ISO 27001:2022 CLIENT GAP ANALYSIS TOOL

Instructions for use:

This gap analysis document provides a simple framework for evaluating your quality management system against the requirements of ISO 27001:2022. It is split into two tables:

- **Part 1: new concepts** – highlighting the new concepts introduced in ISO 27001:2022 and the related clauses, processes and functional activities.
- **Part 2: requirements** – highlighting amended clauses, processes and functional activities between ISO 27001:2013 and ISO 27001:2022.

Please complete each table by recording the evidence acquired from one full internal audit against the requirements of ISO 27001:2022. If you are unable to provide evidence of compliance, you may not be ready to complete the transition to ISO 27001:2022. In this case, please inform NQA that you need additional time to prepare for the transition – we will work with you to select a mutually agreeable date to complete the transition.

Please ensure that this completed document and internal audit records are available to your auditor at the opening meeting of your transition audit.

Client name: Completion date:

Part 1: New concepts

Tip: Ensure that these new concepts have been deployed in a manner that supports the **Process Approach** and **Risk-Based Thinking**.

New requirement	Phase	Clause(s)	Activity
A more explicit requirement for ensuring that interested parties, their needs and expectations relevant to the ISMS have been identified.	**Identify**	**4.2.a.b.c)**	**Have you identified interested parties relevant to the ISMS, their relevant requirements and which of these will be addressed by the ISMS?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
New requirement for the adoption of a process approach (where before this was implied).	**Identify**	**4.4**	**Has planning for the information security management system determined the processes of your organization and interactions with the ISMS?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
Explicit requirement for top management to ensure that information security roles, responsibilities and authorities are communicated within the organization.	**Action**	**5.3**	**Have top management established (and are they supportive of,) a mechanism for communicating responsibilities and authorities for roles relevant to information security within the organization?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
Information security objectives are to be monitored.	**Assess**	**6.2.d)**	**Have you established how information security objectives are to be monitored and whom shall be responsible for this?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
Changes to the ISMS are to be planned.	**Plan**	**6.3**	**Have you established a process for managing changes to the ISMS? How are changes authorised?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Clause(s)	Activity
Changes in the needs and expectations of interested parties are to be addressed during management review.	**Action**	**9.3.2.c)**	**Are the needs and expectations of interested parties (relevant to the ISMS) reviewed during MR?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Threat intelligence	**Plan**	**5.7**	**Have you identified your threat intelligence requirements based upon a risk assessment of information, information storage and information processing assets?**
			What information relating to security threats do you collect/receive?
			Is information relating to security threats analysed and if so, by whom?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Security considerations and controls for cloud services.	**Plan**	**5.23**	**Do you use any cloud services?**
			How do you determine which cloud services are required by your organization and which cloud model is the best fit (IaaS, PaaS, SaaS, etc.)?
			What controls do you have in place to monitor the performance/effectiveness of your cloud service provider?
			Have you planned for changes to or termination of your cloud service(s) provider? What are your processes for this?

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Business continuity and IT readiness	**Plan**	**5.30**	**Does your BCP include requirements to ensure the confidentiality, integrity and availability of information in BC situations?**
			Have the IT requirements for BC been tested?
			Have you established RTO/RPOs for your IT in BC situations?

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Physical security monitoring	**Action**	**7.4**	**How do you ensure that your premises are continuously monitored for unauthorised access?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Configuration management	**Action**	**8.9**	**Do you have a process for ensuring that systems are appropriately configured/hardened?**
			How do you ensure that the above process is being followed?
			Is system configuration monitored and reviewed?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Information deletion	**Plan**	**8.10**	**Have you identified what information you hold as an organization and established rules governing its retention and deletion?**
	Action	**8.10**	**How do you ensure that information (when no longer required,) is deleted from your information systems, devices or other storage media?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Data masking	**Plan**	**8.11**	**Have you identified what sensitive data you hold as an organization and established rules governing the need to mask this data?**
	Plan	**8.11**	**How is access to raw, sensitive data controlled?**
	Action	**8.11**	**Do you have a process for masking data?**
	Plan	**8.11**	**What applicable legislation have you considered with regards to data and data masking?**

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Data leakage prevention	**Action**	**8.12**	**Have you identified what sensitive information you store, process and/or transmit as an organization?**
			Have you identified the systems, apps, tools that are used to store, process and/or transmit this sensitive information?
			Have you assessed your data leakage risks?
			What processes/tools do you have in place to prevent data leakage?

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Monitoring activities	**Action**	**8.16**	**Are your networks monitored for anomalous behaviour?**
	Plan	**8.16**	**If/when detected, how is anomalous behaviour evaluated and reported?**

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Web filtering	**Action**	**8.23**	**Is access to external websites managed to reduce exposure to malicious content?**
			Are employees aware of the information security risks that unmanaged web browsing poses to the organization?

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

New requirement	Phase	Control(s)	Activity
Secure coding	**Plan**	**8.28**	**What secure coding principles and practices have you implemented in your organization?**
			How do you ascertain competence of your developers?

Evidence of compliance *(Client to complete)*	**Has the client demonstrated they have met the requirements of this clause?** *(Assessor to complete)*		**Comments if required** *(Assessor to complete)*
	Yes ☐	No ☐	

Part 2: ISO 27001:2022 Requirements

Tip: Ensure that you can demonstrate that each requirement of ISO 27001:2022 has been addressed within the ISMS.

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
4.1 Understanding the organization and its context	**No change: Have you determined your external and internal issues that are relevant to and affect the ISMS?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
4.3 Determining the scope of the quality management system	**Have external and internal issues and interested parties been considered? Have interfaces and dependencies been identified and considered?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.1 Leadership and commitment	**Can top management demonstrate their degree of leadership and commitment to the ISMS.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.2 Policy	**Is an information security policy available and appropriate to the purpose and context of the organization and does it support the strategic direction of the company?**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.1 Actions to address risks and opportunities	**6.1.2** Do you have a risk assessment process? Have you performed risk assessments of your information and information storage/ processing assets? **6.1.3** Have you produced a Statement of Applicability (SOA) and is it aligned to the new control groups and numbering system? Is the SOA version controlled and dated?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
7.1 Resources	Have resource needs been determined?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
7.4 Communication	**7.4.d)** Have you determined how to communicate?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.1 Operational planning and control	Have you established criteria for the processes identified in Clause 6 and implemented control of those processes? Are these processes and controls documented?

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
9.1 Monitoring, measurement, analysis and evaluation	Organizations are now required to ensure that monitoring and measuring produces valid, comparable and reproductive results. You must also evaluate information security performance and the effectiveness of the ISMS.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
9.2 Internal audit	This has been broken into sub clauses but with no significant change to the requirements.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this clause? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

Annex A Controls

5. Organizational controls

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.1 Policies for information security	Merging of 5.1.1 and 5.1.2 – no significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.8 Information security in project management	Merging of 6.1.5 and 14.1.1 - more explicit requirement than the originals.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.9 Inventory of information and other associated assets	Merging of 8.1.1 and 8.1.2 - No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.10 Acceptable use of information and other associated assets	Merging of 8.1.3 and 8.2.3 with an emphasis on procedures for handling information and other associated assets.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.14 Information transfer	8.2.1 – Updated control introduces the idea of 'transfer facilities' and not solely removable media.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.15 Access control	Merging of 9.1.1 and 9.1.2 - no requirement for an Access Control Policy, however rules governing access (logical and physical,) must be established and implemented.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.16 Identity management	9.2.1 – Now explicitly states 'full lifecycle' that includes registration, de-registration and change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.17 Authentication information	Merging of 9.2.4, 9.3.1, 9.4.3 – Includes reference to advising personnel on appropriate handling of authentication information.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.18 Access rights	Merging of 9.2.2, 9.2.5, 9.2.6 – No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.19 Information security in supplier relationships	15.1.1 – This now focuses on the organization's use of suppliers' products and services and not simply the suppliers' access to organizational assets and information.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.22 Monitoring, review and change management of supplier services	Merging of 15.2.1 and 15.2.2 – No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.27 Learning from information security incidents	16.1.6 – Focus is now on strengthening and improving information security controls.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.29 Information security during disruption	Merging of 17.1.1, 17.1.2, 17.1.3 – Clarifies and simplifies the old requirements.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.31 Legal, statutory, regulatory and contractual requirements	Merging of 18.1.1 and 18.1.5 – No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
5.36 Compliance with policies, rules and standards for information security	Merging of 18.2.2 and 18.2.3 – No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

6. People controls

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.4 Disciplinary process	7.2.3 – Emphasis on information security violation and not breach.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.6 Confidentiality or non-disclosure agreements (NDAs)	13.2.4 – This control now states that NDAs and CAs are to be signed.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.7 Remote working	6.2.2 – This is now explicitly aimed at remote workers and not teleworking sites.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.8 Information security event reporting	16.1.2 and 16.1.3 – No distinction between events and weaknesses. All events either observed or suspected are to be reported.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

7. Physical controls

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
7.2 Physical entry	Merging of 11.1.2 and 11.1.6 – No significant change.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
7.10 Storage media	8.3.1, 8.3.2, 8.3.3, 11.2.5 – The standard now introduces the concept of lifecycle management instead of explicit controls in the 2013 edition.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
7.12 Cabling security	11.2.3 – Cables carrying power (but not data,) are specifically included in the control.

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

8. Technological controls

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.1 User end point devices	**11.2.8 – The emphasis is now on protection of the information that is accessible by the user end point.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.4 Access to source code	**9.4.5 – Includes development tools and software libraries.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.15 Logging	**Merging of 12.4.1, 12.4.2, 12.4.3 – No significant change.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.24 Use of cryptography	**Merging of 10.1.1 and 10.1.2 – No significant change.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.26 Application security requirements	**Merging of 14.1.2 and 14.1.3 – Simplification of the existing controls.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.27 Secure system architecture and engineering principles	**14.2.5 – Introduces the requirement for secure system architecture.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.29 Security testing in development and acceptance	**Merging of 14.2.8 and 14.2.9 – No significant change.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

ISO 27001:2022	ISO 27001:2022 cross reference and the significant changes from the 2013 version
8.32 Change management	**12.1.2, 14.2.2, 14.2.3, 14.2.4 – The new combined control is less prescriptive.**

Evidence of compliance *(Client to complete)*	Has the client demonstrated they have met the requirements of this control? *(Assessor to complete)*		Comments if required *(Assessor to complete)*
	Yes ☐	No ☐	

Areas for further investigation: