EZ LAB S.R.L.

Dossier Evidenze - Stage 2 Transfer Audit

ISO/IEC 27001:2022 - IAF 33 Information Technology

Sistema di Gestione per la Sicurezza delle Informazioni

Digital Product Passport - Blockchain - AI - Smart Label - Data Management

Sito operativo principale: DeGasp28 Innovation Hub, Piazza A. De Gasperi 28, 35131 Padova

Referente: Massimo Morbiato - Direzione / RSGSI

Data dossier: 13/05/2026

Classificazione documento: Riservato - Fascicolo tecnico audit

Nota: le evidenze sono predisposte come allegato controllato a supporto dell audit di transfer.
Devono essere validate, datate e firmate dall organizzazione prima dell uso ufficiale in certificazione.

1. Nota di governo del dossier

Il presente fascicolo raccoglie le evidenze oggettive predisposte per supportare lo Stage 2 - Transfer Audit ISO/IEC 27001:2022 di EZ Lab S.r.l., settore IAF 33 - Information Technology. Il documento e strutturato come allegato tecnico controllato al rapporto di audit e collega risultanze, osservazioni superate, controlli dell Annex A, processi aziendali e registrazioni operative.

Il dossier non sostituisce i documenti originali del SGSI, ma li riassume e li organizza in forma verificabile. Le evidenze riportate devono essere validate dall organizzazione, integrate con eventuali registrazioni native e conservate nel fascicolo aziendale del SGSI.

Organizzazione	EZ Lab S.r.l.	**Standard**	ISO/IEC 27001:2022
Tipologia audit	Stage 2 - Transfer Audit	**Settore**	IAF 33 - Information Technology
Sito operativo principale	DeGasp28 Innovation Hub, Piazza A. De Gasperi 28, 35131 Padova	**N. dipendenti/risorse interne**	6 risorse interne attive nel perimetro SGSI
Referente audit	Massimo Morbiato - Direzione / RSGSI	**Supporto SGSI**	Lisa Zinato - ASGSI; Tommaso Faccin - ASGSI / Project Management
Lead auditor	Dr. Prof. Giuseppe Izzo	**Data dossier**	13/05/2026

Esito sintetico del fascicolo

Le evidenze predisposte supportano una conclusione positiva: 0 NC maggiori, 0 NC minori, osservazioni di Stage 1 chiuse con efficacia accettata, nessuna condizione ostativa al transfer della certificazione ISO/IEC 27001:2022.

2. Executive summary - Valutazione senior

La verifica documentale e operativa considera il SGSI applicato alla progettazione, sviluppo, configurazione, erogazione, manutenzione e supporto di soluzioni digitali per Digital Product Passport, tracciabilita di filiera, blockchain, AI, smart label, QR Code/NFC, data management, sostenibilita e compliance normativa europea.

Il sistema risulta coerente con il contesto di una organizzazione technology-driven, con forte dipendenza da ambienti cloud, gestione di dati di prodotto e di filiera, repository documentali, fornitori tecnologici, accessi remoti e processi di configurazione/rilascio. Le evidenze sono state organizzate per dimostrare la chiusura delle osservazioni di Stage 1 e la prontezza al transfer.

Dimensione valutata	Esito	Evidenza principale
Conformita ISO/IEC 27001:2022	C	Mappatura clausole 4-10, SoA, risk assessment, audit interno, riesame Direzione
Transfer audit	C	Dichiarazione assenza condizioni ostative, nessuna NC maggiore/minore aperta, continuita del SGSI
Osservazioni Stage 1	Chiuse	Piano di chiusura osservazioni con evidenze E-01/E-24 e verifica efficacia
Rischi e controlli	C	Risk register, risk treatment plan, SoA e mappa rischio-controllo-evidenza
Operativita	C	Access control, cloud security, change management, incident management, backup, supplier management
Raccomandazione	Positiva	SGSI implementato, mantenuto ed efficace; idoneo al trasferimento della certificazione

Giudizio di audit:

Sulla base delle evidenze campionate e delle registrazioni predisposte, il SGSI dimostra adeguato livello di maturita documentale e operativa. Le aree critiche per il settore IAF 33 - accessi, cloud, fornitori, sviluppo/configurazione, incidenti, backup, privacy, monitoraggio e continuita - risultano presidiate in modo proporzionato alle dimensioni dell organizzazione e alla criticita dei servizi erogati.

