CLOUD3 S.R.L.

MANUALE DEL SISTEMA DI GESTIONE PER LA QUALITA ISO 9001:2015

Documento di governo del Sistema di Gestione per la Qualita applicato ai servizi ICT, allo sviluppo software, alla consulenza informatica, alle attivita di hosting e ai servizi formativi informatici non legalmente riconosciuti.

Dato	Valore
Codice documento	MQ-9001-CLOUD3
Revisione	01
Data emissione	21/05/2026
Organizzazione	CLOUD3 S.R.L.
Sede legale e operativa	Piazza Golgi 28C, 16011 Arenzano (GE)
C.F. / P.IVA	02497740999
REA	GE - 490668
PEC	amministrazione@pec.cloud3.srl
Referente interno	Simone Cola - cola@cloud3.srl
NACE / ATECO	62.10 / 62.10.00 - Attivita di programmazione informatica

Il presente manuale e redatto come documento interno del Sistema di Gestione per la Qualita di CLOUD3 S.R.L. e deve essere utilizzato per orientare processi, responsabilita, evidenze e controlli richiesti dalla norma ISO 9001:2015.

1. Controllo del documento

Il manuale definisce l impostazione, l architettura e le regole operative del Sistema di Gestione per la Qualita adottato da CLOUD3 S.R.L. per assicurare la capacita sistematica di fornire servizi conformi ai requisiti del cliente, ai requisiti cogenti applicabili e agli impegni interni di miglioramento. Il documento ha funzione di riferimento principale per Direzione, responsabili di processo, personale operativo e soggetti coinvolti nella pianificazione, erogazione e verifica dei servizi ICT.

Il controllo del documento assicura che le informazioni documentate siano identificate, riesaminate, approvate, distribuite, conservate e aggiornate in modo coerente con la dimensione aziendale e con la complessita dei processi. In un contesto aziendale snello, caratterizzato da 4 addetti e da servizi ad alto contenuto tecnico, il manuale privilegia un approccio pragmatico: le responsabilita sono chiare, le registrazioni sono proporzionate e le evidenze sono orientate alla dimostrazione della conformita durante audit interni, riesami e verifiche di certificazione.

Revisione	Descrizione modifica	Responsabile approvazione	Stato
Rev. 00	Prima emissione del manuale SGQ ISO 9001:2015	Direzione	Approvato
Rev. 01	Riedizione completa con sviluppo esteso dei capitoli, eliminazione di riferimenti esterni non pertinenti e rafforzamento delle sezioni operative	Direzione	Approvato

1.1 Regole di gestione e diffusione

Il manuale e disponibile in formato elettronico controllato. La copia elettronica conservata nell archivio documentale aziendale rappresenta la versione di riferimento. Eventuali stampe sono considerate copie non controllate, salvo diversa indicazione formalizzata dalla Direzione. La distribuzione interna avviene verso le persone che contribuiscono ai processi di vendita, progettazione, sviluppo, assistenza, hosting, formazione e miglioramento del sistema.

Le modifiche al manuale sono valutate dalla Direzione sulla base di cambiamenti organizzativi, variazioni del campo di applicazione, aggiornamenti normativi, esiti di audit, reclami, non conformita, cambiamenti tecnologici o nuove esigenze di mercato. Ogni revisione deve mantenere la coerenza tra scopo, processi, responsabilita, rischi, obiettivi, indicatori e registrazioni.

La conservazione delle versioni precedenti puo essere effettuata in archivio storico, con accesso limitato, per dimostrare la tracciabilita delle decisioni e l evoluzione del sistema. I documenti superati non devono essere utilizzati per l erogazione operativa, salvo consultazione storica autorizzata.

Il presente manuale non sostituisce procedure operative, istruzioni tecniche, contratti, offerte, piani di progetto, ticket, registrazioni di test, report di collaudo e riesami. Esso li coordina e ne stabilisce la logica di governo, indicando quali evidenze devono essere mantenute per dimostrare efficacia e conformita del sistema.

1.2 Matrice di distribuzione

Destinatario	Finalita della distribuzione	Modalita	Evidenza
Direzione	Governo del sistema, approvazione obiettivi e riesame	Archivio elettronico controllato	Registro revisioni e approvazioni
Responsabile SGQ	Gestione documentale, audit, NC, azioni correttive e KPI	Repository interno	Lista documenti e report di audit
Area tecnica software/ICT	Applicazione requisiti nei processi di sviluppo, test, rilascio e assistenza	Accesso controllato a procedure e moduli	Ticket, piani di progetto, checklist
Area commerciale/amministrativa	Gestione offerte, contratti, ordini, fatturazione e comunicazioni cliente	Accesso controllato a modelli e procedure	Offerte, conferme, comunicazioni, reclami
Auditor interni/esterni	Verifica del sistema e delle evidenze	Consultazione autorizzata	Piani audit e rapporti di audit

2. Indice generale del manuale

L indice e organizzato secondo la struttura della norma ISO 9001:2015 e secondo i processi effettivi di CLOUD3 S.R.L. Le sezioni successive sviluppano contenuti, responsabilita, criteri di controllo e registrazioni necessarie per sostenere un audit di certificazione e le successive sorveglianze.

3. Profilo dell organizzazione e dati identificativi

CLOUD3 S.R.L. e una societa a responsabilita limitata con sede in Arenzano, attiva nei servizi ICT, nella produzione e personalizzazione di software, nella progettazione e manutenzione di piattaforme web, nella consulenza informatica, nella configurazione di personal computer e server, nei servizi connessi alle tecnologie dell informazione, nell hosting specialistico e nella formazione professionale informatica non legalmente riconosciuta. La natura tecnica dei servizi richiede un sistema di qualita capace di governare requisiti del cliente, requisiti tecnici, tempi di consegna, continuita del servizio, gestione delle modifiche, protezione delle informazioni e controllo delle competenze.

La dimensione organizzativa e contenuta: la visura camerale riporta 4 addetti, con 3 dipendenti e 1 indipendente, oltre a 1 collaboratore. Tale dimensione comporta una struttura decisionale snella, con forte coinvolgimento della Direzione, linee di comunicazione brevi e necessita di presidiare con registrazioni essenziali i punti critici del processo. La proporzionalita e un principio guida del presente manuale: il sistema deve essere completo e auditabile, senza generare complessita documentale non necessaria.

Il modello di business combina attivita progettuali e servizi continuativi. Le attivita progettuali comprendono analisi, sviluppo, personalizzazione, configurazione, test, rilascio e manutenzione evolutiva. I servizi continuativi comprendono assistenza, gestione richieste, hosting, supporto applicativo, monitoraggio e interventi correttivi. Le attivita formative richiedono invece controllo di contenuti, competenze dei docenti, registrazioni di partecipazione e valutazioni di efficacia, anche quando non si tratta di corsi legalmente riconosciuti.

Elemento	Informazione aziendale	Implicazione per il SGQ
Denominazione	CLOUD3 S.R.L.	Identificazione univoca del soggetto certificabile e del campo di applicazione
Sede	Piazza Golgi 28C, 16011 Arenzano (GE)	Sito principale da considerare negli audit e nelle registrazioni operative
C.F./P.IVA	02497740999	Identificazione fiscale e amministrativa nei contratti e nelle offerte
REA	GE - 490668	Riferimento camerale e legale
Forma giuridica	Societa a responsabilita limitata	Governo societario con responsabilita della Direzione
Capitale sociale	Euro 10.000,00	Dato identificativo e amministrativo
Costituzione	24/10/2017	Anzianita organizzativa e consolidamento del know-how
Avvio attivita	08/01/2018	Esperienza operativa nei processi ICT
ATECO/NACE	62.10.00 - Attivita di programmazione informatica / NACE 62.10	Definizione del settore e del perimetro tecnico
Addetti	4 addetti rilevati al 31/12/2025, di cui 3 dipendenti e 1 indipendente; 1 collaboratore	Sistema proporzionato a micro/piccola organizzazione tecnica
Albo	Albo Imprese Artigiane GE n. 128672	Rilevanza per qualificazione artigiana e attivita dichiarate

3.1 Natura dei servizi e aspettative del mercato

Il mercato ICT richiede rapidita di risposta, competenza tecnica, sicurezza delle informazioni, stabilita degli ambienti, capacita di comprendere requisiti spesso non completamente formalizzati e gestione ordinata delle modifiche. Per CLOUD3 S.R.L. la qualita non coincide solo con la consegna del software o del servizio, ma con la capacita di governare l intero ciclo: ascolto del cliente, definizione dei requisiti, progettazione, esecuzione tecnica, verifica, rilascio, supporto e miglioramento.

I servizi software e web presentano rischi specifici: ambiguita dei requisiti, dipendenza da infrastrutture e fornitori esterni, vulnerabilita informatiche, variazioni normative privacy, indisponibilita dei sistemi, difetti applicativi, perdita di tracciabilita delle decisioni, ritardi nei rilasci e scarsa comprensione del cliente rispetto alle implicazioni tecniche. Il SGQ deve trasformare tali rischi in controlli pratici e registrazioni verificabili.

