REPORT EVIDENZE

AUDIT DI CERTIFICAZIONE - STAGE 2

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), Italia
Riferimento cliente	ST120260706194
Fase dell'audit	Stage 2 - Audit iniziale di certificazione
Data del rapporto	16 luglio 2026
Lead Auditor	dott. Giuseppe Izzo
Schema / area	ISO/IEC 27001:2022/Amd 1:2024 - IAF 17 - NACE/ATECO 28.15.00
Esito proposto	CONFORME - Raccomandazione al rilascio della certificazione

Finalità del report

Raccogliere in forma strutturata le evidenze oggettive utilizzate nello Stage 2, documentare la conformità del SGSI e supportare la revisione tecnica e la decisione di certificazione dell'Organismo di Certificazione.

Rev. 00 - 16 luglio 2026

1. Sintesi esecutiva

L'audit di Stage 2 ha riguardato l'attuazione e l'efficacia del Sistema di Gestione per la Sicurezza delle Informazioni applicato ai processi di progettazione, fabbricazione e vendita di organi di trasmissione, ingranaggi e riduttori, comprese le lavorazioni meccaniche correlate, presso la sede unica di Schio.

Il campionamento documentale, le interviste e le verifiche operative hanno evidenziato un SGSI proporzionato alle dimensioni dell'organizzazione, coerente con il contesto e con i rischi informativi associati ai disegni tecnici, ai file CAD, alle specifiche dei clienti, ai dati commerciali e alle infrastrutture IT.

Conclusione dell'audit

Non sono state rilevate non conformità maggiori o minori. Le risultanze dello Stage 1 risultano trattate e le evidenze rese disponibili consentono di formulare una raccomandazione positiva al rilascio della certificazione, subordinatamente alla revisione tecnica e alla decisione indipendente dell'Organismo di Certificazione.

1.1 Risultati sintetici

Indicatore	Risultato	Valutazione
Requisiti ISO/IEC 27001, clausole 4-10	Conformi	C
Controlli Annex A applicabili	Implementati e campionati	C
Non conformità maggiori	0	C
Non conformità minori	0	C
Osservazioni	0	C
Raccomandazione	Rilascio della certificazione	Positiva

1.2 Campo di audit

IT: Audit del Sistema di Gestione per la Sicurezza delle Informazioni a supporto dei processi di progettazione, fabbricazione e vendita di organi di trasmissione, ingranaggi e riduttori, comprese le lavorazioni meccaniche correlate, presso la sede di Via Lago di Alleghe 16, 36015 Schio (VI).

EN: Audit of the Information Security Management System supporting the design, manufacture and sale of power transmission components, gears and gearboxes, including related mechanical machining, at the site located in Via Lago di Alleghe 16, 36015 Schio (VI), Italy.

Campo rivisto: confermato senza variazioni rispetto allo Stage 1. Nessuna esclusione dei requisiti della norma; gli eventuali controlli Annex A non applicabili sono motivati nella SoA.

1.3 Team e modalità

Lead Auditor	dott. Giuseppe Izzo
Auditor	Non previsto
Esperto tecnico	Non previsto
Referente organizzazione	ing. Fabio Cecchinato - Top Management
Modalità	Audit Stage 2 presso la sede, con interviste e campionamento documentale e operativo

2. Base documentale ed evidenze campionate

Le evidenze sono state valutate secondo criteri di identificazione, datazione, approvazione, coerenza con il campo di applicazione, tracciabilità rispetto ai rischi e disponibilità di registrazioni operative. Il presente dossier deve essere utilizzato unitamente ai documenti originali e alle registrazioni effettivamente mostrate durante l'audit.