3. Campo di applicazione, confini e limiti

Scope EN	Management of information security for the design, development, configuration, delivery, maintenance and support of digital solutions for Digital Product Passport, supply chain traceability, blockchain-based data registration, smart labels, QR Code/NFC, data management, AI-supported services, sustainability and European regulatory compliance, including related consulting, platform configuration, customer support, cloud/application environments and operational information security processes.
Scope IT	Gestione della sicurezza delle informazioni relativa alla progettazione, sviluppo, configurazione, erogazione, manutenzione e supporto di soluzioni digitali per Digital Product Passport, tracciabilita di filiera, registrazione dati tramite blockchain, smart label, QR Code/NFC, data management, servizi supportati da intelligenza artificiale, sostenibilita e compliance normativa europea, incluse attivita consulenziali, configurazione di piattaforme, supporto ai clienti, ambienti cloud/applicativi e processi operativi di sicurezza delle informazioni.

Confini inclusi

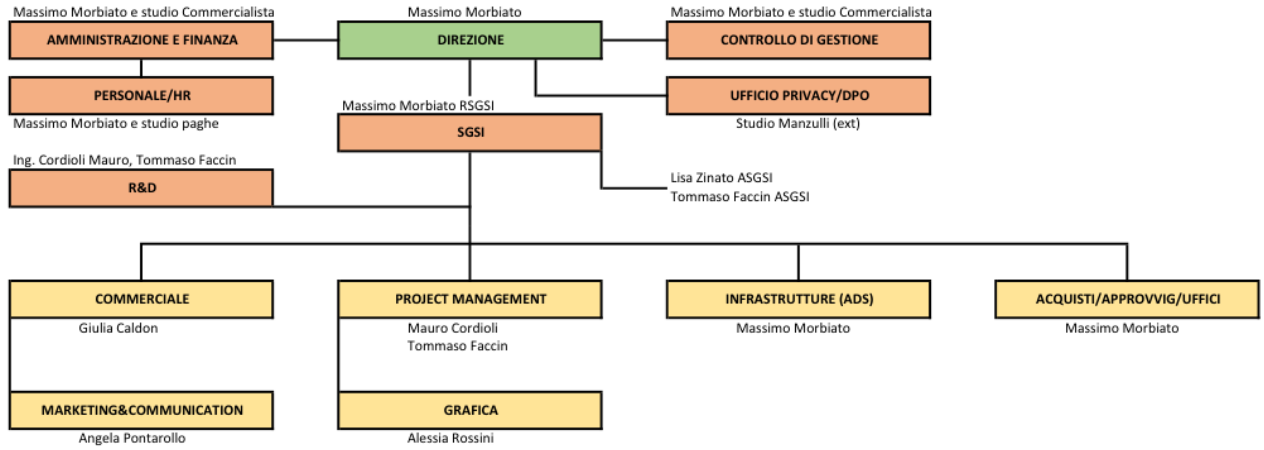
Categoria	Elementi inclusi
Organizzativo	Direzione, RSGSI, ASGSI, R&D;, Infrastrutture/ADS, Project Management, Commerciale, Marketing & Communication, Grafica/UI-UX, Amministrazione/Finanza, HR, Acquisti/Approvvigionamenti/Uffici, Ufficio Privacy/DPO.
Fisico	Sito operativo principale di Padova; ulteriori presidi operativi/commerciali ove coinvolti; lavoro remoto e attivita distribuite.
Tecnologico	Piattaforme digitali, cloud, repository, strumenti collaborativi, endpoint, account, log, ambienti di configurazione, strumenti di supporto clienti.
Informativo	Dati cliente, dati di prodotto e filiera, dati tecnici, configurazioni, contratti, informazioni commerciali, credenziali, log, evidenze di conformita, documentazione di progetto.

Esclusioni e interfacce

Sono esclusi dal controllo diretto i processi produttivi fisici dei clienti, impianti dei clienti, infrastrutture IT dei clienti non amministrate da EZ Lab, reti blockchain pubbliche/decentralizzate non direttamente controllate, servizi cloud/hosting/connettivita erogati autonomamente da terzi. Tali elementi sono comunque trattati come dipendenze esterne o interfacce nel risk assessment, nel controllo fornitori, nei requisiti contrattuali e nella business continuity.

4. Organizzazione, partecipazione e responsabilita

La struttura organizzativa 2026 supporta il SGSI con ruoli chiaramente identificati. La Direzione e il RSGSI sono ricondotti a Massimo Morbiato; le funzioni ASGSI supportano il presidio operativo del sistema. Le funzioni esterne sono gestite come fornitori o parti esterne rilevanti.