Il posizionamento professionale di una societa ICT di piccole dimensioni si fonda sulla fiducia. La fiducia viene sostenuta da evidenze: offerte chiare, ordini confermati, requisiti tracciati, registrazioni di progetto, versionamento, test, ticket, comunicazioni, verbali, riesami e misurazione della soddisfazione. Il manuale rende tali evidenze parte integrante del modo di lavorare, evitando che la conformita sia percepita come attivita separata dalla produzione di valore.

4. Campo di applicazione del Sistema di Gestione per la Qualita

Campo di applicazione proposto: Progettazione, sviluppo, personalizzazione, configurazione, manutenzione e assistenza di software e piattaforme web; consulenza informatica; configurazione di personal computer e server; servizi di hosting specialistico e servizi applicativi in rete; erogazione di corsi di formazione e aggiornamento professionale in ambito hardware e software non legalmente riconosciuti.

Il campo di applicazione e costruito in coerenza con le attivita dichiarate dall organizzazione e con la natura dei servizi effettivamente erogati. Esso include le attivita tecniche principali, le attivita di supporto al cliente, i processi commerciali e i processi gestionali necessari a garantire la conformita del servizio. Il perimetro comprende la sede di Arenzano e, ove applicabile, le attivita svolte presso il cliente o da remoto, secondo le condizioni contrattuali e operative concordate.

La clausola 8.3 della norma ISO 9001:2015 e considerata applicabile, poiche CLOUD3 S.R.L. realizza e personalizza software, piattaforme web e soluzioni informatiche che richiedono attivita di progettazione, definizione requisiti, controllo degli input, sviluppo, verifica, validazione e gestione delle modifiche. Non e corretto escludere la progettazione quando l organizzazione interviene sulla definizione della soluzione, sulla configurazione funzionale o sulla costruzione tecnica di software e servizi digitali.

La clausola 7.1.5 relativa alle risorse per il monitoraggio e la misurazione e applicata in modo proporzionato. Per i servizi ICT non sono normalmente presenti strumenti metrologici fisici soggetti a taratura nel senso tradizionale; tuttavia sono utilizzati strumenti software, checklist, ambienti di test, log, metriche di disponibilita, controlli di versione, validazioni funzionali e verifiche di rilascio. Tali risorse devono essere idonee allo scopo, controllate e coerenti con i criteri di accettazione definiti.

4.1 Applicabilita delle clausole ISO 9001:2015

Clausola	Applicabilita	Motivazione
4 Contesto	Applicabile	Necessario per comprendere mercato ICT, requisiti clienti, dimensione aziendale, requisiti cogenti e scenari tecnologici.
5 Leadership	Applicabile	La Direzione ha ruolo centrale nel governo, nella politica, negli obiettivi e nelle responsabilita.
6 Pianificazione	Applicabile	Rischi e opportunita sono rilevanti per software, hosting, sicurezza, privacy, fornitori e continuita.
7 Supporto	Applicabile	Risorse, competenze, infrastrutture, conoscenza organizzativa e informazioni documentate sono elementi essenziali.
8 Operazioni	Applicabile	Sono inclusi requisiti cliente, progettazione, sviluppo, rilascio, assistenza, formazione e servizi esterni.
8.3 Progettazione e sviluppo	Applicabile	La societa sviluppa, personalizza e configura soluzioni software e web.
9 Valutazione prestazioni	Applicabile	Richiesti KPI, soddisfazione cliente, audit interno e riesame.
10 Miglioramento	Applicabile	NC, reclami, incidenti di servizio e opportunita devono generare miglioramento.

5. Riferimenti normativi e criteri interpretativi

- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualita - Requisiti.
- UNI EN ISO 9000:2015 - Sistemi di gestione per la qualita - Fondamenti e vocabolario.
- UNI EN ISO 19011:2018 - Linee guida per audit di sistemi di gestione.
- Regolamento UE 2016/679 - GDPR, per aspetti connessi al trattamento di dati personali nei servizi ICT e nelle relazioni con clienti e fornitori.
- D.Lgs. 81/2008 per la salute e sicurezza nei luoghi di lavoro, applicabile alla gestione organizzativa e agli ambienti di lavoro.
- Codice Civile e normativa societaria, per aspetti di governo, contratti, responsabilita e amministrazione.
- Normativa in materia di proprieta intellettuale, licenze software e diritto d autore applicabile ai prodotti e componenti utilizzati.
- Requisiti contrattuali, SLA, capitolati, ordini, offerte e specifiche cliente applicabili ai servizi erogati.

I riferimenti normativi sono gestiti con approccio dinamico. La Direzione verifica periodicamente l impatto di modifiche legislative, regolamentari, contrattuali o tecniche sul SGQ. L organizzazione non deve limitarsi a un elenco statico: deve dimostrare che i requisiti rilevanti sono tradotti in controlli pratici, registrazioni e responsabilita operative.

6. Termini, definizioni e abbreviazioni

Termine	Definizione operativa
SGQ	Sistema di Gestione per la Qualita adottato da CLOUD3 S.R.L.

Cliente	Soggetto che richiede o riceve servizi software, web, hosting, consulenza, assistenza o formazione.
Requisito	Esigenza o aspettativa esplicita, implicita o cogente che il servizio deve soddisfare.
Ticket	Registrazione strutturata di richiesta, problema, modifica, assistenza o comunicazione operativa.
Rilascio	Messa a disposizione controllata di software, configurazione, correzione, aggiornamento o servizio.
Validazione	Conferma che il servizio o prodotto software soddisfa l uso previsto o le esigenze del cliente.
Verifica	Conferma oggettiva che i requisiti specificati sono stati soddisfatti.
NC	Non conformita: mancato soddisfacimento di un requisito ISO, cliente, cogente o interno.
OFI	Opportunity for Improvement: opportunita di miglioramento non bloccante.
KPI	Indicatore chiave di prestazione, utilizzato per misurare efficacia ed efficienza dei processi.
SLA	Service Level Agreement, impegno di servizio concordato con il cliente o definito internamente.
Change request	Richiesta di modifica tecnica, funzionale o organizzativa rispetto a requisiti gia concordati.

7. Contesto dell organizzazione - ISO 9001 clausola 4

La comprensione del contesto e il punto di partenza del SGQ. CLOUD3 S.R.L. opera in un ambiente caratterizzato da rapida evoluzione tecnologica, crescente dipendenza dei clienti dai sistemi digitali, forte rilevanza della sicurezza informatica, aspettative di continuita dei servizi, necessita di tempi di risposta rapidi e attenzione alla conformita privacy. Il sistema qualita deve quindi interpretare il contesto non come adempimento formale, ma come base per scegliere priorita, rischi, obiettivi e controlli.

L analisi del contesto viene riesaminata almeno annualmente in sede di riesame della Direzione e ogni volta che intervengono cambiamenti significativi: acquisizione di nuovi clienti strategici, introduzione di nuove tecnologie, variazione di fornitori critici, modifica del campo di applicazione, reclami rilevanti, cambiamenti normativi, incidenti di servizio o modifiche organizzative. Gli esiti sono registrati nel verbale di riesame o in apposite analisi documentate.

Fattore esterno	Descrizione	Risposta SGQ
Evoluzione tecnologica	Nuovi framework, linguaggi, servizi cloud, strumenti di automazione e aspettative di integrazione continua.	Aggiornamento competenze, valutazione fornitori, revisione standard tecnici.
Mercato e concorrenza	Clienti orientati a tempi rapidi, soluzioni personalizzate e costi sostenibili.	Chiarezza commerciale, definizione requisiti, controllo cambiamenti.
Sicurezza informatica	Aumento di minacce, vulnerabilita, rischi di indisponibilita e compromissione dati.	Hardening, backup, patch management, controlli accesso, logging.
Privacy e compliance	Servizi ICT possono trattare dati personali o dati aziendali dei clienti.	DPA, istruzioni privacy, controllo accessi, riservatezza.
Fornitori tecnologici	Dipendenza da hosting, licenze, connettivita, piattaforme, tool e servizi esterni.	Qualifica e monitoraggio fornitori, piani alternativi, SLA.
Economia e continuita	Fluttuazioni della domanda e pressione sui margini.	Pianificazione risorse, priorita, controllo commesse.

7.1 Fattori interni

Fattore interno	Descrizione	Controllo previsto
Dimensione snella	4 addetti e struttura decisionale corta.	Ruoli chiari, registrazioni essenziali, forte coinvolgimento Direzione.
Know-how tecnico	Competenze concentrate su software, web, hosting e consulenza ICT.	Matrice competenze, formazione, condivisione conoscenza.
Flessibilita operativa	Capacita di adattarsi al cliente e al progetto.	Gestione controllata delle modifiche e dei requisiti.
Dipendenza da persone chiave	In alcune attivita il know-how puo essere concentrato.	Documentazione tecnica, backup delle competenze, affiancamento.
Uso di strumenti digitali	Ticket, repository, email, ambienti di test e tool di sviluppo.	Regole di controllo, backup, tracciabilita, accessi.
Esperienza consolidata	Attivita avviata dal 2018 e operativita continuativa.	Capitalizzazione delle lezioni apprese e standardizzazione.

La Direzione deve mantenere evidenza della modalita con cui i fattori esterni e interni sono monitorati. Le fonti possono includere feedback clienti, ticket ricorrenti, esiti di progetto, aggiornamenti normativi, report fornitori, analisi di mercato, reclami, performance dei servizi e osservazioni del personale tecnico. La valutazione non richiede necessariamente report complessi, ma deve essere ripetibile e documentata.

L analisi del contesto alimenta il registro rischi e opportunita. Ad esempio, il rischio di requisiti incompleti genera controlli nella fase di offerta e analisi; il rischio di difetti software genera controlli di test e rilascio; il rischio di indisponibilita hosting genera monitoraggio, backup e valutazione fornitori; il rischio di competenze obsolete genera piani di formazione.

Il contesto e anche la base per determinare obiettivi misurabili. In un azienda ICT non basta misurare il fatturato: occorre misurare puntualita dei rilasci, rispetto dei tempi di risposta, reclami, ticket riaperti, efficacia dei test, disponibilita dei servizi, soddisfazione clienti, stato delle azioni correttive e completamento delle attivita formative interne.

8. Parti interessate e requisiti rilevanti

La norma ISO 9001 richiede di determinare le parti interessate rilevanti e i loro requisiti pertinenti al SGQ. Per CLOUD3 S.R.L. le parti interessate non sono solo i clienti finali: includono personale, collaboratori, fornitori tecnologici, autorita pubbliche, partner, utenti dei sistemi, titolari dei dati, organismi di certificazione e soggetti che dipendono dalla continuita e affidabilita dei servizi digitali. La rilevanza di ciascuna parte interessata viene determinata in base al suo impatto sulla capacita dell organizzazione di fornire servizi conformi.

Parte interessata	Requisiti rilevanti	Evidenze/controlli
Clienti	Servizi conformi, tempi certi, comunicazioni chiare, supporto, protezione dati, stabilita delle soluzioni.	Offerte, contratti, requisiti, ticket, verbali, SLA, report di collaudo, feedback.
Utenti finali	Usabilita, disponibilita, correttezza funzionale, sicurezza e continuita.	Test funzionali, validazione cliente, gestione anomalie, manuali o istruzioni.
Direzione	Controllo processi, redditivita sostenibile, reputazione, riduzione rischi, crescita competenze.	KPI, riesame, obiettivi, audit, azioni correttive.
Personale e collaboratori	Ruoli chiari, strumenti adeguati,	Matrice competenze, piani formazione,

	formazione, ambiente collaborativo, priorita gestibili.	assegnazioni, comunicazioni interne.
Fornitori ICT	Requisiti chiari, pagamenti, interazioni tecniche definite, gestione accessi e responsabilita.	Qualifica fornitori, ordini, contratti, SLA, valutazioni periodiche.
Autorita e enti	Conformita societaria, fiscale, lavoro, sicurezza, privacy, proprieta intellettuale.	Visura, adempimenti, DVR, registri, informative, contratti.
Organismo di certificazione	Evidenze oggettive, campo chiaro, conformita ISO, gestione NC e miglioramento.	Manuale, procedure, registrazioni, audit interno, riesame.
Partner e subfornitori	Coordinamento, specifiche, responsabilita, riservatezza e tracciabilita.	Accordi, NDAs, ordini, comunicazioni tecniche, controlli output.

Il monitoraggio delle parti interessate avviene tramite relazione diretta con i clienti, comunicazioni operative, analisi dei ticket, valutazione dei fornitori, riesame di reclami e feedback, aggiornamento normativo e analisi delle prestazioni. La Direzione valuta se nuovi requisiti devono essere integrati nei processi, nei contratti, nelle procedure o nella formazione.

Il requisito del cliente deve essere chiarito prima dell accettazione dell ordine. Nei servizi software e ICT e frequente che l esigenza iniziale sia incompleta o espressa in termini di risultato atteso piu che di specifiche tecniche. Il SGQ richiede quindi attivita di chiarimento, registrazione delle assunzioni, gestione delle esclusioni, approvazione delle modifiche e mantenimento della tracciabilita fino al rilascio.

I requisiti cogenti devono essere considerati per quanto applicabili. Tra questi assumono particolare rilievo privacy, sicurezza delle informazioni, gestione licenze software, salute e sicurezza del lavoro, norme contrattuali, obblighi fiscali e societari. La conformita non e trattata come elemento separato: deve entrare nelle scelte progettuali, nei contratti, nella gestione accessi, nella conservazione delle evidenze e nella relazione con i fornitori.

9. Architettura dei processi e interazioni

Il SGQ e organizzato per processi. Ogni processo riceve input, produce output, utilizza risorse, applica controlli, genera registrazioni e contribuisce agli obiettivi di qualita. L approccio per processi consente di evitare una gestione frammentata dei servizi ICT e collega le attivita commerciali, tecniche e gestionali in una sequenza controllata. In CLOUD3 S.R.L. i processi sono proporzionati alla dimensione dell organizzazione, ma sufficientemente strutturati per garantire tracciabilita e ripetibilita.

La sequenza tipica parte dal contatto commerciale e dalla raccolta dei requisiti, prosegue con valutazione di fattibilita, offerta, accettazione ordine, pianificazione del progetto o servizio, esecuzione tecnica, verifica, rilascio, assistenza, misurazione della soddisfazione e miglioramento. I processi di supporto forniscono competenze, infrastrutture, documenti, fornitori e strumenti. I processi di governo misurano, auditano e migliorano il sistema.

Processo	Input principali	Output/evidenze
P01 Direzione e governance	Contesto, politica, obiettivi, risorse, riesame, priorita strategiche	Politica, obiettivi, verbale riesame, decisioni, azioni
P02 Commerciale e gestione offerte	Richieste cliente, requisiti, fattibilita, preventivi, contratti	Offerta, conferma ordine, condizioni, requisiti
P03 Analisi requisiti e pianificazione	Esigenze cliente, specifiche, vincoli, rischi, risorse	Piano progetto, backlog, requisiti approvati, stima tempi
P04 Progettazione e sviluppo software	Requisiti, architettura, standard, strumenti	Codice, configurazioni, documentazione tecnica, versioni
P05 Test, validazione e rilascio	Output sviluppo, casi di test, criteri accettazione	Report test, esito collaudo, release note, approvazione
P06 Hosting e servizi continuativi	Ambienti, SLA, monitoraggio, richieste operative	Log, ticket, report disponibilita, azioni correttive
P07 Assistenza e ticketing	Segnalazioni, richieste, anomalie, change request	Ticket chiusi, analisi cause, comunicazioni cliente
P08 Formazione informatica	Fabbisogni, contenuti, docenti, partecipanti	Programmi, registri presenze, valutazioni efficacia
P09 Fornitori e approvvigionamenti	Esigenze hardware/software/servizi esterni	Ordini, qualifiche, valutazioni, controlli output
P10 Risorse e competenze	Ruoli, competenze richieste, formazione	Matrice competenze, piani e registri formazione
P11 Gestione documentale	Documenti, registrazioni, versioni, accessi	Lista documenti, archivi, revisioni, conservazione
P12 Audit, NC e miglioramento	KPI, reclami, audit, anomalie, rischi	Rapporti audit, NC, azioni correttive, lezioni apprese

9.1 Criteri di controllo dei processi

Ogni processo deve avere un responsabile, anche quando piu persone partecipano all attivita. Il responsabile assicura che input e output siano chiari, che le registrazioni minime siano mantenute e che eventuali problemi siano comunicati alla Direzione. In una struttura snella, una stessa persona puo ricoprire piu ruoli, ma cio non elimina la necessita di distinguere le responsabilita in termini di decisione, esecuzione, verifica e approvazione.

I criteri di accettazione devono essere definiti prima della consegna. Nei progetti software tali criteri possono includere funzionalita completate, assenza di anomalie bloccanti, conferma del cliente, esecuzione dei test previsti, configurazione ambiente, backup iniziale, documentazione minima e accettazione delle limitazioni note. Nei servizi di assistenza i criteri possono riguardare tempi di risposta, risoluzione, correttezza della comunicazione e aggiornamento del ticket.

Le interazioni tra processi devono essere visibili nelle evidenze. Una richiesta commerciale deve generare requisiti, i requisiti devono alimentare progettazione e sviluppo, lo sviluppo deve generare test, i test devono condurre al rilascio, il rilascio deve generare supporto e feedback, il feedback deve alimentare miglioramento. L audit deve poter ricostruire questa catena senza affidarsi solo a dichiarazioni verbali.

Quando l attivita e svolta presso il cliente o da remoto, si applicano gli stessi criteri di controllo: identificazione della richiesta, autorizzazione, requisiti, registrazione dell intervento, verifica del risultato, comunicazione di chiusura e, ove applicabile, aggiornamento della documentazione tecnica. La sede fisica non modifica il requisito di tracciabilita.

10. Leadership, politica e responsabilita - ISO 9001 clausola 5

La Direzione di CLOUD3 S.R.L. assume la responsabilita ultima dell efficacia del SGQ. Tale responsabilita comprende definizione della politica, assegnazione delle risorse, promozione dell orientamento al cliente, integrazione dei requisiti qualita nei processi operativi, riesame dei risultati, gestione dei rischi e promozione del miglioramento continuo. In una organizzazione di piccole dimensioni la leadership e visibile nella partecipazione diretta alle decisioni tecniche e commerciali.

