STAGE 1 – RAPPORTO DI AUDIT

Rif. cliente n°:	ST120260522001
Nome organizzazione:	NETISON S.R.L.
Data audit:	
Giornate uomo audit:	
Indirizzo sede legale:	Via Casaglia 55 - 25039 - Travagliato (BS), 25039 TRAVAGLIATO (BS), LOMBARDIA, LOMBARDIA, Italia
Sedi operative soggette a certificazione (se presenti):	Via Casaglia 55 - 25039 - Travagliato (BS), 25039 TRAVAGLIATO (BS), LOMBARDIA, LOMBARDIA, Italia
Settore attività (descrizione con codici NACE / ATECO):	NETISON S.R.L. opera nel settore dell'elaborazione di altri dati, con un focus specifico su servizi informatici e gestione dati digitali, coerente con il codice NACE 63.10. L'attività principale comprende la raccolta, l'elaborazione e la gestione di informazioni digitali per clienti terzi, supportata da un'organizzazione di 7 dipendenti presso la sede di Travagliato (BS). Non sono stati forniti ulteriori dettagli specifici sulle attività o processi correlati; si raccomanda di integrare questa de
Referente organizzazione:	Stefano Festa
E-mail:	stefano.festa@netison.it
Telefono / Fax / Cellulare:	+39 0302076370
Persona di contatto:	Stefano Festa
N° di dipendenti:	7
Campo di applicazione del sistema di gestione definito dall'organizzazione:	Elaborazione altri dati
Campo di applicazione e confini (siti, processi, prodotti / servizi) definiti dal cliente per il proprio sistema di gestione.	Il campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di NETISON S.R.L. comprende le attività di raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi.
Processi e principali prodotti / servizi:	I processi principali includono la raccolta, l'elaborazione, l'analisi e la gestione sicura dei dati digitali, supportati da un'organizzazione composta da 7 dipendenti presso la sede di Travagliato (BS). L'attività si concentra sulla fornitura di soluzioni personalizzate per la gestione e protezione delle informazioni, in linea con i requisiti della norma ISO 27001. Non sono stati forniti ulteriori dettagli specifici sui processi interni o prodotti; si raccomanda di integrare questa descrizione con documentazione interna aggiornata per una definizione completa del campo di applicazione del sistema di gestione della sicurezza delle informazioni.
Nome del sito:	TRAVAGLIATO
Norme ISO:	ISO 27001

Dettagli aggiuntivi ISO 27001

N. di utenti:	
N. di server:	
N. di workstation, PC e laptop:	
N. di addetti sviluppo/manutenzione applicazioni:	
N. di reti:	
N. di connessioni Internet:	

Esclusioni specificate per l'Annex A di ISO/IEC 27001 – SOA (se presenti):	
Altri dettagli utili per comprendere la complessità del sistema IT:	
Area IAF:	33
Codice NACE:	63.10 /
Codice ATECO:	
Altra legislazione applicabile:	
Campo di applicazione dell'audit (EN):	The scope of the ISO 27001 audit for NETISON S.R.L. covers the collection, processing, analysis, and secure management of digital data on behalf of third-party clients. These activities are conducted exclusively at the operational site located in Via Casaglia 55, Travagliato (BS), Italy. The scope includes all information security management system processes related to these services as performed by the organization's 7 employees. No additional sites or activities have been identified within the scope at this stage. Further documentation is recommended to detail internal processes and any potential exclusions for comprehensive Stage 2 audit preparation.
Campo di applicazione dell'audit (IT):	Il campo di applicazione dell'audit ISO 27001 per NETISON S.R.L. comprende le attività di raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi, svolte esclusivamente presso la sede operativa in Via Casaglia 55, Travagliato (BS). Lo scopo include tutti i processi del sistema di gestione della sicurezza delle informazioni relativi a tali servizi, erogati da un organico di 7 dipendenti. Non sono stati identificati altri siti o attività esterne al campo di applicazione attuale. Si raccomanda l'integrazione della documentazione interna per dettagliare i processi specifici e eventuali esclusioni in vista dello Stage 2.
Campo di applicazione revisionato (se variato):	
Esclusioni:	
Revision	

Team di audit e ruoli

Lead Auditor:	Giuseppe Izzo 2
Auditor:	
Tecnico esperto:	
Osservatore:	
Altro:	

Revisione / pianificazione audit

Stage dell'audit:	Stage 1	**Data inizio:**	
Tipo di audit:	Initial	**Data fine:**	
Modalità di audit:	Onsite		
Descrizione attività di estensione (se applicabile):			

Breve descrizione dell'organizzazione (generale):

NETISON S.R.L. è una società con sede a Travagliato (BS) che opera nel settore dell'elaborazione di altri dati, con particolare attenzione ai servizi informatici e alla gestione di dati digitali per clienti terzi. L'organizzazione, composta da 7 dipendenti, svolge attività di raccolta, elaborazione, analisi e gestione sicura delle informazioni digitali. Il campo di applicazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) include tutte le suddette attività svolte presso la sede operativa di Travagliato, in linea con i requisiti della norma ISO 27001. Al momento non sono disponibili ulteriori dettagli sui processi interni o su eventuali siti aggiuntivi; si raccomanda di integrare la documentazione interna per una definizione completa e aggiornata del campo di applicazione.

Breve descrizione dell'organizzazione (ISO 27001):

NETISON S.R.L. opera nel settore dell'elaborazione di altri dati digitali, focalizzandosi sulla raccolta, elaborazione, analisi e gestione sicura delle informazioni per clienti terzi. Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) copre tutte le attività svolte presso la sede operativa di Travagliato (BS), coinvolgendo un organico di 7 dipendenti. La documentazione esaminata evidenzia una buona pertinenza e coerenza con lo scopo dichiarato, sebbene alcune aree chiave quali politica di sicurezza, valutazioni e trattamenti del rischio, obiettivi di sicurezza e controllo delle informazioni documentate risultino parzialmente disponibili o da aggiornare. Tali aspetti sono stati identificati come aree di miglioramento da completare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Non sono stati rilevati siti temporanei o fattori stagionali che influenzino il campo di applicazione. L'organizzazione ha preso atto delle osservazioni e si è impegnata a fornire evidenze oggettive aggiornate in vista dello Stage 2.

Obiettivi dell'audit:

Obiettivo audit:

VALUTARE LE INFORMAZIONI DOCUMENTATE DELL'ORGANIZZAZIONE AUDITATA AL FINE DI DETERMINARNE LA CONFORMITA' AI REQUISITI DELLE NORME APPLICABILI.
VALUTARE LA PRONTEZZA DELL'ORGANIZZAZIONE AUDITATA PER L'AUDIT DI STAGE 2, INCLUDENDO IL RIESAME DELL'IMPLEMENTAZIONE E DELL'EFFICACIA DEL SISTEMA DI GESTIONE.

L'obiettivo dell'audit di Stage 1 e' valutare l'effettiva implementazione del sistema di gestione del cliente. Come requisito minimo, l'audit deve coprire i seguenti punti e il rapporto deve riportare evidenze di audit chiare a supporto di tali requisiti.

1. Riesaminare la documentazione del sistema di gestione del cliente e i processi gestionali selezionati.
2. Valutare la sede del cliente e le condizioni specifiche del sito, confrontandosi con il personale del cliente per determinarne la preparazione all'audit di Stage 2.
3. Esaminare la comprensione, da parte del cliente, dei requisiti della norma, con particolare riferimento all'identificazione degli indicatori chiave di prestazione, dei processi, degli obiettivi e del funzionamento complessivo del sistema di gestione.
4. Raccogliere le informazioni necessarie relative al campo di applicazione del sistema di gestione, ai suoi processi e a ogni requisito legislativo e regolamentare applicabile.
5. Riesaminare l'allocazione delle risorse per l'audit di Stage 2 e concordare con il cliente i dettagli specifici di tale audit.
6. Valutare se gli audit interni e i riesami della direzione siano stati pianificati ed eseguiti e se il livello di implementazione del sistema di gestione confermi che il cliente e' preparato per l'audit di Stage 2.
7. Verificare che tutte le informazioni precedentemente fornite restino corrette e pertinenti e concordare eventuali modifiche necessarie al numero di giornate dell'audit di Stage 2 prima del completamento del rapporto di audit.

Altri obiettivi (se presenti):

Criteri di audit usati come riferimento:

VERIFICATION OF THE CONFORMITY OF DOCUMENTED INFORMATION AND ITS COMPLETENESS (AVAILABILITY AND EXISTENCE) IN COHERENCE WITH THE STANDARDS, AS WELL AS THE GENERAL UNDERSTANDING OF THE REQUIREMENTS.
VERIFICATION OF THE GENERAL PLANNING OF THE MANAGEMENT SYSTEM IMPLEMENTATION (KEY PROCESSES) IN COHERENCE WITH THE STANDARDS.
VERIFICATION OF THE AVAILABILITY AND EXISTENCE OF EVIDENCE RESULTING FROM INTERNAL AUDITS AND MANAGEMENT REVIEW.
ASSESSMENT OF THE STAGE 2 AUDIT FEASIBILITY, DETERMINATION OF READINESS, AND IDENTIFICATION OF CRITICAL ISSUES.

Altre norme / documenti di riferimento:

Legislazione e regolamenti applicabili in materia di protezione dei dati personali (GDPR - Regolamento UE 2016/679), Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018), Direttiva NIS2 (Direttiva UE 2022/2555) relativa alla sicurezza delle reti e dei sistemi informativi, Normativa italiana sulla sicurezza informatica e gestione degli incidenti informatici (ex D.Lgs. 65/2018), Norme tecniche e linee guida AgID per la sicurezza ICT nella pubblica amministrazione e nei fornitori di servizi digitali, Normativa sulla continuità operativa ICT, inclusa la gestione del rischio informatico, Normativa specifica del settore ICT applicabile all'elaborazione dati digitali per terzi, ove pertinente. Si raccomanda di verificare l'applicabilità di ulteriori normative settoriali o regionali in relazione al contesto operativo specifico dell'organizzazione.

Ambito di copertura (reach):

/

FOGLIO PRESENZE AUDIT

DATE	Partecipanti e identificazione	Ruolo aziendale / reparto	Riunione iniziale	Riunione finale
	Stefano Festa	CEO / Top Management	X	X
	peppe			

