REPORT EVIDENZE

E PIANO DI CHIUSURA DEI RILIEVI - STAGE 1

Sistema di Gestione per la Sicurezza delle Informazioni

ISO/IEC 27001:2022/Amd 1:2024

Organizzazione	RIDUTTORI ITALIA S.R.L.
Sede	Via Lago di Alleghe 16, 36015 Schio (VI)
Riferimento cliente	ST120260706194
Data Stage 1	16 luglio 2026
Lead Auditor	dott. Giuseppe Izzo
Area indicata nel rapporto	IAF 17 - NACE/ATECO 28.15.00
Stato del documento	Documento di lavoro per la readiness allo Stage 2

Finalità del report

Organizzare in modo verificabile le evidenze richieste dal rapporto di Stage 1, definire le azioni di chiusura e consentire una valutazione documentata della readiness prima della pianificazione o conferma dello Stage 2.

Rev. 00 - 16 luglio 2026

1. Sintesi esecutiva

Il rapporto di Stage 1 registra 0 non conformità maggiori, 2 non conformità minori e 17 osservazioni/aree di attenzione. Le due non conformità minori riguardano l'assenza o l'insufficienza delle evidenze relative al programma e allo svolgimento dell'audit interno del SGSI. Le osservazioni documentali interessano il contesto, le parti interessate, l'accettazione dei rischi residui, gli obiettivi, la gestione delle modifiche, le competenze, il riesame della direzione, la gestione delle non conformità e la formalizzazione dell'interazione tra i processi.

La conclusione del rapporto indica carenze significative e suggerisce la ripetizione dello Stage 1 dopo l'attuazione delle azioni necessarie. Il documento, tuttavia, presenta anche alcune incongruenze formali e valutative che devono essere chiarite con l'Organismo di Certificazione prima di procedere, in particolare per il riesame della direzione, la modalità di audit, la composizione del team e la classificazione IAF.

Indicatore	Risultato	Interpretazione
Non conformità maggiori	0	Nessun blocco classificato come Major.
Non conformità minori	2	Clausola 9.2: programma, esecuzione e registrazioni dell'audit interno.
Osservazioni / aree di attenzione	17	10 rilievi documentali, 1 rilievo sui processi e 6 punti di readiness da formalizzare.
Esito riportato	Stage 1 da ripetere	La raccomandazione finale non risulta selezionata nelle apposite caselle.
Priorità immediata	Alta	Audit interno completo, riesame della direzione e revisione SoA prima dello Stage 2.

Giudizio di readiness proposto

Il SGSI può essere portato allo Stage 2 solo dopo la chiusura documentata delle due NC minori, l'esecuzione del riesame della direzione, la revisione completa della SoA e la correzione delle incongruenze formali del rapporto. La semplice produzione di documenti non è sufficiente: devono essere disponibili registrazioni datate, approvate e coerenti con la reale operatività aziendale.

2. Documenti e informazioni esaminati

Documento	Contenuto	Valutazione sintetica
Rapporto di audit Stage 1	AR_01.2 Rev. 000 - 16/07/2026	Fonte primaria dei rilievi e della conclusione.
Documento SGSI	Manuale/descrizione del sistema	Presente; necessita allineamento e controllo delle revisioni.
Politica Sicurezza Informazioni	Politica SGSI	Presente.
Registro dei Rischi	Valutazione rischi	Presente; integrare accettazione dei rischi residui.
Piano di Trattamento del Rischio	Azioni e controlli	Presente; collegare scadenze, owner ed evidenze.
Statement of Applicability	Dichiarazione di applicabilità	Presente; da revisionare integralmente.
Procedure SGSI	Procedure operative	Presenti; verificare implementazione effettiva e registrazioni.

3. Criteri per considerare una evidenza accettabile

- Identificazione univoca del documento, revisione, data, autore e approvatore.
- Coerenza con il campo di applicazione, gli asset e i processi reali di Riduttori Italia S.r.l.
- Presenza di registrazioni operative: non solo procedure, ma log, verbali, report, test e firme.
- Tracciabilità tra rischio, controllo SoA, attività, responsabile, scadenza e verifica di efficacia.
- Disponibilità della evidenza prima dello Stage 2 e possibilità di campionamento durante l'audit.

4. Chiusura delle non conformità minori

Le due NC minori hanno la stessa causa di fondo: non sono state presentate evidenze sufficienti per dimostrare che il SGSI sia stato sottoposto a un audit interno pianificato, indipendente, completo e registrato. La chiusura deve essere trattata come un unico progetto di audit interno, con due evidenze di chiusura distinte.

ID	Clausola	Rilievo	Evidenza di chiusura richiesta	Owner	Stato
NC-MIN-01	ISO/IEC 27001:2022, 9.2	Mancata evidenza di audit interni condotti a intervalli pianificati.	Programma annuale approvato; piano audit; criteri, campo e metodi; nomina auditor competente e indipendente; checklist completa; rapporto finale; rilievi e follow-up.	Direzione / Responsabile SGSI	DA PRODURRE
NC-MIN-02	ISO/IEC 27001:2022, 9.2	Non disponibile la data dell'ultimo audit interno e le relative registrazioni.	Rapporto di audit interno datato e firmato; foglio presenze; evidenze campionate; registro rilievi; piano azioni; verifica di efficacia e chiusura.	Responsabile SGSI	DA PRODURRE

4.1 Sequenza minima dell'audit interno

Fase	Attività obbligatoria
1	Approvare il programma di audit interno che copra tutte le clausole 4-10 e i controlli Annex A applicabili.
2	Definire piano e checklist, includendo il perimetro fisico, organizzativo e tecnologico.
3	Assicurare indipendenza: l'auditor non deve verificare attività da lui direttamente progettate o gestite senza adeguate salvaguardie.
4	Eseguire interviste, campionamento documentale e test delle evidenze operative.
5	Emettere rapporto con conformità, NC, osservazioni e opportunità di miglioramento.
6	Aprire le azioni correttive, svolgere analisi causa, attuare correzioni e verificare efficacia.
7	Portare i risultati al riesame della direzione.

Criterio di chiusura

Le NC possono essere considerate chiuse solo quando il pacchetto di audit interno è completo e l'efficacia delle azioni correttive è verificata. Un programma non eseguito o un verbale privo di campionamenti non sono sufficienti.

5. Piano evidenze per le osservazioni documentali

ID	Clausola	Rilievo	Evidenza richiesta	Stato
OBS-01	4.1	Contesto interno ed esterno parziale.	Analisi aggiornata con fattori tecnologici, supply chain, minacce cyber, dipendenze IT/OT, clima e continuità; data e approvazione.	DA AGGIORNARE
OBS-02	4.2	Parti interessate e requisiti parziali.	Matrice con clienti, dipendenti, fornitori IT, subfornitori, autorità, assicurazioni e OdC; esigenze, obblighi e modalità di monitoraggio.	DA AGGIORNARE
OBS-03	6.1.3	Accettazione rischi residui	Registro dei rischi residui con	DA PRODURRE

ID	Clausola	Rilievo	Evidenza richiesta	Stato
		non formalizzata.	valore post-trattamento, criterio di accettazione, owner, decisione e firma della Direzione.	
OBS-04	6.2	Obiettivi e piani di attuazione incompleti.	Obiettivi misurabili con KPI, baseline, target, responsabile, risorse, data e frequenza di monitoraggio.	DA AGGIORNARE
OBS-05	6.3	Pianificazione delle modifiche incompleta.	Registro modifiche SGSI/IT con impatto, rischio, approvazione, test, rollback e verifica post-implementazione.	DA PRODURRE
OBS-06	7.2	Piano formazione e competenze parziale.	Matrice competenze; piano annuale; attestati; test di apprendimento; formazione phishing, password, incidenti e uso sicuro dispositivi.	DA AGGIORNARE
OBS-07	9.2	Programma audit interno parziale.	Vedi chiusura NC-MIN-01.	DA PRODURRE
OBS-08	9.2	Rapporti audit interno parziali.	Vedi chiusura NC-MIN-02.	DA PRODURRE
OBS-09	9.3	Riesame della Direzione non disponibile.	Verbale completo con input/output richiesti, risultati audit, KPI, incidenti, rischi, risorse, opportunità e decisioni.	DA PRODURRE
OBS-10	10.2	NC e azioni correttive parziali.	Procedura applicata e registro con correzione, analisi causa, azione, owner, scadenza, evidenza e verifica efficacia.	DA AGGIORNARE
OBS-11	4.4	Interazione dei processi da formalizzare.	Mappa processi SGSI con input/output, owner, indicatori e collegamenti tra commerciale, tecnico, produzione, IT e supporto.	DA AGGIORNARE

6. Revisione della Dichiarazione di Applicabilità (SoA)

La SoA è formalmente presente, ma il rapporto di Stage 1 evidenzia esclusioni e stati incoerenti. Prima dello Stage 2 deve essere riesaminata per tutti i 93 controlli dell'Annex A, collegando ciascun controllo ai rischi, ai requisiti applicabili e alle evidenze di attuazione.