La politica per la qualita deve essere coerente con la finalita dell organizzazione: fornire servizi ICT affidabili, personalizzati e sostenibili, con particolare attenzione a chiarezza dei requisiti, competenza tecnica, rispetto degli impegni, sicurezza e riservatezza delle informazioni, tempestivita del supporto, controllo delle modifiche e miglioramento basato su dati. La politica e comunicata internamente e resa disponibile alle parti interessate quando appropriato.

L orientamento al cliente si concretizza nella comprensione dei bisogni, nella valutazione di fattibilita prima dell impegno, nella gestione trasparente di tempi e limiti, nella comunicazione delle variazioni, nella registrazione dei feedback e nella gestione tempestiva di anomalie e reclami. Il cliente deve poter comprendere cosa e incluso, cosa e escluso, quali sono i tempi, quali sono le responsabilita reciproche e quali evidenze attestano il completamento del servizio.

Le responsabilita e autorita sono definite in modo proporzionato. Il responsabile di processo puo essere la Direzione o una funzione tecnica; in ogni caso devono risultare chiari: chi approva offerte, chi accetta requisiti, chi pianifica progetti, chi sviluppa, chi verifica, chi rilascia, chi gestisce ticket, chi tratta reclami, chi approva fornitori, chi esegue audit interni e chi mantiene la documentazione SGQ.

Ruolo	Responsabilita SGQ	Evidenze tipiche
Direzione	Politica, obiettivi, risorse, campo di applicazione, riesame, decisioni e priorita	Politica, riesame, piano obiettivi, registro azioni
Responsabile SGQ	Documenti, audit, NC, KPI, monitoraggio azioni e supporto ai processi	Lista documenti, piani audit, rapporti, registri NC
Responsabile tecnico	Analisi tecnica, progettazione, sviluppo, test, rilascio e standard tecnici	Piani progetto, requisiti, repository, test, release note
Area commerciale/amministrativa	Offerte, ordini, comunicazioni clienti, archiviazione e supporto amministrativo	Offerte, conferme, email, contratti, fatture
Personale operativo	Esecuzione attivita assegnate, registrazioni, segnalazione problemi e miglioramenti	Ticket, checklist, timesheet, note tecniche

11. Pianificazione, rischi, opportunita e obiettivi - ISO 9001 clausola 6

La pianificazione del SGQ parte da contesto e parti interessate. L organizzazione determina rischi e opportunita che possono influenzare la conformita dei servizi, la soddisfazione del cliente e l efficacia del sistema. La gestione dei rischi non richiede modelli eccessivamente complessi, ma deve essere documentata, coerente, aggiornata e collegata ad azioni concrete. I rischi piu rilevanti per CLOUD3 S.R.L. riguardano requisiti incompleti, difetti software, indisponibilita servizi, sicurezza informatica, dipendenza da fornitori, competenze, protezione dati e controllo delle modifiche.

Rischio	Effetto potenziale	Controlli	Evidenze
Requisiti incompleti o ambigui	Rilavorazioni, ritardi, contestazioni cliente	Checklist requisiti, conferma scritta, prototipi, verbali	Ticket/progetto con requisiti approvati
Difetti software in rilascio	Disservizi, reclami, perdita fiducia	Test, code review, ambiente staging, release note	Report test e approvazione rilascio
Indisponibilita hosting o servizi esterni	Interruzione servizio e impatto cliente	Monitoraggio, backup, fornitori qualificati, escalation	Log, report, ticket fornitore
Accessi non controllati	Rischio privacy e sicurezza	Ruoli, credenziali nominali, revoca accessi, tracciamento	Registro accessi o evidenza tecnica
Competenze obsolete	Qualita tecnica insufficiente	Piano formazione, autoaggiornamento, condivisione know-how	Matrice competenze e registri formazione
Fornitore critico non performante	Ritardi, servizi non conformi	Qualifica, monitoraggio, piani alternativi	Valutazioni fornitori
Change request non controllate	Scope creep, conflitti su costi e tempi	Valutazione impatto, approvazione cliente, aggiornamento piano	Registro modifiche e comunicazioni

11.1 Obiettivi qualita e pianificazione

Gli obiettivi qualita devono essere coerenti con la politica, misurabili, monitorati, comunicati e aggiornati. Per una societa ICT di dimensione ridotta, gli obiettivi devono essere pochi ma significativi, collegati a processi reali e sostenuti da dati disponibili. Ogni obiettivo deve indicare responsabile, risorse, frequenza di misura, target, fonte dati e azioni in caso di scostamento.

Obiettivo	Indicatore	Target iniziale	Fonte dati	Responsabile
Ridurre rilavorazioni software	Ticket riaperti / ticket chiusi	<= 8%	Ticketing e report assistenza	Responsabile tecnico
Migliorare puntualita rilasci	Rilasci completati entro data concordata	>= 90%	Piani progetto e release note	Direzione/tecnico
Aumentare	Valutazione media	>= 4/5	Questionari o feedback	Direzione

soddisfazione cliente	feedback		strutturati	
Gestire tempestivamente anomalie	Tempo medio prima risposta ticket critici	<= 1 giorno lavorativo	Ticketing/email	Responsabile supporto
Mantenere competenze aggiornate	Ore aggiornamento tecnico per addetto	>= 8 ore/anno	Registro formazione	Direzione
Migliorare controllo fornitori	Fornitori critici valutati	100% annuale	Schede valutazione fornitori	Responsabile SGQ

12. Supporto, risorse, competenza e informazioni documentate - ISO 9001 clausola 7

Le risorse includono persone, infrastrutture, strumenti software, hardware, ambienti di sviluppo e test, repository, sistemi di comunicazione, fornitori, conoscenze e documenti. La Direzione determina le risorse necessarie in base a progetti attivi, carico ticket, competenze richieste, criticita dei clienti e obiettivi del SGQ. La pianificazione delle risorse deve prevenire sovraccarichi e dipendenza non controllata da singole persone.

Le competenze sono centrali per la qualita. Per ogni ruolo devono essere definite competenze minime: analisi requisiti, sviluppo, testing, gestione database, configurazione sistemi, sicurezza di base, privacy, relazione cliente, documentazione e gestione ticket. La competenza puo essere dimostrata da esperienza, formazione, affiancamento, certificazioni, risultati di progetto o valutazione della Direzione.

La consapevolezza riguarda politica qualita, obiettivi, contributo personale, conseguenze delle non conformita e importanza della registrazione delle evidenze. In una organizzazione tecnica e frequente dare priorita alla soluzione del problema rispetto alla documentazione: il SGQ richiede equilibrio, perche una soluzione non tracciata puo diventare un rischio in caso di reclamo, manutenzione futura o audit.

Le informazioni documentate devono essere controllate ma snelle. Sono richiesti identificazione, versione, approvazione, disponibilita, protezione, conservazione e recupero. Per CLOUD3 S.R.L. le evidenze possono essere digitali: email, ticket, repository, documenti tecnici, piani progetto, verbali, report test, screenshot, log, checklist, contratti e report di monitoraggio. Il criterio non e il formato, ma la capacita di dimostrare il requisito.

Categoria risorsa	Descrizione	Controllo SGQ	Registrazione
Persone	Direzione, personale tecnico, supporto amministrativo, collaboratori	Matrice competenze, ruoli, formazione	Schede competenza, registro formazione
Infrastruttura ICT	PC, server, ambienti cloud, repository, strumenti ticket	Accessi, backup, aggiornamenti, disponibilita	Log, inventory, checklist
Ambienti software	Sviluppo, test, staging, produzione	Separazione ambienti, autorizzazione rilascio	Report test, release note
Conoscenza organizzativa	Standard tecnici, lezioni apprese, configurazioni, manuali interni	Condivisione, aggiornamento, archiviazione	Wiki, procedure, note progetto
Documenti e registrazioni	Manuale, procedure, moduli, contratti, ticket, audit	Versionamento, conservazione, protezione	Lista documenti e archivi

13. Pianificazione ed erogazione operativa - ISO 9001 clausola 8

La pianificazione operativa definisce come i servizi vengono trasformati da esigenze del cliente in output conformi. Per CLOUD3 S.R.L. la qualita operativa dipende dalla capacita di tradurre richieste spesso eterogenee in requisiti controllati, piani di lavoro, attivita tecniche verificabili, rilasci approvati e supporto post-consegna. Il processo deve mantenere proporzionalita: progetti complessi richiedono piu pianificazione; interventi semplici possono essere gestiti tramite ticket strutturato.

Ogni incarico deve avere almeno: identificazione del cliente, descrizione richiesta, requisiti principali, criteri di accettazione o chiusura, responsabilita, tempi, eventuali esclusioni, rischi rilevanti, autorizzazioni e registrazioni. L assenza di questi elementi aumenta il rischio di contestazione e rende debole l evidenza audit. La documentazione puo essere raccolta in offerta, conferma ordine, ticket, piano progetto o verbale, purche sia rintracciabile.

