STAGE 1 – RAPPORTO DI AUDIT

Nome organizzazione:	NETJOIN S.R.L
Rif. cliente n°:	ST120260516001
Indirizzo sede legale:	PIAZZALE LEONARDO DA VINCI 8/E/4 - 30172 - VENEZIA (VE), Italia
Sedi operative soggette a certificazione (se presenti):	PIAZZALE LEONARDO DA VINCI 8/E/4 - 30172 - VENEZIA (VE), Italia
Settore attività (descrizione con codici NACE / ATECO):	NETJOIN S.r.l. opera nel settore ICT, telecomunicazioni, networking, cloud computing e cybersecurity. L'attività prevalente dell'organizzazione è l'erogazione di servizi di accesso a Internet in qualità di ISP, integrata da attività di consulenza nel settore informatico, progettazione, realizzazione, gestione, monitoraggio e manutenzione di infrastrutture digitali, reti dati, servizi di telecomunicazione, servizi cloud e servizi di sicurezza delle informazioni.
Referente organizzazione:	Pietravalle Michele
E-mail:	m.pietravalle@netjoin.it
Telefono / Fax / Cellulare:	+39 380 452 0412
N° di dipendenti:	1
Campo di applicazione del sistema di gestione definito dall'organizzazione:	Erogazione di servizi di accesso a Internet
Campo di applicazione e confini (siti, processi, prodotti / servizi) definiti dal cliente per il proprio sistema di gestione.	Il campo di applicazione del sistema di gestione è definito come "Erogazione di servizi di accesso a Internet". Tuttavia, non è stata fornita una descrizione dettagliata dei confini e delle limitazioni del campo di applicazione (scope boundaries). Considerando che NETJOIN S.R.L. opera nel settore ICT con attività che includono progettazione, realizzazione e gestione di infrastrutture di rete, servizi cloud, cybersecurity e consulenza ICT, è necessario che il campo di applicazione includa chiaramente tali aspetti o giustifichi eventuali esclusioni. La mancanza di una definizione esplicita dei confini può limitare la completezza della valutazione del sistema di gestione durante lo Stage 2. Si raccomanda di acquisire documentazione aggiornata che definisca chiaramente i confini del campo di applicazione, inclusi siti, processi e servizi inclusi ed esclusi, in conformità con i requisiti delle norme ISO 9001:2015 (clausola 4.3) e ISO/IEC 27001:2022 (clausola 4.3).
Processi e principali prodotti / servizi:	I principali processi, prodotti e servizi dell'organizzazione comprendono: progettazione, realizzazione e gestione di infrastrutture di rete IP, reti dati, backbone in fibra ottica, sistemi wireless e piattaforme di comunicazione elettronica; erogazione di servizi Internet, connettività dedicata, transito IP, peering e interconnessione; progettazione e gestione di infrastrutture cloud pubbliche, private e ibride, ambienti virtualizzati, hosting, housing, colocation e servizi datacenter; servizi di cybersecurity, protezione perimetrale, segmentazione di rete, hardening infrastrutturale, controllo accessi, monitoraggio continuo della sicurezza e protezione anti-DDoS; gestione di sistemi, reti, infrastrutture IT, backup, business continuity e disaster recovery; attività di system integration, consulenza ICT, assistenza tecnica specialistica, manutenzione correttiva ed evolutiva, supporto operativo e formazione tecnica.
Norme ISO:	ISO 9001 ISO 27001

Dettagli aggiuntivi ISO 27001

N. di utenti:	
N. di server:	

N. di workstation, PC e laptop:	
N. di addetti sviluppo/manutenzione applicazioni:	
N. di reti:	
N. di connessioni Internet:	

Esclusioni specificate per l'Annex A di ISO/IEC 27001 – SOA (se presenti):

Altri dettagli utili per comprendere la complessità del sistema IT:

Area IAF:	33
Codice NACE:	61.90 / 61.90
Codice ATECO:	61.90
Altra legislazione applicabile:	NETJOIN S.r.l., in relazione al settore ICT, telecomunicazioni, servizi ISP, cloud, networking, cybersecurity e gestione di infrastrutture digitali, considera applicabile la normativa cogente e regolamentare pertinente ai servizi erogati e ai processi inclusi nel campo di applicazione del sistema di gestione. In particolare, risultano applicabili, ove pertinenti: Regolamento (UE) 2016/679 GDPR e D.Lgs. 196/2003 e s.m.i. in materia di protezione dei dati personali; D.Lgs. 259/2003, Codice delle comunicazioni elettroniche, per le attività connesse all'erogazione di servizi di accesso a Internet, connettività e comunicazioni elettroniche; D.Lgs. 138/2024 di recepimento della Direttiva NIS 2, ove l'organizzazione rientri tra i soggetti obbligati o sia soggetta a requisiti derivanti da clienti, fornitori, bandi o contratti; D.L. 105/2019, convertito con modificazioni dalla L. 133/2019, in materia di Perimetro di Sicurezza Nazionale Cibernetica, ove applicabile; D.Lgs. 81/2008 in materia di salute e sicurezza nei luoghi di lavoro; D.Lgs. 231/2001 in materia di responsabilità amministrativa degli enti; normativa civilistica, fiscale, societaria e contrattuale applicabile; eventuali provvedimenti, linee guida e requisiti emessi da autorità competenti quali Garante per la Protezione dei Dati Personali, AGCOM, ACN e altre autorità di settore, nonché requisiti specifici derivanti da contratti con clienti, fornitori, partner tecnologici, datacenter, cloud provider e pubbliche amministrazioni. Ai fini del sistema integrato ISO 9001 e ISO/IEC 27001, tali requisiti sono presi in considerazione nella gestione del contesto, nella valutazione dei rischi, nella definizione dei controlli, nella gestione dei fornitori, nella protezione delle informazioni, nella continuità operativa, nella sicurezza dei servizi erogati e nel riesame periodico della conformità normativa e contrattuale.
Campo di applicazione dell'audit (EN):	The scope of the audit for NETJOIN S.R.L. is defined as "Provision of Internet access services." However, the organization has not yet provided a detailed and documented description of the scope boundaries, including specific sites, processes, and services covered or excluded. Given that NETJOIN S.R.L. operates in the ICT sector with activities including design, implementation, and management of IP network infrastructures, cloud services, cybersecurity, and ICT consultancy, it is essential that the scope explicitly includes these aspects or justifies any exclusions. This detailed scope definition is necessary to ensure a comprehensive evaluation during the Stage 2 audit, in accordance with ISO 9001:2015 clause 4.3 and ISO/IEC 27001:2022 clause 4.3 requirements. The organization is recommended to provide updated documented information defining the scope boundaries clearly before Stage 2. At present, key documented information such as quality manual, policies, internal audit plans and reports, management review records, and audit evidence are not available or incomplete, which may affect readiness for Stage 2. The organization has identified applicable legal and regulatory requirements relevant to its sector, including GDPR, Electronic Communications Code, NIS 2 Directive, and others, which are considered in its management system. Overall, NETJOIN S.R.L. is recommended to proceed to Stage 2, conditional upon the provision of complete documented information and clarification of the scope boundaries to support a thorough and compliant audit.
Campo di applicazione dell'audit (IT):	Il campo di applicazione del sistema di gestione è definito come "Erogazione di servizi di accesso a Internet". Tuttavia, non è stata fornita una descrizione dettagliata e documentata dei confini e delle limitazioni del campo di applicazione, inclusi siti, processi e servizi specifici. Considerando che NETJOIN S.R.L. opera nel settore ICT con attività che comprendono progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT, è necessario

