RAPPORTO EVIDENZE AUDIT STAGE 2

Sistema di Gestione per la Sicurezza delle Informazioni

ISO/IEC 27001:2022

CLOUD3 S.R.L.

Piazza Camillo Golgi 28 C, 16011 Arenzano (GE), Italia

Dato	Valore
Organizzazione	CLOUD3 S.R.L.
Sede oggetto di verifica	Piazza Camillo Golgi 28 C, 16011 Arenzano (GE), Italia
Tipo audit	Stage 2 - First certification
Standard di riferimento	ISO/IEC 27001:2022
Campo di applicazione	Attivita' di programmazione informatica
IAF / NACE	IAF 33 - NACE 62.1
Referente audit	Simone Cola - Amministratore Unico / Referente audit
Email	amministrazione@cloud3.srl
Numero addetti	4
Fonte documentale primaria	Audit Report - Stage 2, Form AR_01.2, Rev. 004 del 29/08/2025

Documento redatto come rapporto di consolidamento delle evidenze oggettive a supporto dell'audit Stage 2 ISO/IEC 27001:2022. Le evidenze sono organizzate secondo clausole normative, controlli Annex A, processi verificati, risultati, elementi di supporto e azioni di presidio raccomandate.

Indice del documento

1. Premessa e finalità del rapporto

Il presente rapporto ha lo scopo di raccogliere, ordinare e rendere immediatamente utilizzabili le evidenze oggettive emerse dall'audit Stage 2 ISO/IEC 27001:2022 di CLOUD3 S.R.L., con riferimento al Sistema di Gestione per la Sicurezza delle Informazioni applicato alle attività di programmazione informatica.

Il documento non sostituisce il rapporto ufficiale di audit, ma ne costituisce una sintesi tecnica di alto livello, finalizzata a supportare la gestione del fascicolo di certificazione, la preparazione della decisione certificativa, il monitoraggio delle azioni post-audit e la pianificazione della successiva sorveglianza.

L'impostazione segue il criterio di audit evidence richiesto dagli schemi di certificazione: ogni conclusione deve essere riconducibile a documenti, registrazioni, interviste, osservazioni operative, campionamenti di processo, evidenze di efficacia e collegamento con i requisiti della norma applicabile.

Nota tecnica di coerenza del fascicolo

Nel rapporto Stage 2 allegato sono presenti sezioni intermedie che riportano rilievi, osservazioni e richieste di rafforzamento documentale, mentre la sezione conclusiva riporta raccomandazione al proceeding to certification. Il presente rapporto consolida tali elementi come evidenze e azioni di presidio da monitorare, senza alterare il contenuto del report sorgente e senza introdurre conclusioni non supportate dal documento di audit.

2. Profilo dell'organizzazione e campo di applicazione

CLOUD3 S.R.L. opera nel settore della programmazione informatica, con focus sullo sviluppo e manutenzione di software personalizzati. Il campo di applicazione del SGSI comprende l'intera attività svolta presso la sede operativa di Piazza Camillo Golgi 28 C, 16011 Arenzano (GE), senza esclusioni dichiarate. I processi principali includono analisi dei requisiti, progettazione software, sviluppo, testing, consegna del prodotto finito, supporto tecnico e assistenza post-vendita.

La dimensione aziendale, pari a 4 addetti, richiede un SGSI proporzionato, snello e tracciabile: la documentazione deve essere adeguata alla complessità reale, ma le registrazioni essenziali devono permettere la dimostrazione della conformità e dell'efficacia del sistema.

Elemento	Descrizione/evidenza
Processi core	Analisi requisiti; progettazione; sviluppo software; testing; consegna; manutenzione; supporto post-vendita.
Asset informativi principali	Codice sorgente, repository, ambienti di sviluppo, documentazione tecnica, credenziali, dati cliente, ticket, backup, dispositivi endpoint e strumenti cloud utilizzati a supporto dei processi.
Confini fisici	Sede operativa unica di Arenzano (GE). Non risultano sedi temporanee o ulteriori siti operativi nel report.
Confini organizzativi	Intero organico coinvolto nelle attività SGSI: 4 dipendenti/addetti.
Confini logici	Processi e strumenti ICT usati per sviluppo software, supporto tecnico, gestione documentale, accessi e protezione delle informazioni.

3. Criteri, metodologia e fonti di evidenza

L'audit Stage 2 è stato condotto con riferimento alla ISO/IEC 27001:2022, alle clausole 4-10, ai controlli pertinenti dell'Annex A e ai requisiti cogenti applicabili alla sicurezza delle informazioni, con particolare attenzione al GDPR e alla normativa italiana ed europea in materia di protezione dei dati personali.

Le fonti di evidenza considerate dal rapporto di audit comprendono riesame documentale, interviste, campionamento dei processi, evidenze Stage 1/Stage 2, allegati disponibili e osservazione diretta dell'audit. L'approccio è proporzionato alla dimensione aziendale e al rischio informativo connesso allo sviluppo software e alla gestione di informazioni cliente.

Fonte/metodo	Applicazione nel rapporto evidenze
Riesame documentale	Politica SGSI, campo di applicazione, analisi contesto, registro parti interessate, risk assessment, piano trattamento rischi, SoA, procedure operative, registrazioni e piani di miglioramento.
Interviste	Confronto con referente aziendale e personale coinvolto nei processi di sviluppo, supporto, gestione documentale, sicurezza operativa e controllo accessi.
Campionamento processi	Verifica dei processi di analisi requisiti, progettazione, sviluppo, testing, consegna software, assistenza post-vendita, gestione documentale e monitoraggio SGSI.
Osservazione audit	Verifica della sede operativa, modalità di gestione delle attività,

Fonte/metodo	Applicazione nel rapporto evidenze
	comunicazioni, consapevolezza e applicazione dei controlli di sicurezza pertinenti.
Criteri di valutazione	Conformità, efficacia, tracciabilità, proporzionalità, evidenza oggettiva, coerenza tra rischio, controllo, responsabilità e registrazione.

4. Sintesi direzionale dell'esito Stage 2

- Il rapporto Stage 2 conferma che il SGSI di CLOUD3 S.R.L. copre integralmente le attività di programmazione informatica e i processi correlati, senza esclusioni dichiarate.
- Il sistema risulta impostato su una struttura documentale coerente con i requisiti ISO/IEC 27001:2022 e con il perimetro ICT/software dell'organizzazione.
- Sono presenti aree di rafforzamento relative a tracciabilità delle evidenze, completezza delle registrazioni, gestione dei rischi, SoA, controlli operativi, asset, accessi, fornitori, incidenti, backup e riesame della direzione.
- Il rapporto conclude con raccomandazione al proceeding to certification, pur richiedendo il mantenimento di presidi documentali e azioni di follow-up sulle aree evidenziate.

Voce	Sintesi
Raccomandazione finale	Recommended for proceeding to certification
Campo coperto	Attività di programmazione informatica presso sede unica di Arenzano
Modalità audit	On-site
Lavoro notturno / stagionalità	Non applicabili / non rilevati nel report
Punti di forza	SGSI coerente con processi software, perimetro definito, controlli principali impostati, evidenza di approccio al rischio e conformità GDPR.
Aree da presidiare	Formalizzazione contesto, requisiti legali, risk assessment, trattamento rischi, SoA, gestione asset, accessi, incidenti, backup, audit interno e riesame direzione.

5. Matrice delle evidenze per clausole ISO/IEC 27001

La seguente matrice consolida i requisiti verificati, l'esito indicativo e le evidenze da mantenere nel fascicolo audit. La classificazione C/O è usata quando il requisito risulta conforme ma accompagnato da raccomandazioni di rafforzamento o monitoraggio.

Clausola	Processo/requisito	Esito	Evidenza e presidio
4.1 - 4.2	Contesto e parti interessate	C/O	Evidenza positiva: Il report indica che il contesto e le parti interessate sono stati considerati in relazione allo scopo SGSI e ai processi di programmazione informatica. Area da presidiare: Rafforzare la formalizzazione delle analisi e il collegamento tra requisiti delle parti interessate, rischi, asset e controlli. Follow-up raccomandato: Aggiornare registro parti interessate, matrice requisiti SGSI e riesame periodico del contesto.
4.3 - 4.4	Campo di applicazione e processi SGSI	C	Evidenza positiva: Lo scopo copre l'intera attività di programmazione informatica, senza esclusioni, presso sede unica. Area da presidiare: Rendere maggiormente espliciti confini fisici, logici, cloud, fornitori e processi esternalizzati. Follow-up raccomandato: Mantenere il documento di scopo aggiornato e collegato a SoA, risk assessment e asset inventory.
5.1 - 5.3	Leadership, politica, ruoli e responsabilità	C/O	Evidenza positiva: Il report rileva impegno della direzione, politica di sicurezza e ruoli formalizzati. Area da presidiare: Rafforzare la tracciabilità della comunicazione della politica e delle responsabilità SGSI. Follow-up raccomandato: Conservare verbali, comunicazioni,

Clausola	Processo/requisito	Esito	Evidenza e presidio
			organigramma, nomine e job description con riferimento a sicurezza informazioni.
6.1.1	Azioni per rischi e opportunità	C	Evidenza positiva: Le azioni sono impostate a partire da contesto e stakeholder. Area da presidiare: Assicurare collegamento formale tra opportunità, azioni, responsabili, tempi e indicatori. Follow-up raccomandato: Integrare nel piano miglioramento e nel riesame direzione.
6.1.2	Risk assessment	C/O	Evidenza positiva: Sono presenti criteri e risultati di valutazione del rischio. Area da presidiare: Alcune evidenze richiedono rafforzamento su criteri di accettazione, aggiornamento e correlazione agli asset. Follow-up raccomandato: Aggiornare metodologia, registro rischi e collegamenti asset-minaccia-vulnerabilità-controllo.
6.1.3	Risk treatment e SoA	C/O	Evidenza positiva: Il trattamento rischi e la SoA risultano disponibili e coerenti con i controlli applicabili. Area da presidiare: Migliorare correlazione tra rischi, controlli, responsabili, stato di attuazione e giustificazioni inclusione/esclusione. Follow-up raccomandato: Aggiornare piano trattamento rischi e SoA con evidenza di approvazione residui.
6.2	Obiettivi sicurezza informazioni	C/O	Evidenza positiva: Gli obiettivi sono definiti e integrati con processi operativi. Area da presidiare: Rafforzare misurabilità e monitoraggio periodico degli obiettivi. Follow-up raccomandato: Collegare obiettivi a KPI, dashboard e riesame direzione.
6.3	Gestione cambiamenti	C	Evidenza positiva: I cambiamenti risultano pianificati e autorizzati. Area da presidiare: Mantenere valutazione preventiva degli impatti su rischi, controlli e continuità. Follow-up raccomandato: Formalizzare change request, approvazioni, test e rollback.
7.1 - 7.4	Risorse, competenza, awareness e comunicazione	C/O	Evidenza positiva: Risorse e competenze sono proporzionate alla dimensione aziendale. Area da presidiare: Rafforzare evidenza di efficacia formazione e canali di comunicazione incidenti/segnalazioni. Follow-up raccomandato: Mantenere piano formazione, test awareness, registri presenze e comunicazioni SGSI.
7.5	Informazioni documentate	C	Evidenza positiva: La documentazione SGSI è disponibile, strutturata e controllata. Area da presidiare: Assicurare controllo versioni, protezione da modifiche non autorizzate e rintracciabilità registrazioni. Follow-up raccomandato: Mantenere elenco documenti, revisioni, approvazioni e criteri di conservazione.
8.1 - 8.3	Pianificazione operativa e trattamento rischi	C/O	Evidenza positiva: Le attività operative risultano pianificate in coerenza con i trattamenti del rischio. Area da presidiare: Per alcuni processi è opportuno rafforzare evidenze di pianificazione, responsabilità e registrazioni. Follow-up raccomandato:

Clausola	Processo/requisito	Esito	Evidenza e presidio
			Conservare log, checklist, ticket, approvazioni, esiti test e registrazioni operative.
9.1 - 9.2	Monitoraggio, misurazione e audit interno	C/O	Evidenza positiva: Sono richiamate attività di monitoraggio e audit interno. Area da presidiare: Rafforzare KPI, risultati di audit, campionamenti e verifica efficacia azioni. Follow-up raccomandato: Mantenere dashboard, audit program, rapporti audit, check-list e CAPA.
9.3	Riesame della direzione	O	Evidenza positiva: Il riesame è trattato come requisito da presidiare. Area da presidiare: Il report evidenzia la necessità di rafforzare o documentare compiutamente il riesame direzione. Follow-up raccomandato: Predisporre verbale completo con input/output ISO 27001, decisioni, azioni, responsabili e follow-up.
10.1 - 10.2	Miglioramento e azioni correttive	C/O	Evidenza positiva: Il processo di miglioramento risulta impostato e collegato alle evidenze emerse. Area da presidiare: Garantire analisi causa, azioni e verifica efficacia per ogni rilievo. Follow-up raccomandato: Tenere registro NC/azioni correttive e piano miglioramento SGSI.

6. Evidenze sui controlli Annex A maggiormente significativi

Per un'organizzazione che sviluppa e mantiene software personalizzato, i controlli Annex A più rilevanti riguardano asset informativi, accessi, fornitori ICT, incidenti, backup, continuità, sviluppo sicuro e gestione delle modifiche. Il fascicolo audit deve dimostrare non solo l'esistenza dei controlli, ma la loro applicazione effettiva e la tracciabilità delle registrazioni.

Controllo	Area	Evidenze attese/verificate	Presidio raccomandato
A.5.9	Gestione asset	Inventario asset informativi, identificazione proprietario, classificazione, aggiornamento periodico, collegamento al risk assessment.	Aggiornare asset inventory e responsabilità; assicurare tracciabilità di asset, proprietari, classificazioni e stato di revisione.
A.5.15 - A.5.18 / A.8.2 / A.8.5	Controllo accessi	Matrice accessi, autorizzazioni, revoche, privilegi amministrativi, autenticazione, revisione periodica.	Rafforzare evidenze di revisione periodica e processo joiner-mover-leaver.
A.5.19 - A.5.23	Sicurezza fornitori	Valutazione fornitori ICT, requisiti contrattuali di sicurezza, monitoraggio livelli di servizio, gestione cloud/servizi terzi.	Integrare criteri security nei rapporti contrattuali e nella valutazione periodica fornitori.
A.5.24 - A.5.28	Gestione incidenti	Procedura incidenti, registro eventi, classificazione, escalation, risposta, lesson learned.	Migliorare completezza di classificazione, registrazione, escalation e apprendimento post-incidente.
A.5.30 / A.8.13	Backup e continuità	Politica backup, log backup, restore test, responsabilità, continuità operativa per processi critici.	Rafforzare evidenze periodiche di test di ripristino e relativi esiti.
A.8.25 - A.8.32	Sviluppo sicuro e modifiche	Policy di sviluppo sicuro, change management, separazione ambienti, test, code review, gestione vulnerabilità e rilascio.	Mantenere evidenze complete su change request, review, test, approvazione rilascio e controllo modifiche.

7. Analisi dei rilievi, osservazioni e azioni di presidio

Il rapporto sorgente riporta più aree di miglioramento e rafforzamento documentale. Ai fini della gestione del fascicolo, tali aree devono essere trasformate in un piano di presidio con responsabile, scadenza, evidenza di chiusura e verifica dell'efficacia.

Clausola	Area	Tipo	Azione richiesta/raccomandata	Evidenza di chiusura
4.3	Chiarezza perimetro SGSI	Osservazione	Integrare confini fisici, logici, cloud e fornitori esterni nel documento di scopo.	Scopo SGSI aggiornato; mappa processi e sistemi; approvazione direzione.

Clausola	Area	Tipo	Azione richiesta/raccomandata	Evidenza di chiusura
5.2	Comunicazione politica sicurezza	Osservazione	Rafforzare tracciabilità di comunicazione, comprensione e disponibilità della politica.	Registro comunicazioni; verbale riunione; awareness test.
6.1.2	Risk assessment	Rilievo di rafforzamento	Rendere più espliciti criteri di accettazione, aggiornamento e collegamento agli asset.	Metodologia risk assessment aggiornata; risk register revisionato.
6.1.3 / SoA	Piano trattamento e SoA	Rilievo di rafforzamento	Completare correlazione rischi-controlli-responsabili-stato attuazione e giustificazioni SoA.	Risk treatment plan; SoA aggiornata; approvazione rischi residui.
7.2 - 7.3	Competenze e awareness	Osservazione	Misurare efficacia della formazione e consapevolezza del personale.	Piano formazione; test awareness; valutazione efficacia.
8.1	Controlli operativi	Rilievo di rafforzamento	Rendere complete evidenze di pianificazione, responsabilità e registrazioni operative.	Checklist operative; ticket; log; approvazioni; evidenze di rilascio.
A.5.9	Inventario asset	Rilievo di rafforzamento	Integrare proprietario, classificazione, aggiornamento e collegamento al rischio.	Inventario asset aggiornato; owner; classificazione; data revisione.
A.5.15-A.5.18 / A.8.5	Accessi	Rilievo di rafforzamento	Rafforzare revisioni periodiche, autorizzazioni e revoche.	Matrice accessi; log autorizzazioni; verbale review accessi.
A.5.19-A.5.22	Fornitori ICT	Osservazione	Integrare requisiti sicurezza nei criteri di selezione, contratti e monitoraggio fornitori.	Schede fornitore; clausole security; valutazioni periodiche.
A.5.24-A.5.26	Incident management	Rilievo di rafforzamento	Completare classificazione, escalation, registrazione e lesson learned.	Registro incidenti/eventi; procedura escalation; report post-evento.
A.8.13	Backup e restore	Osservazione	Pianificare evidenze periodiche di restore test.	Log backup; verbale restore test; esito e azioni.

8. Evidenze operative per processi ICT/software

Le evidenze operative devono dimostrare che la sicurezza delle informazioni è integrata nel ciclo di vita del software e nelle attività di supporto. Per CLOUD3 S.R.L., il campionamento efficace deve coprire almeno una commessa o progetto software, un ticket di supporto, un cambio rilasciato, una verifica accessi, un backup e un'evidenza di awareness.

Processo	Aspetti SGSI da dimostrare	Evidenze oggettive
Analisi requisiti	Raccolta requisiti cliente, requisiti sicurezza, requisiti privacy, responsabilità e accettazione.	Scheda requisiti; email cliente; verbale; ticket; analisi rischi.
Progettazione software	Definizione architettura, segregazione ambienti, gestione dati, criteri sicurezza by design.	Documento tecnico; diagrammi; decisioni progettuali; review.
Sviluppo	Controllo repository, gestione branch, code review, protezione credenziali e segreti.	Log repository; merge request; evidenza review; policy sviluppo sicuro.
Testing	Test funzionali e, ove applicabile, test sicurezza, verifica difetti, tracciabilità correzioni.	Piano test; esiti test; bug list; approvazioni.
Rilascio/consegna	Autorizzazione rilascio, checklist, comunicazione cliente, controllo versione.	Release note; checklist rilascio; approvazione; ticket chiuso.
Supporto post-vendita	Gestione segnalazioni, tempi risposta, escalation e protezione dati cliente.	Ticket; SLA; log assistenza; report intervento.
Backup e continuità	Backup di repository/documentazione critica e test periodici di ripristino.	Log backup; restore test; evidenza esito.
Gestione accessi	Autorizzazioni, privilegi, revoche, MFA ove applicabile, revisione periodica.	Matrice accessi; approval; log revoca; verbale review.

