REPORT DELLE EVIDENZE

Audit Stage 2 - ISO 9001 e ISO/IEC 27001

LCC INNOVA SRL - Modica (RG)

Elemento	Dettaglio
Organizzazione	LCC INNOVA SRL
Sede verificata	Via Alcide De Gasperi 4, 97015 Modica (RG), Sicilia
Campo di applicazione	Commercio all'ingrosso di computer, unita periferiche e software; approvvigionamento, gestione magazzino, vendita e distribuzione di prodotti informatici a rivenditori e clienti professionali.
Standard	ISO 9001 - Sistema di gestione per la qualita; ISO/IEC 27001 - Sistema di gestione della sicurezza delle informazioni.
Modalita audit	Remote; sede unica; n. 3 dipendenti; n. 4 utenti/PC indicati nel profilo ISO 27001.
Fonte	Stage2_AuditReport_LCC_INNOVA_SRL_ID82.pdf - Audit Report Stage 2, form AR_01.2 rev. 004, 29 August 2025.
Documento prodotto	Sintesi senior delle evidenze, dei rilievi e delle priorita di follow-up, in formato A4 PDF.

Perimetro del documento

Il presente report non sostituisce l'audit report originale. Ne riorganizza le evidenze in chiave executive e senior, focalizzandosi su maturita del sistema, rischi residui, coerenza documentale e priorita di trattamento.

Data di elaborazione: 22/05/2026 - Documento confidenziale per uso interno

1. Executive summary

Valutazione sintetica delle evidenze raccolte nello Stage 2 e del livello di presidio dei sistemi di gestione.

0	14	10	SI
Major finali nel riepilogo conclusivo	Non conformita minori consolidate	Osservazioni consolidate	Raccomandazione a procedere alla certificazione

Dalla lettura dell'audit Stage 2 emerge un sistema di gestione complessivamente coerente con lo scopo certificativo e con la struttura aziendale di LCC INNOVA SRL. Il perimetro operativo e concentrato su una sede unica e su processi di commercio all'ingrosso ICT: approvvigionamento, gestione magazzino, vendita e distribuzione. L'audit team conclude raccomandando il prosieguo verso la certificazione, considerando raggiunti gli obiettivi di audit, adeguato lo scopo e complessivamente efficace il sistema di gestione.

Il profilo delle evidenze non evidenzia un fallimento sistemico del modello di gestione; evidenzia invece una necessita di rafforzamento della tracciabilita documentale, della dimostrazione dell'efficacia e della correlazione tra rischi, controlli, responsabilita e registrazioni. Le aree piu sensibili sono l'asset management, il controllo accessi, la gestione incidenti, la risk methodology, il piano di trattamento dei rischi, la SoA e la robustezza del ciclo di audit interno/azioni correttive.

Punto di coerenza documentale	Il riepilogo finale del report indica 0 Major, 14 Minor e 10 Observation. Tuttavia, una sezione intermedia del documento qualifica il controllo ISO 27001 A.8.25-A.8.32 come Major. Questa incoerenza formale deve essere trattata come punto di quality control del fascicolo: prima dell'archiviazione definitiva occorre allineare il prospetto dei findings, il riepilogo NC/Observation e la conclusione di raccomandazione alla certificazione.

Giudizio senior: procedibilita positiva, con follow-up strutturato. L'organizzazione puo essere considerata certificabile a condizione che le NC minori siano prese in carico con analisi causa, azioni, responsabilita, tempi e verifica di efficacia; le osservazioni devono alimentare il piano di miglioramento e il riesame della direzione.

2. Base dati e metodo di lettura

Aspetto	Sintesi
Documento esaminato	Audit Report Stage 2 - LCC INNOVA SRL - ID82, form AR_01.2 rev. 004.
Tecniche di raccolta evidenze	Riesame documentale, interviste, campionamento processi, evidenze Stage 1/Stage 2, allegati disponibili e osservazione audit.
Criteri	Requisiti ISO 9001, ISO/IEC 27001 e controlli Annex A pertinenti al perimetro ICT e commerciale.
Approccio	Analisi per processo, valutazione della tracciabilita, coerenza tra contesto/rischi/controlli/registrazioni e classificazione delle evidenze.
Limitazione	Audit condotto per campionamento; l'assenza di rilievi in un'area non garantisce assenza assoluta di anomalie in aree non campionate.