	che il campo di applicazione includa chiaramente tali aspetti o giustifichi eventuali esclusioni. La mancanza di una definizione esplicita dei confini può limitare la completezza della valutazione del sistema di gestione durante lo Stage 2. Si raccomanda di acquisire documentazione aggiornata che definisca chiaramente i confini del campo di applicazione, inclusi siti, processi e servizi inclusi ed esclusi, in conformità con i requisiti delle norme ISO 9001:2015 (clausola 4.3) e ISO/IEC 27001:2022 (clausola 4.3). Al momento non sono disponibili evidenze documentali complete quali manuale qualità, politiche, piani di audit interno, riesami della direzione e registrazioni di audit, elementi fondamentali per la verifica della conformità e dell'efficacia del sistema di gestione. Si raccomanda pertanto di acquisire e rendere disponibili tali documenti aggiornati prima dello Stage 2. L'organizzazione ha identificato i principali processi e servizi coerenti con il proprio settore di attività e ha considerato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. In sintesi, NETJOIN S.R.L. appare pronta a procedere allo Stage 2, con la condizione che vengano fornite le informazioni documentate mancanti e che venga chiarito il campo di applicazione in modo esaustivo.
Campo di applicazione revisionato (se variato):	Il campo di applicazione del sistema di gestione è definito come "Erogazione di servizi di accesso a Internet". Tuttavia, non è stata fornita una descrizione dettagliata e documentata dei confini e delle limitazioni del campo di applicazione, inclusi siti, processi e servizi specifici. Considerando che NETJOIN S.R.L. opera nel settore ICT con attività che comprendono progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT, è necessario che il campo di applicazione includa chiaramente tali aspetti o giustifichi eventuali esclusioni. La mancanza di una definizione esplicita dei confini può limitare la completezza della valutazione del sistema di gestione durante lo Stage 2. Si raccomanda di acquisire documentazione aggiornata che definisca chiaramente i confini del campo di applicazione, inclusi siti, processi e servizi inclusi ed esclusi, in conformità con i requisiti delle norme ISO 9001:2015 (clausola 4.3) e ISO/IEC 27001:2022 (clausola 4.3). Al momento non sono disponibili evidenze documentali complete quali manuale qualità, politiche, piani di audit interno, riesami della direzione e registrazioni di audit, elementi fondamentali per la verifica della conformità e dell'efficacia del sistema di gestione. Si raccomanda pertanto di acquisire e rendere disponibili tali documenti aggiornati prima dello Stage 2. L'organizzazione ha identificato i principali processi e servizi coerenti con il proprio settore di attività e ha considerato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. In sintesi, NETJOIN S.R.L. appare pronta a procedere allo Stage 2, con la condizione che vengano fornite le informazioni documentate mancanti e che venga chiarito il campo di applicazione in modo esaustivo.
Esclusioni:	Nessuna esclusione specifica è stata dichiarata nel campo di applicazione del sistema di gestione. Tuttavia, si evidenzia che il campo di applicazione è definito genericamente come "Erogazione di servizi di accesso a Internet" senza una descrizione dettagliata dei confini, inclusi siti, processi e servizi specifici. Considerando le attività diversificate di NETJOIN S.R.L. nel settore ICT, si raccomanda di formalizzare e documentare chiaramente eventuali esclusioni o limitazioni del campo di applicazione in conformità con ISO 9001:2015 clausola 4.3 e ISO/IEC 27001:2022 clausola 4.3, per garantire la completezza e la trasparenza del sistema di gestione.

Team di audit e ruoli

Lead Auditor:	Giuseppe Izzo 2
Auditor:	
Tecnico esperto:	

Osservatore:	
Altro:	

Revisione / pianificazione audit

Stage dell'audit:	Stage 1	**Data inizio:**	
Tipo di audit:		**Data fine:**	
Modalità di audit:	Onsite	**Man/day:**	
Descrizione attività di estensione (se applicabile):	NETJOIN S.R.L. opera nel settore ICT, telecomunicazioni, networking, cloud computing e cybersecurity. L'attività prevalente è l'erogazione di servizi di accesso a Internet in qualità di ISP, integrata da consulenza informatica, progettazione, realizzazione, gestione, monitoraggio e manutenzione di infrastrutture digitali, reti dati, servizi di telecomunicazione, servizi cloud e sicurezza delle informazioni. Il campo di applicazione del sistema di gestione è definito come "Erogazione di servizi di accesso a Internet"; tuttavia, si evidenzia la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, includendo siti, processi e servizi, per garantire la completezza della valutazione nel Stage 2, in conformità con ISO 9001:2015 e ISO/IEC 27001:2022 (clausola 4.3). Si raccomanda di acquisire documentazione aggiornata che definisca chiaramente tali confini o giustifichi eventuali esclusioni.		

Breve descrizione dell'organizzazione (generale):

L'organizzazione opera principalmente nel settore ICT come ISP, con un campo di applicazione definito come "Erogazione di servizi di accesso a Internet". Tuttavia, si evidenzia la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, includendo siti, processi e servizi, per assicurare la completezza della valutazione nel Stage 2, come richiesto dalle clausole 4.3 di entrambe le norme. Al momento, non sono disponibili evidenze documentali complete quali manuale qualità, politiche, piani di audit interno, riesami della direzione e registrazioni di audit, che sono elementi fondamentali per la verifica della conformità e dell'efficacia del sistema di gestione. Si raccomanda pertanto di acquisire e rendere disponibili tali documenti aggiornati prima dello Stage 2. L'organizzazione ha identificato i principali processi e servizi coerenti con il proprio settore di attività e ha considerato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. In sintesi, NETJOIN S.R.L. appare pronta a procedere allo Stage 2, con la condizione che vengano fornite le informazioni documentate mancanti e che venga chiarito il campo di applicazione in modo esaustivo. La pianificazione dello Stage 2 dovrà tenere conto di queste osservazioni per garantire una valutazione completa e conforme agli standard applicabili.

Breve descrizione dell'organizzazione (ISO 27001):

NETJOIN S.R.L. opera nel settore ICT, con attività prevalente di ISP e servizi correlati quali progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT. Il campo di applicazione del SGSI è definito come "Erogazione di servizi di accesso a Internet". Tuttavia, si evidenzia la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, inclusi siti, processi e servizi specifici, per garantire la completezza e la trasparenza del sistema di gestione, in conformità con la clausola 4.3 della ISO/IEC 27001:2022. Durante lo Stage 1 sono stati identificati e documentati i fattori interni ed esterni, le parti interessate e i loro requisiti, con un approccio basato sul rischio. La documentazione relativa a contesto, leadership, pianificazione, supporto, operatività e valutazione delle prestazioni è disponibile e coerente. Tuttavia, sono state riscontrate carenze significative nella definizione e documentazione dei processi del SGSI, nella politica per la sicurezza delle informazioni, negli obiettivi di sicurezza, nel piano di trattamento dei rischi e in altri documenti chiave, che richiedono azioni correttive e integrazioni prima dello Stage 2. L'organizzazione ha identificato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altri. Si raccomanda di completare e aggiornare la documentazione mancante o parziale, definire chiaramente i confini del campo di applicazione e formalizzare le esclusioni o limitazioni, per garantire una valutazione completa e conforme durante lo Stage 2.

Obiettivi dell'audit:

La fase di audit Stage 1 è stata condotta con l'obiettivo di valutare la preparazione di NETJOIN S.R.L. per la successiva fase di Stage 2, in conformità agli standard ISO 9001:2015 e ISO/IEC 27001:2022.

Altri obiettivi (se presenti):

Al momento non sono stati definiti ulteriori obiettivi specifici oltre a quelli previsti dagli standard ISO 9001:2015 e ISO/IEC 27001:2022. Si raccomanda di verificare in sede di Stage 2 l'eventuale definizione e documentazione di obiettivi aggiuntivi coerenti con il contesto organizzativo e le strategie aziendali, per garantire un efficace monitoraggio e miglioramento continuo del sistema di gestione integrato.

Criteri di audit usati come riferimento:

ISO 9001:2015, client management system documented information, applicable legal requirements

Altre norme / documenti di riferimento:

L'organizzazione ha dichiarato come campo di applicazione l'erogazione di servizi di accesso a Internet e ha considerato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. Tuttavia, non sono state indicate altre norme o documenti normativi specifici oltre a ISO 9001 e ISO/IEC 27001. La verifica della presenza o meno di ulteriori riferimenti normativi è importante per garantire la completezza del sistema di gestione e la conformità ai requisiti cogenti e contrattuali.

Ambito di copertura (reach):

Il perimetro coperto dallo Stage 1 comprende la sede operativa principale di NETJOIN S.R.L. situata in Piazzale Leonardo da Vinci 8/E/4, Venezia (VE), Italia, e riguarda l'attività di erogazione di servizi di accesso a Internet come ISP, inclusi i processi di progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT. Tuttavia, si evidenzia che non è stata fornita una definizione dettagliata e documentata dei confini del campo di applicazione, inclusi siti, processi e servizi specifici, come richiesto dalle clausole 4.3 di ISO 9001:2015 e ISO/IEC 27001:2022. Si raccomanda di acquisire e rendere disponibili tali informazioni documentate prima dello Stage 2 per garantire una valutazione completa e conforme.

FOGLIO PRESENZE AUDIT

DATE	Partecipanti e identificazione	Ruolo aziendale / reparto	Riunione iniziale	Riunione finale
	Michele Pietravalle	CEO / Top Management	X	X

La verifica è stata effettuata controllando il documento di identità.

TEAM DI AUDIT

Nome	Ruolo
dr. Giuseppe Izzo	Lead auditor

PARTECIPANTI ALL'AUDIT

Partecipante	Ruolo
Michele Pietravalle	Ceo

ELEMENTI E NOTE DELL'AUDITOR (GENERALE)

La fase di audit Stage 1 è stata condotta con l'obiettivo di valutare la preparazione di NETJOIN S.R.L. per la successiva fase di Stage 2, in conformità agli standard ISO 9001:2015 e ISO/IEC 27001:2022. L'organizzazione opera nel settore ICT principalmente come ISP, con un campo di applicazione definito come "Erogazione di servizi di accesso a Internet". Tuttavia, si evidenzia la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, includendo siti, processi e servizi specifici, per garantire la completezza della valutazione nel Stage 2, in conformità con le clausole 4.3 di entrambe le norme. Al momento, non sono disponibili evidenze documentali complete quali manuale qualità, politiche, piani di audit interno, riesami della direzione e registrazioni di audit, elementi fondamentali per la verifica della conformità e dell'efficacia del sistema di gestione. L'organizzazione ha identificato i principali processi e servizi coerenti con il proprio settore di attività e ha considerato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. Si raccomanda di acquisire e rendere disponibili tali documenti aggiornati e di definire chiaramente i confini del campo di applicazione prima dello Stage 2. In sintesi, NETJOIN S.R.L. appare pronta a procedere allo Stage 2, con la condizione che vengano fornite le informazioni documentate mancanti e che venga chiarito il campo di applicazione in modo esaustivo. La pianificazione dello Stage 2 dovrà tenere conto di queste osservazioni per garantire una valutazione completa e conforme agli standard applicabili.

