27001:2022
* **Part 2** covers the new and changed Annex A controls
* **Part 3** covers the changes and additions that are likely to be required to an already operational information security management system (ISMS) as a result of addressing the changes defined in parts 1 and 2

**Transition dates and deadlines**

* **Existing ISO 27001:2017 certificates**: By **31st October 2025** (3 years after publication of ISO 27001:2022) all organisations must have completed the transition to the updated version ISO 27001 and hold an updated certificate. **All ISO 27001:2017 certificates will have an expiry date no later than 31st October 2025.**

**Step-by-step guide to the transition process:**

* **Step one (Client)** – Complete the 27001:2022 transition application form and submit this to Centre for Assessment as soon as possible, and at least 4 months prior to your transition audit taking place.
* **Step two (Head Office)** – Centre for Assessment’s head office staff will review the application and inform you of the cost’s involved, which you should have received along with this ISO 27001 Client Transition Checklist Template.
* **Step three (Auditor)** – Centre for Assessment’s auditor will contact you and agree the date for the transition audit.
* **Step four (Client) –** Complete the 27001 Client Transition Checklist Template including details of actions taken and evidence demonstrating compliance and have the completed document **ready for the transition audit**. *Please note that failure to complete the Checklist will result in a chargeable cancellation of the transition audit.*
* **Step five (Auditor)** – Centre for Assessment’s auditor will complete the transition audit and identify any findings requiring a Continual Improvement Record to be completed. Note: If the transition audit identifies major non-conformances a further audit may be required.
* **Step six (Client)** – If applicable, you should complete and return the Continual Improvement Record to the Auditor, along with evidence of correction and corrective action.
* **Step seven (Auditor)** –Upon receipt, Centre for Assessment’s auditor will review the Continual Improvement Record and evidence for acceptance. If additional actions are required, you will be asked to resubmit. Once accepted, this document and associated evidence will be passed to Centre for Assessment head office for a certification decision.
* **Step eight (Head Office)** – Centre for Assessment’s head office will undertake a panel technical review and make a certification decision.
* **Step nine (Head office)** – upon a successful outcome of the transition audit, Centre for Assessment will issue you with a ISO 27001 certificate. See transition guide and FAQ for more details.
* **END OF TRANSITION PROCESS**

# CHECKLIST AND ACTION LOG

## Part 1 - Changes and additions to the main clauses 4 to 10 of ISO 27001:2022

| **Amendments in clauses 4 to 10 of ISO 27001:2022** | **Summary of additional, or changed, requirements within the standard** | **CLIENT ACTIONS** | **RESPONSIBILITY** | **BY WHEN** |
| --- | --- | --- | --- | --- |
| 4.2 [addition of 4.2(c)]  “which of these [interested party] requirements will be addressed through the information security management system” | Requirement to define which of the interested party requirements will result in subsequent actions being taken (such as identification of risk and implementation of risk treatment / control). |  |  |  |
| 4.4 [addition of …]  “including the processes needed [for the maintenance and improvement of the ISMS] and their interactions, in accordance with the requirements of this document. | Requirement that, dependent on the existing structure of the ISMS, organisations should consider and review ISMS processes and the implementation of process-based auditing. |  |  |  |
| 6.1.3 [amended wording underlined below]  “Annex A contains a list of possible [rather than previously “comprehensive”] information security controls.” | Change of emphasis from Annex A being ‘comprehensive’ to listing only possible controls. Organisations to consider the need for additional controls (other than just the 93 in ISO 27001:2022 Annex A) |  |  |  |
| 6.3 [new clause, aligning with other management system Standards]  “Planning of Changes” [to the ISMS] | A new requirement, aligning with other management system standard requirements, in that there should be evidence that changes made to the ISMS are made in a controlled manner. |  |  |  |
| 8.1 [additional wording underlined]  “The organisation shall ensure that externally provided process, products or services that are relevant to the ISMS are controlled”  [i.e. not just “processes” as was previously defined] | This is a clarification of existing requirements. Externally provided products and services (and processes) that are relevant to information security are to be controlled. |  |  |  |
| 9.3.2(c) [addition of]  “changes and needs and expectations of interested parties that are relevant to the information security management system.” | An enhanced requirement in that the management review is now to include “changes and needs and expectations of interested parties that are relevant to the information security management system.” |  |  |  |

## 

## Part 2 - Annex A new and changed information security controls

Notes:

1. Comprehensive guidance for determining and implementing the new and changed Annex A controls is defined in ISO 27002:2022
2. ISO 27002:2022 states “A control is defined as a measure that modifies or maintains risk”. Therefore, each of the new and changed controls in the table below, if declared applicable in the Statement of Applicability, needs to be associated with a risk (or risks) on the risk assessment.
3. Where a control is defined as being not applicable, the reason(s) should be summarised

| **New ISO 27001:2022 Annex A controls** | **Summary of changes / additions** | **CLIENT ACTIONS** | **RESPONSIBILITY** | **BY WHEN** |
| --- | --- | --- | --- | --- |
| 5.7 Threat intelligence.  Information relating to information security threats should be collected and analysed to produce threat  intelligence | Threat information to be gathered, analysed and, as necessary, addressed through risk management.  Appropriate actions should be defined to detect, respond to, prevent and to reduce threat impacts. |  |  |  |
| 5.16 Identity Management  The full life cycle of identities shall be managed. | This control is to ensure the unique identification of individuals and systems accessing an information and associated assets, thereby enabling appropriate assignment of access rights.  This control enhances the old ISO 27001:2013 control A.9.2.1  Identities can be assigned to an individual person, groups of persons, i.e. shared identities, or to a IT device or asset.  Identities should be controlled, and relevant records should be maintained.  There should be a process for managing changes to identities as well as identities provided by third parties. |  |  |  |
| 5.17 Authentication Information  Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information. | This control replaces ISO 27001:2013 controls A9.2,4, A9.3.1 and 9.4.3 but has been significantly enhanced and includes:   * personal passwords or PINs, * new, replacement or temporary authentication provision and verification of the user identity. * Authentication information transmission. * Post set-up changes to system and software default authentication information provided by suppliers / manufacturers. * Retention of records of the allocation and management of authentication information and events. * Awareness around confidentiality of authentication information |  |  |  |
| 5.23 Information security for use of cloud services.  Processes for acquisition, use, management and exit from cloud services should be established in  accordance with the organization’s information security requirements. | Cloud services should be controlled from the point of procurement, through their ongoing use and management and, when no longer required, the termination of the cloud service and transfer to another provider should be carried out in a controlled manner. Risks and controls to be considered. |  |  |  |
| 5.29 Information Security during disruption  The organisation should plan how to maintain information security at an appropriate level during disruption. | This control includes similar continuity requirements as in ISO 27001:2013 controls A17.1.1, A17.1.2, A17.1.3, i.e. developing, implementing, testing, reviewing and evaluating plans for the security of information of critical business processes following interruption or failure.  However, there is now more emphasis on “restoration”. |  |  |  |
| 5.30 ICT readiness for business continuity  ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements | Information and communication technology (ICT) readiness arrangements need to be in place and tested to cover an ICT disaster, crisis or disruption. |  |  |  |
| 6.6 Confidentiality or non-disclosure agreements  Confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. | This control includes similar non-disclosure and confidentiality requirements as the ISO 27001:2013 Annex A13.2.4 but now specifically requires signature by personnel and other relevant interested parties. |  |  |  |
| 6.7 Remote working  Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation’s premises | This has replaced the old ISO 27001:2013 control A6.2.2 “Teleworking”.  A topic-specific policy on remote working may be issued or an alternative option chosen. |  |  |  |
| 7.4 Physical security monitoring  Premises should be continuously monitored for unauthorized physical access | The physical areas that need to be monitored should be defined along with the arrangements for continual monitoring. |  |  |  |
| 7.9  Security of assets off-premises  Off-site assets shall be protected. | This enhances the old ISO 27001:2013 control A.11.2.6 with the specific addition of protection of ‘bring your own devices’ (BYOD). |  |  |  |
| 7.10  Storage media  Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation’s classification scheme and handling requirements. | This enhances the old ISO 27001:2013 controls A.8.3 and A.11.2.5.  A topic-specific policy may be created or an alternative option chosen. |  |  |  |
| 8.1 User Endpoint Devices  Information stored on, processed by or accessible via user end point devices shall be protected | This control enhances the ISO 27001:2013 Annex A6.2.1 and A11.2.8 controls for mobile devices by requiring all endpoints to be controlled, not just mobile devices. |  |  |  |
| 8.9 Configuration management  Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed. | Security configurations of hardware, software, services and networks need to be documented, implemented, monitored and reviewed, including:   * Security configurations need to be recorded. * Evidence to be available of monitoring security configurations. * Manufacturers’ default security configurations risks review. |  |  |  |
| 8.10 Information deletion  Information stored in information systems, devices or in any other storage media should be deleted when no longer required. | Information, particularly sensitive information, should be deleted when no longer needed and this includes business information not just PII.  Records should be kept of deletion, internal or those provided by external providers. |  |  |  |
| 8.11 Data masking  Data masking should be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. | Sensitive information, particularly PII, should be masked using techniques such as data masking, pseudonymization, anonymization, encryption and obfuscation.  The requirements of legislation should be considered.  Appropriate checks should be carried out to ensure that the information has been satisfactorily masked. |  |  |  |
| 8.12 Data leakage prevention  Data leakage prevention measures should be applied to systems, networks and any other devices that  process, store or transmit sensitive information. | Consideration needs to be given to what information should be subject to data leakage prevention (DLP) measures. Also, leakage channels should be considered. |  |  |  |
| 8.16 Monitoring activities  Networks, systems and applications should be monitored for anomalous behaviour and appropriate  actions taken to evaluate potential information security incidents. | The relevant networks, systems and applications that would benefit from regular monitoring for anomalous behaviour and potential security incidents should be identified.  Records of monitoring should be maintained. |  |  |  |
| 8.23 Web filtering  Access to external websites should be managed to reduce exposure to malicious content. | Access to external websites to be controlled. |  |  |  |
| 8.26 Application Security Requirements  Information security requirements should be identified, specified and approved when developing or  acquiring applications. | This control replaces the ISO 27001:2013 controls A14.1.2 and A14.1.3 controls but there is now a wider scope and clearer definition of the requirements.  Whether internally developed or acquired, application security requirements should be defined and approved.  The security requirements for transactional services should be defined, as should the security requirements for electronic ordering and payment applications. |  |  |  |
| 8.28 Secure coding  Secure coding principles should be applied to software development | Secure coding principles and minimum standards should be defined in order to reduce security vulnerabilities in developed software. |  |  |  |
| 8.34  Protection of information systems during audit testing  Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management. | This enhances the old ISO 27001:2013 control A.12.7.1 and now includes management approval. |  |  |  |