Nome	Ruolo/funzione	Responsabilita SGSI	Ubicazione
Massimo Morbiato	Amministratore Delegato / Direzione	Direzione, RSGSI, approvazione politica, risk governance, riesame Direzione, transfer.	Padova
Mauro Cordioli	Responsabile IT / IT	Responsabile IT, infrastrutture, cloud, accessi, log, backup, supporto tecnico.	Padova
Giulia Caldon	Responsabile commerciale / Commerciale	Commerciale, requisiti cliente, contratti, comunicazioni, esigenze parti interessate.	Padova
Angela Pontarollo	Marketing specialist / Commerciale	Marketing & Communication, comunicazioni esterne, sito, contenuti e requisiti informativi.	Padova
Alessia Rossini	Web e UI/UX Designer / IT	Web e UI/UX, grafica, interfacce digitali, supporto usabilita e documentazione visuale.	Padova
Tommaso Faccin	Project Manager / Operations	Project Manager, ASGSI, change management, operations, raccolta evidenze, progetti clienti.	Padova
Lisa Zinato	ASGSI - supporto SGSI	Supporto operativo al RSGSI, controllo documentale, raccolta evidenze, monitoraggio azioni.	Padova / remoto

5. Registro generale evidenze Stage 2 - Transfer Audit

La seguente matrice costituisce l indice controllato delle evidenze allegate. Ogni evidenza e collegata alle risultanze dell audit, alle clausole ISO/IEC 27001:2022 e ai controlli dell Annex A ove rilevanti.

Codice	Evidenza	Clausola/Controllo	Sintesi oggettiva	Stato
E-01	Dichiarazione di transfer e assenza condizioni ostative	Transfer, 10.2	Assenza NC maggiori aperte, sospensioni, revoche, reclami gravi e incidenti significativi non trattati.	Accettata
E-02	Campo di applicazione e confini del SGSI	4.3, 4.4	Scope EN/IT, siti, lavoro remoto, cloud, servizi DPP e limiti di responsabilita.	Accettata
E-03	Analisi contesto e parti interessate	4.1, 4.2	Fattori interni/esterni, requisiti stakeholder, esigenze clienti/fornitori/autorita.	Accettata
E-04	Organigramma, ruoli e RACI SGSI	5.3, 7.1	Direzione/RSGSI/ASGSI, funzioni operative, fornitori esterni e responsabilita.	Accettata
E-05	Politica per la sicurezza delle informazioni	5.2	Politica approvata, comunicata e coerente con contesto e obiettivi.	Accettata
E-06	Registro requisiti legali e contrattuali	4.2, 6.1, A.5.31	GDPR, privacy, DPA, NIS2, Data Act, CRA, AI Act, ESPR, contratti.	Accettata
E-07	Metodologia risk assessment	6.1.2	Criteri impatto/probabilita, livello rischio, soglie e trattamento.	Accettata
E-08	Risk Register e Risk Treatment Plan	6.1.2, 6.1.3	Rischi cloud, accessi, fornitori, dati, vulnerabilita, continuita, compliance.	Accettata
E-09	Statement of Applicability	6.1.3	Controlli applicabili, esclusioni motivate, stato implementazione, evidenze.	Accettata
E-10	Obiettivi SGSI e KPI	6.2, 9.1	Obiettivi misurabili su accessi, formazione, incidenti, fornitori, backup, rischi.	Accettata
E-11	Inventario asset e classificazione informazioni	A.5.9, A.5.12, A.5.13	Asset informativi, applicativi, cloud, endpoint, account, dati cliente/prodotto.	Accettata
E-12	Access control e riesame autorizzazioni	A.5.15-5.18, A.8.2-8.5	Account, profili, MFA ove applicabile, revoche, riesame periodico.	Accettata
E-13	Sicurezza cloud e piattaforme digitali	A.5.23, A.8.9, A.8.20-8.22	Configurazioni, log, responsabilita condivise, provider, segregazione, backup.	Accettata
E-14	Fornitori critici e supply chain security	A.5.19-5.22	Qualifica, classificazione criticita, DPA/SLA, clausole riservatezza, riesame.	Accettata
E-15	Secure development e change management	6.3, A.8.25-8.32	Richiesta, impatto, approvazione, test, rilascio, rollback, evidenza cambio.	Accettata
E-16	Incident management e data breach	A.5.24-5.28, A.5.34	Registrazione, classificazione, escalation, contenimento, analisi causa, chiusura.	Accettata
E-17	Backup, restore e continuita operativa	A.5.29, A.5.30, A.8.13, A.8.14	Backup, test ripristino, continuita, criticita servizi e recovery.	Accettata
E-18	Logging, monitoraggio e vulnerability management	A.8.8, A.8.15-8.17	Log accessi, monitoraggio, vulnerabilita, aggiornamenti e anomalie.	Accettata
E-19	Formazione e awareness	7.2, 7.3	Piano formazione, phishing, credenziali, privacy, incident reporting, cloud.	Accettata
E-20	Audit interno SGSI	9.2	Piano, checklist, rapporto 09/05/2026, risultanze, azioni di miglioramento.	Accettata
E-21	Riesame della Direzione	9.3	Verbale 10/05/2026, input/output, decisioni, risorse, obiettivi, rischi.	Accettata
E-22	Reclami, segnalazioni e comunicazioni	7.4, 9.1, 10.2	Registro reclami/segnalazioni, assenza reclami gravi, flussi escalation.	Accettata
E-23	Chiusura osservazioni Stage 1	10.1, 10.2	Registro azioni, stato chiusura, verifica efficacia accettata.	Accettata
E-24	Sintesi risultati Stage 2 e raccomandazione	Transfer	0 NC maggiori, 0 NC minori, nessuna condizione ostativa, raccomandazione positiva.	Accettata

6. Registro chiusura osservazioni Stage 1

Le osservazioni e aree di attenzione emerse durante lo Stage 1 sono state riesaminate in Stage 2. La verifica ha riguardato la presenza di evidenze oggettive, il trattamento delle azioni, la coerenza con risk assessment/SoA e l efficacia delle misure adottate.

ID	Osservazione Stage 1	Azione eseguita	Evidenza	Efficacia
OB-01	Rafforzare il collegamento tra contesto, parti interessate, perimetro e processi.	Aggiornati contesto, stakeholder register, scope e mappa processi.	E-02, E-03	Accettata
OB-02	Rendere piu tracciabile il collegamento risk assessment - trattamento - SoA.	Inseriti riferimenti incrociati rischio/controllo/azione/evidenza.	E-07, E-08, E-09	Accettata
OB-03	Formalizzare riesame periodico degli accessi.	Completato registro accessi e verbale di riesame autorizzazioni.	E-12	Accettata
OB-04	Rafforzare registro fornitori critici.	Aggiornata classificazione fornitori, DPA/SLA, requisiti sicurezza e monitoraggio.	E-14	Accettata
OB-05	Documentare backup, restore e continuita.	Prodotti registro backup, test restore e piano continuita.	E-17	Accettata
OB-06	Consolidare change management e rilasci.	Formalizzata procedura con richiesta, approvazione, test, rilascio e rollback.	E-15	Accettata
OB-07	Completare evidenze audit interno e riesame Direzione.	Disponibili rapporto audit interno 09/05/2026 e riesame Direzione 10/05/2026.	E-20, E-21	Accettata
OB-08	Formalizzare assenza condizioni ostative al transfer.	Predisposta dichiarazione transfer con registri NC, reclami, incidenti e modifiche.	E-01, E-24	Accettata

Conclusione sulla chiusura osservazioni

Tutte le osservazioni di Stage 1 risultano chiuse. La verifica di efficacia e stata accettata. Non permangono non conformita maggiori o minori aperte; eventuali residui sono classificabili come opportunita di miglioramento non ostative.

7. Estratto Risk Register e piano trattamento

L estratto seguente dimostra il collegamento tra asset, rischio, trattamento, controlli ISO/IEC 27001:2022 e stato. Il livello di dettaglio e proporzionato alla dimensione dell organizzazione e alla criticita dei servizi digitali.

ID	Scenario di rischio	Impatto	Controlli / trattamento	Rischio residuo	Stato
R-01	Accesso non autorizzato ad ambienti cloud, repository o piattaforme DPP.	Alto	MFA ove applicabile, least privilege, registro account, riesame accessi, revoca tempestiva, log accessi.	Medio-basso	Trattato
R-02	Errore di configurazione su smart label, QR/NFC o dati DPP con impatto su integrita delle informazioni pubblicate.	Alto	Change management, test, validazione, approvazione rilascio, controllo versioni, registrazione modifiche.	Medio	Trattato
R-03	Indisponibilita di servizi cloud o repository critici.	Alto	Backup, piano continuita, monitoraggio fornitori, SLA, test restore, procedure di escalation.	Medio	Trattato
R-04	Compromissione di credenziali di personale, collaboratori o fornitori.	Alto	Awareness phishing, policy password, MFA, access review, revoca accessi, incident reporting.	Medio-basso	Trattato
R-05	Fornitore critico non adeguatamente controllato con impatto su sicurezza, privacy o disponibilita.	Medio-alto	Classificazione fornitori, DPA/SLA, clausole sicurezza, monitoraggio periodico, riesame rischi.	Medio	Trattato
R-06	Data breach su dati personali o informazioni di progetto.	Alto	Procedure privacy, data breach, access control, classificazione, logging, incident management, DPA.	Medio	Trattato
R-07	Vulnerabilita tecnica non gestita su piattaforme, endpoint o dipendenze software.	Medio-alto	Vulnerability log, aggiornamenti, configurazioni sicure, monitoraggio tecnico, fornitori specializzati.	Medio	Trattato
R-08	Perdita di tracciabilita delle evidenze di audit, modifiche o controlli.	Medio	Repository evidenze, registro documenti, versioning, audit interno, riesame Direzione, KPI.	Basso	Trattato

8. Estratto Statement of Applicability - controlli prioritari

L estratto della SoA dimostra i controlli ritenuti ad alta rilevanza per il perimetro EZ Lab. L applicabilita e giustificata dal risk assessment e dalla natura cloud/software dei servizi erogati.

Annex A	Controllo	Applicabilita	Evidenza di attuazione	Stato
A.5.9	Inventory of information and other associated assets	Applicabile	Inventario asset informativi, piattaforme cloud, endpoint, account, repository, dati cliente/prodotto.	Implementato
A.5.12	Classification of information	Applicabile	Schema classificazione informazioni e criteri di protezione.	Implementato
A.5.15-5.18	Access control and identity management	Applicabile	Procedura accessi, MFA, least privilege, registro account, riesame autorizzazioni.	Implementato
A.5.19-5.22	Supplier relationships	Applicabile	Registro fornitori critici, valutazioni, DPA/SLA, requisiti contrattuali.	Implementato
A.5.23	Information security for use of cloud services	Applicabile	Registro piattaforme cloud, responsabilita condivise, configurazioni, monitoraggio provider.	Implementato
A.5.24-5.28	Information security incident management	Applicabile	Procedura incidenti, registro eventi, escalation, analisi cause, azioni correttive.	Implementato
A.5.29-5.30	Information security during disruption / ICT readiness	Applicabile	Piano continuita, procedure escalation, test restore, misure recupero.	Implementato
A.5.31, A.5.34	Legal, statutory, regulatory and contractual requirements / privacy	Applicabile	Registro requisiti, registro trattamenti, informative, DPA, procedura data breach.	Implementato
A.8.8	Management of technical vulnerabilities	Applicabile	Registro vulnerabilita, aggiornamenti, monitoraggio tecnico, configurazioni sicure.	Implementato
A.8.13	Information backup	Applicabile	Registro backup, frequenze, responsabilita, test restore.	Implementato
A.8.15-8.17	Logging, monitoring and clock synchronization	Applicabile	Log accessi, monitoraggio, criteri conservazione, verifiche eventi.	Implementato
A.8.25-8.32	Secure development life cycle / Change management	Applicabile	Procedura sviluppo/configurazione sicura, registro modifiche, test, rilascio controllato.	Implementato

9. Registro requisiti legali, normativi e contrattuali

Il SGSI considera i requisiti applicabili alla sicurezza delle informazioni e al trattamento dei dati nel contesto di servizi digitali, cloud, DPP, AI, blockchain e data management. L applicabilita diretta di alcune normative e riesaminata in funzione di dimensione, servizi erogati, clienti e mercati serviti.

Requisito	Ambito rilevante	Presidio SGSI	Evidenza
GDPR / D.Lgs. 196/2003	Dati personali di clienti, referenti, utenti, fornitori, collaboratori, log, account, form e supporto.	Registro trattamenti, informative, DPA, misure tecniche, data breach, minimizzazione e conservazione.	E-06, E-16
NIS 2 / recepimento nazionale	Cyber governance, risk management, supply chain, incidenti, continuita ove applicabile.	Valutazione applicabilita, risk assessment, incident management, supplier security, business continuity.	E-06, E-08, E-14, E-17
Reg. UE 2024/1781 - ESPR/DPP	Servizi Digital Product Passport, accesso dati, interoperabilita, sicurezza, privacy.	Analisi requisiti DPP, data management, tracciabilita, controlli su informazioni di prodotto.	E-02, E-08, E-13
Reg. UE 2023/2854 - Data Act	Accesso, interoperabilita, condivisione dati, data processing, smart contract.	Requisiti contrattuali, gestione dati, sicurezza cloud, controllo fornitori, portabilita.	E-06, E-13, E-14
Reg. UE 2024/2847 - Cyber Resilience Act	Software/prodotti con elementi digitali, secure by design, vulnerabilita e aggiornamenti.	Secure development, change management, vulnerability management, documentazione tecnica.	E-15, E-18
Reg. UE 2024/1689 - AI Act	Funzionalita AI ove sviluppate, integrate o utilizzate.	Classificazione uso AI, governance dati, logging, trasparenza, gestione rischi.	E-06, E-08, E-13
Contratti cliente/fornitore, NDA, DPA, SLA	Riservatezza, disponibilita, data protection, ruoli privacy, livelli servizio.	Registro contratti, DPA, SLA, supplier review, requisiti sicurezza.	E-14, E-22

10. Evidenze operative critiche: accessi, cloud, fornitori

Queste evidenze sono state considerate prioritarie per il settore IAF 33, perche incidono direttamente sulla riservatezza, integrita e disponibilita delle informazioni trattate nelle piattaforme digitali e negli ambienti cloud.

10.1 Access control

Controllo	Evidenza campionata	Valutazione auditor
Identificazione utenti	Registro account attivi, responsabile, profilo e sistema associato.	Adeguato. Account associati a ruoli aziendali e necessita operative.
Autorizzazione e least privilege	Matrice profili e autorizzazioni, autorizzazioni RSGSI/IT.	Adeguato. Profilazione coerente con mansione e perimetro.
MFA e credenziali	Evidenze configurazione MFA ove applicabile, policy credenziali.	Adeguato. Controllo proporzionato ai rischi cloud.
Riesame periodico	Verbale riesame accessi, revoche e conferme.	Osservazione Stage 1 chiusa. Efficacia accettata.

10.2 Cloud e piattaforme digitali

Area	Presidio	Evidenza
Piattaforme cloud	Registro piattaforme, responsabili, dati trattati, criticita e provider.	E-13
Configurazioni	Misure di sicurezza, accessi amministrativi, log, backup, segregazione.	E-13, E-18
Responsabilita condivise	Clausole provider, DPA/SLA, sicurezza dei servizi cloud.	E-14
Servizi DPP / DPP Studio	Configurazioni, dati prodotto/filiera, QR/NFC, smart label e supporto clienti.	E-02, E-13, E-15

10.3 Fornitori critici

Sono trattati come fornitori critici i soggetti esterni che incidono su sicurezza, disponibilita, riservatezza o conformita dei servizi: provider cloud, hosting, sviluppo, consulenza, privacy/DPO, studio paghe, studio commercialista e partner tecnologici. La classificazione e basata su accesso ai dati, criticita servizio, impatto su continuita e requisiti contrattuali.

11. Secure development, configurazione e change management

Il processo di sviluppo/configurazione sicura e gestione delle modifiche e rilevante per i servizi digitali EZ Lab, in quanto una modifica non controllata puo incidere su dati DPP, smart label, integrazioni cliente, accessi, disponibilita del servizio e conformita contrattuale.

Fase	Requisito minimo	Evidenza prevista	Esito
Richiesta modifica	Descrizione esigenza, origine, sistemi interessati, responsabile.	Ticket o registro modifica con ID univoco.	Conforme
Valutazione impatto	Impatto su sicurezza, privacy, dati cliente, continuita, integrazioni, fornitori.	Valutazione rischio/impatti collegata a risk register se necessario.	Conforme
Approvazione	Autorizzazione del responsabile processo/RSGSI/IT in base alla criticita.	Campo approvatore e data approvazione.	Conforme
Test e validazione	Verifica funzionale, sicurezza, compatibilita, rollback ove applicabile.	Evidenza test, esito e responsabile validazione.	Conforme
Rilascio controllato	Tracciabilita versione, data rilascio, comunicazione a interessati.	Registro release e note rilascio.	Conforme
Post-release	Monitoraggio anomalie, feedback cliente, eventuale correzione.	Log evento, ticket supporto, chiusura modifica.	Conforme

Evidenza di efficacia

La precedente osservazione sulla formalizzazione del change management risulta chiusa: il processo e documentato, le registrazioni di modifica sono disponibili e il collegamento con risk assessment e SoA e verificabile.

12. Incidenti, reclami, segnalazioni e comunicazioni

Il SGSI definisce un processo integrato per gestire reclami, segnalazioni, eventi di sicurezza, incidenti e potenziali data breach. Il processo prevede registrazione, classificazione, escalation, contenimento, comunicazione alle parti interessate ove necessario, analisi causa e verifica efficacia.