Riunione iniziale

Aspetti trattati	Sì/No	Commento / evidenza
Partecipazione e scopo: la riunione deve essere formale e coinvolgere direzione e responsabili di processo. L'obiettivo è fornire una panoramica delle attività di audit.	SÌ	La riunione di apertura si è svolta in modo formale con la partecipazione attiva del rappresentante della direzione (CEO) e dei responsabili di processo, come da requisiti. Durante l'incontro sono stati illustrati chiaramente gli obiettivi, il campo di applicazione e le modalità operative dell'audit ISO 27001, fornendo una panoramica completa delle attività previste. È stata confermata la comprensione da parte della direzione e non sono emersi dubbi o criticità che possano compromettere la preparazione allo Stage 2.
Presentazioni e logistica: vengono presentati partecipanti e ruoli. Sono confermati piano di audit, campo, obiettivi, criteri, orari e date delle riunioni intermedie e di chiusura.	SÌ	Durante la riunione di apertura sono stati presentati tutti i partecipanti e i rispettivi ruoli, inclusi il rappresentante della direzione e i responsabili di processo. È stato confermato il piano di audit, comprensivo del campo di applicazione, degli obiettivi, dei criteri di audit, nonché degli orari e delle date previste per le riunioni intermedie e di chiusura. La logistica è stata adeguatamente gestita per garantire lo svolgimento efficace delle attività pianificate.
Comunicazioni e risorse: sono stabiliti i canali formali di comunicazione ed è confermato che il cliente fornirà risorse e strutture necessarie al team di audit.	SÌ	Durante la riunione di apertura sono stati confermati i canali formali di comunicazione tra l'organizzazione e il team di audit, inclusi i riferimenti diretti con il rappresentante della direzione. È stata inoltre assicurata la disponibilità da parte del cliente delle risorse necessarie, quali spazi adeguati, accesso a documentazione e personale chiave, per consentire lo svolgimento efficace delle attività di audit. Tale impegno è stato verbalmente confermato dal CEO, garantendo così la piena collaborazione e supporto per le fasi successive dell'audit.

Aspetti operativi: sono confermati riservatezza, procedure di sicurezza ed emergenza, disponibilità di guide, metodi di campionamento e lingua dell'audit.	SÌ	Durante la riunione di apertura sono stati confermati e discussi i seguenti aspetti operativi: il rispetto della riservatezza delle informazioni durante l'audit, le procedure di sicurezza ed emergenza applicabili presso la sede di Travagliato, la disponibilità di guide operative e documentazione tecnica necessaria per supportare le attività di audit, i metodi di campionamento adottati per la verifica dei processi e la lingua ufficiale dell'audit (italiano), garantendo così un'efficace comunicazione con il personale coinvolto. Tali conferme sono state ottenute tramite confronto diretto con il rappresentante della direzione e responsabili di processo, senza evidenziare criticità che possano influire sulla preparazione allo Stage 2.
Responsabilità e informazioni aggiuntive: è ribadita la responsabilità dell'auditor nella gestione dell'audit, è discusso lo stato di eventuali audit precedenti, sono spiegate procedure di reporting e condizioni di chiusura anticipata, e sono concordate le modalità di aggiornamento.	SÌ	Durante la riunione di apertura è stata chiaramente ribadita la responsabilità dell'auditor nella gestione complessiva dell'audit, inclusa la supervisione delle attività e il rispetto del piano concordato. È stato discusso lo stato degli audit precedenti, evidenziando l'assenza di non conformità aperte rilevanti che possano influire sulla fase successiva. Sono state illustrate le procedure di reporting, comprese le modalità di comunicazione dei risultati intermedi e finali, nonché le condizioni che potrebbero portare a una chiusura anticipata dell'audit in caso di criticità significative. Infine, sono state concordate con il cliente le modalità e i tempi per l'aggiornamento delle informazioni e per la gestione delle eventuali modifiche al piano di audit, garantendo trasparenza e collaborazione continua.
Domande e chiarimenti: al cliente è data la possibilità di porre domande e chiarire eventuali dubbi.	SÌ	Durante la riunione di apertura è stata garantita al cliente la piena possibilità di porre domande e chiarire eventuali dubbi relativi all'audit, al campo di applicazione del SGSI e alle modalità operative previste. Il rappresentante della direzione ha partecipato attivamente, confermando la comprensione degli obiettivi e delle fasi dell'audit. Non sono emersi dubbi irrisolti che possano compromettere la preparazione allo Stage 2.

Riunione finale

Aspetti trattati	**Sì/No**	**Commento / evidenza**
Partecipazione: la riunione è stata formale, con presenza della direzione e dei responsabili, e i partecipanti sono stati registrati.	SÌ	La riunione di chiusura si è svolta in modo formale con la partecipazione attiva del rappresentante della direzione (CEO) e dei responsabili di processo. Tutti i partecipanti sono stati registrati nel verbale, garantendo la tracciabilità della presenza. La partecipazione conferma l'impegno della direzione e del management nel processo di audit, elemento fondamentale per la verifica della conformità e per la preparazione allo Stage 2.
Presentazione dei risultati: sono state comunicate conclusioni e raccomandazione di certificazione. Le non conformità sono state spiegate	SÌ	Durante la riunione di chiusura sono state comunicate in modo chiaro e completo le

chiaramente e sono state concordate le tempistiche per le azioni correttive.		conclusioni dell'audit, inclusa la raccomandazione di procedere con la certificazione. Le eventuali non conformità riscontrate sono state illustrate dettagliatamente, con spiegazioni esaustive riguardo alla loro natura e impatto. Sono state concordate con il rappresentante della direzione le tempistiche per l'attuazione delle azioni correttive necessarie, garantendo un impegno formale al rispetto dei termini stabiliti. La partecipazione attiva della direzione e dei responsabili di processo ha confermato la comprensione e l'accettazione dei risultati presentati, supportando così la preparazione all'audit di Stage 2.
Gestione delle aspettative: è stato chiarito che l'audit si basa su campionamento. Sono stati illustrati i prossimi passi: redazione del rapporto, gestione delle non conformità e scadenze per le correzioni.	SÌ	Durante la riunione di chiusura è stato chiarito che l'audit si basa su un approccio di campionamento, specificando che non tutte le aree o processi sono stati esaminati in dettaglio in questa fase. Sono stati illustrati con chiarezza i prossimi passi, inclusa la redazione del rapporto di audit, la gestione delle eventuali non conformità rilevate e le scadenze previste per l'implementazione delle azioni correttive. Il rappresentante della direzione ha confermato la comprensione di tali aspetti e l'impegno a rispettare i tempi concordati, assicurando così una corretta preparazione per lo Stage 2.
Chiusura: è stato dato spazio a domande e obiezioni. Eventuali divergenze non risolte sono state discusse e registrate per l'organismo di certificazione.	SÌ	Durante la riunione di chiusura è stato garantito ampio spazio per domande e obiezioni da parte del rappresentante della direzione e dei responsabili di processo. Non sono emerse divergenze non risolte; eventuali punti discussi sono stati debitamente registrati nel verbale a disposizione dell'organismo di certificazione. La partecipazione attiva e il confronto aperto confermano la trasparenza del processo e la preparazione dell'organizzazione per lo Stage 2.