Le evidenze sono state riclassificate in quattro livelli: conformita documentata, presidio sostanziale con opportunita di rafforzamento, non conformita minore per carenza di evidenza/efficacia, e criticita di coerenza del fascicolo. La priorita non dipende solo dal numero di rilievi, ma dall'impatto sul controllo operativo, sulla capacita di dimostrare efficacia e sulla tenuta del sistema in sorveglianza.

3. Profilo dell'organizzazione e campo di applicazione

Elementi essenziali di contesto emersi dal report di audit.

Dimensione	Evidenza
Identita	Societa con sede a Modica (RG), operante nel commercio all'ingrosso di computer, unita periferiche e software.
Processi principali	Approvvigionamento, gestione magazzino, vendita all'ingrosso e distribuzione di prodotti informatici.
Clienti/mercato	Rivenditori e clienti professionali del settore ICT.
Confini	Sede unica; nessun sito aggiuntivo o attivita esterna esclusa dallo scopo dichiarato.
SGQ	Sistema ISO 9001 focalizzato su qualita, soddisfazione cliente, presidio dei processi e miglioramento continuo.
SGSI	Sistema ISO 27001 applicato ai processi e agli asset informativi connessi alle attivita ICT e commerciali.
Complessita ICT	4 utenti, 4 workstation/PC/laptop, 1 rete, 2 addetti sviluppo/manutenzione indicati nel profilo ISO 27001.

Il campo di applicazione risulta coerente con l'operativita effettiva e con la dimensione organizzativa. La concentrazione su un'unica sede riduce la complessita logistica, ma aumenta l'importanza della tracciabilita centralizzata delle responsabilita, delle registrazioni e dei controlli documentali. In un'organizzazione snella, la sostenibilita del sistema dipende dalla capacita di produrre evidenze semplici, aggiornate, attribuite e verificabili.

4. Valutazione complessiva delle evidenze

Area	Livello evidenziale	Lettura senior
Perimetro e scopo	Buono	Campo coerente con attivita, sede unica e processi principali. Da rafforzare la descrizione di confini fisici/logici, processi affidati all'esterno e componenti cloud.
Governance e leadership	Adeguato con rafforzamenti	Ruoli e responsabilita risultano definiti, ma le interfacce operative e la dimostrazione di efficacia devono essere piu tracciabili.
Risk management	Medio	Rischi e opportunita sono presenti; occorre maggiore correlazione tra criteri, priorita, azioni, controlli, responsabilita e verifica di efficacia.
Documented information	Adeguato	Documenti chiave disponibili; permane l'esigenza di controllo strutturato di aggiornamento, distribuzione, approvazione e conservazione.
Operativita SGQ	Adeguato	Processi commerciali e di erogazione coerenti con lo scopo; fornitori e azioni correttive richiedono evidenze piu robuste.
Operativita SGSI	Medio/critico	Controlli attuati, ma con gap evidenziali su asset, accessi, incidenti, SoA, risk treatment e controlli operativi.
Miglioramento	Adeguato con follow-up	Audit interni, riesame e reclami sono presenti; servono migliore profondita di causa radice e verifica efficacia.

Il pattern dei rilievi evidenzia un sistema in esercizio, non un sistema solo documentale. Tuttavia, la capacita di sostenere la certificazione nel tempo dipendera dalla normalizzazione del fascicolo evidenze: per ciascun requisito rilevante devono essere disponibili registrazione, owner, data, criterio di riesame, esito e collegamento a rischio/obiettivo/controllo quando applicabile.

5. Evidenze ISO 9001 - lettura senior

Sintesi dei punti di forza e delle aree da consolidare nel sistema di gestione per la qualita.

Il sistema ISO 9001 risulta coerente con il modello operativo di LCC INNOVA SRL. Sono presenti elementi documentali relativi a contesto, campo di applicazione, processi, politica, obiettivi, gestione fornitori, audit interni, riesame e miglioramento. Le non conformita minori non sembrano riguardare l'assenza totale dei processi, ma la necessita di rendere le evidenze piu complete, misurabili e verificabili.

Tema	Evidenza positiva	Gap / presidio da rafforzare
Contesto e parti interessate	Analisi disponibile e coerente con attivita e sede unica.	Collegare fattori interni/esterni, requisiti monitorabili, responsabilita e frequenze di riesame.
Mappa processi	Processi principali identificati e coerenti con scopo.	Esplicitare input, output, indicatori, interazioni e criteri operativi per i processi campionati.
Leadership e ruoli	Struttura organizzativa e ruoli presenti.	Formalizzare meglio interfacce tra funzioni operative e controllo qualita.
Rischi e opportunita	Registro o analisi presente.	Rafforzare criteri di priorita, azioni associate, responsabili, tempi e verifica efficacia.
Competenza	Gestione competenze attiva.	Documentare efficacia della formazione e riesame periodico delle competenze.
Fornitori	Qualifica e controllo fornitori presenti.	Migliorare criteri di rivalutazione e registrazioni di monitoraggio, soprattutto per fornitori critici.
Audit e riesame	Programma audit e riesame effettuati.	Assicurare piena copertura di processi/requisiti e collegamento tra input, decisioni, azioni e follow-up.
Azioni correttive	Processo presente.	Rafforzare analisi causa radice e verifica documentata dell'efficacia.