Fase operativa	Attivita chiave	Controlli richiesti	Evidenze
Richiesta cliente	Ricezione contatto, analisi esigenza, apertura pratica/ticket	Identificazione cliente e servizio richiesto	Email, ticket, CRM, note chiamata
Revisione requisiti	Chiarimento requisiti espliciti e impliciti, verifica fattibilita	Coerenza tecnica, tempi, risorse, requisiti cogenti	Checklist requisiti, offerta, verbale
Accettazione ordine	Conferma condizioni, tempi, responsabilita, prezzo	Approvazione del cliente e Direzione	Ordine, contratto, email conferma
Pianificazione	Sequenza attivita, assegnazioni, milestone, rischi	Piano proporzionato alla complessita	Piano progetto o backlog
Esecuzione tecnica	Sviluppo, configurazione, consulenza, hosting, assistenza	Standard tecnici, controllo accessi, registrazioni	Repository, ticket, report intervento
Verifica e validazione	Test, controllo requisiti, approvazione cliente se prevista	Criteri accettazione e tracciabilita	Report test, collaudo, release note
Rilascio e chiusura	Messa in produzione, comunicazione, supporto	Autorizzazione e gestione post rilascio	Email rilascio, ticket chiuso, verbale

14. Progettazione e sviluppo software

La progettazione e sviluppo software e un processo centrale e pienamente applicabile alla ISO 9001. Il processo comprende raccolta requisiti, definizione architettura, scelta soluzioni tecniche, pianificazione, implementazione, controllo versioni, verifica, validazione, gestione modifiche, rilascio e manutenzione. L intensita documentale varia in funzione della complessita: un piccolo intervento puo essere documentato nel ticket, mentre un progetto strutturato richiede un piano con requisiti, milestone e criteri di accettazione.

Gli input di progettazione devono essere adeguati, completi, non ambigui e compatibili tra loro. Possono includere requisiti funzionali, requisiti non funzionali, vincoli di sicurezza, privacy, performance, compatibilita, interfacce, requisiti grafici, dati da migrare, requisiti di hosting, SLA, browser supportati, sistemi operativi, licenze, normative applicabili e requisiti di manutenzione. Gli input conflittuali devono essere chiariti prima di procedere.

I controlli di progettazione includono riesami tecnici, verifica delle scelte architetturali, valutazione dei rischi, controllo delle dipendenze software, code review ove applicabile, test unitari o funzionali, test di regressione, validazione con il cliente o utente, verifica sicurezza di base, controllo configurazioni e gestione delle modifiche. La tracciabilita deve collegare requisiti, output, test e rilascio.

Gli output di progettazione possono includere codice sorgente, configurazioni, database, pagine web, documentazione tecnica, manuali utente, script, specifiche API, release note, piani di deployment e report di test. Gli output devono essere adeguati per le fasi successive e devono indicare, ove necessario, requisiti essenziali per uso corretto, sicurezza, manutenzione e supporto.

Elemento 8.3	Applicazione in CLOUD3 S.R.L.	Evidenza oggettiva attesa
Pianificazione D&D	Definizione fasi, responsabilita, strumenti, tempi e controlli proporzionati al progetto	Piano progetto, backlog, ticket, milestones
Input D&D	Requisiti cliente, vincoli tecnici, requisiti cogenti, compatibilita e sicurezza	Scheda requisiti, email, specifiche, verbali
Controlli D&D	Riesami, verifiche, validazioni, test, code review, controllo difetti	Report test, checklist, merge request, log
Output D&D	Software, configurazioni, documentazione, release note, istruzioni	Repository, pacchetto rilascio, manuali, release note
Modifiche D&D	Change request, analisi impatto, autorizzazione, aggiornamento requisiti e test	Registro modifiche, ticket, approvazione cliente

15. Hosting, assistenza e servizi ICT continuativi

I servizi continuativi richiedono controllo diverso rispetto al progetto. La qualita si misura nella disponibilita, nella tempestivita di risposta, nella correttezza della diagnosi, nella gestione delle priorita, nella comunicazione al cliente e nella prevenzione della ricorrenza. Gli accordi di servizio devono definire cosa e incluso, quali sono i tempi di risposta, quali sono i canali di comunicazione, come sono gestite urgenze e quali attivita dipendono da fornitori esterni.

L hosting specialistico e i servizi applicativi in rete possono dipendere da infrastrutture proprie o di terzi. Il SGQ richiede che siano identificati i fornitori critici, monitorati gli elementi essenziali del servizio, mantenuti backup o misure di continuita proporzionate, controllati gli accessi e registrati incidenti, disservizi e azioni correttive. La responsabilita verso il cliente deve essere chiara, in particolare quando l infrastruttura e esterna.

L assistenza deve essere tracciata. Ogni ticket dovrebbe indicare richiedente, data, descrizione, priorita, classificazione, responsabile, azioni svolte, esito, tempo di risposta, tempo di chiusura e comunicazioni rilevanti. Per anomalie ricorrenti o critiche, il ticket deve alimentare analisi causa, azione correttiva o miglioramento preventivo.

Il supporto post-rilascio e parte della qualita del servizio. Dopo un rilascio rilevante, devono essere previsti controlli iniziali, disponibilita a gestire anomalie, raccolta feedback e, se necessario, rollback o patch correttiva. La chiusura del rilascio non deve avvenire solo per completamento tecnico, ma quando i criteri di accettazione sono soddisfatti o quando il cliente accetta eventuali limitazioni residue.

Servizio	Rischio principale	Controllo	Registrazione
Hosting web/applicativo	Indisponibilita, perdita dati, degrado prestazioni	Monitoraggio, backup, fornitori qualificati, escalation	Log, report disponibilita, ticket
Assistenza software	Ritardi, diagnosi incompleta, ticket riaperti	Classificazione priorita, tracciamento, verifica chiusura	Ticket e comunicazioni
Manutenzione evolutiva	Modifiche non autorizzate o impatto su funzionalita esistenti	Change request, test regressione, release note	Registro modifiche e report test
Configurazione sistemi	Configurazioni non documentate o non replicabili	Checklist, backup configurazioni, approvazione cliente	Report intervento
Formazione tecnica	Contenuti non adeguati al bisogno	Programma corso, valutazione partecipanti, feedback	Registro presenze e questionari

16. Controllo dei fornitori e dei servizi esterni

I fornitori esterni possono incidere direttamente sulla capacita di CLOUD3 S.R.L. di erogare servizi conformi. Rientrano in questa categoria fornitori di hosting, cloud, domini, connettivita, licenze software, componenti, hardware, servizi professionali, consulenti specialistici, piattaforme di comunicazione, strumenti di sviluppo e servizi di sicurezza. La criticita del fornitore determina il livello di controllo necessario.

La qualifica del fornitore non deve essere burocratica. Deve considerare affidabilita, competenza, continuita, sicurezza, supporto, condizioni contrattuali, disponibilita di SLA, reputazione, esperienza pregressa e impatto sul cliente finale. Per fornitori marginali puo bastare il controllo dell ordine e dell output; per fornitori critici occorre monitoraggio periodico e piani alternativi.

Le informazioni comunicate ai fornitori devono essere chiare: oggetto della fornitura, requisiti tecnici, tempi, standard attesi, requisiti privacy/sicurezza, accessi autorizzati, modalita di verifica, responsabilita e criteri di accettazione. Quando il fornitore tratta dati o accede a sistemi cliente, devono essere valutate le condizioni privacy e riservatezza.

Tipo fornitore	Criticita	Criteri di valutazione	Evidenze
Hosting/cloud	Alta se sostiene servizi cliente	Uptime, supporto, sicurezza, backup, SLA, incidenti	Contratti, report, ticket, valutazioni
Licenze software/tool	Media/alta secondo uso	Validita licenza, supporto, aggiornamenti, sicurezza	Ordini, fatture, contratti
Hardware	Media	Conformita, garanzia, tempi consegna, assistenza	Ordini, DDT, collaudi
Consulenti/subfornitori	Variabile	Competenza, riservatezza, puntualita, qualita output	Accordi, CV, report attivita
Servizi generali	Bassa/media	Affidabilita e conformita amministrativa	Ordini e valutazioni se critici

17. Valutazione delle prestazioni - ISO 9001 clausola 9

La valutazione delle prestazioni trasforma il SGQ da sistema documentale a sistema gestionale. CLOUD3 S.R.L. deve stabilire cosa monitorare, come misurarlo, con quale frequenza, chi analizza i dati e quali decisioni sono prese in caso di scostamento. Gli indicatori devono essere pochi, rilevanti e collegati ai rischi maggiori: soddisfazione cliente, puntualita, difetti, ticket, fornitori, formazione, audit e azioni correttive.

La soddisfazione del cliente puo essere monitorata con questionari, feedback post-commessa, email, rinnovi, reclami, ticket, valutazioni informali registrate e indicatori di fidelizzazione. In un contesto B2B di piccole dimensioni, la relazione diretta e un vantaggio, ma deve essere trasformata in evidenze utili al riesame.

