ISO 27001:2022
GUIDA AI GAP

53,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 100 OPERATING COUNTRIES

CARBON NEUTRAL

INTRODUZIONE

Questo documento fornisce una panoramica delle principali modifiche tra la versione 2013 e 2022 della ISO 27001. I nuovi requisiti sono mostrati di seguito. Dovrai prepararti al cambiamento e adattare il tuo sistema di gestione della sicurezza delle informazioni per soddisfare i nuovi requisiti e le tempistiche di transizione.

STRUTURA DELLA ISO 27001:2022

La struttura della ISO 27001:2022 segue la struttura di alto livello definita in Annex SL:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Annex A

5. Organizational controls
6. People controls
7. Physical controls
8. Technological controls

I NOSTRI VALORI

Ti aiuteremo a comprendere i cambiamenti, a interpretare i nuovi concetti e il modo in cui influiscono sul tuo Sistema di gestione ISMS.

Non esitate a contattarci se avete domande.

GAP GUIDE AND GUIDANCE

N.	REQUISITI	GAP
4	**Context of the organization**	
4.2	Understanding the needs and expectations of interested parties	Questo controllo richiede adesso esplicitamente che la tua organizzazione sia in grado di dimostrare quale dei requisiti rilevanti delle parti interessate deve esser soddisfatto attraverso l'ISMS.
4.4	Information Security Management System (ISMS)	Ora l'organizzazione deve concentrarsi sui processi e su come interagiscono con l'ISMS.
5	**Leadership**	
5.3	Organizational roles, responsibilities and authorities	Questo requisito introduce un esplicito riferimento in merito alla comunicazione dei ruoli, responsabilità e autorità all'interno della propria organizzazione.
6	**Planning**	
6.2.d	Information security objectives and planning to achieve them	Gli obiettivi sulla sicurezza delle informazioni devono essere stabiliti ai livelli pertinenti all'interno dell'organizzazione. La ISO 27001:2022 richiede il monitoraggio degli obiettivi e dei progressi per il loro raggiungimento.
6.3	Planning of changes	Questo è un nuovo requisito. L'organizzazione deve adesso dimostrare come pianifica eventuali modifiche all'ISMS.
9	**Performance evaluation**	
9.3.2.c	Management review inputs	Durante il riesame della direzione, l'organizzazione deve valutare eventuali modifiche alle esigenze e alle aspettative delle parti interessate rilevanti.

ANNEX A

N.	REQUISITI	GAP
5	**Organizational controls**	
5.7	Threat intelligence	La Threat Intelligence consiste nella raccolta sistemica ed analisi di informazioni (log) relative a minacce alla sicurezza delle informazioni (non necessariamente incidenti), allo scopo di analizzarle e produrre misure di resilienza preventive o correttive.
5.23	Information security for use of cloud services	In conseguenza dell'uso sempre più diffuso dei provider cloud, il controllo richiede vengano istituiti processi che garantiscano che l'uso del cloud applichi concetti di sicurezza specificati, gestiti e amministrati, a partire dall'analisi dell'offerta/contratto del fornitore.
5.30	ICT readiness for business continuity	Questo controllo richiede l'identificazione dei requisiti di business continuity delle infrastrutture ITC (server e rete) che impattano sul business aziendale, al fine di dimostrare di essere pronti a reagire (piano di business continuity) in caso di eventi avversi.
7	**Physical controls**	
7.4	Physical security monitoring	Sebbene non sia un concetto nuovo, lo standard ora introduce l'obbligo di stabilire e attuare le modalità più opportune per monitorare i locali in cui vengono custoditi gli Asset, dentro e fuori gli orari di presenza lavorativa, per prevenire o controllare sistemicamente eventuali accessi fisici non autorizzati.

ANNEX A

N.	REQUISITI	GAP
8	**Technological controls**	
8.9	Configuration management	I cambi incontrollati di configurazioni hardware e software e di sistemi operativi introducono vulnerabilità. Il controllo chiede di definire le configurazioni degli Asset che custodiscono le informazioni ed istituire un meccanismo di controllo volto alla identificazione di minacce, punti deboli e vulnerabilità alle configurazioni di sicurezza.
8.10	Information deletion	Questo controllo richiede delle politiche di cancellazione sicura delle informazioni sensibili che non è più necessario o non si è più titolati a custodire, anche in relazione ai principi legali e normativi applicabili .
8.11	Data masking	Un nuovo requisito che richiede un incremento della protezione dei dati più sensibili utilizzando tecniche di mascheratura indirizzate rispetto ai requisiti legali, statutari, contrattuali o normativi applicabili
8.12	Data leakage prevention	Questo nuovo controllo richiede l'implementazione di misure di prevenzione della perdita indesiderata (leakage) di dati causate da accessi, trasferimenti o estrazioni non autorizzate di informazioni.
8.16	Monitoring activities	Questo controllo è un'estensione della "ISO 27001:2013 A.12.4 Registrazione e monitoraggio". All'organizzazione è richiesto di stabilire monitoraggi in continuo di reti e sistemi per rilevare proattivamente comportamento anomali o sospetti tale, una volta stabiliti i relativi criteri soglia
8.23	Web filtering	L'introduzione di questo controllo enfatizza la necessità di stabilire policy tecniche per prevenire attacchi cyber via web o quantomeno prevenire l'accesso a siti con contenuti non in linea con le politiche etiche aziendali.
8.28	Secure coding	Le organizzazioni sono tenute a garantire principi di codifica sicura applicati durante tutto il ciclo di vita dello sviluppo del sofware. Con l'applicazione di questo controllo le organizzazioni sono tenute a dimostrare che nel corso della scrittura del codice non si introducano violazioni ai principi di sicurezza delle informazioni.