Focus operativo Priorita ISO 9001: trasformare le evidenze da 'documenti presenti' a 'evidenze gestite'. Ogni requisito critico deve dimostrare chi ha fatto cosa, quando, con quale criterio, con quale risultato e con quale verifica successiva.

6. Evidenze ISO/IEC 27001 - lettura senior

Sintesi dei punti piu rilevanti per SGSI e Annex A.

Il SGSI copre i processi principali e considera asset, rischi, controlli, accessi, fornitori, incidenti, backup e continuita. La principale esposizione non e l'assenza di un framework, ma la tracciabilita non sempre completa tra perimetro, risk assessment, SoA, controlli Annex A, responsabilita e registrazioni operative. Questo e tipico di sistemi ISO 27001 in fase iniziale: la maturita cresce quando il registro rischi, il piano di trattamento, la SoA e le evidenze operative diventano un unico sistema informativo coerente.

Tema	Evidenza positiva	Gap / presidio da rafforzare
Perimetro SGSI	Campo definito e coerente con sede/processi.	Chiarire confini fisici, logici, cloud, fornitori esterni e responsabilita condivise.
Politica sicurezza	Politica disponibile.	Dimostrare comunicazione, comprensione e disponibilita verso parti interessate pertinenti.
Risk assessment	Metodologia presente.	Rendere espliciti criteri di accettazione, aggiornamento e collegamento agli asset.
Risk treatment	Piano disponibile.	Correlare rischi, controlli, owner, scadenze, stato attuazione e residuo accettato.
SoA	Dichiarazione di Applicabilita presente nella sintesi finale.	Dettagliare motivazioni di inclusione/esclusione, stato dei controlli e riferimenti evidenziali.
Asset inventory	Inventario disponibile.	Evidenziare proprietario, classificazione, criticita, aggiornamento periodico e trattamento.
Access control	Gestione accessi definita.	Completare evidenze di autorizzazione, revisione periodica e revoca.
Incident management	Procedura prevista.	Rafforzare classificazione, registrazione, escalation, lesson learned e trend analysis.
Backup	Backup gestiti.	Formalizzare test di restore, esiti, anomalie e azioni conseguenti.

7. Registro consolidato dei rilievi

Sintesi dei 24 rilievi consolidati nella parte finale del report: 14 NC minori e 10 osservazioni.

Standard	Clausola	Tipo	Evidenza / rilievo sintetico
ISO 9001	4.1	Observation	Analisi contesto disponibile; da rafforzare il collegamento con fattori interni/esterni, rischi e indirizzi strategici.
ISO 9001	4.2	Minor	Parti interessate identificate, ma requisiti monitorabili e responsabilita di aggiornamento non sempre definiti.
ISO 9001	4.3	Observation	Scopo coerente; da rendere piu chiaro rispetto a sedi, outsourcing e confini operativi.
ISO 9001	4.4	Minor	Mappa processi presente; indicatori, input, output e interazioni non sempre pienamente definiti.
ISO 9001	5.3	Observation	Ruoli definiti; interfacce tra funzioni operative e controllo qualita da formalizzare meglio.
ISO 9001	6.1	Minor	Rischi e opportunita presenti; criteri di priorita, azioni e verifica efficacia non sempre evidenti.
ISO 9001	6.2	Observation	Obiettivi qualita definiti; migliorare misurabilita, target, frequenze e responsabilita.
ISO 9001	7.2	Minor	Competenze gestite; evidenza di efficacia formativa non sempre completa.
ISO 9001	8.4	Minor	Controllo fornitori attuato; criteri di rivalutazione e monitoraggio non sempre documentati.
ISO 9001	9.2	Minor	Audit interno presente; copertura di processi, requisiti e risultati precedenti da rendere piu tracciabile.
ISO 9001	9.3	Observation	Riesame effettuato; correlazione input, decisioni, azioni e verifica successiva migliorabile.
ISO 9001	10.2	Minor	Gestione NC presente; analisi causa e verifica efficacia da approfondire.
ISO 27001	4.3	Observation	Perimetro SGSI definito; confini fisici/logici/cloud e processi esterni da chiarire.
ISO 27001	5.2	Observation	Politica disponibile; tracciabilita della comunicazione alle parti interessate da rafforzare.
ISO 27001	6.1.2	Minor	Metodologia risk assessment presente; criteri di accettazione, aggiornamento e collegamento asset non sempre chiari.
ISO 27001	6.1.3	Minor	Piano trattamento rischi disponibile; correlazione rischi, controlli, responsabilita e stato attuazione incompleta.
ISO 27001	6.1.3 / SoA	Minor	SoA presente; giustificazioni di inclusione/esclusione e stato controlli da dettagliare.
ISO 27001	7.2	Observation	Competenze sicurezza gestite; efficacia formazione e awareness da rafforzare.
ISO 27001	8.1	Minor	Controlli operativi attuati; pianificazione, responsabilita e registrazioni non sempre complete.
ISO 27001	A.5.9	Minor	Inventario asset disponibile; proprietario, classificazione e aggiornamento periodico non sempre evidenti.
ISO 27001	A.5.15/A.5.18/A.8.5	Minor	Accessi definiti; evidenze di revisione periodica, autorizzazione o revoca non sempre complete.
ISO 27001	A.5.19/A.5.22	Observation	Fornitori ICT gestiti; requisiti di sicurezza nei rapporti contrattuali migliorabili.
ISO 27001	A.5.24/A.5.26	Minor	Gestione incidenti prevista; classificazione, registrazione, escalation e lesson learned da completare.
ISO 27001	A.8.13	Observation	Backup gestiti; documentazione dei test di ripristino e relativi esiti da rafforzare.

8. Priorita di trattamento evidenziale

Azioni di presidio richieste in chiave di evidenza, non come prescrizione operativa di soluzione.

Priorita	Area	Perche rileva	Evidenza minima attesa
P1	Allineamento findings e chiusura incoerenze	Il fascicolo deve essere internamente coerente tra tabella rilievi, riepilogo NC/Observation e conclusione.	Versione finale del registro rilievi, con classificazione unica, esito cliente, piano azioni e responsabilita.
P1	Risk assessment e risk treatment ISO 27001	Determina la robustezza dell'intero SGSI e la giustificazione dei controlli Annex A.	Metodologia, criteri di accettazione, registro rischi aggiornato, piano trattamento con owner, scadenze, controlli e residuo.
P1	SoA	E' il documento cardine per dimostrare applicabilita e stato dei controlli ISO 27001.	SoA con controllo, applicabilita, motivazione, stato, riferimento evidenza e collegamento al rischio.
P1	Asset e accessi	Sono controlli ad alto impatto su riservatezza, integrita e disponibilita.	Inventario asset con owner/classificazione; matrice accessi; log o verbali di revisione, autorizzazione e revoca.
P2	Audit interno e azioni correttive	Garantisce ciclo PDCA e tenuta del sistema in sorveglianza.	Programma audit collegato a processi/requisiti; rapporti; NC; causa radice; azioni; verifica efficacia.
P2	Fornitori e outsourcing	Impatta su qualita del servizio e sicurezza della supply chain ICT.	Criteri qualifica/rivalutazione; requisiti sicurezza; evidenze monitoraggio fornitori critici.
P2	Incidenti e backup	Elementi essenziali per resilienza operativa e gestione eventi di sicurezza.	Registro incidenti, criteri escalation, lesson learned; pianificazione e risultati dei test di restore.
P3	Obiettivi, riesame e contesto	Migliora la maturita gestionale e la misurabilita del miglioramento.	Obiettivi misurabili, riesame con input/decisioni/azioni, aggiornamento contesto e parti interessate.

La priorita P1 dovrebbe essere trattata prima della formalizzazione del fascicolo di certificazione e comunque prima di successive verifiche di follow-up. Le priorita P2 e P3 alimentano il piano di miglioramento e il riesame della direzione. Il report originale richiede inoltre la comunicazione delle azioni correttive e delle date di implementazione entro 10 giorni lavorativi dalla chiusura dell'audit.

