CONFORMITÀ AI REQUISITI 27001:2017

CHECK LIST-01

Informazioni per l'impiego della check list

La presente check list ha lo scopo di elencare i requisiti della norma **ISO 27001:2017**, nella loro formulazione più generale, per consentire all'organizzazione di verificare e comprendere se il sistema di gestione per la sicurezza delle informazioni viene strutturato, mantenuto e migliorato secondo i requisiti normativi.

I punti della check list riguardano la struttura più alta della norma quella denominata High Level Structure (HLS). L'attenzione rivolta alla struttura più alta della norma è giustificata dall'opportunità di assicurare la possibilità di integrare tale sistema di gestione della sicurezza delle informazioni con altri sistemi **ISO** che si basano sulla medesima struttura quali:

- Il sistema di gestione per la qualità (ISO 9001)
- Il sistema di gestione dell'ambiente (ISO 14001)
- Il sistema di gestione per la sicurezza sul lavoro (ISO 45001)
- Il sistema di gestione per la prevenzione della corruzione (ISO 37001)
- Il sistema di gestione dell'innovazione tecnologica (ISO 56002)

L'HLS, per quanto possibile, permette un'apprezzabile compatibilità anche con i sistemi che gestiscono i requisiti relativi alla prevenzione dei reati presupposto previsti dal D.Lgs.n.231/01, per i quali l'organizzazione si "protegge" dalla responsabilità amministrativa. Anche i sistemi che gestiscono la privacy alla luce del nuovo regolamento europeo 679/2016 (GDPR) di solito apprezzano l'applicazione di tale struttura.

Eventuali check list che approfondiscono la verifica della conformità dei requisiti appartenenti ad un livello sottostante della struttura della norma vengono redatte, in relazione alle esigenze del piano di audit, dall'Internal Auditor e indicate all'interno del piano.

CONFORMITÀ AI REQUISITI 27001:2017

CHECK LIST-01

PUNTO	CONTROLLI	NC	DESCRIZIONE
6.2	▪ Sono stati stabiliti gli obiettivi per la sicurezza delle informazioni? ▪ Tali obiettivi sono coerenti con la politica? ▪ È stata documentata la pianificazione per il raggiungimento degli obiettivi di sicurezza delle informazioni?	☐	
7.1	▪ L'organizzazione ha determinato e messo a disposizione le risorse necessarie al funzionamento del sistema di gestione?	☐	
7.2	▪ L'organizzazione seleziona le persone in relazione alle competenze necessarie per far funzionare il sistema di gestione? ▪ L'organizzazione provvede alle attività formative inerenti alle competenze necessarie?	☐	
7.3	▪ Le persone che lavorano nell'organizzazione sono consapevoli della politica per la sicurezza delle informazioni? ▪ Sono consapevoli della maniera in cui possono contribuire al perseguimento dell'obiettivo strategico (finalità strategica) del sistema di gestione? ▪ Sono consapevoli delle conseguenze di eventuali non conformità?	☐	
7.4	▪ L'organizzazione ha disciplinato la comunicazione interna ed esterna in merito ai contenuti del sistema di gestione?	☐	
7.5	▪ L'organizzazione ha sviluppato un sistema documentale coerente? ▪ Sono disciplinate le modalità con cui i documenti sono creati ed aggiornati? ▪ Le informazioni documentate del sistema sono gestite in maniera tale da permettere il funzionamento efficiente del sistema?	☐	
8.1	▪ L'organizzazione ha stabilito e documentato i processi che permettono di tenere al sicuro le informazioni? ▪ L'organizzazione ha stabilito la modalità con cui le procedure che disciplinano i processi vengono adeguate ai cambiamenti del contesto?	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST- 02

Informazioni per l'impiego della check list

La presente check list riporta, conformemente a quanto dispone l'Annex A della norma ISO 27001:2017, i controlli previsti per la sicurezza delle informazioni impiegati dall'organizzazione.

In relazione a ciascun controllo è presente il numero identificativo che corrisponde al numero del controllo stabilito dall'Annex A, il titolo e la relativa descrizione. In fase di audit, ciascun controllo indicato dall'allegato **MOD-610-B- Piano di sicurezza delle informazioni,** e riportato nella check list presente, deve essere verificato nella sua effettiva ed efficace attuazione.

In assenza della sua applicazione o in presenza di evidenti disfunzioni applicative che ne rendono l'impiego non compiutamente efficace, l'organizzazione segnala la non conformità e la descrive brevemente affinché venga riportata nei documenti di audit e in quelli relativi alla gestione delle non conformità.

