



ISO 27001:2022 ANÁLISIS DE DEFICIENCIAS

Instrucciones de uso:

Este documento de análisis de deficiencias proporciona un marco sencillo para evaluar su sistema de gestión de la calidad con respecto a los requisitos de la norma ISO 27001:2022. Está dividido en dos tablas:

- **Parte 1: nuevos conceptos** - destaca los nuevos conceptos introducidos en la norma ISO 27001:2022 y las cláusulas, procesos y actividades funcionales relacionados.
- **Parte 2: requisitos** - destacando las cláusulas modificadas, los procesos y las actividades funcionales entre ISO 27001:2013 e ISO 27001:2022.

Complete el documento con las pruebas adquiridas en una auditoría interna con respecto a la norma ISO 27001:2022. Si no puede aportar pruebas de cumplimiento, es posible que no esté preparado para completar la transición a la ISO 27001:2022. En este caso, informe a NQA de que necesita tiempo adicional para preparar la transición.

Asegúrese de que este documento cumplimentado y los registros de auditoría interna estén a disposición de su auditor en la reunión de apertura de su auditoría de transición.

Cliente:

Fecha:

Parte 1: Conceptos nuevos

Consejo: Asegúrese de que los conceptos se han desarrollado soportando el Enfoque por Procesos y el Pensamiento Basado en el Riesgo.

Nuevo requisito	Fase	Claúsula	Actividad
Un requisito más explícito para garantizar que se han identificado las partes interesadas, sus necesidades y expectativas relevantes para el SGSI.	Identificar	4.2.a.b.c)	¿Ha identificado a las partes interesadas relevantes para el SGSI, sus requisitos pertinentes y cuáles de ellos serán abordados por el SGSI?
Pruebas de cumplimiento (completar por cliente)	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? (completar por auditor)		Comentarios (completar por auditor)
<input type="text"/>	Sí <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

Nuevo requisito	Fase	Claúsula	Actividad
Nuevo requisito para la adopción de un enfoque por procesos (donde antes estaba implícito).	Identificar	4.4	¿La planificación del sistema de gestión de la seguridad de la información ha determinado los procesos de su organización y las interacciones con el SGSI?
Pruebas de cumplimiento (completar por cliente)	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? (completar por auditor)		Comentarios (completar por auditor)
<input type="text"/>	Sí <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

Nuevo requisito	Fase	Claúsula	Actividad
Requisito explícito para que la alta dirección garantice que las funciones, responsabilidades y autoridades en materia de seguridad de la información se comunican dentro de la organización.	Acción	5.3	¿Ha establecido la dirección un mecanismo para comunicar las responsabilidades y autoridades de las funciones relevantes para la seguridad de la información dentro de la organización?
Pruebas de cumplimiento (completar por cliente)	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? (completar por auditor)		Comentarios (completar por auditor)
<input type="text"/>	Sí <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