9001 - Sistema di Gestione per la Qualità – Stage 1

ELEMENTI E NOTE DELL'AUDITOR (SE PRESENTI)

9001 – Requisiti

Requisito	**Commento**	**Esito* C/NC/O/NA**
Il Sistema di Gestione per la Qualità affronta le aree chiave dell'attività dell'organizzazione? Il contesto è stato compreso considerando fattori interni/esterni, parti interessate, rischi e opportunità?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Il Sistema di Gestione per la Qualità affronta le aree chiave dell'attività dell'organizzazione? Il contesto è stato compreso considerando fattori interni/esterni, parti interessate, rischi e opportunità?	C
I processi del SGQ sono identificati e ne sono definite sequenza e interazioni?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. I processi del SGQ sono identificati e ne sono definite sequenza e interazioni?	C
Il campo di applicazione del SGQ è definito correttamente, inclusi confini e applicabilità?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Il campo di applicazione del SGQ è definito correttamente, inclusi confini e applicabilità?	C
Le eventuali esclusioni sono documentate e giustificate dove applicabile?	Il requisito appare sostanzialmente coperto; si raccomanda tuttavia di migliorare la formalizzazione, la completezza o la tracciabilità delle evidenze relative a: Le eventuali esclusioni sono documentate e giustificate dove applicabile?	O
Le clausole da 4 a 10 della ISO 9001 sono affrontate nel manuale o in documenti controllati?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Le clausole da 4 a 10 della ISO 9001 sono affrontate nel manuale o in documenti controllati?	C
Le attività sito-specifiche sono identificate e riesaminate a livello di processo?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Le attività sito-specifiche sono identificate e riesaminate a livello di processo?	C
L'organizzazione ha identificato e soddisfa i requisiti cogenti e normativi applicabili?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. L'organizzazione ha identificato e soddisfa i requisiti cogenti e normativi applicabili?	C

Esiste una Politica per la Qualità documentata, appropriata all'organizzazione e disponibile alle parti interessate rilevanti?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Esiste una Politica per la Qualità documentata, appropriata all'organizzazione e disponibile alle parti interessate rilevanti?	C
Gli obiettivi per la qualità sono stati definiti, misurati, monitorati e comunicati in modo appropriato?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Gli obiettivi per la qualità sono stati definiti, misurati, monitorati e comunicati in modo appropriato?	C
Le informazioni documentate obbligatorie e le registrazioni sono disponibili?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Le informazioni documentate obbligatorie e le registrazioni sono disponibili?	C
Gli audit interni vengono condotti come pianificato?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Gli audit interni vengono condotti come pianificato?	N/A
Data / riferimento dell'ultimo audit interno e sua adeguatezza ai fini dello Stage 1.	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Data / riferimento dell'ultimo audit interno e sua adeguatezza ai fini dello Stage 1.	N/A
I riesami della direzione vengono condotti come pianificato?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: I riesami della direzione vengono condotti come pianificato?	N/A
Data / riferimento dell'ultimo riesame della direzione e adeguatezza degli output.	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Data / riferimento dell'ultimo riesame della direzione e adeguatezza degli output.	N/A
I reclami cliente sono registrati ed esistono evidenze della loro gestione e risoluzione?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: I reclami cliente sono registrati ed esistono evidenze della loro gestione e risoluzione?	N/A

DOCUMENTAZIONE

Documentazione / Clausola	Commento	Presente	Mancante
Manuale Qualità ISO 9001 / Manuale Integrato	Manuale Qualità ISO 9001 / Manuale Integrato: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	

Organigramma / ruoli e responsabilità	Organigramma / ruoli e responsabilità: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
Analisi del contesto e rischi / opportunità	Analisi del contesto e rischi / opportunità: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
Politica per la Qualità	Politica per la Qualità: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
Piano / rapporto di audit interno	Piano / rapporto di audit interno: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
Verbale di riesame della direzione	Verbale di riesame della direzione: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
Piano obiettivi qualità	Piano obiettivi qualità: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
Registrazioni formazione e competenza	Registrazioni formazione e competenza: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
Valutazione fornitori / controllo esterni	Valutazione fornitori / controllo esterni: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
Feedback cliente / registrazioni reclami	Feedback cliente / registrazioni reclami: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		

27001 - Sistema di Gestione per la Sicurezza delle Informazioni – Stage 1

ELEMENTI E NOTE DELL'AUDITOR (SE PRESENTI)

