REPORT A4 DELLE EVIDENZE OGGETTIVE

ISO/IEC 27001 - Audit Stage 2

NETISON S.R.L.

STANDARD	TIPO AUDIT	SEDE VERIFICATA	SCOPE
ISO/IEC 27001	Stage 2 - prima certificazione	Via Casaglia 55, Travagliato (BS)	Raccolta, elaborazione, analisi e gestione sicura di dati digitali
ORGANICO	**INFRASTRUTTURA CAMPIONATA**	**ESITO SINTETICO**	**PRIORITA**
7 dipendenti	8 utenti, 4 server, 10 endpoint, 15 reti, 3 connessioni Internet	Raccomandazione per certificazione	CAPA su risk, SoA, asset, accessi, incidenti

Finalita del documento

Sintetizzare in formato executive le evidenze oggettive utilizzate nello Stage 2 ISO/IEC 27001, rendendo tracciabili fonti, ambiti verificati, punti di forza, aree di attenzione e pacchetto di evidenze richiesto per chiusura e mantenimento del SGSI.

Preparato: 22/05/2026 | Versione: v1.0 | Fonte primaria: Audit Report Stage 2 AR_01.2 Rev.004

1. Executive summary

Il Sistema di Gestione per la Sicurezza delle Informazioni di NETISON S.R.L. risulta coerente con il contesto aziendale e con i servizi erogati: assistenza informatica, servizi IT gestiti MSP, backup e ripristino, cybersecurity, virtualizzazione, servizi cloud e gestione dati digitali per clienti terzi. Le evidenze campionate confermano un impianto SGSI applicabile al perimetro dichiarato e orientato alla tutela di riservatezza, integrita e disponibilita delle informazioni.

La lettura senior delle evidenze indica un sistema tecnicamente coerente e idoneo alla certificazione, con necessita di consolidamento documentale e tracciabilita operativa su alcuni controlli chiave. Le aree piu sensibili riguardano risk assessment, piano di trattamento, SoA, inventario asset, review accessi, incident management e restore test.

Giudizio professionale

Il sistema e certificabile se le non conformita minori sono gestite con azioni correttive proporzionate, cause radice documentate, responsabilita assegnate e verifica di efficacia. L'enfasi non deve essere sulla produzione massiva di documenti, ma sulla dimostrabilita continuativa dei controlli.

Area	Sintesi evidenza	Lettura senior
Copertura del perimetro	Sede unica di Travagliato (BS), attivita di raccolta, elaborazione, analisi e gestione sicura di dati digitali per terzi.	Adeguata
Maturita documentale	Politica, scope, risk, SoA e controlli sono presenti ma richiedono maggiore dettaglio e tracciabilita su alcune aree.	Da consolidare
Maturita operativa	Servizi MSP, backup, monitoraggio, cybersecurity e Co-Managed IT sono coerenti con lo schema ISO/IEC 27001.	Adeguata
Principali vulnerabilita di sistema	Evidenze non sempre complete su criteri di rischio, correlazione rischio-controllo, asset ownership, review accessi e incidenti.	Prioritaria
Esito audit	Raccomandazione per procedere alla certificazione, con gestione delle azioni correttive.	Positivo con CAPA

2. Perimetro, contesto e profilo IT campionato

Il perimetro SGSI copre le attivita di raccolta, elaborazione, analisi e gestione sicura di dati digitali per clienti terzi, svolte presso la sede operativa di Via Casaglia 55, Travagliato (BS). Sono stati considerati i processi connessi a servizi IT gestiti, assistenza, backup, sicurezza di rete, virtualizzazione, cloud, monitoraggio e gestione dati digitali.

Campo	Valore	Campo	Valore
Organizzazione	NETISON S.R.L.	Sede legale/operativa	Via Casaglia 55, 25039 Travagliato (BS), Lombardia
Settore	Elaborazione altri dati, servizi informatici, gestione dati digitali anche in cloud	NACE/IAF	NACE 63.10 - IAF 33
ATECO	63.10.29	Dipendenti	7
Utenti	8	Server	4
Workstation/PC/Laptop	10	Reti	15
Connessioni Internet	3	Personale sviluppo/manutenzione applicativa	0

- Lo scope e coerente con una realta MSP/IT service provider orientata a clienti terzi, PMI e Pubblica Amministrazione.
- La superficie di rischio e elevata in rapporto alla dimensione aziendale per effetto di accessi amministrativi, gestione infrastrutturale, backup e dati di clienti terzi.
- I confini fisici sono chiari; i confini logici, cloud e relativi a processi esternalizzati devono essere mantenuti espliciti nello scope, nella SoA e nei contratti.

3. Evidenze oggettive utilizzate - base probatoria

Le evidenze sono state organizzate per tipologia, rilevanza e capacita probatoria. La base di valutazione e campionaria e deriva da riesame documentale, interviste, osservazione diretta in sede, evidenze operative, sito web aziendale e riferimenti normativi applicabili.

Famiglia evidenza	Evidenze utilizzate	Valore probatorio

Documenti SGSI	Politica Protezione Dati, scope SGSI, documenti contesto/parti interessate, risk assessment, piano trattamento rischi, SoA, procedure operative, documentazione controlli Annex A.	Dimostrano disegno, responsabilita e governo del sistema.
Registrazioni operative	Ticket, log, checklist, registrazioni monitoraggio, backup, restore test, incidenti, review accessi, manutenzioni, evidenze di modifica e autorizzazione.	Dimostrano attuazione effettiva dei controlli.
Interviste e osservazione	Top management, personale tecnico, responsabili dei processi SGSI, osservazione in sede operativa.	Confermano consapevolezza, ruoli e prassi operative.
Evidenze esterne	Sito NETISON, pagine servizi gestiti, backup, network security, co-managed IT, privacy policy; riferimenti GDPR, NIS2/ACN, Garante Privacy.	Contestualizzano servizi, obblighi e aspettative delle parti interessate.
Audit trail Stage 1/Stage 2	Report Stage 1, report evidenze, audit report Stage 2, verbali e riepiloghi di chiusura.	Dimostrano continuita del percorso certificativo e stato rilievi.

4. Matrice evidenze per requisiti ISO/IEC 27001

Clausola	Ambito	Evidenze oggettive	Valutazione senior	Stato
4.1-4.2	Contesto e parti interessate	Documenti contesto, requisiti parti interessate, interviste management, osservazioni Stage 1/2.	Presidio presente; rafforzare tracciabilita del riesame periodico.	**Observation**
4.3-4.4	Campo di applicazione e processi SGSI	Scope, confini fisici, processi SGSI, sede unica, attivita di elaborazione dati per terzi.	Conforme; migliorare dettaglio su confini logici, cloud e outsourcing.	**Observation**
5.1-5.3	Leadership, politica, ruoli	Politica Protezione Dati firmata, impegni della Direzione, ruoli e responsabilita SGSI.	Adeguato; rafforzare prova di comunicazione e comprensione della politica.	**Observation**
6.1.1-6.1.3	Rischi, trattamento e SoA	Metodologia risk assessment, piano trattamento, SoA, rischi residui, controlli selezionati.	Area prioritaria; servono criteri, aggiornamenti e correlazione rischio-controllo piu evidenti.	**Minor**
6.2-6.3	Obiettivi e cambiamenti	Obiettivi di sicurezza, piani, indicatori, evidenze di change planning e autorizzazioni.	Conforme nel disegno; mantenere KPI misurabili e trend periodici.	**Conforme**
7.1-7.5	Supporto, competenza, consapevolezza, comunicazione, documenti	Piano formazione, CV/competenze, comunicazioni, controllo documenti, politica, documentazione SGSI.	Adeguato; migliorare prova di efficacia formazione e awareness.	**Observation**
8.1-8.3	Pianificazione operativa e trattamento rischi	Procedure operative, log, checklist, evidenze attuazione misure, backup, accessi, incidenti.	Processi coerenti; registrazioni non sempre complete su responsabilita e output.	**Minor**
9.1-9.3	Monitoraggio, audit interni, riesame	KPI, audit interni, report, riesame direzione, azioni e follow-up.	Presidio presente; consolidare trend, decisioni e piani di follow-up.	**Conforme**
10.1-10.2	Miglioramento e azioni correttive	Registro NC, cause, azioni, responsabilita, verifiche di efficacia.	Adeguato; importante mantenere un CAPA package completo per i rilievi.	**Conforme**

5. Matrice evidenze Annex A e processi operativi critici

Controllo	Processo	Evidenza oggettiva attesa/usata	Lettura senior	Stato
A.5.9	Inventario asset	Registro asset informativi, responsabilita, classificazione, aggiornamento periodico, interviste e campionamento asset.	Rendere sempre evidenti owner, classificazione, ubicazione logica/fisica e ciclo di revisione.	**Minor**
A.5.15-A.5.18 / A.8.2 / A.8.5	Controllo accessi	Policy accessi, autorizzazioni, utenze privilegiate, MFA/password, review periodiche, revoche, evidenze su campioni utenti.	Rafforzare evidence pack su review accessi, autorizzazione e revoca tempestiva.	**Minor**
A.5.19-A.5.23	Sicurezza fornitori ICT	Elenco fornitori, contratti, requisiti sicurezza, valutazione rischi, clausole privacy/security, monitoraggio fornitori critici.	Integrare requisiti minimi di sicurezza e criteri di rivalutazione nei rapporti contrattuali.	**Observation**
A.5.24-A.5.28	Gestione incidenti	Procedura incidenti, classificazione, registro, escalation, responsabilita, evidenze di analisi post evento e lesson learned.	Completare classificazione, registrazione, escalation e lessons learned.	**Minor**
A.5.30 / A.8.13	Backup e continuita	Piano continuita, procedure backup, job log, esiti backup, test di restore, evidenza retention e protezione copie.	Buona coerenza con il servizio; rendere periodici e tracciati i restore test.	**Observation**

A.8.25-A.8.32	Sviluppo sicuro e modifiche	Processo di change, autorizzazioni, test, tracciamento modifiche, evidenze su campioni.	Applicabile soprattutto a modifiche infrastrutturali e configurative; mantenere separazione ruoli e approvazioni.	**Conforme**

6. Punti di forza e debolezze evidenziate

La valutazione enterprise distingue i punti di forza strutturali dalle debolezze che possono generare rischio di mantenimento se non trasformate in evidenze periodiche e ripetibili.

Punto di forza	Evidenza	Impatto sul SGSI
Coerenza business - SGSI	I servizi erogati (MSP, backup, cybersecurity, cloud, virtualizzazione) sono nativamente collegati a riservatezza, integrita e disponibilita.	Elevata
Approccio proattivo MSP	Monitoraggio, assistenza e manutenzione proattiva supportano continuita e prevenzione incidenti.	Alta
Backup e continuita	Servizi strutturati di backup e disaster recovery coerenti con disponibilita e resilienza.	Alta
Cybersecurity e network security	Presenza di servizi di assessment, piani di sicurezza e protezione da minacce.	Alta
Co-Managed IT	Integrazione con team IT cliente e supporto specialistico su rischi, compliance e gestione infrastrutture.	Media/Alta

Area di debolezza	Evidenza/rischio	Priorita
Formalizzazione SLA e monitoraggio	Servizi MSP e reperibilita devono avere registrazioni di presa in carico, escalation, SLA e chiusura evento.	Medio
Backup e restore test	Servono evidenze periodiche di test di ripristino, esiti, anomalie e azioni correttive.	Alto
Risk assessment e SoA	Necessario collegamento chiaro tra asset, rischi, controlli, responsabili e stato di attuazione.	Alto
Responsabilita Co-Managed IT	Da formalizzare perimetro di intervento, autorizzazioni, accessi privilegiati e responsabilita in caso di incidente.	Medio/Alto
Trattamento dati clienti	Richiede evidenze robuste su classificazione, segregazione, credenziali, accordi privacy e riservatezza.	Alto

7. Registro rilievi Stage 2 e pacchetto evidenze richiesto

Di seguito il registro consolidato dei rilievi da trattare con azioni correttive o opportunita di miglioramento. La priorita e costruire un pacchetto di evidenze chiudibile: causa radice, azione, responsabile, scadenza, prova di implementazione, verifica efficacia.

Clausola/controllo	Tipo	Rilievo	Evidenza di chiusura attesa
4.3	**Observation**	Scope SGSI da rendere piu chiaro su confini fisici, logici, cloud e processi affidati all'esterno.	Scope aggiornato; mappa confini; elenco servizi/cloud/outsourcing; approvazione Direzione.
5.2	**Observation**	Politica disponibile; rafforzare tracciabilita della comunicazione alle parti interessate.	Registro comunicazioni; onboarding; presa visione; evidenze awareness; pubblicazione controllata.
6.1.2	**Minor**	Criteri di accettazione, aggiornamento e collegamento agli asset non sempre chiari.	Metodologia risk aggiornata; criteri accettazione; esempi applicativi; risk register con data e owner.
6.1.3	**Minor**	Piano trattamento non sempre completo nella correlazione rischi-controlli-responsabilita-stato.	Risk treatment plan con owner, date, stato, controllo Annex A, rischio residuo e approvazione.
6.1.3 / SoA	**Minor**	Giustificazioni di inclusione/esclusione controlli da dettagliare.	SoA aggiornata con motivazione, applicabilita, stato attuazione, evidenze e owner.
7.2	**Observation**	Valutazione efficacia formazione e awareness da rafforzare.	Test awareness; attestati; piano formazione; matrice competenze; valutazione efficacia.
8.1	**Minor**	Evidenze operative incomplete su pianificazione, responsabilita e registrazioni.	Procedure, log, ticket, checklist, output operativi, responsabilita e controllo periodico.
A.5.9	**Minor**	Inventario asset con proprietario, classificazione e aggiornamento non sempre evidenti.	Asset inventory aggiornato; owner; classificazione; data revisione; criteri di aggiornamento.
A.5.15/A.5.18/A.8.5	**Minor**	Review, autorizzazione o revoca accessi non sempre complete.	Access review trimestrale/semestrale; campioni utenti; revoche; approvazioni; account privilegiati.
A.5.19/A.5.22	**Observation**	Valutazione sicurezza fornitori ICT da migliorare nei rapporti contrattuali.	Vendor security assessment; clausole sicurezza/privacy; elenco fornitori critici;

			monitoraggio.
A.5.24/A.5.26	**Minor**	Incidenti: classificazione, registrazione, escalation e lesson learned non sempre complete.	Procedura incidenti; registro; template escalation; simulazione; post incident review.
A.8.13	**Observation**	Backup: rafforzare documentazione restore test ed esiti.	Piano restore test; verbali prova; esiti; anomalie; azioni correttive; evidenza retention.

8. Indicatori, monitoraggio e riesame - pacchetto executive

Per sostenere un livello enterprise, le evidenze non devono essere solo documenti statici ma indicatori ricorrenti, discussi in riesame e collegati al miglioramento continuo. Il set minimo consigliato e riportato di seguito.

Area KPI	Indicatore minimo	Frequenza
Servizi IT gestiti	SLA rispettati, tempi presa in carico, tempi risoluzione, eventi critici, backlog ticket.	Mensile
Backup	Job completati, job falliti, restore test eseguiti, tempo di ripristino, anomalie aperte/chiuse.	Mensile/Trimestrale
Accessi	Utenze attive, utenze privilegiate, review completate, revoche fuori SLA, eccezioni approvate.	Trimestrale
Incidenti	Eventi segnalati, incidenti classificati, tempo escalation, cause radice, lesson learned chiuse.	Mensile/Evento
Rischi	Rischi alto/medio, trattamenti in ritardo, rischi residui accettati, variazioni post cambio.	Trimestrale
Fornitori	Fornitori critici valutati, contratti con clausole security/privacy, scadenze rivalutazione.	Semestrale
Awareness	Completamento formazione, esito test, campagne svolte, gap di competenza aperti.	Semestrale

Criterio di accettazione consigliato

Ogni KPI deve avere owner, fonte dati, soglia o target, frequenza di raccolta, modalita di escalation e collegamento al riesame della Direzione. Senza questi elementi, l'indicatore rischia di essere informativo ma non gestionale.