Nuevo requisito	Fase	Claúsula	Actividad
Hay que supervisar los objetivos de seguridad de la información.	Evaluar	6.2.d)	¿Ha establecido cómo se van a supervisar los objetivos de seguridad de la información y quién será responsable de ello?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Claúsula	Actividad
Deben planificarse los cambios en el SGSI.	Planificar	6.3	¿Ha establecido un proceso para gestionar los cambios en el SGSI? ¿Cómo se autorizan los cambios?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Clausula	Actividad
Los cambios en las necesidades y expectativas de las partes interesadas deben abordarse durante la revisión de la gestión.	Acción	9.3.2.c)	¿Se revisan las necesidades y expectativas de las partes interesadas (relevantes para el SGSI) durante la revisión por la dirección?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Controles	Actividad
Información sobre amenazas	Planificar	5.7	¿Ha identificado información sobre amenazas basándose en una evaluación de riesgos de los activos de información, su almacenamiento y procesamiento? ¿Qué información relativa a las amenazas a la seguridad recopilan/reciben? ¿Se analiza la información relativa a las amenazas para la seguridad y, en caso afirmativo, quién lo hace?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Consideraciones y controles de seguridad para los servicios en la nube.	Planificar	5.23	¿Utiliza algún servicio en la nube?
			¿Cómo determina qué servicios en la nube necesita su organización y qué modelo de nube es el más adecuado (IaaS, PaaS, SaaS, etc.)?
			¿De qué controles dispone para supervisar el rendimiento/eficacia de su proveedor de servicios en la nube?
			¿Ha previsto cambios o la finalización de su proveedor de servicios en la nube? ¿Cuáles son sus procesos para ello?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Continuidad empresarial y preparación informática	Planificar	5.30	¿Incluye su PCB requisitos para garantizar la confidencialidad, integridad y disponibilidad de la información en situaciones de BC?
			¿Ha comprobado los requisitos informáticos para la CB?
			¿Ha establecido RTO/RPO para su TI en situaciones de BC?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Vigilancia de la seguridad física	Acción	7.4	¿Cómo se asegura de que sus instalaciones están vigiladas para evitar accesos no autorizados?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Gestión de la configuración	Acción	8.9	¿Dispone de un proceso para garantizar que los sistemas están configurados adecuadamente?
			¿Cómo se asegura de que se sigue el proceso anterior?
			¿Se supervisa y revisa la configuración del sistema?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Eliminación de información	Planificar	8.10	¿Ha identificado qué información posee como organización y ha establecido normas que rijan su conservación y eliminación?
	Acción	8.10	¿Cómo se asegura de que la información (no necesaria) se elimina de sus sistemas de información, dispositivos u otros medios de almacenamiento?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Enmascaramiento de datos	Planificar	8.11	¿Ha identificado qué datos sensibles posee como organización y ha establecido normas que regulen la necesidad de enmascarar estos datos?
	Planificar	8.11	¿Cómo se controla el acceso a datos sensibles en bruto?
	Acción	8.11	¿Dispone de un proceso para enmascarar los datos?
	Planificar	8.11	¿Qué legislación ha tenido en cuenta en relación con los datos y el enmascaramiento de datos?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Prevención de fugas de datos	Acción	8.12	¿Ha identificado qué información sensible almacena, procesa y/o transmite como organización?
			¿Ha identificado los sistemas, aplicaciones, herramientas que se utilizan para almacenar, procesar y/o transmitir esta información sensible?
			¿Ha evaluado sus riesgos de fuga de datos?
			¿De qué procesos/herramientas dispone para evitar la fuga de datos?
Pruebas de cumplimiento <i>(completar por cliente)</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? <i>(completar por auditor)</i>		Comentarios <i>(completar por auditor)</i>
	Sí <input type="checkbox"/>	No <input type="checkbox"/>	

Nuevo requisito	Fase	Control	Actividad
Actividades de seguimiento	Acción	8.16	¿Supervisa sus redes para detectar anomalías?
	Planificar	8.16	Si/cuando se detecta, ¿cómo se evalúa y se notifica el comportamiento anómalo?
Pruebas de cumplimiento / <i>U_ bMSclbadUjWfVf</i>	¿Ha demostrado el cliente que ha cumplido los requisitos de esta cláusula? / <i>U_ bMSclbadSgVfafi</i>		<i>5a_ WScjae/U_ bMSdbadSgVfafi</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>	Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>	Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>	Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this clause? <i>(Assessor to complete)</i>	Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>

ISO 27001:2022		ISO 27001:2022 cross reference and the significant changes from the 2013 version
6.1 Actions to address risks and opportunities		<p>6.1.2 Do you have a risk assessment process? Have you performed risk assessments of your information and information storage/processing assets?</p> <p>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?</p>
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)
<input type="text"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/> No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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)
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <input type="checkbox"/>	No <input type="checkbox"/>	

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 <input type="checkbox"/>	No <input type="checkbox"/>	

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 <input type="checkbox"/>	No <input type="checkbox"/>	

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 <input type="checkbox"/>	No <input type="checkbox"/>	

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 <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
	Yes <input type="checkbox"/>	No <input type="checkbox"/>	

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

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 <i>(Client to complete)</i>	Has the client demonstrated they have met the requirements of this control? <i>(Assessor to complete)</i>		Comments if required <i>(Assessor to complete)</i>
<input type="text"/>	Yes <input type="checkbox"/>	No <input type="checkbox"/>	<input type="text"/>

Areas for further investigation:

