Rapporto Senior delle Evidenze Audit Stage 1 - ISO/IEC 27001

Organizzazione: NETISON S.R.L.
Campo di applicazione: raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi presso la sede di Travagliato (BS).
Fonte analizzata: Rapporto di Audit - Stage 1, rif. cliente ST120260522001, FORM AR_01.2 Rev.004, 23 pagine.
Finalita: consolidare, in forma executive e verificabile, le evidenze emerse in Stage 1, le aree di attenzione e le azioni necessarie per la preparazione allo Stage 2.

Norma	ISO/IEC 27001
Tipo audit	Initial - Stage 1
Sede	Via Casaglia 55, 25039 Travagliato (BS), Italia
Personale	7 dipendenti
Lead auditor indicato	Giuseppe Izzo
Referente organizzazione	Stefano Festa - CEO / Top Management
Data report evidenze	22/05/2026

Giudizio senior sintetico: il sistema appare procedibile verso lo Stage 2 solo con presidio strutturato delle azioni di chiusura documentale e con rafforzamento delle evidenze oggettive su rischio, obiettivi, SoA, attuazione dei controlli e monitoraggio del SGSI.

Documento redatto come report di evidenze e readiness. Non sostituisce il rapporto ufficiale dell'organismo di certificazione e non costituisce decisione di certificazione.

1. Executive summary

Lo Stage 1 evidenzia un SGSI complessivamente pertinente e coerente rispetto al perimetro operativo di NETISON S.R.L., centrato su servizi informatici, elaborazione dati digitali e gestione sicura delle informazioni per clienti terzi. Il campo di applicazione risulta sostanzialmente coerente con le attivita svolte presso l'unica sede operativa dichiarata.

La readiness per Stage 2 non presenta blocchi immediati sul piano logistico o di scope: non risultano siti temporanei, fattori stagionali, turni notturni o variazioni di dipendenti/scopo da considerare nella pianificazione. Tuttavia, sul piano delle evidenze di conformita la maturita documentale risulta ancora disomogenea.

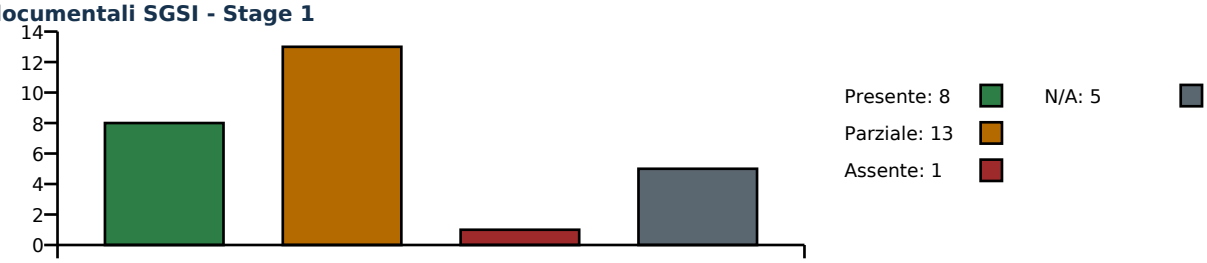
La catena del rischio - valutazione, trattamento, SoA, accettazione del rischio residuo, evidenze di attuazione e monitoraggio - e il principale asse di rafforzamento. La sua incompletezza espone l'organizzazione a rilievi rilevanti in Stage 2, perche ISO/IEC 27001 richiede coerenza end-to-end fra contesto, rischi, controlli applicabili, obiettivi, attuazione operativa e risultati misurati.

Un secondo punto senior riguarda la coerenza formale del rapporto: le pagine dei rilievi riportano numerose osservazioni e aree di concern, mentre la sezione di sintesi indica n. 0 osservazioni. Prima dello Stage 2 e opportuno sanare questa discontinuita, distinguendo chiaramente tra osservazioni, opportunita di miglioramento, aree di concern e non conformita.

Area	Evidenza Stage 1	Giudizio senior
Scope e contesto	Scope definito: raccolta, elaborazione, analisi e gestione sicura di dati digitali presso Travagliato. Contesto e processi principali disponibili.	Adeguato come base, da completare su parti interessate e tracciabilita del riesame del contesto.
Leadership	Partecipazione del CEO alle riunioni di apertura e chiusura; politica e ruoli indicati come parziali.	Commitment presente, ma da tradurre in policy approvata, RACI e accettazione rischio residuo.
Pianificazione e rischio	Criteri di valutazione rischio presenti; risultati, piano trattamento, SoA e rischio residuo parziali; obiettivi 6.2 assenti.	Area prioritaria. Richiede chiusura documentale prima di campionamento Stage 2.
Supporto e competenza	Formazione, competenza, consapevolezza e comunicazione risultano presenti.	Adeguato per Stage 1; in Stage 2 servira evidenza di efficacia e tracciabilita nominativa.
Operativita e controlli	Pianificazione operativa, aggiornamento rischi, attuazione trattamento e monitoraggio risultano parziali.	Richiede campioni operativi: log, ticket, backup test, access review, incident register, change records.
Performance e miglioramento	Audit interno, riesame direzione e CAPA indicati N/A; monitoraggio 9.1 parziale.	Da rivalutare. Per un SGSI certificabile 9.2 e 9.3 sono normalmente requisiti essenziali.

Dashboard evidenze documentali

Stato evidenze documentali SGSI - Stage 1



Indice calcolato sulle voci di documentazione SGSI presenti nel rapporto Stage 1: 8 evidenze presenti, 13 parziali/da aggiornare, 1 assente, 5 marcate N/A. Il campione Annex A riportato risulta invece presente per tutte le voci elencate.

2. Perimetro, criteri e base evidenziale

Il rapporto Stage 1 esamina la conformita e la completezza delle informazioni documentate e la readiness generale del SGSI rispetto alla ISO/IEC 27001. L'organizzazione e descritta come societa di elaborazione dati digitali per clienti terzi, con 7 dipendenti, sede unica a Travagliato (BS) e codice NACE 63.10.

La base evidenziale considerata include: descrizione dell'organizzazione, scope, riunione iniziale e finale, documentazione SGSI per clausola, requisiti Stage 1, documentazione Annex A, rilievi, risposta del cliente e sintesi finale.

Elemento	Evidenza dal rapporto Stage 1	Valutazione senior
Campo SGSI	Attivita di raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi presso Via Casaglia 55, Travagliato.	Perimetro chiaro e coerente con l'attivita dichiarata. Da dettagliare meglio processi interni, asset, interfacce clienti e fornitori critici.
Modalita audit	Audit onsite, Stage 1, initial; riunioni formali di apertura e chiusura con partecipazione direzione.	Adeguato. Buona disponibilita del management; utile formalizzare lista partecipanti completa e funzioni operative intervistate.
Legislazione richiamata	GDPR, Codice privacy italiano, NIS2, sicurezza ICT e continuita operativa, linee guida AgID ove applicabili.	Riferimenti corretti ma da trasformare in registro requisiti cogenti con ownership, obblighi, evidenze e frequenza di riesame.
Risorse e logistica	Canali di comunicazione, risorse, accesso a documentazione e personale chiave confermati.	Non emergono impedimenti organizzativi per Stage 2.

3. Evidenze positive consolidate

- Lo scope SGSI e coerente con il modello operativo dichiarato e con il servizio principale di elaborazione e gestione sicura dei dati digitali.
- La sede operativa e unica; non risultano siti temporanei, cantieri, fattori stagionali o turni notturni da includere in modo specifico nella pianificazione Stage 2.
- La direzione ha partecipato alle riunioni di apertura e chiusura, confermando disponibilita di risorse, accesso documentale e collaborazione.
- Sono presenti documenti chiave su contesto, campo di applicazione, processi SGSI, criteri di valutazione del rischio, pianificazione modifiche, formazione, consapevolezza e comunicazione.
- Per il campione Annex A riportato risultano disponibili evidenze su asset, incident response, continuita ICT, fornitori, backup, access control/cifratura e ciclo di sviluppo sicuro.

4. Aree critiche di attenzione

Priorita	Area	Evidenza	Impatto Stage 2
Alta	**Obiettivi SGSI - 6.2**	Documento indicato come assente nella tabella documentale.	Senza obiettivi misurabili non e dimostrabile il controllo delle performance del SGSI.
Alta	**Risk management - 6.1.2, 6.1.3, 8.2, 8.3**	Risultati valutazione rischio, piano trattamento, SoA, accettazione rischio residuo e attuazione trattamento risultano parziali.	Rischio di rilievi sostanziali se non viene dimostrata la tracciabilita completa rischio-controllo -evidenza.
Alta	**Performance e riesame - 9.1, 9.2, 9.3**	Monitoraggio parziale; audit interni e riesame direzione indicati N/A.	Da rivalutare: audit interno e riesame direzione sono normalmente elementi necessari per la certificabilita del sistema.
Media	**Policy, ruoli, parti interessate - 4.2, 5.2, 5.3**	Documentazione parzialmente disponibile o da aggiornare.	Rischio di debolezza su governance, responsabilita e allineamento strategico.

Priorita	Area	Evidenza	Impatto Stage 2
Media	**Controllo documentale - 7.5.1, 7.5.3**	Informazioni documentate richieste e controllo documentale parziali.	Rischio di evidenze non governate, versioni non approvate o tracciabilita insufficiente.
Media	**Coerenza report**	Presenza di rilievi/observations nelle pagine dedicate, ma sintesi con n. 0 osservazioni.	Da sanare prima di formalizzare conclusioni e piano Stage 2.

5. Matrice senior delle evidenze per clausola ISO/IEC 27001

La tabella seguente trasforma le risultanze Stage 1 in un piano di evidenze oggettive da predisporre. La priorita e determinata considerando centralita del requisito, rischio di rilievo in Stage 2 e impatto sulla coerenza del SGSI.

Clausola	Stato Stage 1	Evidenza/lettura senior	Evidenza richiesta per Stage 2
4.1 Contesto	Presente	Analisi contesto disponibile e coerente, da confermare con controllo revisioni e approvazione.	Analisi SWOT/PESTLE o equivalente, minacce/opportunita, collegamento a rischi SGSI, riesame periodico.
4.2 Parti interessate	Parziale	Mappa parti interessate da aggiornare/completare.	Registro parti interessate con requisiti, obblighi contrattuali, privacy, clienti, fornitori, autorita e criteri di monitoraggio.
4.3 Scope	Presente	Campo di applicazione coerente con servizi e sede.	Statement approvato, confini fisici/logici, sistemi inclusi/esclusi, processi, servizi, interfacce e giustificazioni.
4.4 Processi SGSI	Presente	Processi e interazioni descritti.	Mappa processi con input/output, owner, KPI, evidenze, rischi e controlli associati.
5.2 Policy	Parziale	Politica sicurezza non pienamente disponibile/aggiornata.	Policy approvata dalla direzione, comunicata, disponibile alle parti rilevanti e coerente con obiettivi e risk appetite.
5.3 Ruoli	Parziale	Struttura organizzativa e responsabilita da completare.	Organigramma, RACI SGSI, nomine, job description, responsabilita incidenti, risk owner, asset owner, control owner.
6.1.2 Risk criteria	Presente	Criteri valutazione/accettazione rischio presenti.	Metodologia approvata, scale impatto/probabilita, criteri accettazione e riesame, coerenza con asset e requisiti cogenti.
6.1.2 Risk results	Parziale	Risultati valutazione rischio da aggiornare/completare.	Risk register completo con asset, minacce, vulnerabilita, controlli esistenti, rischio inerente/residuo, owner e date.
6.1.3 Treatment plan	Parziale	Piano trattamento rischio non pienamente disponibile.	Piano approvato con azioni, controlli, responsabili, scadenze, stato, risorse, accettazione rischio e collegamento alla SoA.
6.1.3 SoA	Parziale	Dichiarazione di applicabilita da completare/approvare.	SoA Annex A 2022 con controlli applicabili/non applicabili, motivazioni, stato attuazione, evidenze, owner e riferimenti al risk treatment.
6.1.3 Rischi residui	Parziale	Decisione sui rischi residui accettati da aggiornare.	Verbale o registro di accettazione rischio residuo firmato/approvato dal top management o risk owner autorizzati.
6.2 Obiettivi	Assente	Obiettivi sicurezza e piani di attuazione non resi disponibili.	Obiettivi misurabili con KPI, baseline, target, owner, frequenza monitoraggio, piani di conseguimento e risultati.

Clausola	Stato Stage 1	Evidenza/lettura senior	Evidenza richiesta per Stage 2
6.3 Modifiche	Presente	Pianificazione modifiche disponibile.	Change log, criteri impatto sicurezza, approvazioni, test, rollback, comunicazioni e review post-change.
7.2 Competenza	Presente	Piano formazione ed evidenze competenza presenti.	Matrice competenze, registri formazione, valutazione efficacia, ruoli critici e competenze specialistiche.
7.3 Awareness	Presente	Evidenze consapevolezza presenti.	Campagne awareness, test, phishing simulation se applicabile, registri partecipazione, evidenza comprensione policy.
7.4 Comunicazione	Presente	Piano comunicazione interna/esterna disponibile.	Matrice comunicazioni: cosa, quando, a chi, responsabile, canale, requisiti contrattuali e incident notification.
7.5.1 Info documentate	Parziale	Informazioni documentate richieste da SGSI/norma da completare.	Master list documenti, requisiti normativi, documenti obbligatori, registrazioni e retention.
7.5.3 Controllo documenti	Parziale	Controllo informazioni documentate parziale.	Procedura controllo documenti, versioning, approvazioni, distribuzione, accessi, archiviazione, protezione e obsolescenza.
8.1 Controllo operativo	Parziale	Pianificazione e controllo operativo da rafforzare.	Procedure operative, istruzioni, evidenze di esecuzione, controlli su outsourcing, accessi, change, backup, incidenti, vulnerabilita.
8.2 Valutazione rischio	Parziale	Risultati aggiornati valutazione rischio parziali.	Aggiornamento periodico e trigger-based, versioni, approvazione e confronto con cambiamenti tecnologici/contrattuali.
8.3 Trattamento rischio	Parziale	Evidenze attuazione trattamento rischio parziali.	Campioni di controlli implementati, test, log, ticket, report backup, access review, incident drill, supplier review.
9.1 Monitoraggio	Parziale	Registrazioni monitoraggio/misurazione/analisi parziali.	KPI/KRI SGSI, trend, soglie, responsabilita, analisi risultati, decisioni e azioni di miglioramento.
9.2 Audit interno	N/A nel report	Indicazione da rivalutare in ottica certificativa.	Programma audit interno, piano, checklist, report, rilievi, azioni e verifica indipendenza/competenza auditor.
9.3 Riesame direzione	N/A nel report	Indicazione da rivalutare in ottica certificativa.	Verbale riesame con input/output ISO 27001: prestazioni, audit, rischi, incidenti, obiettivi, risorse, opportunita, decisioni.
10.2 NC e CA	N/A nel report	Gestione NC/CAPA indicata non applicabile.	Procedura NC/CAPA, registro eventuali NC/osservazioni, analisi cause, azioni, verifica efficacia; anche assenza NC va governata.

6. Evidenze Annex A e controlli tecnici/organizzativi

Nel campione Annex A riportato in Stage 1 le informazioni documentate risultano presenti per tutte le voci elencate. In Stage 2 la disponibilita documentale dovra essere supportata da evidenza di implementazione, efficacia e tracciabilita operativa.

Controllo Annex A	Stato	Focus Stage 2
A.5.9 Inventario asset informativi e responsabilita	Presente	Campionare asset register, owner, classificazione, lifecycle, aggiornamento e coerenza con risk assessment.
A.5.24-A.5.27 Incident response e registro incidenti	Presente	Verificare procedure, ruoli, escalation, registro incidenti, lessons learned, tempi di risposta e notifiche privacy/contrattuali.
A.5.30 Continuita operativa e prontezza ICT	Presente	Verificare BIA/continuita ICT, RTO/RPO, test, esiti, remediation, dipendenze cloud/fornitori.
A.5.19-A.5.22 Sicurezza fornitori e accordi	Presente	Campionare contratti, SLA, DPA, security requirements, valutazioni periodiche e trattamento rischio terze parti.
A.8.13 Backup e registrazioni test	Presente	Verificare politica backup, schedulazioni, restore test, segregazione, cifratura, retention e report di esito.
A.5.15-A.5.18, A.8.5, A.8.2 Accessi, autenticazione, cifratura	Presente	Verificare access review, MFA, provisioning/deprovisioning, password policy, privilegi, cifratura e gestione chiavi.
A.8.25-A.8.29 Ciclo sviluppo sicuro e test sicurezza	Presente	Verificare secure SDLC, segregation ambienti, code review, test security, vulnerability management e change approval.

7. Incongruenze formali e punti da sanare

Punto	Rilievo senior	Azione raccomandata
Rilievi vs sintesi	Le pagine dei rilievi riportano molte osservazioni e aree di concern, mentre la sintesi indica n. 0 Major, n. 0 Minor, n. 0 Osservazioni.	Allineare formalmente la classificazione: distinguere NC, osservazioni, OFI e concern logistici/non applicabili. Aggiornare summary e allegati.
Raccomandazione finale	La sezione finale riporta checkbox non selezionate per la raccomandazione Stage 2.	Formalizzare una raccomandazione coerente: proceed to Stage 2 con piano di chiusura, oppure deferimento fino a evidenze oggettive completate.
N/A su requisiti core	Audit interno, riesame direzione e CAPA sono indicati N/A, ma in un SGSI certificabile sono normalmente requisiti del sistema.	Rivalutare la classificazione e predisporre evidenze minime prima dello Stage 2 o motivazione tecnica molto robusta.
Dati IT non valorizzati	Campi relativi a utenti, server, workstation, reti e connessioni Internet non compilati.	Integrare inventario dimensionale IT a supporto di complessita, campionamento e pianificazione audit.

8. Piano evidenze raccomandato prima dello Stage 2

Il piano seguente e ordinato per priorita di chiusura. L'obiettivo non e produrre documenti formali isolati, ma dimostrare un SGSI implementato, riesaminato e misurabile.

Priorita	Deliverable	Owner suggerito	Evidenza oggettiva attesa
1	**Risk register completo e aggiornato**	Responsabile SGSI / Risk owner	Registro rischi approvato con criteri, asset, minacce, vulnerabilita, rischio inerente/residuo e owner.
2	**Piano trattamento rischio e SoA**	Top management / Responsabile SGSI	Piano treatment con controlli, scadenze, stato; SoA Annex A 2022 firmata e collegata a rischi e controlli.
3	**Accettazione rischi residui**	CEO / Risk owner	Verbale o registro approvato con soglie, rischi accettati, motivazioni e responsabilita.
4	**Obiettivi 6.2 e KPI/KRI 9.1**	Top management / Responsabile SGSI	Obiettivi misurabili, target, piano attuazione, risultati monitorati, dashboard e analisi periodica.
5	**Politica sicurezza e comunicazione**	CEO	Policy approvata, pubblicata/comunicata, evidenze di presa visione e allineamento con obiettivi.
6	**RACI, ruoli e responsabilita SGSI**	CEO / HR / Responsabile SGSI	Organigramma, nomine, RACI, responsabilita per asset, rischi, incidenti, accessi, fornitori.
7	**Controllo documentale**	Quality/SGSI	Procedura, master list, versioning, approvazioni, retention, accessi e protezione documenti.
8	**Audit interno e riesame direzione**	Auditor interno indipendente / CEO	Programma audit, report, rilievi, azioni; verbale riesame con input/output ISO 27001.
9	**Evidenze operative controlli Annex A**	IT / Process owner	Campioni: access review, backup restore test, incident register, supplier review, change, vulnerability/security test.
10	**Registro requisiti cogenti**	Compliance / DPO / SGSI	GDPR, NIS2 se applicabile, contratti, settore ICT, obblighi cliente; evidenze di compliance e monitoraggio.