9. Struttura consigliata del fascicolo evidenze

Cartella / sezione	Contenuto atteso	Output di controllo
01 - Governance	Scopo, politica, organigramma, ruoli, responsabilita, comunicazioni.	Evidenza di approvazione, diffusione e riesame.
02 - Contesto e parti interessate	Analisi contesto, stakeholder, requisiti, obblighi cogenti, matrice normativa.	Responsabile aggiornamento e frequenza riesame.
03 - Processi ISO 9001	Mappa processi, indicatori, input/output, controlli operativi, registrazioni principali.	Dashboard processi e trend periodici.
04 - Rischi e opportunita	Registro rischi SGQ e SGSI, criteri, priorita, azioni e monitoraggio.	Tracciabilita rischio-azione-owner-esito.
05 - SoA e controlli Annex A	SoA, controlli applicabili, evidenze operative, eccezioni, riesami.	Stato controlli aggiornato e collegato ai rischi.
06 - Asset e accessi	Inventario asset, classificazione, proprietari, autorizzazioni, revisioni accessi.	Report periodico di asset/access review.
07 - Fornitori	Qualifica, contratti, requisiti sicurezza/qualita, monitoraggi, rivalutazioni.	Esito rivalutazione e azioni su fornitori critici.
08 - Incidenti, backup e continuita	Incident log, escalation, lesson learned, backup e restore test.	Evidenze di esercizio e miglioramento.
09 - Audit, riesame, miglioramento	Audit plan/report, NC, azioni correttive, riesame direzione, KPI.	Chiusura PDCA con verifica di efficacia.

10. Conclusione senior

Decisione, rischi residui e criteri di follow-up.

La conclusione dell'audit team e favorevole al prosieguo verso la certificazione. Il sistema di gestione e stato ritenuto efficace e lo scopo adeguato, con audit completato sui processi, sulle funzioni e sugli aspetti indicati nel piano. Il profilo dei rilievi consolidati, pari a 14 non conformita minori e 10 osservazioni, e compatibile con una raccomandazione positiva, a condizione che l'organizzazione gestisca le minori con metodo strutturato e dimostri il rafforzamento delle evidenze prima dei successivi punti di controllo.

La principale area di rischio residuo riguarda la dimostrabilita. Molti rilievi non contestano l'esistenza del processo, ma la sua capacita di lasciare evidenze oggettive, coerenti e riesaminabili. Questo e particolarmente rilevante per ISO 27001, dove il sistema di controllo deve poter dimostrare la relazione tra asset, minacce, rischi, controlli, responsabilita e stato di attuazione.

Ambito	Giudizio senior	Follow-up atteso
Procedibilita certificativa	Positiva	Procedere, mantenendo evidenza della gestione delle NC minori e delle osservazioni.
Rischio documentale	Medio	Allineare report, registro rilievi, piani correttivi e riferimenti alle evidenze.
Rischio SGQ	Basso/medio	Rafforzare processi, fornitori, audit interni, competenze e azioni correttive.
Rischio SGSI	Medio	Rafforzare risk assessment, SoA, asset, accessi, incidenti, backup e controlli operativi.
Maturita	In consolidamento	Passare da documenti disponibili a sistema evidenziale integrato e misurabile.

Raccomandazione Raccomandazione finale: mantenere la decisione favorevole alla certificazione, ma chiudere il quality control del fascicolo e assicurare che ogni NC minore abbia causa, azione, owner, scadenza, evidenza di implementazione e criterio di verifica efficacia. Le osservazioni devono essere integrate nel piano di miglioramento e nel prossimo riesame della direzione.

11. Note di qualita del fascicolo

Elementi formali da sanare o verificare prima dell'archiviazione definitiva.

Elemento	Rischio	Azione di controllo
Data audit non valorizzata	Il frontespizio indica Stage 2 Date '-' pur riportando revisione 29 August 2025.	Confermare e valorizzare la data effettiva dell'audit nel fascicolo definitivo.
Major intermedia A.8.25-A.8.32	Una sezione intermedia indica Major, mentre il riepilogo finale indica 0 Major.	Allineare classificazione, risposta cliente e conteggio finale; conservare evidenza della rettifica.
Tabelle findings non omogenee	Alcuni rilievi nelle tabelle intermedie non coincidono pienamente con il registro finale consolidato.	Identificare un unico registro ufficiale dei rilievi, con codifica progressiva e riferimenti pagina/evidenza.
Conteggio finale	Il riepilogo finale riporta 14 Minor e 10 Observation, ma la riga 'n. 0' puo generare ambiguita grafica.	Rendere il conteggio esplicito e graficamente univoco nel report finale.
Termini di follow-up	Il report richiede comunicazione delle azioni entro 10 giorni lavorativi.	Inserire data di chiusura audit, data limite e responsabilita di invio del piano.

Fine del report.