## Part 3 – Other changes necessary to a ISMS as a result of ISO 27001:2022

Notes:

1. Various other changes are likely to be required to an already operational information security management system (ISMS) as a result of addressing the changes defined in parts 1 and 2 above and transitioning to ISO 27001:2022
2. These changes are summarised below and evidence is required of the effective implementation of these in the table below

| **Oher ISMS changes** | **Other considerations** | **CLIENT ACTIONS** | **RESPONSIBILITY** | **BY WHEN** |
| --- | --- | --- | --- | --- |
| 5.2 Information Security policy [statement] …  Updated if necessary | Update as necessary. |  |  |  |
| 6.1.2 Risk assessment results | If an organisation has used the Annex A control references within their risk assessment results and risk treatment plan, the control numbers will need to be updated or a suitable cross reference provided. |  |  |  |
| 6.1.3 Statement of applicability …  updated with new controls | The Statement of Applicability needs to be updated with the new controls or a cross reference from the 2013 controls to the 2022 controls. There needs to be justification for inclusion or exclusion of the new controls. |  |  |  |
| 6.3 “Planning of Changes” [to the ISMS] | As required by clause 6.3, for the changes made to the ISMS as a result of implementing the ISO 27001:2022, there should be evidence of planning and control of these changes. |  |  |  |
| 7.2, A6.3 Competence and information security system awareness | Relevant employees and contractors should have been made aware of the new and changed requirements and controls in the ISMS to ensure that they are competent to implement and maintain these. Documented evidence of any new competences, awareness and training should be maintained |  |  |  |
| 7.5, A5.1 ISMS documentation updated if required …..  such as an ISMS manual, topic-specific policies (as defined in A5.1), audit checklists, etc. | ISMS documentation needs to be updated as required to reflect the new controls and the changed numbering of existing controls. |  |  |  |
| 9.2 Internal audits carried out by the client (of the new and changed ISO 27001:2022 requirements. Including the new Annex A controls) | The new and changed requirements in clauses 4 to 10 and in Annex A need to be subject to internal audit. CfA strongly urges clients to carry out these audits prior to the external ISO 27001:2022 transition audit. However, in lieu of the audits being completed, CfA will accept an internal audit programme that shows when these new and changed requirements will be audited within reasonable timescales and based on risk. Note also the potential need for process audits, as defined in clause 4.4 above (in part 1 of this report), if process audits were not previously carried out |  |  |  |
| 9.3 Management review carried out by the client (of the new and changed ISO 27001:2022 requirements) | The new and changed requirements in clauses 4 to 10 and in Annex A need to be subject to management review. CfA strongly urges clients to carry out this management review prior to the external ISO 27001:2022 migration audit. However, in lieu of a full management review, CfA will accept evidence of clause 9.3.2(c) only being reviewed by top management and a planned date for the full review taking place within reasonable timescales |  |  |  |