Controllo	Tema	Criticità	Azione/evidenza
A.5.23	Cloud services	Indicato non applicabile, ma sono richiamati servizi SaaS/cloud.	Rivalutare come applicabile; definire selezione, responsabilità, configurazione, uscita e monitoraggio fornitori cloud.
A.5.24	Incident management planning	Indicato non applicabile, mentre esistono rischi phishing/ransomware.	Rendere applicabile; approvare piano, ruoli, escalation e test/esercitazione.
A.5.29	Information security during disruption	Indicato non applicabile, ma l'IT è critico per la produzione.	Rendere applicabile; collegare BCP, priorità, procedure degradate e responsabilità.
A.5.30	ICT readiness for business continuity	Applicabile ma stato "not applicable".	Correggere lo stato e fornire test di ripristino/continuità.
A.8.8	Technical vulnerabilities	Applicabile ma stato "not applicable".	Correggere; produrre patching, vulnerability review e registrazioni.
A.8.9	Configuration management	Applicabile ma stato "not applicable".	Correggere; inventario configurazioni, baseline e change record.
A.8.11	Data masking	Potenzialmente non applicabile.	Mantenere N/A solo con motivazione verificabile: nessun uso di dati reali in test/formazione e nessun requisito di mascheramento.
A.8.12	Data leakage prevention	Indicato non applicabile nonostante il valore dei disegni tecnici.	Rivalutare applicabilità; implementare misure proporzionate su e-mail, USB, condivisione e trasferimenti.
A.8.23	Web filtering	Indicato non applicabile con rischio phishing/malware.	Rivalutare; documentare DNS/web filtering o misure equivalenti.
A.8.24	Use of cryptography	Indicato non applicabile, ma sono trattati dati riservati e backup/cloud.	Rivalutare; definire cifratura in transito/a riposo, gestione chiavi e dispositivi.
A.8.25-8.29	Secure development lifecycle	Nel rapporto risultano presenti evidenze.	Confermare l'effettiva attività di sviluppo/manutenzione applicativa; in assenza, delimitare e motivare l'applicabilità.

6.1 Contenuti minimi della SoA revisionata

- identificativo e titolo di ogni controllo Annex A;
- decisione di applicabilità con motivazione specifica;
- rischi e requisiti che giustificano la decisione;
- stato di attuazione reale: implementato, parziale, pianificato o non applicabile;
- riferimento puntuale a procedura, registro, configurazione o altra evidenza;
- owner del controllo e data del prossimo riesame.

7. Chiusura dei punti di readiness classificati come “Area of concern”

Sei punti sono stati riportati come non soddisfatti perché la risposta corretta era “No”. In base alla formulazione delle domande, tali risposte non rappresentano necessariamente una carenza. Devono essere chiuse con dichiarazioni oggettive e, ove necessario, con la rettifica del rapporto.

Punto	Domanda	Risposta	Evidenza di chiusura
#3	È necessaria una modifica dello scopo?	No	Conferma scritta che lo scope è invariato e coerente con attività, sede e processi.
#4	Sono presenti siti temporanei?	No	Dichiarazione che non esistono cantieri, sedi di progetto o siti temporanei nel perimetro.
#7	Sono presenti fattori di stagionalità?	No	Dichiarazione di assenza di stagionalità significativa ai fini del campionamento.
#13	Ci sono variazioni dello scopo?	No	Conferma di assenza variazioni dalla domanda/contratto di certificazione.
#14	Sono presenti ulteriori informazioni?	No	Dichiarazione che non vi sono ulteriori elementi capaci di modificare durata o piano audit.
#15	È necessario verificare il turno notturno?	No	Dichiarazione di assenza di turno notturno o di attività rilevanti fuori orario.

Azione raccomandata

Trasmettere all’Organismo di Certificazione una nota di chiarimento e richiedere che tali punti non siano conteggiati come osservazioni qualora la risposta “No” descriva correttamente il contesto aziendale.