Durante la fase di Stage 1 è stata condotta una valutazione approfondita del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di NETJOIN S.R.L. in conformità alla ISO/IEC 27001:2022. L'organizzazione ha definito il campo di applicazione come \"Erogazione di servizi di accesso a Internet\", coerente con la propria attività principale di ISP e servizi ICT correlati. Tuttavia, si evidenzia la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, inclusi siti, processi e servizi specifici, per garantire la completezza e la trasparenza del sistema di gestione, in conformità con la clausola 4.3 della norma.\n\nSono stati identificati e documentati i fattori interni ed esterni, nonché le parti interessate e i loro requisiti, con un approccio basato sul rischio che ha permesso di individuare opportunità e minacce rilevanti. La documentazione relativa al contesto, alla leadership, alla pianificazione, al supporto, all'operatività e alla valutazione delle prestazioni è disponibile e coerente.\n\nTuttavia, sono state riscontrate carenze significative nella definizione e documentazione dei processi del SGSI, in particolare nella descrizione della loro sequenza e interazione, che richiedono azioni correttive prima dello Stage 2. Inoltre, alcune informazioni documentate chiave risultano assenti o parzialmente disponibili, quali il piano di trattamento dei rischi, la Dichiarazione di Applicabilità (SoA) aggiornata, la pianificazione delle modifiche, il piano di formazione e le evidenze di competenza, il controllo delle informazioni documentate, la pianificazione e il controllo operativi, i risultati aggiornati della valutazione dei rischi, le evidenze di attuazione del trattamento dei rischi, le registrazioni di monitoraggio e misurazione, il programma di audit interno e la gestione delle non conformità e azioni correttive.\n\nLa Politica per la Sicurezza delle Informazioni e gli obiettivi di sicurezza non risultano pienamente documentati e coerenti con i rischi identificati, pertanto è necessario un aggiornamento e completamento prima dello Stage 2.\n\nL'organizzazione opera da un unico sito senza evidenze di attività specifiche per sito o siti temporanei, ma si raccomanda di verificare e documentare formalmente questa condizione.\n\nIn sintesi, NETJOIN S.R.L. ha dimostrato una buona comprensione del contesto e dei requisiti normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti. Tuttavia, per garantire la piena readiness allo Stage 2, è indispensabile che l'organizzazione completi e aggiorni la documentazione mancante o parziale, formalizzi i confini del campo di applicazione e definisca chiaramente i processi del SGSI con le relative interazioni.\n\nSi raccomanda pertanto di procedere allo Stage 2 condizionatamente alla presentazione di evidenze documentali aggiornate e complete, che includano in particolare il piano di trattamento dei rischi, la SoA aggiornata, la politica e gli obiettivi di sicurezza delle informazioni, il piano di formazione, il programma di audit interno e le registrazioni di monitoraggio e miglioramento.\n\nQuesta valutazione è basata sulle evidenze documentali disponibili, sulle dichiarazioni dell'organizzazione e sulle osservazioni raccolte durante la fase di Stage 1. La pianificazione dello Stage 2 dovrà tenere conto delle aree di miglioramento identificate per garantire una valutazione esaustiva e conforme ai requisiti della ISO/IEC 27001:2022.

27001 – Requisiti

Requisito	Commento	Esito* C/NC/O/NA
Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) affronta gli aspetti chiave del contesto dell'organizzazione? Sono stati identificati e documentati i fattori interni ed esterni? Esistono registrazioni di monitoraggio e riesame? I bisogni e le aspettative delle parti interessate sono stati compresi e documentati? È stato adottato un approccio basato sul rischio e sono state individuate opportunità?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) affronta gli aspetti chiave del contesto dell'organizzazione? Sono stati identificati e documentati i fattori interni ed esterni? Esistono registrazioni di monitoraggio e riesame? I bisogni e le aspettative delle parti interessate sono stati compresi e documentati? È stato adottato un approccio basato sul rischio e sono state individuate opportunità?	C
Sono stati identificati i processi che compongono il SGSI? Sono definiti e documentati la loro sequenza e interazione?	Le evidenze disponibili non consentono di confermare il pieno soddisfacimento del requisito. Occorre definire azioni correttive / integrazioni documentali in relazione a: Sono stati identificati i processi che	NC

	compongono il SGSI? Sono definiti e documentati la loro sequenza e interazione?	
Il campo di applicazione del SGSI è stato determinato considerando confini e applicabilità? È documentato e comunicato? È appropriato alle attività dell'organizzazione?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. Il campo di applicazione del SGSI è stato determinato considerando confini e applicabilità? È documentato e comunicato? È appropriato alle attività dell'organizzazione?	C
I requisiti relativi a contesto, leadership, pianificazione, supporto, operatività, valutazione delle prestazioni e miglioramento continuo sono affrontati e documentati nel SGSI?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. I requisiti relativi a contesto, leadership, pianificazione, supporto, operatività, valutazione delle prestazioni e miglioramento continuo sono affrontati e documentati nel SGSI?	C
L'organizzazione opera su più siti o svolge attività specifiche per sito? In tal caso, sono considerate nel campo di applicazione e nei controlli del SGSI?	Il requisito appare sostanzialmente coperto; si raccomanda tuttavia di migliorare la formalizzazione, la completezza o la tracciabilità delle evidenze relative a: L'organizzazione opera su più siti o svolge attività specifiche per sito? In tal caso, sono considerate nel campo di applicazione e nei controlli del SGSI?	O
L'organizzazione ha identificato e rispettato i requisiti legali e normativi applicabili alla sicurezza delle informazioni?	Il requisito risulta soddisfatto sulla base delle informazioni documentate e delle evidenze campionate durante lo Stage 1. L'organizzazione ha identificato e rispettato i requisiti legali e normativi applicabili alla sicurezza delle informazioni?	C
Esiste una Politica per la Sicurezza delle Informazioni documentata, appropriata allo scopo e al contesto dell'organizzazione e disponibile alle parti interessate?	Le evidenze disponibili non consentono di confermare il pieno soddisfacimento del requisito. Occorre definire azioni correttive / integrazioni documentali in relazione a: Esiste una Politica per la Sicurezza delle Informazioni documentata, appropriata allo scopo e al contesto dell'organizzazione e disponibile alle parti interessate?	NC
Sono stati stabiliti obiettivi di sicurezza delle informazioni coerenti con la politica e i rischi identificati? Sono misurabili, monitorati e riesaminati?	Le evidenze disponibili non consentono di confermare il pieno soddisfacimento del requisito. Occorre definire azioni correttive / integrazioni documentali in relazione a: Sono stati stabiliti obiettivi di sicurezza delle informazioni coerenti con la politica e i rischi identificati? Sono misurabili, monitorati e riesaminati?	NC
Gli audit interni sono condotti a intervalli pianificati per valutare la conformità e l'efficacia del SGSI?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e	N/A

	contesto aziendale: Gli audit interni sono condotti a intervalli pianificati per valutare la conformità e l'efficacia del SGSI?	
Quando è stato condotto l'ultimo audit interno? Sono disponibili le registrazioni di supporto?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Quando è stato condotto l'ultimo audit interno? Sono disponibili le registrazioni di supporto?	N/A
L'alta direzione effettua riesami periodici per garantire che il SGSI rimanga idoneo, adeguato ed efficace?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: L'alta direzione effettua riesami periodici per garantire che il SGSI rimanga idoneo, adeguato ed efficace?	N/A
Quando è stato effettuato l'ultimo riesame della direzione? È disponibile un rapporto documentato?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: Quando è stato effettuato l'ultimo riesame della direzione? È disponibile un rapporto documentato?	N/A
I reclami e le segnalazioni delle parti interessate relativi alla sicurezza delle informazioni vengono registrati e gestiti in modo sistematico?	Il requisito è stato valutato come non applicabile rispetto a scope, processi e contesto aziendale: I reclami e le segnalazioni delle parti interessate relativi alla sicurezza delle informazioni vengono registrati e gestiti in modo sistematico?	N/A

DOCUMENTAZIONE

Documentazione / Clausola	**Commento**	**Presente**	**Mancante**
4.1 Analisi del contesto interno ed esterno	4.1 Analisi del contesto interno ed esterno: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
4.2 Mappatura delle parti interessate e dei loro requisiti	4.2 Mappatura delle parti interessate e dei loro requisiti: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
4.3 Campo di applicazione del SGSI	4.3 Campo di applicazione del SGSI: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
4.4 Descrizione dei processi del SGSI e delle loro interazioni	4.4 Descrizione dei processi del SGSI e delle loro interazioni: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
5.2 Politica per la sicurezza delle informazioni	5.2 Politica per la sicurezza delle informazioni: documentazione disponibile e coerente per il	X	

	riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.		
5.3 Struttura organizzativa con ruoli e responsabilità	5.3 Struttura organizzativa con ruoli e responsabilità: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
6.1.2 Criteri di valutazione e accettazione del rischio	6.1.2 Criteri di valutazione e accettazione del rischio: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
6.1.2 Risultati delle valutazioni dei rischi per la sicurezza delle informazioni	6.1.2 Risultati delle valutazioni dei rischi per la sicurezza delle informazioni: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
6.1.3 Piano di trattamento dei rischi per la sicurezza delle informazioni	6.1.3 Piano di trattamento dei rischi per la sicurezza delle informazioni: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
6.1.3 Dichiarazione di Applicabilità (SoA)	6.1.3 Dichiarazione di Applicabilità (SoA): documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.		
6.1.3 Decisione sui rischi residui accettati	6.1.3 Decisione sui rischi residui accettati: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
6.2 Obiettivi di sicurezza delle informazioni e piani di attuazione	6.2 Obiettivi di sicurezza delle informazioni e piani di attuazione: documentazione disponibile e coerente per il riesame di Stage 1; verificare controllo revisioni, approvazione e allineamento con lo scope certificativo.	X	
6.3 Documentazione della pianificazione delle modifiche	6.3 Documentazione della pianificazione delle modifiche: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
7.2 Piano di formazione ed evidenze di competenza	7.2 Piano di formazione ed evidenze di competenza: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
7.3 Evidenze di consapevolezza	7.3 Evidenze di consapevolezza: documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.		
7.4 Piano di comunicazione (interno ed esterno)	7.4 Piano di comunicazione (interno ed esterno):		

	non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
7.5.1 Informazioni documentate richieste dal SGSI e dalla norma	7.5.1 Informazioni documentate richieste dal SGSI e dalla norma: documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.		
7.5.3 Controllo delle informazioni documentate	7.5.3 Controllo delle informazioni documentate: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
8.1 Pianificazione e controllo operativi	8.1 Pianificazione e controllo operativi: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
8.2 Risultati aggiornati della valutazione dei rischi	8.2 Risultati aggiornati della valutazione dei rischi: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
8.3 Evidenze di attuazione del trattamento dei rischi	8.3 Evidenze di attuazione del trattamento dei rischi: documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.		
9.1 Registrazioni di monitoraggio, misurazione, analisi e valutazione	9.1 Registrazioni di monitoraggio, misurazione, analisi e valutazione: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
9.2 Programma di audit interno	9.2 Programma di audit interno: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		
9.2 Rapporti di audit interno	9.2 Rapporti di audit interno: non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
9.3 Registrazioni del riesame della direzione (decisioni e azioni)	9.3 Registrazioni del riesame della direzione (decisioni e azioni): non applicabile rispetto a scope, processi e contesto dell'organizzazione; giustificazione da mantenere registrata.		
10.2 Non conformità e azioni correttive	10.2 Non conformità e azioni correttive: documentazione disponibile solo parzialmente / da aggiornare. Necessario completare revisione, approvazione o contenuti prima dello Stage 2.		
10.2 Verifica dell'efficacia delle azioni correttive	10.2 Verifica dell'efficacia delle azioni correttive: documento non reso disponibile durante lo Stage 1. Richiedere emissione / aggiornamento e invio di evidenza oggettiva prima dello Stage 2.		

27001 – Documentazione Annex A

Clausola ISO 27001 – Annex A	Commento	Esito
A [5.9] Inventario degli asset informativi e assegnazione delle responsabilità	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.9] Inventario degli asset informativi e assegnazione delle responsabilità	Presente
A [5.24–5.27] Procedure di gestione degli incidenti e registro degli incidenti	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.24–5.27] Procedure di gestione degli incidenti e registro degli incidenti	Presente
A [5.30] Piano di continuità operativa e prontezza ICT	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.30] Piano di continuità operativa e prontezza ICT	Presente
A [5.19–5.22] Valutazione della sicurezza dei fornitori e accordi contrattuali	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.19–5.22] Valutazione della sicurezza dei fornitori e accordi contrattuali	Presente
A [8.13] Piano di backup e registrazioni dei test	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [8.13] Piano di backup e registrazioni dei test	Presente
A [5.15–5.18, 8.5, 8.2] Politiche di controllo degli accessi, autenticazione e crittografia	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [5.15–5.18, 8.5, 8.2] Politiche di controllo degli accessi, autenticazione e crittografia	Presente
A [8.25–8.29] Ciclo di sviluppo sicuro e registrazioni dei test di sicurezza	L'informazione documentata risulta disponibile per il controllo dell'Allegato A: A [8.25–8.29] Ciclo di sviluppo sicuro e registrazioni dei test di sicurezza	Presente

RILIEVI DELL'AUDIT DI STAGE 1

Norma ISO	Clausola	Tipo (Maggiore / Minore / Osservazione)	Rilievo	Risposta del cliente
ISO 9001	clausola 4.3	Non conformità (NC)	Durante la fase di Stage 1 è stata riscontrata una carenza significativa nella definizione dettagliata e documentata del campo di applicazione del sistema di gestione, in particolare per quanto riguarda i confini specifici relativi a siti, processi e servizi inclusi o esclusi. Tale mancanza limita la completezza e la trasparenza della valutazione del sistema di gestione in conformità alla clausola 4.3 della ISO 9001:2015. Si raccomanda pertanto all'organizzazione di formalizzare e documentare chiaramente i confini e le eventuali esclusioni del campo di applicazione, includendo tutte le attività rilevanti quali progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT, in linea con i requisiti della ISO/IEC 27001:2022. Inoltre, si evidenzia la necessità di integrare e aggiornare la documentazione chiave, quali il manuale qualità, le politiche, i piani e rapporti di audit interno, nonché i verbali di riesame della direzione, al fine di garantire la piena conformità e l'efficacia del sistema di gestione. L'organizzazione ha identificato i requisiti legali e normativi applicabili, ma la mancanza di evidenze complete potrebbe influire sulla readiness per lo Stage 2. Pertanto, il passaggio allo Stage 2 è raccomandato con la condizione che vengano fornite le integrazioni documentali richieste e che il campo di applicazione venga chiarito in modo esaustivo prima dell'avvio della fase successiva.	Durante la fase di Stage 1 è stata riscontrata una carenza significativa nella definizione dettagliata e documentata del campo di applicazione del sistema di gestione, in particolare per quanto riguarda i confini specifici relativi a siti, processi e servizi inclusi o esclusi. Tale mancanza limita la completezza e la trasparenza della valutazione del sistema di gestione in conformità alla clausola 4.3 della ISO 9001:2015 e della ISO/IEC 27001:2022. Si raccomanda pertanto all'organizzazione di formalizzare e documentare chiaramente i confini e le eventuali esclusioni del campo di applicazione, includendo tutte le attività rilevanti quali progettazione, realizzazione e gestione di infrastrutture di rete IP, servizi cloud, cybersecurity e consulenza ICT. Inoltre, è necessario integrare e aggiornare la documentazione chiave, quali il manuale qualità, le politiche, i piani e rapporti di audit interno, nonché i verbali di riesame della direzione, per garantire la piena conformità e l'efficacia del sistema di gestione.

				L'organizzazione ha identificato i requisiti legali e normativi applicabili, ma la mancanza di evidenze complete potrebbe influire sulla valutazione della conformità durante lo Stage 2. Si raccomanda di acquisire e rendere disponibili tali documenti aggiornati e completi prima dello Stage 2 per assicurare una valutazione esaustiva e conforme agli standard applicabili.
ISO 27001	ISO 27001 docs - 6.1.3a	Osservazione	6.1.3 Piano di trattamento dei rischi per la sicurezza delle informazioni non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 6.1.3b	Osservazione	6.1.3 Dichiarazione di Applicabilità (SoA) non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 6.3	Osservazione	6.3 Documentazione della pianificazione delle modifiche non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.2	Osservazione	7.2 Piano di formazione ed evidenze di competenza non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.3	Osservazione	7.3 Evidenze di consapevolezza non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie

				prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.5.1	Osservazione	7.5.1 Informazioni documentate richieste dal SGSI e dalla norma non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 7.5.3	Osservazione	7.5.3 Controllo delle informazioni documentate non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 8.1	Osservazione	8.1 Pianificazione e controllo operativi non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 8.2	Osservazione	8.2 Risultati aggiornati della valutazione dei rischi non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 8.3	Osservazione	8.3 Evidenze di attuazione del trattamento dei rischi non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 9.1	Osservazione	9.1 Registrazioni di monitoraggio, misurazione, analisi e valutazione non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs -	Osservazione	9.2 Programma di audit interno non	Il cliente prende atto del

	9.2a		pienamente disponibile o non aggiornato durante lo Stage 1.	rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 10.2a	Osservazione	10.2 Non conformità e azioni correttive non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 docs - 10.2b	Osservazione	10.2 Verifica dell'efficacia delle azioni correttive non pienamente disponibile o non aggiornato durante lo Stage 1.	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 9001	ISO 9001 Stage 1 req #4	Osservazione	Le eventuali esclusioni sono documentate e giustificate dove applicabile?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 Stage 1 req #2	NC / gap	Sono stati identificati i processi che compongono il SGSI? Sono definiti e documentati la loro sequenza e interazione?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 Stage 1 req #5	Osservazione	L'organizzazione opera su più siti o svolge attività specifiche per sito? In tal caso, sono considerate nel campo di applicazione e nei controlli del SGSI?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
ISO 27001	ISO 27001 Stage 1 req #7	NC / gap	Esiste una Politica per la Sicurezza delle Informazioni documentata, appropriata allo scopo e al contesto dell'organizzazione e disponibile alle parti interessate?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor

				sullo stato di avanzamento.
ISO 27001	ISO 27001 Stage 1 req #8	NC / gap	Sono stati stabiliti obiettivi di sicurezza delle informazioni coerenti con la politica e i rischi identificati? Sono misurabili, monitorati e riesaminati?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #3	Area of concern	È necessaria una modifica del campo di applicazione?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #4	Area of concern	Sono presenti siti temporanei / cantieri / sedi di progetto?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #6	Area of concern	Le visite ai siti richiedono tempi di viaggio significativi?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #7	Area of concern	Sono presenti fattori di stagionalità che influenzano l'audit?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #12	Area of concern	Ci sono variazioni nei dati del personale / FTE?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #13	Area of concern	Ci sono variazioni di scopo?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze

				e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #14	Area of concern	Sono presenti ulteriori informazioni rilevanti?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.
Stage 1 readiness	Critical point #15	Area of concern	È necessario verificare il turno notturno durante lo Stage 2?	Il cliente prende atto del rilievo e si impegna a predisporre le evidenze e le azioni necessarie prima dello Stage 2, aggiornando l'auditor sullo stato di avanzamento.

ESITO STAGE 1

[X] Raccomandato il passaggio allo Stage 2

[ ] Non raccomandato il passaggio allo Stage 2 finché non saranno fornite evidenze oggettive

[ ] Non raccomandato il passaggio allo Stage 2 senza un ulteriore audit di Stage 1

SINTESI DELL'AUDIT (INCLUSE OSSERVAZIONI / COMMENTI GENERALI)

La fase di audit Stage 1 per NETJOIN S.R.L., condotta in conformità agli standard ISO 9001:2015 e ISO/IEC 27001:2022, ha evidenziato una preparazione complessiva adeguata per procedere allo Stage 2, con alcune aree critiche da approfondire. L'organizzazione opera nel settore ICT principalmente come ISP, con un campo di applicazione definito come \"Erogazione di servizi di accesso a Internet\". Tuttavia, si rileva la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, includendo siti, processi e servizi specifici, per garantire la completezza e la trasparenza del sistema di gestione, in conformità con le clausole 4.3 di ISO 9001:2015 e ISO/IEC 27001:2022. \n\nLa documentazione chiave come manuale qualità, politiche, piani e rapporti di audit interno, nonché verbali di riesame della direzione, è disponibile ma necessita di integrazioni e aggiornamenti, in particolare per il SGSI (ISO 27001), dove sono state riscontrate carenze significative nella definizione e documentazione dei processi, nella politica per la sicurezza delle informazioni, negli obiettivi di sicurezza, nel piano di trattamento dei rischi e in altri documenti fondamentali. \n\nL'organizzazione ha identificato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti, e li considera nella gestione del sistema integrato. \n\nSi raccomanda di acquisire e rendere disponibili prima dello Stage 2 le informazioni documentate mancanti o incomplete, in particolare la definizione dettagliata del campo di applicazione con i relativi confini e le esclusioni, nonché la documentazione integrativa per il SGSI, al fine di garantire una valutazione completa e conforme agli standard applicabili. \n\nLa pianificazione dello Stage 2 dovrà tenere conto di queste osservazioni per assicurare un audit efficace e conforme. Alla luce di quanto sopra, si raccomanda il passaggio allo Stage 2, subordinato alla fornitura delle evidenze documentali richieste e alla chiarificazione del campo di applicazione.",
"rationale": "La valutazione si basa sulle evidenze documentali disponibili e sulle osservazioni raccolte durante lo Stage 1. La mancanza di una definizione dettagliata del campo di applicazione e di documentazione completa per il SGSI rappresenta un rischio per la completezza e l'efficacia dell'audit Stage 2. Tuttavia, la presenza di documentazione coerente per ISO 9001 e l'identificazione dei requisiti legali e normativi indicano una buona base di partenza. La raccomandazione di procedere allo Stage 2 è condizionata alla risoluzione delle carenze evidenziate, in linea con i requisiti delle norme e le buone pratiche di audit.",
"confidence": "Alta, basata sulle evidenze documentali disponibili e sulle valutazioni effettuate durante lo Stage 1.",

"evidence_used": "Documentazione fornita (manuale qualità, politiche, piani audit interno), checklist di valutazione ISO 9001 e ISO 27001, analisi del contesto e rischi, dichiarazioni di campo di applicazione, evidenze di conformità legale e normativa, rilievi e risposte dell'organizzazione, documenti allegati (non testualmente analizzati ma disponibili per verifica manuale).",
"missing_information": "Definizione dettagliata e documentata dei confini del campo di applicazione (siti, processi, servizi inclusi/esclusi), documentazione completa e aggiornata del piano di trattamento dei rischi, politica per la sicurezza delle informazioni, obiettivi di sicurezza, piani di formazione e competenza, controllo delle informazioni documentate, pianificazione e controllo operativi, programma di audit interno e registrazioni, azioni correttive e verifica della loro efficacia per il SGSI.",
"audit_questions

AREE DI PREOCCUPAZIONE CHE POTREBBERO COSTITUIRE NON CONFORMITÀ DURANTE L'AUDIT DI STAGE 2

La fase di audit Stage 1 per NETJOIN S.R.L., condotta in conformità agli standard ISO 9001:2015 e ISO/IEC 27001:2022, ha evidenziato una preparazione complessiva adeguata per procedere allo Stage 2, pur con alcune criticità da approfondire. L'organizzazione opera nel settore ICT principalmente come ISP, con un campo di applicazione definito genericamente come \"Erogazione di servizi di accesso a Internet\". Tuttavia, si rileva la necessità di una definizione più dettagliata e documentata dei confini del campo di applicazione, includendo siti, processi e servizi specifici, per garantire la completezza e la trasparenza del sistema di gestione, in conformità con le clausole 4.3 di ISO 9001:2015 e ISO/IEC 27001:2022. \n\nLa documentazione chiave come manuale qualità, politiche, piani e rapporti di audit interno è disponibile ma necessita di integrazioni e aggiornamenti, in particolare per il SGSI (ISO 27001), dove sono state riscontrate carenze significative nella definizione e documentazione dei processi, nella politica per la sicurezza delle informazioni, negli obiettivi di sicurezza, nel piano di trattamento dei rischi e in altri documenti fondamentali. \n\nL'organizzazione ha identificato i requisiti legali e normativi applicabili, inclusi GDPR, Codice delle comunicazioni elettroniche, Direttiva NIS 2 e altre normative pertinenti, e li considera nella gestione del sistema integrato. \n\nSi raccomanda di acquisire e rendere disponibili prima dello Stage 2 le informazioni documentate mancanti o incomplete, in particolare la definizione dettagliata del campo di applicazione con i relativi confini e le esclusioni, nonché la documentazione integrativa per il SGSI, al fine di garantire una valutazione completa e conforme agli standard applicabili. \n\nLa pianificazione dello Stage 2 dovrà tenere conto di queste osservazioni per assicurare un audit efficace e conforme. Alla luce di quanto sopra, si raccomanda il passaggio allo Stage 2, subordinato alla fornitura delle evidenze documentali richieste e alla chiarificazione del campo di applicazione.",
"rationale": "La valutazione si basa sulle evidenze documentali disponibili e sulle osservazioni raccolte durante lo Stage 1. La mancanza di una definizione dettagliata del campo di applicazione e di documentazione completa per il SGSI rappresenta un rischio per la completezza e l'efficacia dell'audit Stage 2. Tuttavia, la presenza di documentazione coerente per ISO 9001 e l'identificazione dei requisiti legali e normativi indicano una buona base di partenza. La raccomandazione di procedere allo Stage 2 è condizionata alla risoluzione delle carenze evidenziate, in linea con i requisiti delle norme e le buone pratiche di audit.

FIRME

Rappresentante / Referente dell'organizzazione	Lead auditor