ID	Documento	Contenuto verificato	Data
E2-01	Visura ordinaria	Dati societari, sede, attività, amministratore, addetti e certificazione ISO 9001.	12/05/2026
E2-02	Rapporto Stage 1	Risultati, rilievi, campo, complessità IT e pianificazione della readiness.	16/07/2026
E2-03	Report evidenze Stage 1	Piano di chiusura e tracciabilità delle evidenze richieste prima dello Stage 2.	16/07/2026
E2-04	Documento SGSI	Contesto, campo, processi, ruoli e architettura generale del sistema.	15/07/2026
E2-05	Politica Sicurezza Informazioni	Impegni, obiettivi, responsabilità e criteri di riesame.	15/07/2026
E2-06	Registro dei Rischi	Asset, minacce, vulnerabilità, impatti, probabilità e rischi residui.	15/07/2026
E2-07	Piano di Trattamento del Rischio	Azioni, controlli, responsabilità, scadenze e stato di attuazione.	15/07/2026
E2-08	Statement of Applicability	Applicabilità dei 93 controlli, motivazioni, responsabili e stato.	15/07/2026
E2-09	Procedure SGSI	Gestione accessi, backup, incidenti, fornitori, continuità, documenti e modifiche.	15/07/2026

2.1 Registrazioni operative campionate

ID	Registrazione / evidenza operativa
E2-10	Inventario asset e assegnazione degli owner
E2-11	Elenco utenti, autorizzazioni e riesame periodico degli accessi
E2-12	Log dei backup e registrazione del test di ripristino
E2-13	Registro incidenti/eventi e canali di segnalazione
E2-14	Piano formazione, attestazioni e sensibilizzazione del personale
E2-15	Programma e rapporto di audit interno del SGSI
E2-16	Verbale del riesame della Direzione e relativo piano di azione
E2-17	Registro modifiche, non conformità, azioni correttive e verifica di efficacia
E2-18	Elenco fornitori critici, accordi e verifiche di sicurezza
E2-19	Report di monitoraggio KPI, patching e vulnerabilità tecniche

Nota di utilizzazione

Le registrazioni E2-10 - E2-19 devono corrispondere ai documenti reali, datati e approvati messi a disposizione durante l'audit. Il presente report non sostituisce gli originali né la decisione dell'Organismo di Certificazione.

3. Evidenze di conformità - Clausole 4, 5 e 6

ID	Clausola	Evidenze oggettive utilizzate	Esito
C4-01	4.1	Analisi del contesto interno ed esterno aggiornata; considerati mercato industriale, dipendenza IT, minacce cyber, fornitori, continuità e protezione della proprietà intellettuale. Coerenza verificata con rischi e campo SGSI.	C
C4-02	4.2	Registro delle parti interessate con clienti, personale, fornitori IT e produttivi, autorità, assicurazioni e Organismo di Certificazione; requisiti tracciati nei rischi e nei controlli.	C
C4-03	4.3	Campo documentato e confermato per la sede unica di Schio, inclusi confini fisici, organizzativi, tecnologici e rapporti con terze parti.	C
C4-04	4.4	Mappa dei processi e interazioni tra Direzione, commerciale, progettazione, produzione, approvvigionamento, IT e supporto; definiti owner, input, output e indicatori.	C
C5-01	5.1	Impegno della Direzione verificato mediante approvazione della politica, assegnazione di risorse, partecipazione al riesame e integrazione del SGSI nei processi aziendali.	C
C5-02	5.2	Politica approvata, comunicata e coerente con riservatezza, integrità, disponibilità, obblighi applicabili e miglioramento continuo.	C
C5-03	5.3	Ruoli e responsabilità formalizzati nell'organigramma e nelle nomine; responsabilità operative comprese dai soggetti intervistati.	C
C6-01	6.1.1	Rischi e opportunità determinati considerando contesto e parti interessate; azioni integrate nella pianificazione del SGSI.	C
C6-02	6.1.2	Metodo di valutazione documentato, con criteri di probabilità, impatto e accettazione; applicazione coerente agli asset e aggiornamento in caso di cambiamenti.	C
C6-03	6.1.3	Piano di trattamento e SoA coerenti con i risultati della valutazione; owner e scadenze tracciati; rischi residui approvati dalla Direzione.	C
C6-04	6.2	Obiettivi definiti con indicatori, target, responsabilità, risorse e frequenze di monitoraggio; allineamento verificato con politica e rischi.	C
C6-05	6.3	Registro delle modifiche SGSI/IT con valutazione preventiva dei rischi, autorizzazione, test, rollback e verifica post-implementazione.	C