Lo scopo della check list infatti è quella di costituire una griglia di conformità da impiegare in maniera rapida e sinottica per assicurare di non trascurare nessun controllo previsto dalla norma (Annex A) e ritenuto applicabile dall'organizzazione

	POLITICA PER LA SIUREZZA DELLE INFORMAZIONI			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
5.1.1	Politica per la sicurezza delle informazioni	Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.	☐	
5.1.2	Riesame delle politiche per la sicurezza delle informazioni	Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST- 02

7	SICUREZZA DELLEL RISORSE UMANE			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
7.1.1	Screening	Devono essere svolti dei controlli per la verifica del background su tutti i candidati all'impiego in accordo con le leggi, con i regolamenti pertinenti e con l'etica e devono essere proporzionati alle esigenze di business, alla classificazione delle informazioni da accedere e ai rischi percepiti	☐	
7.1.2	Termini e condizioni di impiego	Gli accordi contrattuali con il personale e con i collaboratori devono specificare le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni.	☐	
7.2.1	Responsabilità della direzione	La direzione deve richiedere a tutto il personale e ai collaboratori di applicare la sicurezza delle informazioni in conformità con le politiche e le procedure stabilite dall'organizzazione.	☐	
7.2.2	Consapevolezza, istruzione, formazione e addestramento della sicurezza delle informazioni	Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.	☐	
7.2.3	Processo disciplinare	Deve essere istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni	☐	
7.3.1	Cessazione o variazione delle responsabilità durante il rapporto di lavoro	Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o al collaboratore e resi effettivi.	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST 02

8	GESTIONE DEGLI ASSET			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
8.1.1	Inventario degli asset	Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato	☐	
8.1.2	Responsabilità degli asset	Gli asset censiti nell'inventario devono avere un responsabile	☐	
8.1.3	Utilizzo accettabile degli asset	Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate.	☐	
8.1.4	Restituzione degli asset	Tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato	☐	
8.2.1	Classificazione delle informazioni	Le informazioni devono essere classificate in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate	☐	
8.2.2	Etichettatura delle informazioni	Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione	☐	
8.2.3	Trattamento degli asset	Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione	☐	
8.3.1	Gestione dei supporti rimovibili	Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione	☐	
8.3.2	Dismissione dei supporti	La dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali	☐	
8.3.3.	Trasporto dei supporti fisici	I supporti che contengono informazioni devono essere protetti da accessi non autorizzati, utilizzi impropri o manomissioni durante il trasporto	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST-02

9	CONTROLLO DEGLI ACCESSI			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
9.1.1	Politica di controllo degli accessi	Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni	☐	
9.1.2	Accesso alle reti e ai servizi di rete	Agli utenti devono essere forniti solo degli accessi alle reti ed ai servizi di rete per il cui uso sono stati specificatamente autorizzati	☐	
9.2.1	Registrazione e de-registrazione degli utenti	Deve essere attuato un processo formale di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di accesso	☐	
9.2.2	Provisioning degli accessi degli utenti	Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi	☐	
9.2.3	Gestione dei diritti di accesso privilegiato	L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati	☐	
9.2.4	Gestione delle informazioni segrete di autenticazione degli utenti	L'assegnazione di informazioni segrete di autenticazione deve essere controllata attraverso un processo di gestione formale	☐	
9.2.5	Riesame dei diritti di accesso degli utenti	I responsabili degli asset devono riesaminare ad intervalli regolari i diritti di accesso degli utenti	☐	
9.2.6	Rimozione o adattamento dei diritti di accesso	I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione.	☐	
9.3.1	Utilizzo delle informazioni segrete di autenticazione	Gli utenti devono essere tenuti a seguire le prassi dell'organizzazione nell'uso di informazioni segrete di autenticazione	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST- 02

15	RELAZIONE CON I FORNITORI			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
15.1.1	Politica per la sicurezza delle informazioni nei rapporti con i fornitori	I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori devono essere concordati con i fornitori stessi e documentati	☐	
15.1.2	Indirizzare la sicurezza all'interno degli accordi con i fornitori	Tutti i requisiti relativi alla sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione	☐	
15.1.3	Filiera di fornitura per l'ICT (Information and communication technology)	Gli accordi con i fornitori devono includere i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT	☐	
15.2.1	Monitoraggio e riesame dei servizi dei fornitori	Le organizzazioni devono regolarmente monitorare, riesaminare e sottoporre a audit l'erogazione dei servizi da parte dei fornitori	☐	
15.2.2	Gestione dei cambiamenti ai servizi dei fornitori	I cambiamenti alla fornitura dei servizi da parte dei fornitori, incluso il mantenimento e il miglioramento delle attuali politiche, procedure e controlli per la sicurezza delle informazioni, devono essere gestiti, tenendo conto della criticità delle informazioni di business, dei sistemi e processi coinvolti e della rivalutazione dei rischi	☐	

APPLICAZIONE DEI CONTROLLI DI SICUREZZA (ANNEX A 27001:2017)

CHECK LIST- 02

16	GESTIONE INCIDENTI ALLA SICUREZZA DELLE INFORMAZIONI			
PUNTO	**CATEGORIA**	**CONTROLLI**	**NC**	**DESCRIZIONE DELLA NON CONFORMITÀ**
16.1.1	Responsabilità e procedure	Devono essere stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni	☐	
16.1.2	Segnalazione degli eventi relativi alla sicurezza delle informazioni	Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali	☐	
16.1.3	Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni	Deve essere richiesto a tutto il personale ed ai collaboratori che utilizzano i sistemi informativi ed i servizi dell'organizzazione di registrare e segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi	☐	
16.1.4	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	Gli eventi relativi alla sicurezza devono essere valutati e deve essere deciso se classificarli come incidenti relativi alla sicurezza delle informazioni	☐	
16.1.5	Risposta agli incidenti relativi alla sicurezza delle informazioni	Si deve rispondere agli incidenti relativi alla sicurezza delle informazioni in accordo alle procedure documentate	☐	
16.1.6	Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto degli incidenti futuri	☐	
16.1.7	Raccolta di evidenze	L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze	☐	