9. Conformità legislativa e GDPR

Il rapporto Stage 2 richiama espressamente la necessità di verificare e documentare i requisiti legali e regolamentari applicabili, con particolare riferimento al GDPR e alle normative italiane ed europee sulla

protezione dei dati personali. Per un'organizzazione che sviluppa software personalizzato, il presidio privacy e sicurezza deve essere dimostrato attraverso un registro dei requisiti applicabili, ruoli privacy, istruzioni operative, misure tecniche e organizzative, gestione fornitori, eventuali nomine a responsabile del trattamento e controllo degli accessi ai dati cliente.

Ambito legale/compliance	Evidenze da mantenere	Presidio
GDPR / protezione dati	Registro trattamenti ove applicabile, ruoli privacy, informative, DPA, misure tecniche e organizzative, data breach process.	Aggiornare e collegare al risk assessment SGSI.
Sicurezza delle informazioni	Policy, procedure, asset, accessi, incidenti, backup, continuità, sviluppo sicuro.	Mantenere evidenze operative e test di efficacia.
Contratti cliente/fornitore	Clausole di riservatezza, sicurezza, responsabilità, SLA, gestione dati e subfornitori.	Integrare requisiti security nei contratti e nella valutazione fornitori.
Conservazione documentale	Controllo versioni, retention, protezione documenti, accessi riservati.	Definire tempi, responsabilità e supporti.

10. Conclusione di audit e raccomandazione

Sulla base del rapporto Stage 2, il SGSI di CLOUD3 S.R.L. risulta impostato e implementato in modo coerente con il campo di applicazione certificativo e con la dimensione dell'organizzazione. Il rapporto contiene raccomandazione al proceeding to certification e conferma l'adeguatezza del perimetro verificato, dei processi principali e dell'approccio generale al rischio.

Ai fini della piena robustezza del fascicolo audit, si raccomanda di consolidare le evidenze indicate nel presente documento entro il primo ciclo di sorveglianza, attribuendo responsabilità, scadenze, registrazioni di chiusura e verifica di efficacia. Particolare priorità deve essere data a: risk assessment, risk treatment plan, SoA, inventario asset, access review, incident management, restore test, audit interno e riesame direzione.

Valutazione finale del rapporto evidenze

Il rapporto evidenze supporta la raccomandazione al proceeding to certification, subordinatamente al mantenimento del piano di presidio documentale e alla gestione ordinata delle aree di rafforzamento evidenziate. Non sono introdotte nuove non conformità rispetto al documento sorgente; le aree indicate sono classificate come elementi di supporto alla sorveglianza e al miglioramento continuo.

11. Allegato - Piano evidenze per sorveglianza

Tempistica	Azione	Responsabile	Evidenza attesa
Entro 30 giorni	Aggiornamento scopo SGSI e confini fisici/logici/cloud/fornitori	Direzione / Responsabile SGSI	Scopo SGSI aggiornato e approvato
Entro 30 giorni	Aggiornamento risk assessment e criteri di accettazione	Responsabile SGSI	Risk assessment revisionato
Entro 45 giorni	Aggiornamento piano trattamento rischi e SoA	Responsabile SGSI / Direzione	RTP e SoA con stato controlli e approvazione rischio residuo
Entro 45 giorni	Aggiornamento inventario asset e proprietà	Responsabile IT / SGSI	Inventario asset con owner, classificazione e data review
Entro 60 giorni	Revisione periodica accessi e gestione privilegi	Responsabile IT	Verbale review accessi e log revoche/autorizzazioni
Entro 60 giorni	Test restore backup e registrazione esito	Responsabile IT	Verbale restore test e azioni eventuali
Entro 60 giorni	Riesame direzione SGSI completo	Direzione	Verbale riesame con input/output ISO 27001 e piano azioni
Continuativo	Awareness e formazione sicurezza informazioni	Responsabile SGSI	Registro formazione, test efficacia, comunicazioni periodiche

Fine del rapporto evidenze.