3.1 Evidenze rappresentative

Sono state campionate la corrispondenza tra il campo SGSI e l'attività societaria, la tracciabilità tra rischi e controlli, l'approvazione della politica e dei rischi residui, nonché la disponibilità di obiettivi misurabili. Le interviste alla Direzione hanno confermato la comprensione del contesto e l'assunzione delle responsabilità previste.

4. Evidenze di conformità - Clausole 7 e 8

ID	Clausola	Evidenze oggettive utilizzate	Esito
C7-01	7.1	Risorse umane, tecnologiche e infrastrutturali adeguate alla dimensione e alla complessità del perimetro: 3 utenti IT, 1 server, 3 postazioni, 2 reti, 1 connessione Internet e supporto IT dedicato.	C
C7-02	7.2	Matrice delle competenze, CV, incarichi, formazione e aggiornamento disponibili per i ruoli che influenzano il SGSI; carenze formative gestite mediante piano annuale.	C
C7-03	7.3	Consapevolezza verificata a campione su politica, password, phishing, segnalazione incidenti, gestione documenti e responsabilità individuali.	C
C7-04	7.4	Matrice di comunicazione interna ed esterna; canali definiti per incidenti, clienti, fornitori e autorità; responsabilità e tempi chiaramente assegnati.	C
C7-05	7.5	Documenti identificati con titolo, data, revisione e approvazione; accesso controllato, conservazione, protezione e disponibilità delle registrazioni verificate.	C
C8-01	8.1	Processi operativi pianificati e controllati mediante procedure, responsabilità, checklist, log e registrazioni; modifiche pianificate e non pianificate gestite.	C
C8-02	8.2	Rivalutazione dei rischi prevista e applicata a fronte di cambiamenti significativi di tecnologie, processi, fornitori, minacce e requisiti.	C
C8-03	8.3	Misure di trattamento attuate e verificate a campione: accessi, backup, malware protection, patching, sicurezza fornitori, incident response e continuità.	C

4.1 Campionamenti operativi

Area	Evidenza campionata	Esito
Gestione accessi	Elenco utenze, autorizzazioni, principio del minimo privilegio e riesame periodico.	C
Backup e ripristino	Pianificazione, log di esecuzione, conservazione e test di ripristino.	C
Incidenti	Canale di segnalazione, classificazione, escalation, registro e lezioni apprese.	C
Fornitori	Valutazione, clausole di riservatezza, accessi remoti e verifica dei servizi critici.	C
Modifiche	Richiesta, analisi impatto, approvazione, test e chiusura.	C
Documenti tecnici	Protezione dei disegni, file CAD, specifiche e documentazione dei clienti.	C

Valutazione operativa

I controlli risultano proporzionati al rischio e integrati nelle attività aziendali. La verifica è stata svolta mediante campionamento e non costituisce una prova esaustiva di ogni transazione o configurazione tecnica.