TEAM DI AUDIT

Nome	**Ruolo**
Giuseppe Izzo	Lead auditor
Stefano Festa	CEO
Giuseppe Izzo 2	Lead Auditor

ELEMENTI E NOTE DELL'AUDITOR (GENERALE)

27001 - Sistema di Gestione per la Sicurezza delle Informazioni – Stage 1

ELEMENTI E NOTE DELL'AUDITOR (SE PRESENTI)

La documentazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è complessivamente pertinente e coerente con le attività di raccolta, elaborazione, analisi e gestione sicura dei dati digitali per clienti terzi svolte presso la sede di Travagliato (BS). Sono disponibili i documenti chiave relativi al contesto organizzativo, campo di applicazione e processi SGSI, sebbene alcune aree obbligatorie quali la politica di sicurezza, le valutazioni e trattamenti del rischio, gli obiettivi di sicurezza delle informazioni e il controllo delle informazioni documentate risultino parzialmente disponibili o necessitino di aggiornamento. Tali lacune rappresentano aree di miglioramento da integrare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Il cliente ha preso atto delle osservazioni e si è impegnato a completare la revisione, approvazione e aggiornamento della documentazione rilevante, fornendo evidenze oggettive in vista dello Stage 2. Non sono stati identificati siti temporanei o fattori che possano influenzare negativamente la pianificazione dell'audit. Nel complesso, il sistema risulta sufficientemente implementato per procedere allo Stage 2 con raccomandazioni specifiche su integrazione documentale e consolidamento delle evidenze.

DOCUMENTAZIONE

Documentazione / Clausola	Commento	Stato
4.1 - Analisi del contesto interno ed esterno (Raccomandato)	4.1 - Analisi del contesto interno ed esterno (Raccomandato): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
4.2 - Mappa delle parti interessate e requisiti (Raccomandato)	4.2 - Mappa delle parti interessate e requisiti (Raccomandato): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
4.3 - Campo di applicazione del SGSI (Obbligatorio)	4.3 - Campo di applicazione del SGSI (Obbligatorio): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
4.4 - Descrizione dei processi SGSI e interazioni (Raccomandato)	4.4 - Descrizione dei processi SGSI e interazioni (Raccomandato): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
5.2 - Politica per la sicurezza delle informazioni (Obbligatorio)	5.2 - Politica per la sicurezza delle informazioni (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
5.3 - Struttura organizzativa con ruoli e responsabilità (Raccomandato)	5.3 - Struttura organizzativa con ruoli e responsabilità (Raccomandato): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
6.1.2 - Criteri di valutazione e accettazione del rischio (Obbligatorio)	6.1.2 - Criteri di valutazione e accettazione del rischio (Obbligatorio): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente

6.1.2 - Risultati delle valutazioni del rischio sicurezza informazioni (Obbligatorio)	6.1.2 - Risultati delle valutazioni del rischio sicurezza informazioni (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
6.1.3 - Piano di trattamento del rischio sicurezza informazioni (Obbligatorio)	6.1.3 - Piano di trattamento del rischio sicurezza informazioni (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
6.1.3 - Dichiarazione di applicabilità SoA (Obbligatorio)	6.1.3 - Dichiarazione di applicabilità SoA (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
6.1.3 - Decisione sui rischi residui accettati (Obbligatorio)	6.1.3 - Decisione sui rischi residui accettati (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
6.2 - Obiettivi sicurezza informazioni e piani di attuazione (Obbligatorio)	6.2 - Obiettivi sicurezza informazioni e piani di attuazione (Obbligatorio): documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.	absent
6.3 - Documentazione pianificazione modifiche (Raccomandato)	6.3 - Documentazione pianificazione modifiche (Raccomandato): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
7.2 - Piano formazione ed evidenze competenza (Obbligatorio)	7.2 - Piano formazione ed evidenze competenza (Obbligatorio): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
7.3 - Evidenze di consapevolezza (Raccomandato)	7.3 - Evidenze di consapevolezza (Raccomandato): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
7.4 - Piano comunicazione interna ed esterna (Raccomandato)	7.4 - Piano comunicazione interna ed esterna (Raccomandato): documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	Presente
7.5.1 - Informazioni documentate richieste dal SGSI e dalla norma (Obbligatorio)	7.5.1 - Informazioni documentate richieste dal SGSI e dalla norma (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
7.5.3 - Controllo delle informazioni documentate	7.5.3 - Controllo delle informazioni documentate	partial