9. Strategia di campionamento consigliata per Stage 2

Per evitare che lo Stage 2 si limiti a verifica documentale, e opportuno preparare campioni reali per processo e per controllo. I campioni devono essere recenti, versionati, riconducibili a owner e coerenti con rischio, SoA e obiettivi.

Processo/tema	Campioni consigliati
Gestione accessi	Elenco utenti attivi, privilegi amministrativi, evidenza MFA, richiesta/autorizzazione accesso, revoca accesso ex dipendente/collaboratore, access review periodica.
Backup e continuita	Piano backup, log esecuzione, report restore test, esito recovery, eccezioni e azioni correttive.
Incident management	Registro incidenti/eventi, classificazione, escalation, comunicazioni, lessons learned, esercitazione se assenza incidenti reali.
Fornitori	Vendor list, valutazione sicurezza, clausole contrattuali/DPA, SLA, monitoraggio e rivalutazione periodica.
Sviluppo sicuro	Change request, code review, test security, segregazione ambienti, gestione vulnerabilita, approvazione rilascio.
Consapevolezza	Piano formazione, presenze, test apprendimento, comunicazioni policy, evidenze di consapevolezza dei ruoli critici.

10. Raccomandazione senior

La raccomandazione operativa e di procedere alla pianificazione dello Stage 2 solo dopo una verifica preliminare di chiusura delle evidenze ad alta priorita, con particolare riferimento a: obiettivi 6.2, risk register, piano trattamento, SoA, accettazione rischio residuo, controllo documentale, monitoraggio 9.1, audit interno e riesame direzione.

Scenario	Condizione	Raccomandazione
Proceed to Stage 2	Evidenze ad alta priorita completate, approvate e campionabili; coerenza formale del rapporto sanata.	Accettabile. Stage 2 pianificabile con focus su efficacia e implementazione.
Proceed with caution	Documenti prodotti ma non ancora consolidati o privi di evidenze operative sufficienti.	Possibile, ma con rischio elevato di rilievi. Consigliata pre-verifica documentale prima dell'audit.
Defer Stage 2	Persistono assenza di obiettivi, SoA non chiusa, rischio non tracciato, audit interno/riesame direzione non effettuati.	Rinviare fino a presentazione di evidenze oggettive e chiusura dei concern critici.

Conclusione

NETISON S.R.L. presenta una base SGSI idonea per completare il percorso di certificazione, ma lo Stage 1 mostra una prevalenza di evidenze parziali nelle aree che costituiscono il nucleo della ISO/IEC 27001: risk management, obiettivi, controllo documentale, performance e miglioramento. La priorita non e aumentare la quantita documentale, ma dimostrare una catena logica e verificabile: contesto - parti interessate - rischi - controlli - obiettivi - evidenze operative - misurazioni - riesame - miglioramento.

Dal punto di vista senior, il sistema puo essere accompagnato allo Stage 2 con un piano di chiusura stretto, formalmente tracciato, con responsabilita assegnate e riesame preliminare delle evidenze oggettive. In assenza di tale consolidamento, il rischio di rilievi sostanziali in Stage 2 e significativo.

Allegato - Fonti interne al documento Stage 1

Sezione Stage 1	Pagine fonte	Informazione utilizzata
Anagrafica e scope	1-3	Organizzazione, sito, dipendenti, NACE, scope SGSI e obiettivi audit.
Riunioni audit	4-6	Partecipazione, logistica, comunicazioni, chiusura e ruoli.
Documentazione SGSI	7-9	Stato documenti per clausola: presente, parziale, assente, N/A.
Requisiti Stage 1	10-13	Esiti C/O/N/A, criteri audit, readiness e durata Stage 2.
Annex A	13-14	Controlli documentati campionati come presenti.
Rilievi e risposte cliente	15-21	Osservazioni e aree di concern con impegni di aggiornamento.
Sintesi e raccomandazione	22-23	Sintesi finale, conteggio NC/osservazioni, checkbox raccomandazione e firme.