8. Incongruenze formali da chiarire o rettificare

Tema	Dato nel rapporto	Correzione / evidenza
Riesame della direzione	Nel requisito 9.3 è indicato N/A.	Il riesame della direzione è un requisito obbligatorio e non può essere escluso. Produrre verbale e correggere il rapporto.
Raccomandazione finale	Le tre caselle di raccomandazione risultano non selezionate.	Far indicare formalmente l'esito: prosecuzione, chiusura evidenze o ripetizione Stage 1.
Modalità audit	È selezionato Remote audit, ma la modalità è indicata Hybrid.	Uniformare piano, rapporto e registrazioni.
Team di audit	Il Lead Auditor appare duplicato come "Giuseppe Izzo 2".	Correggere l'anagrafica del team.
Tecnico esperto	Fabio Cecchinato risulta sia CEO dell'organizzazione sia Technical Expert del team.	Verificare e correggere per evitare ambiguità su indipendenza e imparzialità.
Numero dipendenti	Il rapporto indica 7; la visura al 31/12/2025 indica 8.	Confermare il numero effettivo alla data di audit e motivare eventuale variazione.
Area IAF	È indicato IAF 17 con NACE/ATECO 28.15.00.	Richiedere conferma formale della corretta classificazione tecnica da parte dell'OdC.
Visita al sito	È indicato viaggio significativo pur trattandosi di audit remoto/ibrido.	Riesaminare la risposta in relazione alla modalità effettiva di audit.
Reclami e segnalazioni	La gestione è indicata N/A.	Anche in assenza di reclami, predisporre registro o modalità di registrazione e dichiarare "nessun caso nel periodo".

9. Dossier evidenze da consegnare prima dello Stage 2

Codice	Evidenza	Criterio di completezza	Termine
EVD-01	Analisi contesto e parti interessate	Rev. approvata e datata	T-10 giorni
EVD-02	Mappa processi e interazioni SGSI	Diagramma + schede processi	T-10 giorni
EVD-03	Scope e dichiarazioni readiness	Scope, assenza siti temporanei/stagionalità/notturno	T-10 giorni
EVD-04	Registro rischi e accettazione residui	Firma Direzione su rischi accettati	T-10 giorni
EVD-05	Obiettivi e KPI	Piano annuale con target e misure	T-10 giorni
EVD-06	Registro modifiche	Change plan e almeno un esempio applicato	T-10 giorni
EVD-07	Competenze e formazione	Matrice, piano, attestati e test	T-10 giorni
EVD-08	Programma e piano audit interno	Approvati e completi	T-10 giorni
EVD-09	Rapporto audit interno	Eseguito, firmato e con follow-up	T-7 giorni
EVD-10	Riesame della Direzione	Verbale successivo all'audit interno	T-5 giorni
EVD-11	Registro NC/azioni correttive	Include chiusura NC Stage 1 e audit interno	T-5 giorni
EVD-12	SoA revisionata	Tutti i 93 controlli e riferimenti evidenze	T-7 giorni
EVD-13	Registro requisiti legali	GDPR, contratti, cyber e altri requisiti applicabili	T-10 giorni
EVD-14	Inventario IT e schema rete	Utenti, server, endpoint, reti, cloud e backup	T-10 giorni
EVD-15	Test backup/ripristino e continuità	Verbale test con esito, tempi e azioni	T-7 giorni
EVD-16	Gestione incidenti	Piano + esercitazione/table-top + registro	T-7 giorni
EVD-17	Sicurezza fornitori	Valutazione fornitori critici e clausole	T-7 giorni

10. Checklist di readiness finale

Verifica	Esito
NC-MIN-01 chiusa con programma ed esecuzione audit interno	[ ]
NC-MIN-02 chiusa con rapporto, registrazioni e follow-up	[ ]
Riesame della Direzione eseguito e firmato	[ ]
SoA revisionata su tutti i 93 controlli	[ ]
Rischi residui formalmente accettati dalla Direzione	[ ]
Obiettivi/KPI monitorati con almeno una registrazione	[ ]
Formazione e consapevolezza documentate	[ ]
Test backup/ripristino disponibile	[ ]
Gestione incidenti testata o simulata	[ ]
Incongruenze del rapporto chiarite con l'OdC	[ ]
Tutti i file raccolti in dossier indicizzato e versionato	[ ]

Decisione proposta del Lead Auditor

Raccomandare la pianificazione dello Stage 2 esclusivamente dopo la verifica documentale positiva del dossier EVD-01/EVD-17 e la chiusura delle due NC minori. In caso di mancanza dell'audit interno o del riesame della direzione, confermare la necessità di ulteriore Stage 1/readiness review.

11. Approvazione e presa in carico

Per RIDUTTORI ITALIA S.R.L.	**Lead Auditor**
Nome e ruolo: _____	dott. Giuseppe Izzo
Data e firma: _____	Data e firma: _____

Nota: il presente documento è un report di evidenze e un piano operativo di chiusura. Non sostituisce il rapporto ufficiale dell'Organismo di Certificazione né modifica autonomamente la classificazione dei rilievi. Ogni chiusura deve essere confermata sulla base di evidenze oggettive e della decisione dell'Organismo di Certificazione.