Elemento	Stato verificato	Evidenza	Nota
Registro eventi/incidenti	Disponibile e mantenuto	E-16	Non risultano incidenti significativi aperti o non trattati.
Procedura incident management	Disponibile	E-16	Include criteri di classificazione, escalation e chiusura.
Data breach	Presidiato	E-06, E-16	Integrato con requisiti privacy e comunicazioni ove applicabili.
Reclami e segnalazioni	Disponibile registro	E-22	Non risultano reclami gravi aperti o comunicati dall OdC.
Comunicazioni	Definite	E-22	Canali, soggetti, responsabilita e flussi di escalation definiti.
Azioni correttive	Disponibili	E-23	Collegamento con non conformita, cause e verifica efficacia.

Esito auditor:

Il processo e adeguato al contesto e non emergono condizioni ostative al transfer. L assenza di reclami gravi e incidenti significativi non trattati e coerente con la dichiarazione di transfer e con i registri campionati.

13. Backup, continuita, logging e monitoraggio

Le evidenze relative a backup, ripristino, continuita operativa, logging e monitoraggio sono fondamentali per dimostrare disponibilita, resilienza e tracciabilita dei servizi digitali. Il livello di controllo risulta proporzionato alla dimensione dell organizzazione e alla criticita dei servizi.

Area	Requisito operativo	Evidenza oggettiva	Esito
Backup	Definizione dati/ambienti inclusi, frequenza, responsabilita e conservazione.	Procedura backup, registro backup, elenco repository/sistemi critici.	Conforme
Restore test	Verifica periodica di recuperabilita e registrazione esito.	Rapporto test restore, esito, eventuali anomalie, azioni.	Conforme
Business continuity	Identificazione servizi critici, scenari di indisponibilita, ruoli e azioni di ripristino.	Piano continuita operativa, contatti escalation, dipendenze esterne.	Conforme
Logging	Registrazione accessi, eventi amministrativi, anomalie e tracciabilita operativa.	Log accessi, criteri conservazione e responsabilita consultazione.	Conforme
Monitoraggio	KPI SGSI, incidenti, fornitori, backup, accessi, formazione e azioni correttive.	Report monitoraggio SGSI e riesame Direzione.	Conforme

Osservazioni Stage 1 superate

Le aree di attenzione relative a backup/restore, continuita e logging risultano chiuse con efficacia accettata. Il sistema deve mantenere evidenze periodiche e aggiornate nel ciclo di sorveglianza.

14. Valutazione prestazioni, audit interno e riesame Direzione

Le attivita di monitoraggio, audit interno e riesame della Direzione costituiscono prova della capacita del SGSI di misurare la propria efficacia, correggere deviazioni e migliorare in modo continuo.

Elemento	Data / frequenza	Input principali	Output / evidenza	Esito
Monitoraggio SGSI	Continuo / periodico	KPI, incidenti, accessi, fornitori, backup, formazione, azioni.	Report monitoraggio e registro obiettivi.	Conforme
Audit interno	09/05/2026	ISO/IEC 27001:2022, SoA, processi, evidenze operative, Stage 1.	Rapporto audit interno, checklist, rilievi, azioni.	Conforme
Riesame Direzione	10/05/2026	Audit interno, rischi, SoA, obiettivi, incidenti, fornitori, risorse.	Verbale riesame, decisioni, azioni e responsabilita.	Conforme
Miglioramento	Continuo	NC, osservazioni, reclami, incidenti, KPI, audit e riesame.	Registro azioni correttive/miglioramento.	Conforme

Note di efficacia

Gli input e output di audit interno e riesame Direzione sono coerenti con ISO/IEC 27001:2022. Le azioni deliberate sono collegate a osservazioni Stage 1, obiettivi SGSI, risk treatment plan e miglioramento continuo. Non risultano non conformita maggiori o minori aperte.

15. Matrice valutazione processi - Stage 2

Processo	Clausole	Risultato	Evidenze oggettive	Nota auditor
Contesto e scope	4.1-4.4	C	E-02, E-03	Coerente con IAF 33, servizi digitali e confini.
Leadership e responsabilita	5.1-5.3	C	E-04, E-05	Direzione/RSGSI coinvolta, ASGSI e funzioni definite.
Rischi e SoA	6.1	C	E-07, E-08, E-09	Tracciabilita rischio-controllo-evidenza adeguata.
Obiettivi e KPI	6.2, 9.1	C	E-10	Obiettivi misurabili e monitorati.
Supporto e documenti	7.1-7.5	C	E-19, E-22	Competenze, comunicazioni e documenti controllati.
Accessi e cloud	A.5.15-5.18, A.5.23	C	E-12, E-13	Controlli adeguati; osservazioni Stage 1 chiuse.
Fornitori	A.5.19-5.22	C	E-14	Registro e valutazioni fornitori critici aggiornati.
Change e sviluppo sicuro	6.3, A.8.25-8.32	C	E-15	Processo di modifica tracciabile e validato.
Incidenti e reclami	A.5.24-5.28, 10.2	C	E-16, E-22	Nessun incidente/reclamo significativo aperto.
Backup e continuita	A.5.29-5.30, A.8.13-8.14	C	E-17	Test restore e piano continuita disponibili.
Audit e riesame	9.2, 9.3	C	E-20, E-21	Audit interno e riesame documentati.
Transfer readiness	Transfer	C	E-01, E-24	Nessuna condizione ostativa rilevata.