L analisi dei dati deve portare a conclusioni. Non e sufficiente raccogliere numeri: occorre valutare tendenze, cause, impatti e azioni. Se aumentano i ticket riaperti, occorre verificare test, requisiti o competenze; se un fornitore genera ritardi, occorre rivalutazione; se i reclami riguardano comunicazione, occorre migliorare offerte, conferme o aggiornamenti al cliente.

Indicatore	Frequenza	Metodo di calcolo	Uso nel riesame
Soddisfazione cliente	Annuale o post-progetto	Media feedback / valutazioni raccolte	Valutare efficacia relazione cliente
Ticket riaperti	Mensile/trimestrale	Ticket riaperti diviso ticket chiusi	Individuare cause di rilavorazione
Puntualita rilasci	Per progetto	Rilasci puntuali diviso rilasci pianificati	Migliorare pianificazione e stime
NC e reclami	Continuo/riesame	Numero, gravita, causa, stato azioni	Priorita di miglioramento
Fornitori critici valutati	Annuale	Valutazioni effettuate su fornitori critici	Gestione rischio esterno
Formazione completata	Annuale	Ore/attivita completate rispetto a pianificate	Adeguatezza competenze

18. Audit interno e riesame della Direzione

L audit interno verifica se il SGQ e conforme ai requisiti ISO 9001, ai requisiti interni e ai requisiti applicabili ai servizi. Deve essere pianificato a intervalli definiti e coprire progressivamente tutte le clausole e tutti i processi. Per un organizzazione piccola e possibile effettuare audit integrati e concentrati, purche siano documentati criteri, campo, auditor, evidenze, risultanze e azioni.

L auditor interno deve mantenere imparzialita rispetto all attivita auditata. Se non e possibile garantire piena indipendenza interna, la Direzione puo valutare supporto esterno o audit incrociati, mantenendo comunque responsabilita interna sulle decisioni e sulle azioni correttive. L audit deve essere basato su evidenze: non basta confermare che una procedura esiste, occorre verificare una commessa, un ticket, un rilascio, un fornitore, una formazione o una NC.

Il riesame della Direzione e il momento in cui i dati del SGQ diventano decisioni. Gli input includono stato azioni precedenti, cambiamenti del contesto, prestazioni dei processi, soddisfazione cliente, obiettivi, NC, audit, reclami, fornitori, adeguatezza risorse, rischi, opportunita e miglioramenti. Gli output devono includere decisioni, azioni, responsabilita, scadenze, risorse e modifiche al sistema se necessarie.

19. Miglioramento, NC e azioni correttive - ISO 9001 clausola 10

Il miglioramento nasce da dati, problemi, opportunita, reclami, errori, idee, audit e cambiamenti. CLOUD3 S.R.L. deve selezionare opportunita che migliorano servizio, processi, soddisfazione cliente e riduzione rischi. Il miglioramento puo essere tecnico, organizzativo o documentale: introduzione di checklist, automazione test, revisione template offerta, aggiornamento formazione, migliore gestione fornitori o rafforzamento backup.

Quando si verifica una non conformita, l organizzazione deve reagire al problema, controllarlo, correggerlo, gestire le conseguenze e valutare se sia necessaria un azione per eliminare la causa. Non tutte le anomalie richiedono azione correttiva formale; tuttavia reclami, errori ricorrenti, difetti gravi, disservizi critici e rilievi di audit devono essere analizzati con metodo.

L analisi della causa deve evitare risposte superficiali. Nei servizi ICT le cause possono essere requisiti ambigui, test insufficienti, modifica non autorizzata, fornitore non affidabile, comunicazione incompleta, competenza carente, assenza di checklist, ambiente di test non rappresentativo o sovraccarico operativo. L azione correttiva deve essere proporzionata alla causa e deve essere verificata per efficacia.

Tipo evento	Trattamento immediato	Analisi causa	Azione correttiva/miglioramento
Difetto software bloccante	Correzione, comunicazione cliente, eventuale rollback	Requisiti/test/release	Rafforzare test o controllo rilascio
Reclamo cliente	Risposta formale e contenimento	Processo, comunicazione, aspettative	Modifica procedura/offerta/ticket
Ritardo progetto	Riprogrammazione e comunicazione	Stima, risorse, change request	Migliorare pianificazione
Disservizio hosting	Ripristino e monitoraggio	Fornitore, configurazione, backup	Rivalutazione fornitore o continuita
Rilievo audit	Correzione documentale/operativa	Sistema, responsabilita, formazione	Azione con verifica efficacia

20. Conformita legislativa, privacy, sicurezza e requisiti cogenti

La conformita legislativa e contrattuale e parte integrante della qualita del servizio. Nei servizi ICT, i requisiti cogenti possono incidere su privacy, sicurezza, conservazione dati, licenze software, proprieta intellettuale, contratti, responsabilita, salute e sicurezza sul lavoro, adempimenti societari e rapporti con collaboratori. Il SGQ non sostituisce sistemi specialistici come ISO 27001, ma assicura che i requisiti rilevanti siano considerati nella pianificazione e nell erogazione dei servizi.

La privacy assume particolare rilievo quando CLOUD3 S.R.L. accede a sistemi, dati o ambienti dei clienti. Devono essere chiariti ruoli privacy, istruzioni, autorizzazioni, credenziali, finalita di accesso, misure di riservatezza e modalita di gestione dati. Le informazioni del cliente devono essere trattate con cura, protette e restituite o cancellate secondo accordi e requisiti applicabili.

La sicurezza informatica, pur non essendo oggetto esclusivo della ISO 9001, influenza direttamente la qualita percepita e la conformita del servizio. Il manuale richiede controlli minimi: gestione accessi, password, backup, aggiornamenti, separazione ambienti, controllo fornitori, registrazione incidenti, limitazione dei privilegi e attenzione alle vulnerabilita nelle soluzioni sviluppate o mantenute.

Ambito	Requisito rilevante	Controllo SGQ	Evidenza
Societario	Identificazione impresa, adempimenti camerali e legali	Mantenimento dati aziendali aggiornati	Visura, PEC, registri
Privacy	Trattamento dati personali e accesso a dati cliente	Ruoli, istruzioni, riservatezza, accessi	Contratti, informative, registri accesso
Sicurezza lavoro	Ambiente di lavoro sicuro e conforme	DVR, formazione, attrezzature	Documenti sicurezza e formazione
Licenze software	Uso legittimo di software, librerie e componenti	Verifica licenze e condizioni	Elenco tool/licenze, ordini
Contratti/SLA	Impegni chiari verso clienti e fornitori	Revisione requisiti e condizioni	Offerte, contratti, ticket
Proprieta intellettuale	Uso e titolarita di codice, contenuti, materiali	Clausole contrattuali e controllo componenti	Contratti, repository, licenze

21. Matrice processi - clausole - evidenze

La matrice seguente collega requisiti ISO 9001, processi aziendali e registrazioni. Essa e utilizzabile come guida audit-ready per preparare audit interni, stage 2, sorveglianze e riesami. La logica e mostrare non solo la presenza di documenti, ma la relazione tra requisito, processo, evidenza e risultato atteso.

Clausola	Requisito	Processo collegato	Evidenza minima
4.1	Contesto	P01 Direzione	Analisi contesto, verbale riesame, registro rischi
4.2	Parti interessate	P01/P02	Matrice parti interessate, requisiti cliente, contratti
4.3	Campo SGQ	P01	Manuale SGQ, dichiarazione campo, giustificazioni applicabilita
4.4	Processi SGQ	Tutti	Mappa processi, schede processo, KPI
5.1	Leadership	P01	Politica, obiettivi, risorse, comunicazioni
5.2	Politica	P01/P11	Politica approvata e comunicata
5.3	Ruoli	P01/P10	Organigramma, mansionario, RACI
6.1	Rischi e opportunita	P01/P12	Registro rischi, azioni, verifica efficacia
6.2	Obiettivi	P01/P12	Piano obiettivi, KPI, monitoraggi
7.1	Risorse	P10/P06	Inventario, strumenti, backup, infrastrutture
7.2	Competenza	P10	Matrice competenze, formazione, evidenze efficacia
7.5	Informazioni documentate	P11	Lista documenti, versioni, archiviazione
8.2	Requisiti cliente	P02/P03	Offerte, ordini, requisiti, comunicazioni
8.3	Progettazione e sviluppo	P04/P05	Input, output, test, validazione, modifiche
8.4	Fornitori	P09	Qualifiche, ordini, valutazioni, SLA
8.5	Erogazione servizio	P04/P06/P07/P08	Ticket, report intervento, release, corsi
8.6	Rilascio	P05	Approvazioni rilascio, collaudi, release note
8.7	Output non conformi	P12	Registro NC, reclami, correzioni
9.1	Monitoraggio	P12	KPI, report, analisi dati
9.2	Audit interno	P12	Piano audit, checklist, rapporto

			audit
9.3	Riesame	P01	Verbale riesame e piano azioni
10.2	Azioni correttive	P12	NC, cause, azioni, verifica efficacia
10.3	Miglioramento	P01/P12	Piano miglioramento, lezioni apprese