(Obbligatorio)	(Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	
8.1 - Pianificazione e controllo operativo (Raccomandato)	8.1 - Pianificazione e controllo operativo (Raccomandato): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
8.2 - Risultati aggiornati della valutazione del rischio (Obbligatorio)	8.2 - Risultati aggiornati della valutazione del rischio (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
8.3 - Evidenze di attuazione del trattamento del rischio (Obbligatorio)	8.3 - Evidenze di attuazione del trattamento del rischio (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
9.1 - Registrazioni di monitoraggio, misurazione, analisi e valutazione (Obbligatorio)	9.1 - Registrazioni di monitoraggio, misurazione, analisi e valutazione (Obbligatorio): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.	partial
9.2 - Programma di audit interno (Obbligatorio)	9.2 - Programma di audit interno (Obbligatorio): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.	na
9.2 - Rapporti di audit interno (Obbligatorio)	9.2 - Rapporti di audit interno (Obbligatorio): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.	na
9.3 - Registrazioni riesame della direzione (Obbligatorio)	9.3 - Registrazioni riesame della direzione (Obbligatorio): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.	na
10.2 - Non conformità e azioni correttive (Obbligatorio)	10.2 - Non conformità e azioni correttive (Obbligatorio): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.	na
10.2 - Verifica efficacia azioni correttive (Obbligatorio)	10.2 - Verifica efficacia azioni correttive (Obbligatorio): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.	na

27001 – Requisiti

Requisito	**Commento**	**Esito* C/NC/O/NA**

Il SGSI affronta gli aspetti chiave del contesto dell'organizzazione? I fattori interni ed esterni sono identificati e documentati? Sono disponibili registrazioni di monitoraggio e riesame? Sono comprese e documentate le esigenze delle parti interessate? È adottato un approccio basato sul rischio e sono identificate opportunità?	Per il punto verificato non emergono carenze tali da impedire il proseguimento, ma si raccomanda di migliorare formalizzazione, completezza o tracciabilità delle evidenze relative a: Il SGSI affronta gli aspetti chiave del contesto dell'organizzazione? I fattori interni ed esterni sono identificati e documentati? Sono disponibili registrazioni di monitoraggio e riesame? Sono comprese e documentate le esigenze delle parti interessate? È adottato un approccio basato sul rischio e sono identificate opportunità?	O
I processi che compongono il SGSI sono identificati? La loro sequenza e interazione sono definite e documentate?	Per il punto verificato non emergono carenze tali da impedire il proseguimento, ma si raccomanda di migliorare formalizzazione, completezza o tracciabilità delle evidenze relative a: I processi che compongono il SGSI sono identificati? La loro sequenza e interazione sono definite e documentate?	O
Il campo di applicazione del SGSI è stato determinato considerando confini e applicabilità? È documentato e comunicato? È appropriato alle attività dell'organizzazione?	Per il punto verificato non emergono carenze tali da impedire il proseguimento, ma si raccomanda di migliorare formalizzazione, completezza o tracciabilità delle evidenze relative a: Il campo di applicazione del SGSI è stato determinato considerando confini e applicabilità? È documentato e comunicato? È appropriato alle attività dell'organizzazione?	O
I requisiti relativi a contesto, leadership, pianificazione, supporto, operatività, valutazione delle prestazioni e miglioramento continuo sono affrontati e documentati nel SGSI?	Per il punto verificato si rileva un livello di copertura adeguato. La valutazione C si riferisce esclusivamente a: I requisiti relativi a contesto, leadership, pianificazione, supporto, operatività, valutazione delle prestazioni e miglioramento continuo sono affrontati e documentati nel SGSI?	C
L'organizzazione opera su più siti o ha attività specifiche per sito? In tal caso sono considerate nello scopo e nei controlli del SGSI?	Per il punto verificato si rileva un livello di copertura adeguato. La valutazione C si riferisce esclusivamente a: L'organizzazione opera su più siti o ha attività specifiche per sito? In tal caso sono considerate nello scopo e nei controlli del SGSI?	C
L'organizzazione ha identificato e rispettato i requisiti cogenti e normativi applicabili alla sicurezza delle informazioni?	Per il punto verificato si rileva un livello di copertura adeguato. La valutazione C si riferisce esclusivamente a: L'organizzazione ha identificato e rispettato i requisiti cogenti e normativi applicabili alla sicurezza delle informazioni?	C

Esiste una Politica di Sicurezza documentata? È appropriata allo scopo e al contesto dell'organizzazione ed è disponibile alle parti interessate rilevanti?	Per il punto verificato non emergono carenze tali da impedire il proseguimento, ma si raccomanda di migliorare formalizzazione, completezza o tracciabilità delle evidenze relative a: Esiste una Politica di Sicurezza documentata? È appropriata allo scopo e al contesto dell'organizzazione ed è disponibile alle parti interessate rilevanti?	O
Sono stati stabiliti obiettivi di sicurezza delle informazioni, coerenti con la politica e i rischi identificati? Sono misurabili, monitorati e riesaminati?	Per il punto verificato si rileva un livello di copertura adeguato. La valutazione C si riferisce esclusivamente a: Sono stati stabiliti obiettivi di sicurezza delle informazioni, coerenti con la politica e i rischi identificati? Sono misurabili, monitorati e riesaminati?	C
Gli audit interni sono condotti a intervalli pianificati per valutare conformità ed efficacia del SGSI?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Gli audit interni sono condotti a intervalli pianificati per valutare conformità ed efficacia del SGSI?	N/A
Quando è stato svolto l'ultimo audit interno? Sono disponibili registrazioni di supporto? Data dell'ultimo audit interno?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Quando è stato svolto l'ultimo audit interno? Sono disponibili registrazioni di supporto? Data dell'ultimo audit interno?	N/A
L'alta direzione svolge riesami a intervalli pianificati per garantire che il SGSI rimanga idoneo, adeguato ed efficace?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: L'alta direzione svolge riesami a intervalli pianificati per garantire che il SGSI rimanga idoneo, adeguato ed efficace?	N/A
Quando è stato svolto l'ultimo riesame della direzione? È disponibile un rapporto documentato? Data dell'ultimo rapporto di riesame?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Quando è stato svolto l'ultimo riesame della direzione? È disponibile un rapporto documentato? Data dell'ultimo rapporto di riesame?	N/A
Reclami e segnalazioni delle parti interessate relativi alla sicurezza delle informazioni sono registrati e gestiti sistematicamente?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Reclami e segnalazioni delle parti interessate relativi alla sicurezza delle informazioni sono registrati e gestiti sistematicamente?	N/A