16. Risultati audit ed evidenze oggettive utilizzate

Risultati dell audit	Evidenze oggettive utilizzate
Contesto dell organizzazione	Analisi contesto, registro parti interessate, scope, mappa processi, registro requisiti legali, risk assessment, SoA.
Punti di forza	Leadership Direzione/RSGSI, ruoli chiari, integrazione risk/SoA, sicurezza cloud, fornitori critici, controllo accessi, compliance DPP.
Debolezze	Nessuna NC maggiore/minore. Opportunita: mantenere evidenze periodiche di access review, log review, backup restore e supplier review.
Conformita legislativa	Registro requisiti legali, GDPR/privacy, DPA, contratti, Data Act, AI Act, CRA, ESPR, monitoraggio normativo.
Leadership e partecipazione	Organigramma, RACI, politica, verbali SGSI, interviste Direzione/RSGSI/ASGSI, formazione e awareness.
Pianificazione e rischi	Metodologia rischio, risk register, treatment plan, SoA, obiettivi e KPI.
Supporto	Matrice competenze, piano formazione, controllo documentale, comunicazioni SGSI, repository evidenze.
Attivita operative	Access control, cloud security, change management, supplier review, incident management, backup, BCP, logging.
Valutazione prestazioni	KPI SGSI, audit interno, riesame Direzione, report monitoraggio, registro azioni.
Miglioramento	Chiusura osservazioni Stage 1, registro miglioramento, azioni correttive, efficacia accettata.
Informazioni specifiche dello schema	Check-list transfer, assenza condizioni ostative, nessuna NC maggiore/minore aperta, raccomandazione positiva.

17. Check-list transfer e raccomandazione

Punto critico transfer	Verifica	Esito	Nota
Certificato precedente e continuita SGSI	Presenza del sistema, campo invariato o modifiche valutate, processi mantenuti.	OK	Continuita documentale e operativa accertata.
Non conformita maggiori aperte	Verifica registro NC e dichiarazione organizzazione.	Nessuna	Nessuna NC maggiore aperta o non trattata.
Sospensioni/revoche	Verifica dichiarazione condizioni ostative.	Nessuna	Nessun elemento ostativo dichiarato.
Reclami gravi non gestiti	Registro reclami/segnalazioni e comunicazioni OdC.	Nessuno	Nessun reclamo grave aperto.
Incidenti significativi non trattati	Registro incidenti e data breach.	Nessuno	Nessun incidente significativo aperto o non gestito.
Modifiche rilevanti non valutate	Registro modifiche, risk assessment e riesame Direzione.	Nessuna	Le modifiche rilevanti sono considerate nel SGSI.
Osservazioni Stage 1	Registro azioni e verifica efficacia.	Chiuse	Efficacia accettata.
Raccomandazione	Valutazione complessiva di conformita ed efficacia.	Positiva	SGSI idoneo al trasferimento della certificazione.

Raccomandazione finale

Sulla base delle evidenze predisposte e delle risultanze di Stage 2 - Transfer Audit, il SGSI di EZ Lab risulta conforme, implementato, mantenuto ed efficace. Non emergono condizioni ostative al trasferimento della certificazione ISO/IEC 27001:2022. Raccomandazione: transfer positivo.

18. Validazione e firme

La presente sezione deve essere completata prima dell inserimento del dossier nel fascicolo ufficiale di certificazione. Le firme attestano la presa visione, la validazione delle evidenze e la disponibilita delle registrazioni originali a supporto.

Ruolo	Nome	Firma	Data
Direzione / RSGSI	Massimo Morbiato		
ASGSI	Lisa Zinato		
ASGSI / Project Management	Tommaso Faccin		
Lead Auditor	Dr. Prof. Giuseppe Izzo		

Dichiarazione di uso controllato

Il presente dossier e predisposto come fascicolo di evidenze a supporto del rapporto Stage 2 - Transfer Audit ISO/IEC 27001:2022. L organizzazione deve conservare gli originali delle registrazioni richiamate e renderli disponibili in sede di audit, sorveglianza o riesame. Ogni modifica successiva deve essere tracciata con numero di revisione, data, responsabile e motivazione.