22.01 Scheda processo - Direzione e governance del SGQ

Scopo del processo: assicurare che politica, obiettivi, risorse, rischi e decisioni siano coerenti con la strategia e con il campo di applicazione Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Direzione. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Contesto, parti interessate, KPI, esiti audit, reclami, rischi, opportunita	Definizione politica, obiettivi, risorse, riesame, priorita, azioni	Politica, obiettivi, verbali, piano azioni, decisioni documentate

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
mancata coerenza tra strategia e processi, obiettivi non misurabili, risorse insufficienti	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	obiettivi raggiunti, azioni chiuse, KPI riesaminati	Verbali riesame, piano obiettivi, registro azioni

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.02 Scheda processo - Commerciale, offerte e contratti

Scopo del processo: garantire che le richieste dei clienti siano comprese, valutate e trasformate in offerte o accordi chiari e sostenibili Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Direzione/Area commerciale. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Richieste clienti, informazioni tecniche, disponibilita risorse, listini, condizioni	Analisi esigenza, fattibilita, preventivazione, revisione, invio offerta, accettazione	Offerte, contratti, ordini, conferme email, requisiti preliminari

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
requisiti incompleti, promesse non sostenibili, esclusioni non chiarite, prezzi non coerenti	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	offerte convertite, reclami commerciali, modifiche post-ordine	Offerta, ordine, email cliente, checklist requisiti

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.03 Scheda processo - Analisi requisiti e pianificazione commessa

Scopo del processo: tradurre l esigenza del cliente in requisiti operativi, piano di lavoro, risorse, tempi e criteri di accettazione Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile tecnico/Direzione. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Ordine, offerta, esigenze utente, vincoli tecnici, sistemi esistenti	Raccolta requisiti, analisi fattibilita, stima, assegnazioni, milestones	Piano progetto, backlog, requisiti approvati, criteri accettazione

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
ambiguita requisiti, sottostima tempi, mancata identificazione vincoli o dipendenze	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	rispetto tempi, change request, rilavorazioni	Piano progetto, verbali, backlog, ticket

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.04 Scheda processo - Progettazione software e architettura

Scopo del processo: definire soluzioni software coerenti con requisiti, sicurezza, manutenibilita, performance e vincoli cliente Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile tecnico. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Requisiti, tecnologie, standard, vincoli infrastrutturali, dati	Analisi architettura, scelta strumenti, definizione moduli, riesame tecnico	Specifiche tecniche, architettura, decisioni, stima rischi

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
scelte tecniche non sostenibili, dipendenze non controllate, requisiti non tracciati	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	difetti in test, modifiche architetturali tardive	Specifiche, note tecniche, diagrammi, decision log

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.05 Scheda processo - Sviluppo, configurazione e versionamento

Scopo del processo: realizzare software, configurazioni e personalizzazioni in modo tracciabile, controllato e verificabile Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Team tecnico. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Specifiche, backlog, ambiente sviluppo, repository, standard coding	Codifica, configurazione, commit, review, gestione branch, documentazione tecnica	Codice, configurazioni, build, note sviluppo, versioni

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
modifiche non tracciate, errore umano, conflitti versione, codice non manutenibile	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	ticket completati, errori post-rilascio, commit tracciati	Repository, commit, checklist sviluppo, ticket

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.06 Scheda processo - Test, verifica e validazione

Scopo del processo: confermare che output software e servizi soddisfino requisiti specificati e uso previsto Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile tecnico. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Output sviluppo, casi test, criteri accettazione, ambiente test	Test funzionali, regressione, controllo requisiti, correzione difetti, validazione cliente	Report test, esiti, difetti, approvazioni, release candidate

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
test insufficienti, ambiente non rappresentativo, difetti bloccanti in produzione	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	difetti per rilascio, ticket riaperti, test completati	Report test, checklist, verbali collaudo

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.07 Scheda processo - Rilascio, deployment e post-rilascio

Scopo del processo: mettere in produzione output approvati riducendo rischi di interruzione e garantendo comunicazione al cliente Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile tecnico/Direzione. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Output validato, approvazione, piano rilascio, backup, finestra intervento	Backup, deployment, verifica, comunicazione, monitoraggio iniziale, chiusura	Release note, conferma rilascio, log, ticket chiuso

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
rilascio non autorizzato, indisponibilita servizio, mancato rollback, comunicazione incompleta	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	rilasci puntuali, incidenti post-rilascio, rollback	Release note, email cliente, log deployment

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.08 Scheda processo - Hosting e servizi continuativi

Scopo del processo: assicurare disponibilita, tracciabilita e gestione controllata dei servizi erogati in continuita Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile tecnico. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Contratti/SLA, ambienti, fornitori, monitoraggio, richieste cliente	Monitoraggio, backup, aggiornamenti, gestione incidenti, escalation fornitori	Log, report disponibilita, ticket, azioni preventive

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o

conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
dipendenza da fornitori, downtime, perdita dati, accessi non controllati	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	uptime, incidenti, tempi ripristino	Log, ticket, backup report, valutazioni fornitori

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.09 Scheda processo - Assistenza, ticketing e reclami

Scopo del processo: gestire richieste e anomalie del cliente con priorita, comunicazione e chiusura controllata Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile supporto. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Email, chiamate, ticket, reclami, segnalazioni utenti	Classificazione, assegnazione, diagnosi, intervento, verifica, comunicazione, chiusura	Ticket chiusi, reclami trattati, comunicazioni, azioni correttive

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
priorita errata, tempi lunghi, ticket riaperti, reclami non analizzati	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	tempo risposta, ticket riaperti, reclami chiusi	Ticket, registro reclami, email, report assistenza

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.10 Scheda processo - Formazione informatica

Scopo del processo: erogare formazione non legalmente riconosciuta con contenuti coerenti, docenti competenti e feedback misurato Il processo e governato con approccio proporzionato alla dimensione di

CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Direzione/Docente. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Fabbisogni, programma, partecipanti, materiali, strumenti didattici	Preparazione corso, erogazione, verifica presenze, feedback, aggiornamento contenuti	Programma, materiali, registro presenze, questionari

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
contenuti non aggiornati, obiettivi non chiari, feedback non raccolto	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	soddisfazione partecipanti, corsi completati	Programmi, presenze, feedback, attestazioni se previste

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.11 Scheda processo - Fornitori e approvvigionamenti

Scopo del processo: selezionare e monitorare fornitori critici per assicurare conformita dei servizi acquistati Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Direzione/Responsabile SGQ. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Esigenza acquisto, requisiti tecnici, budget, criticita servizio	Qualifica, richiesta offerta, ordine, verifica fornitura, valutazione periodica	Ordini, valutazioni fornitori, contratti, evidenze controllo

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni

fornitore non affidabile, SLA non chiaro, licenze non conformi	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	fornitori valutati, disservizi fornitore	Elenco fornitori, ordini, schede valutazione

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.12 Scheda processo - Gestione documentale e registrazioni

Scopo del processo: assicurare disponibilita, protezione, versionamento e recuperabilita delle informazioni documentate Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile SGQ. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Documenti SGQ, procedure, moduli, registrazioni, versioni	Creazione, approvazione, distribuzione, archiviazione, conservazione, ritiro obsoleti	Lista documenti, archivi, revisioni, registri

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
uso documenti obsoleti, perdita evidenze, accessi non autorizzati	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	documenti aggiornati, evidenze recuperabili	Lista documenti, registro revisioni, archivi

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.13 Scheda processo - Risorse umane, competenza e consapevolezza

Scopo del processo: garantire competenze adeguate a ruoli tecnici e gestionali e mantenere consapevolezza SGQ Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Direzione. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
Ruoli, attivita, tecnologie, requisiti cliente, obiettivi	Valutazione competenze, formazione, affiancamento, verifica efficacia	Matrice competenze, piani formazione, registri

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
competenze obsolete, dipendenza da singola persona, formazione non efficace	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla Direzione quando il rischio supera la soglia accettabile.	ore formazione, competenze coperte	Matrice competenze, attestati, registri aggiornamento

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

22.14 Scheda processo - Audit interno, NC e miglioramento

Scopo del processo: verificare conformita, trattare problemi e trasformare dati in miglioramento strutturato Il processo e governato con approccio proporzionato alla dimensione di CLOUD3 S.R.L. e deve produrre evidenze sufficienti per dimostrare conformita, efficacia e controllo durante audit interni e verifiche esterne.

Responsabile principale: Responsabile SGQ/Direzione. La responsabilita comprende pianificazione, esecuzione o supervisione, gestione delle evidenze, valutazione delle anomalie, comunicazione alla Direzione e proposta di miglioramenti. Quando piu ruoli partecipano al processo, le responsabilita operative sono definite nella pianificazione della commessa, nel ticket o nella comunicazione interna.

Input	Attivita principali	Output
KPI, reclami, audit, NC, osservazioni, opportunita	Pianificazione audit, raccolta evidenze, classificazione rilievi, azioni, verifica efficacia	Rapporto audit, registro NC, piano miglioramento

Il processo deve essere avviato solo quando gli input minimi sono disponibili. Qualora un input sia incompleto, il responsabile deve richiedere chiarimenti o registrare le assunzioni operative. Nel settore ICT, procedere senza requisiti chiariti espone a rilavorazioni e contestazioni; pertanto la fase iniziale del processo ha valore preventivo rispetto alla qualita finale del servizio.