Dichiarazione di applicabilità

La Dichiarazione di Applicabilità (SOA) deve contenere i controlli necessari e la giustificazione per la loro inclusione, se questi sono implementati o meno e la giustificazione per eventuali controlli esclusi.

Le organizzazioni devono aver mappato la loro precedente SOA rispetto ai requisiti della norma ISO 27001:2022. L'uso di attributi, che non è obbligatorio, può essere introdotto per comprendere meglio i controlli e il modo in cui affrontano le aree di rischio identificate dalla propria organizzazione.

Valutazione dei rischi/ registrazioni

Il valutatore deve avere evidenze che le valutazioni dei rischi e le registrazioni siano stati aggiornati per tenere conto dei nuovi controlli introdotti dalla norma ISO 27001:2022.

NEXT STEPS

Prepararsi alla transizione alla ISO 27001

- Le organizzazioni devono effettuare la transizione del proprio **sistema di gestione** in conformità con i requisiti della norma ISO 27001:2022 prima che venga condotto l'audit di transizione. Ciò deve includere eventuali modifiche alla documentazione, insieme alle evidenze di eventuali requisiti di processo nuovi o modificati.
- Si sottolinea che le organizzazioni devono condurre un audit interno e un riesame della direzione dei nuovi requisiti prima che venga condotto l'audit di transizione NQA.
- Le organizzazioni possono sottoporsi a una 'transition gap assessment' condotta da NQA prima dell'audit ufficiale di transizione. Ciò potrebbe essere condotto in concomitanza con una precedente sorveglianza ISO 27001:2013, o in qualsiasi altro momento autonomo prima dell'audit di transizione.

Il tuo audit di transizione alla norma ISO 27001

- Tutte le organizzazioni devono sottoporsi a un audit di transizione per confermare l'implementazione del nuovo standard. L'audit di transizione può essere condotto congiuntamente ad un audit esistente, oppure può essere un audit a sé stante.
- Se l'audit di transizione viene condotto in concomitanza con un audit di sorveglianza esistente (ovvero sorveglianza in transizione) o di ricertificazione (ovvero ricertificazione in transizione) verrà aggiunto ulteriore tempo alla durata dell'audit per coprire i nuovi requisiti introdotti dalla ISO 27001: 2022.
- Se per l'audit di transizione viene effettuato un audit autonomo, la durata sarà specificatamente calcolata.

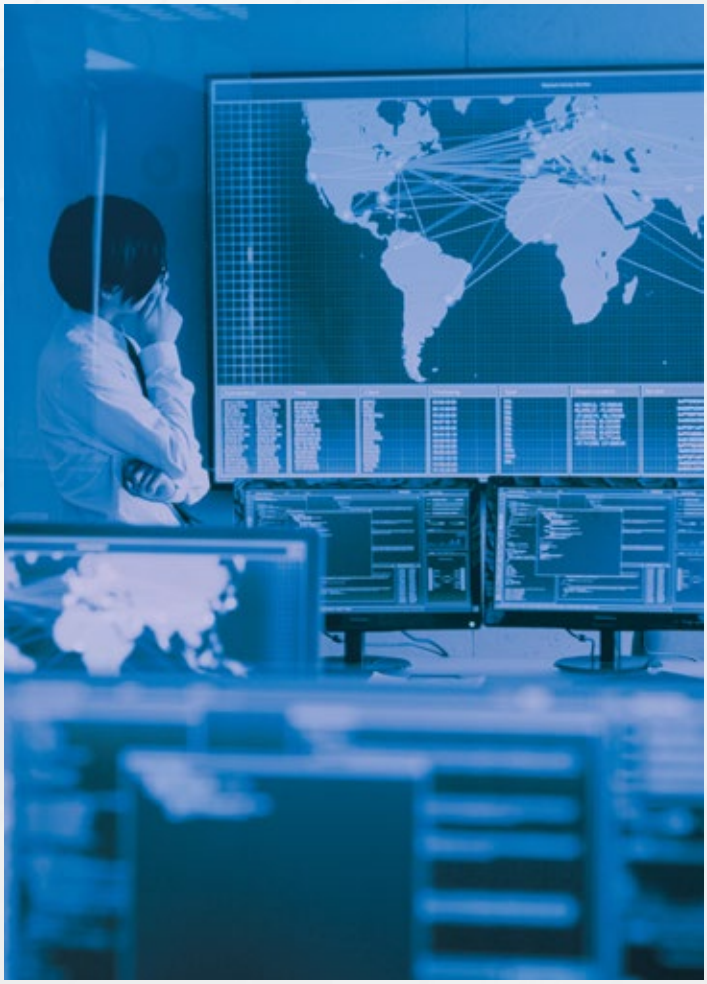
Nota: *La durata specifica degli audit di transizione dipenderà dalle dimensioni della tua organizzazione e dalla complessità dell'ISMS. NQA ti informerà sulla durata specifica dell'audit di transizione.*

Riemissione dei Certificati ISO 27001:2022

Come per qualsiasi audit, le non conformità identificate durante un audit di transizione richiederanno la presentazione e l'approvazione di un piano di azioni correttive. Una certificazione ISO 27001:2022 aggiornata verrà rilasciata a seguito dell'approvazione delle azioni correttive.

L'emissione e la validità del certificato ISO 27001:2022 aggiornato saranno le seguenti:

- **Sorveglianza in transizione**
  L'attuale data di validità dell'organizzazione verrà mantenuta.
- **Ricertificazione in transizione**
  Verrà emessa una nuova data di validità triennale.
- **Transizione autonoma**
  L'attuale data di validità dell'organizzazione verrà mantenuta.



nqa.

www.nqa.com