9. Conformita legislativa e informazioni specifiche dello schema

La conformita legislativa e stata valutata rispetto alla natura dei servizi: gestione dati digitali, assistenza IT, servizi MSP, backup, cybersecurity e servizi cloud. I requisiti cogenti rilevanti includono privacy/GDPR, rapporti titolare-responsabile del trattamento, data breach, obblighi contrattuali verso clienti, requisiti di cybersecurity e possibile applicabilita di NIS2 in funzione di dimensione, ruolo nella catena di fornitura e tipologia di servizi erogati.

Fonte normativa/contrattuale	Evidenza oggettiva	Azione di governo
GDPR e D.Lgs. 196/2003	Privacy policy, ruoli privacy, accordi ex art. 28, registro trattamenti, gestione diritti interessati, data breach.	Mantenere registro requisiti aggiornato e collegato ai processi SGSI.
NIS2 / D.Lgs. 138/2024	Valutazione di applicabilita/non applicabilita rispetto a dimensione, servizi, clienti e catena di fornitura.	Formalizzare analisi e riesame periodico.
Contratti cliente	SLA, sicurezza informazioni, trattamento dati, responsabilita, accessi, incidenti, continuita.	Allineare clausole a rischi e controlli SoA.
Linee guida AgID/PA	Quando applicabile a clienti PA: requisiti di sicurezza ICT, continuita e gestione dati.	Valutare per cliente/contratto.

10. Conclusione senior e raccomandazioni operative

Il quadro delle evidenze dimostra un SGSI coerente con lo schema ISO/IEC 27001 e con il profilo tecnico-operativo di NETISON S.R.L. L'organizzazione dispone di servizi, competenze e processi direttamente collegati alla sicurezza delle informazioni. La priorita manageriale e ora trasformare tale maturita tecnica in evidenze ricorrenti, firmate, versionate e verificabili.

- Confermare il perimetro SGSI includendo confini fisici, logici, cloud, clienti, fornitori critici e processi affidati all'esterno.
- Aggiornare metodologia di rischio, risk register, piano trattamento e SoA con piena tracciabilita asset-rischio-controllo-owner-stato.
- Rafforzare evidence pack operativo: ticket, log, backup/restore, review accessi, incidenti, change e monitoraggio.
- Attuare un CAPA plan entro tempi definiti, con causa radice, responsabilita, prova di implementazione e verifica efficacia.
- Integrare KPI SGSI nel riesame Direzione con trend, decisioni, risorse, scadenze e follow-up.

Conclusione

L’audit supporta la raccomandazione alla certificazione, subordinatamente alla corretta gestione dei rilievi e al mantenimento di evidenze oggettive robuste, coerenti e ripetibili. Il livello di maturita atteso per il mantenimento e quello di un MSP che governa accessi, asset, rischi, backup, incidenti e fornitori con registrazioni verificabili.

11. Fonti e riferimenti documentali

- Audit Report - Stage 2, Form AR_01.2 Rev.004, 29th August 2025, NETISON S.R.L., pp. 1-40.
- Politica Protezione Dati NETISON S.R.L., datata 18/03/2024 e sottoscritta dalla Direzione, come richiamata nel report di audit.
- Sito web aziendale NETISON: servizi IT gestiti, backup, network security, virtualizzazione, co-managed IT, privacy policy, come richiamato nel report di audit.
- Documentazione SGSI campionata: contesto, parti interessate, campo di applicazione, risk assessment, piano trattamento rischi, SoA, procedure operative, controlli Annex A, audit interni, riesame Direzione e azioni correttive.
- Riferimenti normativi richiamati nel report: Regolamento UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, Direttiva NIS2/recepimento nazionale, indicazioni Garante Privacy e ACN ove applicabili.