5. Evidenze di conformità - Clausole 9 e 10

ID	Clausola	Evidenze oggettive utilizzate	Esito
C9-01	9.1	KPI e criteri di misurazione definiti per obiettivi, incidenti, backup, vulnerabilità, formazione, accessi e azioni; risultati analizzati e riportati alla Direzione.	C
C9-02	9.2	Programma di audit interno completo di obiettivi, campo, criteri, frequenza e metodi; audit eseguito da risorsa competente e con adeguate garanzie di indipendenza.	C
C9-03	9.2	Rapporto di audit interno datato e approvato; evidenze campionate, risultati comunicati e follow-up documentato. Chiusura delle risultanze dello Stage 1 verificata.	C
C9-04	9.3	Riesame della Direzione eseguito considerando contesto, parti interessate, rischi, audit, KPI, incidenti, risorse, opportunità e cambiamenti; output e azioni tracciati.	C
C10-01	10.1	Registro delle opportunità e piano di miglioramento attivo; priorità definite sulla base dei rischi, delle prestazioni e dei risultati di audit.	C
C10-02	10.2	Procedura per non conformità e azioni correttive applicata; registrate correzione, analisi della causa, responsabile, scadenza, evidenza e verifica di efficacia.	C

5.1 Chiusura delle risultanze dello Stage 1

Area Stage 1	Evidenza di chiusura verificata	Esito
Audit interno	Programma, piano, checklist, rapporto, evidenze campionate e follow-up.	Chiuso
Riesame della Direzione	Verbale completo con input, output, decisioni e piano di azione.	Chiuso
SoA	Valutazione completa dei 93 controlli e coerenza con rischi e trattamento.	Chiuso
Rischi residui	Accettazione formalizzata e approvata dalla Direzione.	Chiuso
Obiettivi e KPI	Target, owner, risorse, scadenze e monitoraggio definiti.	Chiuso
Competenze e modifiche	Matrice competenze, piano formativo e registro modifiche disponibili.	Chiuso

5.2 Altri elementi di sistema

Consegna del rapporto: prevista secondo le modalità dell'Organismo di Certificazione. Azioni correttive dell'audit precedente: verificate e chiuse. Trasferimento di certificato: non applicabile, trattandosi di prima certificazione. Commenti delle autorità e reclami: non risultano contestazioni o reclami pertinenti. Uso dei logotipi: non rilevato uso improprio; utilizzo consentito solo dopo il rilascio e secondo regolamento.

6. Annex A e Statement of Applicability

La Dichiarazione di Applicabilità è stata riesaminata rispetto ai rischi, ai requisiti cogenti e contrattuali e alle caratteristiche del sistema informativo. La valutazione copre i 93 controlli dell'Annex A, indicando applicabilità, motivazione, stato, responsabilità e riferimenti alle evidenze.

Gruppo	Controlli	Evidenza sintetica	Esito
Organizzativi	A.5.1-A.5.37	Politiche, ruoli, segregazione, inventario, classificazione, accessi, fornitori, cloud, incidenti, continuità, requisiti legali e audit.	C
Persone	A.6.1-A.6.8	Screening, condizioni di impiego, consapevolezza, disciplina, cessazione, NDA, lavoro remoto e segnalazione eventi.	C
Fisici	A.7.1-A.7.14	Perimetri, accessi fisici, protezione aree, monitoraggio, minacce ambientali, desk clear, apparecchiature e smaltimento.	C
Tecnologici	A.8.1-A.8.34	Endpoint, privilegi, accessi, autenticazione, capacità, malware, vulnerabilità, configurazioni, cancellazione, backup, logging, reti, crittografia, sviluppo e test.	C

6.1 Controlli tecnici maggiormente rilevanti

Controllo	Tema	Evidenza verificata	Esito
A.5.15-A.5.18	Gestione degli accessi	Utenze nominali, autorizzazioni, riesami, revoche e minimo privilegio.	C
A.5.19-A.5.23	Fornitori e cloud	Valutazione dei fornitori, requisiti contrattuali, monitoraggio e sicurezza dei servizi cloud.	C
A.5.24-A.5.28	Incident management	Preparazione, classificazione, risposta, lezioni apprese e raccolta delle evidenze.	C
A.5.29-A.5.30	Continuità e ICT readiness	Scenari di interruzione, responsabilità, backup, ripristino e prove periodiche.	C
A.8.7-A.8.9	Malware, vulnerabilità e configurazioni	Protezione endpoint, patching, scansioni, hardening e controllo delle configurazioni.	C
A.8.13-A.8.14	Backup e ridondanza	Backup pianificati, log, conservazione e test di ripristino.	C
A.8.15-A.8.17	Logging e monitoring	Registrazione eventi, protezione dei log e sincronizzazione temporale.	C
A.8.20-A.8.22	Sicurezza delle reti	Separazione logica delle reti, configurazione apparati e controllo dei servizi.	C
A.8.24	Crittografia	Uso di protocolli sicuri e protezione delle chiavi secondo rischio e classificazione.	C

6.2 Vulnerability assessment e penetration testing

Sono stati verificati il processo di identificazione delle vulnerabilità, la pianificazione degli aggiornamenti, la classificazione delle criticità e la tracciabilità delle remediation. Le attività di vulnerability assessment e, ove proporzionato, penetration testing sono registrate e riesaminate in funzione dei cambiamenti e del rischio.

6.3 Controlli crittografici

L'impiego della crittografia è definito sulla base della classificazione e del rischio delle informazioni. Sono controllati protocolli di comunicazione, credenziali, backup e modalità di conservazione, rinnovo, revoca e protezione delle chiavi o dei segreti.

7. Sito, infrastruttura e conformità applicabile

7.1 Dettagli del sito

Organizzazione	RIDUTTORI ITALIA S.R.L.
Indirizzo	Via Lago di Alleghe 16, 36015 Schio (VI), Italia
Tipologia	Sede legale e operativa unica
Attività svolte	Direzione, commerciale, progettazione, fabbricazione, lavorazioni meccaniche, controllo, collaudo, amministrazione e gestione dei sistemi informativi.
Prodotti/servizi	Organi di trasmissione, ingranaggi, riduttori e componenti meccanici speciali realizzati a disegno o su specifica del cliente.

7.2 Complessità del sistema IT

Elemento	Dato / valutazione
Utenti IT	3
Server	1
Postazioni PC/laptop	3
Reti	2
Connessioni Internet	1
Risorsa sviluppo/manutenzione applicazioni	1
Complessità	Media, con criticità medio-alta per la dipendenza dei processi tecnici e produttivi dalla disponibilità dei sistemi e dei file tecnici.

7.3 Informazioni e asset critici

Disegni tecnici 2D/3D, file CAD, distinte base, cicli di lavorazione, specifiche dei clienti, risultati di calcolo e collaudo, dati commerciali e amministrativi, contratti, accordi di riservatezza, dati personali, informazioni sui fornitori, ERP, server, reti, backup e servizi cloud.

7.4 Conformità legislativa e contrattuale

Riferimento	Applicazione / evidenza
Regolamento UE 2016/679 e D.Lgs. 196/2003 s.m.i.	Protezione dei dati personali, ruoli, misure di sicurezza, gestione delle violazioni e rapporti con responsabili esterni.
D.Lgs. 138/2024 - NIS 2, previa verifica di applicabilità	Valutazione dell'applicabilità e presidio dei requisiti di gestione del rischio e notifica, ove pertinenti.
Normativa su proprietà intellettuale e segreti commerciali	Protezione di progetti, disegni, know-how, software e documentazione tecnica.
Reati informatici e conservazione delle evidenze	Gestione degli eventi, protezione dei log e collaborazione con le autorità competenti.
Contratti, NDA e requisiti clienti	Clausole di sicurezza, riservatezza, disponibilità, accesso e restituzione/cancellazione delle informazioni.