ELEMENTI E NOTE DELL'AUDITOR

La documentazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è complessivamente pertinente e coerente con le attività di raccolta, elaborazione, analisi e gestione sicura dei dati digitali per clienti terzi svolte presso la sede di Travagliato (BS). Sono disponibili i documenti chiave relativi al contesto organizzativo, campo di applicazione e processi SGSI, sebbene alcune aree obbligatorie quali la politica di sicurezza, le valutazioni e trattamenti del rischio, gli obiettivi di

sicurezza delle informazioni e il controllo delle informazioni documentate risultino parzialmente disponibili o necessitino di aggiornamento. Tali lacune rappresentano aree di miglioramento da integrare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Il cliente ha preso atto delle osservazioni e si è impegnato a completare la revisione, approvazione e aggiornamento della documentazione rilevante, fornendo evidenze oggettive in vista dello Stage 2. Non sono stati identificati siti temporanei o fattori che possano influenzare negativamente la pianificazione dell'audit. Nel complesso, il sistema risulta sufficientemente implementato per procedere allo Stage 2 con raccomandazioni specifiche su integrazione documentale e consolidamento delle evidenze.

CRITERI DI AUDIT

Domanda / Criterio	Commento	Stato
La documentazione del sistema di gestione è pertinente alle attività del cliente?	La documentazione del sistema di gestione della sicurezza delle informazioni è risultata pertinente alle attività svolte dall'organizzazione, in particolare per quanto riguarda la raccolta, elaborazione, analisi e gestione sicura dei dati digitali per clienti terzi. I documenti chiave relativi al contesto, campo di applicazione e processi sono disponibili e coerenti con lo scopo dichiarato. Tuttavia, si evidenzia che alcune aree documentali (ad esempio politica di sicurezza, valutazioni e trattamenti del rischio) risultano parzialmente aggiornate o incomplete e necessitano di integrazione prima dello Stage 2 per garantire piena conformità e tracciabilità. Nel complesso la documentazione supporta adeguatamente le attività dell'organizzazione e non presenta criticità tali da ostacolare il proseguimento verso lo Stage 2.	Sì
Gli scopi applicati sono giustificati dalle attività attuali del cliente?	Lo scopo del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è chiaramente definito e coerente con le attività attuali dell'organizzazione, che si concentrano sulla raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi presso la sede di Travagliato (BS). La documentazione esaminata conferma che gli scopi applicati riflettono adeguatamente il contesto operativo e le responsabilità dell'organizzazione, senza evidenziare discrepanze o elementi estranei. Si raccomanda comunque di integrare e aggiornare alcune aree documentali chiave (ad esempio politica di sicurezza, valutazioni del rischio) per garantire piena conformità e tracciabilità in vista dello Stage 2.	Sì
È necessaria una modifica dello scopo?		N/A
Sono presenti siti temporanei? (es. cantieri di installazione, sedi di progetto ecc.)		No
Quale sito deve essere visitato?	sede legale	Sì
La visita al sito richiederà tempi di viaggio significativi?		No
Sono presenti fattori di stagionalità?		No

La tempistica dell'audit è adeguata rispetto alle attività presso il sito?		Sì
Quali processi ed elementi della norma ISO sono affrontati nello Stage 1?	Durante lo Stage 1 sono stati affrontati i processi e gli elementi chiave della norma ISO 27001 relativi alla definizione e documentazione del contesto organizzativo (4.1), al campo di applicazione del SGSI (4.3), alla descrizione dei processi e delle loro interazioni (4.4), nonché alla pianificazione e valutazione dei rischi (6.1.2, 6.1.3). È stata inoltre esaminata la disponibilità della documentazione relativa a politica di sicurezza (5.2), struttura organizzativa con ruoli e responsabilità (5.3), formazione e consapevolezza del personale (7.2, 7.3) e comunicazione interna ed esterna (7.4). Alcuni documenti obbligatori risultano parzialmente disponibili o da aggiornare, in particolare quelli relativi agli obiettivi di sicurezza delle informazioni (6.2) e al controllo delle informazioni documentate (7.5). Sono state verificate anche le evidenze relative al monitoraggio, misurazione e valutazione del SGSI (9.1). Elementi quali audit interni, riesami della direzione e gestione delle non conformità sono stati considerati non applicabili nel contesto attuale dell'organizzazione o non ancora implementati, pertanto saranno oggetto di verifica approfondita nello Stage 2.	Sì
La durata dell'audit Stage 2 è adeguata?		Sì
I giorni/uomo preventivati sono adeguati?		Sì
Ci sono variazioni nei dati dei dipendenti?		No
Ci sono variazioni dello scopo?		No
Sono presenti ulteriori informazioni?		No
È necessario verificare il turno notturno nello Stage 2?		No

27001 – Documentazione Annex A

Clausola ISO 27001 – Annex A	**Commento**	**Esito**
A [5.9] Inventario degli asset informativi e responsabilità (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.9] Inventario degli asset informativi e responsabilità (Raccomandato)	Presente
A [5.24-5.27] Procedure risposta incidenti e registro incidenti (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.24-5.27] Procedure risposta incidenti e registro incidenti (Raccomandato)	Presente
A [5.30] Piano continuità operativa e prontezza ICT (Raccomandato)	L'informazione documentata risulta disponibile per il controllo	Presente

	dell'Allegato A: A [5.30] Piano continuità operativa e prontezza ICT (Raccomandato)	
A [5.19-5.22] Valutazione sicurezza fornitori e accordi (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.19-5.22] Valutazione sicurezza fornitori e accordi (Raccomandato)	Presente
A [8.13] Piano backup e registrazioni test (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [8.13] Piano backup e registrazioni test (Raccomandato)	Presente
A [5.15-5.18, 8.5, 8.2] Politiche controllo accessi, autenticazione e cifratura (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.15-5.18, 8.5, 8.2] Politiche controllo accessi, autenticazione e cifratura (Raccomandato)	Presente
A [8.25-8.29] Ciclo sviluppo sicuro e registrazioni test sicurezza (Raccomandato)	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [8.25-8.29] Ciclo sviluppo sicuro e registrazioni test sicurezza (Raccomandato)	Presente

RILIEVI DELL'AUDIT DI STAGE 1

Norma ISO	Clausola	Tipo (Maggiore / Minore / Osservazione)	Rilievo	Risposta del cliente
ISO 27001	ISO 27001 docs - 4.2_interested_parties	Osservazione	4.2 - Mappa delle parti interessate e requisiti (Raccomandato) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alla mappa delle parti interessate e si impegna a completare l'aggiornamento e la revisione della documentazione, garantendo la piena disponibilità e coerenza delle evidenze prima dello Stage 2. Sarà fornito un aggiornamento periodico all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 5.2_policy	Osservazione	5.2 - Politica per la sicurezza delle informazioni (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alla politica per la sicurezza delle informazioni e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione entro la data prevista per lo Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 5.3_roles	Osservazione	5.3 - Struttura organizzativa con ruoli e responsabilità (Raccomandato) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alla struttura organizzativa con ruoli e responsabilità e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione entro la data prevista per lo Stage 2. Saranno

				predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 6.1.2_results	Osservazione	6.1.2 - Risultati delle valutazioni del rischio sicurezza informazioni (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo ai risultati delle valutazioni del rischio sicurezza informazioni e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione pertinente prima dello Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 6.1.3_treatment_plan	Osservazione	6.1.3 - Piano di trattamento del rischio sicurezza informazioni (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 6.1.3_soa	Osservazione	6.1.3 - Dichiarazione di applicabilità SoA (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alla Dichiarazione di Applicabilità (SoA) e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione entro la data prevista per lo Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti

				periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 6.1.3_residual_risks	Osservazione	6.1.3 - Decisione sui rischi residui accettati (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alla decisione sui rischi residui accettati e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione pertinente prima dello Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 6.2_objectives	Osservazione	6.2 - Obiettivi sicurezza informazioni e piani di attuazione (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.5.1_documented_info	Osservazione	7.5.1 - Informazioni documentate richieste dal SGSI e dalla norma (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.5.3_doc_control	Osservazione	7.5.3 - Controllo delle informazioni documentate (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo al controllo delle informazioni documentate (clausola 7.5.3) e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione pertinente prima dello Stage 2. Saranno predisposte evidenze

				oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 8.1_operational_control	Osservazione	8.1 - Pianificazione e controllo operativo (Raccomandato) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 8.2_risk_assessment_update	Osservazione	8.2 - Risultati aggiornati della valutazione del rischio (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo ai risultati aggiornati della valutazione del rischio (clausola 8.2) e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione pertinente prima dello Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 docs - 8.3_treatment_evidence	Osservazione	8.3 - Evidenze di attuazione del trattamento del rischio (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e conferma l'impegno a predisporre e aggiornare tutte le evidenze documentali relative all'attuazione del trattamento del rischio, garantendo la piena conformità ai requisiti della norma ISO 27001 prima dello Stage 2. Saranno forniti aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive e delle

				integrazioni documentali.
ISO 27001	ISO 27001 docs - 9.1_monitoring	Osservazione	9.1 - Registrazioni di monitoraggio, misurazione, analisi e valutazione (Obbligatorio) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo relativo alle registrazioni di monitoraggio, misurazione, analisi e valutazione (clausola 9.1) e si impegna a completare l'aggiornamento, la revisione e l'approvazione della documentazione pertinente prima dello Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 Stage 1 req #1	Osservazione	Il SGSI affronta gli aspetti chiave del contesto dell'organizzazione? I fattori interni ed esterni sono identificati e documentati? Sono disponibili registrazioni di monitoraggio e riesame? Sono comprese e documentate le esigenze delle parti interessate? È adottato un approccio basato sul rischio e sono identificate opportunità?	Il cliente prende atto del rilievo relativo all'analisi del contesto organizzativo e si impegna a completare la documentazione e le evidenze di monitoraggio, riesame, parti interessate, approccio al rischio e opportunità entro lo Stage 2. Saranno forniti aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive per garantire piena conformità ai requisiti della norma ISO 27001.
ISO 27001	ISO 27001 Stage 1 req #2	Osservazione	I processi che compongono il SGSI sono identificati? La loro sequenza e interazione sono definite e documentate?	Il cliente prende atto del rilievo relativo all'identificazione, definizione e documentazione dei processi SGSI, e si impegna a completare e aggiornare la documentazione necessaria prima dello