8. Risultati dell’audit ed evidenze oggettive

Area	Risultato	Evidenze oggettive utilizzate
Contesto dell’organizzazione	Conforme: contesto, parti interessate, processi e campo SGSI definiti e coerenti.	Documento SGSI; analisi contesto; registro parti interessate; mappa processi; visura.
Punti di forza	Competenza tecnica, struttura snella, coinvolgimento diretto della Direzione e attenzione alla protezione della proprietà intellettuale.	Politica; organigramma; interviste; registro asset; procedure e controlli sui documenti tecnici.
Debolezze	Dipendenza da figure chiave e fornitori esterni, riconosciuta e trattata mediante responsabilità, backup, continuità e controllo dei fornitori.	Registro rischi; piano trattamento; incarichi; procedure continuità e fornitori.
Conformità legislativa	Requisiti cogenti e contrattuali identificati e monitorati.	Registro requisiti; GDPR; contratti; NDA; verifiche periodiche.
Leadership e partecipazione	Direzione attiva e personale coinvolto mediante ruoli, comunicazione, formazione e sensibilizzazione.	Politica approvata; nomine; verbali; registri formazione; interviste.
Pianificazione e rischi	Metodo definito, rischi valutati, trattamenti assegnati e residui approvati.	Registro rischi; piano trattamento; SoA; approvazioni.
Supporto	Risorse, competenze, comunicazioni e documenti adeguati.	Matrice competenze; piano formazione; matrice comunicazioni; elenco documenti.
Attività operative	Controlli implementati e integrati nei processi.	Log accessi; backup; incidenti; fornitori; modifiche; procedure.
Valutazione prestazioni	Indicatori monitorati e risultati utilizzati per decisioni e riesame.	KPI; report; trend; stato obiettivi e azioni.
Audit e riesame	Audit interno e riesame della Direzione completati, documentati e utilizzati.	Programma/rapporto audit; checklist; verbale riesame; follow-up.
Miglioramento	Azioni correttive e opportunità gestite con verifica di efficacia.	Registro NC/AC; analisi cause; piano miglioramento; verifiche efficacia.
Informazioni schema	SoA completa e coerente con rischi e trattamento; controlli Annex A campionati.	SoA; inventario asset; schema rete; procedure tecniche; registrazioni.

8.1 Punti di attenzione per il mantenimento

Pur in presenza di conformità, si raccomanda di mantenere continuità nella produzione delle registrazioni, aggiornare periodicamente la valutazione dei rischi e la SoA, verificare l’efficacia dei backup e delle azioni di remediation, riesaminare i fornitori critici e conservare evidenze di formazione, audit e riesame.

9. Conclusioni e raccomandazione

Il Sistema di Gestione per la Sicurezza delle Informazioni di RIDUTTORI ITALIA S.R.L. risulta implementato e mantenuto in conformità ai requisiti della ISO/IEC 27001:2022/Amd 1:2024, nell'ambito definito per la sede di Schio. Il sistema dimostra la capacità di identificare e trattare i rischi, proteggere le informazioni rilevanti, monitorare le prestazioni e attivare il miglioramento continuo.

Le evidenze esaminate supportano la conformità delle clausole 4-10 e dei controlli Annex A applicabili. Non sono state rilevate non conformità maggiori, non conformità minori o osservazioni tali da impedire la certificazione.

Raccomandazione del Lead Auditor

Si raccomanda il rilascio della certificazione ISO/IEC 27001:2022/Amd 1:2024 per il campo di applicazione auditato, subordinatamente alla positiva revisione tecnica e alla decisione indipendente dell'Organismo di Certificazione.

9.1 Dichiarazione sul campionamento

L'audit è stato condotto per campionamento. La conformità espressa nel rapporto non elimina la responsabilità dell'organizzazione di mantenere il SGSI, rispettare i requisiti applicabili e assicurare la validità, completezza e autenticità delle registrazioni mostrate.

9.2 Approvazioni

Lead Auditor	dott. Giuseppe Izzo
Data	16 luglio 2026
Firma	_____
Presa visione dell'organizzazione	ing. Fabio Cecchinato _____

9.3 Elenco allegati richiamati

Visura ordinaria; Rapporto di audit Stage 1; Report evidenze Stage 1; Documento SGSI; Politica Sicurezza Informazioni; Registro dei Rischi; Piano di Trattamento del Rischio; Statement of Applicability; Procedure SGSI; registrazioni operative campionate E2-10 - E2-19.