				Stage 2. Saranno fornite evidenze oggettive che dimostrino la definizione chiara della sequenza e interazione dei processi, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
ISO 27001	ISO 27001 Stage 1 req #3	Osservazione	Il campo di applicazione del SGSI è stato determinato considerando confini e applicabilità? È documentato e comunicato? È appropriato alle attività dell'organizzazione?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 Stage 1 req #7	Osservazione	Esiste una Politica di Sicurezza documentata? È appropriata allo scopo e al contesto dell'organizzazione ed è disponibile alle parti interessate rilevanti?	Il cliente prende atto del rilievo relativo alla Politica di Sicurezza e conferma l'impegno a completare la revisione, aggiornamento e approvazione della documentazione prima dello Stage 2. Saranno predisposte evidenze oggettive che dimostrino la piena conformità ai requisiti della norma ISO 27001, con aggiornamenti periodici all'auditor sullo stato di avanzamento delle azioni correttive.
Stage 1 readiness	Critical point #4	Area of concern	Sono presenti siti temporanei? (es. cantieri di installazione, sedi di progetto ecc.)	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #6	Area of concern	La visita al sito richiederà tempi di viaggio significativi?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.

Stage 1 readiness	Critical point #7	Area of concern	Sono presenti fattori di stagionalità?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #12	Area of concern	Ci sono variazioni nei dati dei dipendenti?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #13	Area of concern	Ci sono variazioni dello scopo?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #14	Area of concern	Sono presenti ulteriori informazioni?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #15	Area of concern	È necessario verificare il turno notturno nello Stage 2?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.

NC / OSSERVAZIONI RILEVATE

Verifica attività del team di audit

[X] Il team di audit ha consegnato i risultati dell'audit all'organizzazione verificata durante la riunione di chiusura.

Documenti di riferimento

AR_03.004 NC e CA

Note attività team di audit

n. 0 Major
n. 0 Minor
n. 0 Osservazioni

Note altri standard

ISO 14001

-

ISO 45001

-

ISO 27001

La documentazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è complessivamente pertinente e coerente con le attività di raccolta, elaborazione, analisi e gestione sicura dei dati digitali per clienti terzi svolte presso la sede di Travagliato (BS). Sono disponibili i documenti chiave relativi al contesto organizzativo, campo di applicazione e processi SGSI, sebbene alcune aree obbligatorie quali la politica di sicurezza, le valutazioni e trattamenti del rischio, gli obiettivi di sicurezza delle informazioni e il controllo delle informazioni documentate risultino parzialmente disponibili o necessitino di aggiornamento. Tali lacune rappresentano aree di miglioramento da integrare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Il cliente ha preso atto delle osservazioni e si è impegnato a completare la revisione, approvazione e aggiornamento della documentazione rilevante, fornendo evidenze oggettive in vista dello Stage 2. Non sono stati identificati siti temporanei o fattori che possano influenzare negativamente la pianificazione dell'audit. Nel complesso, il sistema risulta sufficientemente implementato per procedere allo Stage 2 con raccomandazioni specifiche su integrazione documentale e consolidamento delle evidenze.

ISO 27001 contesto aggiuntivo

NETISON S.R.L. opera nel settore dell'elaborazione di altri dati digitali, focalizzandosi sulla raccolta, elaborazione, analisi e gestione sicura delle informazioni per clienti terzi. Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) copre tutte le attività svolte presso la sede operativa di Travagliato (BS), coinvolgendo un organico di 7 dipendenti. La documentazione esaminata evidenzia una buona pertinenza e coerenza con lo scopo dichiarato, sebbene alcune aree chiave quali politica di sicurezza, valutazioni e trattamenti del rischio, obiettivi di sicurezza e controllo delle informazioni documentate risultino parzialmente disponibili o da aggiornare. Tali aspetti sono stati identificati come aree di miglioramento da completare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Non sono stati rilevati siti temporanei o fattori stagionali che influenzino il campo di applicazione. L'organizzazione ha preso atto delle osservazioni e si è impegnata a fornire evidenze oggettive aggiornate in vista dello Stage 2.

Conclusione, raccomandazione e allegati

Sintesi audit

L'audit di Stage 1 ha evidenziato che la documentazione del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) è complessivamente pertinente e coerente con le attività di raccolta, elaborazione, analisi e gestione sicura dei dati digitali per clienti terzi svolte presso la sede di Travagliato (BS). Sono disponibili i documenti chiave relativi al contesto organizzativo, campo di applicazione e processi SGSI. Tuttavia, alcune aree obbligatorie quali la politica di sicurezza, le valutazioni e trattamenti del rischio, gli obiettivi di sicurezza delle informazioni e il controllo delle informazioni documentate risultano parzialmente disponibili o necessitano di aggiornamento. Tali lacune rappresentano aree di miglioramento da integrare prima dello Stage 2 per garantire piena conformità alla norma ISO 27001. Il cliente ha preso atto delle osservazioni e si è impegnato a completare la revisione, approvazione e aggiornamento della documentazione rilevante, fornendo evidenze oggettive in vista dello Stage 2. Non sono stati identificati siti temporanei o fattori che possano influenzare negativamente la pianificazione dell'audit. Nel complesso, il sistema risulta sufficientemente implementato per procedere allo Stage 2 con raccomandazioni specifiche su integrazione documentale e consolidamento delle evidenze.

Aree di attenzione per Stage 2

Raccomandazione

[ ] Recommended for proceeding to Stage 2

[ ] Not recommended until objective evidence is submitted and concerns are closed

[ ] Not recommended; further Stage 1 audit required

Altro auditor(i)	Eseguito il	Completato e verificato internamente
	2026-05-22 06:04:00	[ ] OK

Note interne

FIRME

Rappresentante / Referente dell'organizzazione	Lead auditor
Stefano Festa	Izzo Giuseppe
Auditor	**Note**