Le attivita sono pianificate e svolte utilizzando strumenti adeguati: email, ticket, repository, checklist, modelli, piani progetto, report e registrazioni tecniche. La scelta dello strumento dipende dalla complessita, ma la registrazione deve sempre consentire di ricostruire chi ha fatto cosa, quando, su quale richiesta, con quale risultato e con quale approvazione.

Gli output devono essere verificati prima della chiusura. La verifica puo consistere in controllo documentale, test funzionale, confronto con requisiti, riesame tecnico, approvazione cliente, controllo amministrativo o conferma del fornitore. L output non verificato non deve essere considerato completato, soprattutto se incide su sistemi in produzione o su impegni contrattuali.

Rischi specifici	Controlli preventivi/correttivi	KPI suggeriti	Registrazioni
azioni non chiuse, cause superficiali, ripetizione problemi	Checklist, riesame, approvazione, tracciabilita ticket/progetto, escalation alla	NC chiuse, azioni efficaci, miglioramenti completati	Piani audit, rapporti, registro NC, azioni

	Direzione quando il rischio supera la soglia accettabile.		

Le non conformita rilevate nel processo devono essere trattate secondo la procedura NC e azioni correttive. Se l anomalia e isolata e priva di impatto rilevante, puo essere sufficiente una correzione registrata; se e ricorrente o critica, occorre analisi causa e azione correttiva. Il responsabile valuta anche se aggiornare rischi, istruzioni operative o competenze.

Il processo e soggetto a audit interno. L auditor verifica campioni reali, non solo documenti descrittivi: una commessa, un ticket, un rilascio, un ordine, un report o una registrazione devono dimostrare l applicazione effettiva delle regole. Eventuali scostamenti sono classificati come NC, osservazioni o opportunita di miglioramento.

Il miglioramento del processo puo derivare da feedback clienti, andamento KPI, reclami, inefficienze, incidenti, ritardi, novita tecnologiche o esigenze del personale. Le azioni di miglioramento devono essere tracciate e riesaminate per verificarne l efficacia nel tempo.

23. Procedure documentate del SGQ

PR-01 Gestione contesto, rischi e opportunita

La procedura disciplina il riesame periodico dei fattori interni ed esterni, delle parti interessate e dei rischi/opportunita. La Direzione aggiorna il registro almeno annualmente e quando avvengono cambiamenti rilevanti. Gli output sono collegati a obiettivi, azioni e risorse.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-02 Gestione offerte, ordini e requisiti cliente

La procedura stabilisce come ricevere richieste, chiarire requisiti, valutare fattibilita, formulare offerte, confermare ordini e gestire modifiche contrattuali. Ogni incarico deve avere criteri di accettazione e responsabilita definite.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-03 Progettazione e sviluppo software

La procedura governa input, pianificazione, controlli, output, modifiche, validazione e rilascio. Il livello di formalizzazione varia secondo criticita, ma la tracciabilita requisiti-output-test deve essere mantenuta.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-04 Gestione ticket, assistenza e reclami

La procedura definisce apertura, classificazione, assegnazione, gestione, comunicazione e chiusura dei ticket. I reclami sono trattati come input di miglioramento e possono generare azioni correttive.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo,	Decisioni, attivita controllate,	Modulo applicabile, registro,	Secondo evento, mensile,

requisiti ISO, requisiti cliente, evidenze operative	registrazioni aggiornate, azioni correttive o migliorative	ticket, verbale, checklist, report o email tracciata	trimestrale o annuale in base alla procedura

PR-05 Gestione fornitori

La procedura definisce criteri di qualifica, approvvigionamento, controllo e rivalutazione dei fornitori, con particolare attenzione a hosting, licenze, cloud, servizi tecnici e subfornitori.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-06 Gestione documentale

La procedura stabilisce identificazione, revisione, approvazione, distribuzione, protezione, archiviazione e conservazione delle informazioni documentate.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-07 Audit interno

La procedura definisce pianificazione, criteri, campo, esecuzione, raccolta evidenze, rapporto, classificazione rilievi e monitoraggio azioni.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-08 Non conformita e azioni correttive

La procedura definisce correzione, contenimento, analisi causa, azione, responsabilita, scadenza, verifica efficacia e aggiornamento rischi.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-09 Riesame della Direzione

La procedura disciplina input, output, responsabilita, registrazioni e frequenza del riesame, garantendo decisioni basate su dati e priorita.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

PR-10 Formazione e competenze

La procedura definisce criteri per determinare competenze, pianificare formazione, verificare efficacia e aggiornare la matrice competenze.

Modalita operativa: il responsabile del processo raccoglie gli input, verifica completezza e correttezza, applica i criteri definiti dal manuale, produce le registrazioni minime e segnala alla Direzione eventuali criticita. Le registrazioni devono essere conservate nel repository o nell archivio definito dalla lista documenti. In caso di dubbio, prevale il principio di tracciabilita: deve essere possibile ricostruire decisione, data, responsabile, requisito e risultato.

Controlli: la procedura e verificata tramite audit interno, campionamento di registrazioni, confronto con KPI e verifica delle azioni derivanti da reclami, anomalie o osservazioni. Le modifiche alla procedura sono approvate dalla Direzione e comunicate alle persone interessate.

Input	Output	Registrazioni	Frequenza controllo
Richieste, dati di processo, requisiti ISO, requisiti cliente, evidenze operative	Decisioni, attivita controllate, registrazioni aggiornate, azioni correttive o migliorative	Modulo applicabile, registro, ticket, verbale, checklist, report o email tracciata	Secondo evento, mensile, trimestrale o annuale in base alla procedura

Politica per la Qualita

CLOUD3 S.R.L. si impegna a fornire servizi ICT, software, web, hosting, consulenza e formazione informatica conformi ai requisiti concordati con il cliente, ai requisiti cogenti applicabili e agli obiettivi interni di affidabilita, competenza e miglioramento. La qualita e intesa come capacita di comprendere correttamente le esigenze, tradurle in soluzioni tecniche sostenibili, controllare le modifiche, verificare gli output, comunicare con trasparenza e mantenere nel tempo un rapporto professionale fondato su fiducia ed evidenze.

La Direzione promuove orientamento al cliente, risk-based thinking, competenza tecnica, sicurezza e riservatezza delle informazioni, puntualita, tracciabilita delle decisioni, controllo dei fornitori e miglioramento continuo. Ogni persona coinvolta nei processi deve contribuire alla qualita registrando le attivita rilevanti, segnalando anomalie, rispettando le procedure e proponendo miglioramenti.

La politica e riesaminata periodicamente per assicurare coerenza con contesto, strategia, campo di applicazione, requisiti del mercato e risultati del SGQ. Essa costituisce il quadro per definire obiettivi misurabili e per valutare l efficacia del sistema nel tempo.

24. Allegati e modelli di registrazione

Gli allegati seguenti costituiscono modelli utilizzabili per generare evidenze. Possono essere mantenuti in formato elettronico e adattati alla dimensione del progetto o del servizio. L obiettivo non e produrre carta, ma garantire che le evidenze minime siano sempre disponibili, leggibili, protette e rintracciabili.

Modulo	Contenuti minimi
M-01 Registro rischi e opportunita	Rischio/opportunita, causa, effetto, probabilita, impatto, livello, azione, responsabile, scadenza, stato, verifica efficacia
M-02 Matrice parti interessate	Parte interessata, requisito, impatto, metodo monitoraggio, evidenza, responsabile
M-03 Scheda requisiti cliente	Cliente, richiesta, requisiti funzionali/non funzionali, esclusioni, vincoli, criteri accettazione, approvazione
M-04 Piano progetto	Fasi, milestone, risorse, responsabilita, rischi, deliverable, test, rilascio, comunicazioni
M-05 Checklist test e rilascio	Versione, ambiente, casi test, esiti, difetti, backup, approvazione, release note
M-06 Registro ticket/reclami	ID, cliente, data, priorita, descrizione, assegnatario, azione, chiusura, causa, esito
M-07 Valutazione fornitori	Fornitore, servizio, criticita, criteri, punteggio, problemi, decisione, azioni
M-08 Matrice competenze	Ruolo, competenza richiesta, livello attuale, evidenza, gap, formazione, verifica efficacia
M-09 Piano audit interno	Data, criterio, campo, processi, auditor, persone intervistate, documenti, campioni
M-10 Rapporto audit interno	Evidenze, conformita, NC, osservazioni, raccomandazioni, azioni, responsabili
M-11 Registro NC e azioni correttive	NC, requisito, descrizione, correzione, causa, azione, responsabile, scadenza, efficacia
M-12 Verbale riesame Direzione	Input ISO 9001, dati, decisioni, risorse, obiettivi, rischi, output, piano azioni

25. Piano di mantenimento della certificazione

Il mantenimento della certificazione richiede continuita. Dopo il conseguimento del certificato, CLOUD3 S.R.L. deve evitare che il SGQ resti fermo al momento dell audit iniziale. Le attivita minime annuali comprendono aggiornamento contesto e rischi, monitoraggio obiettivi, audit interno, riesame della Direzione, valutazione fornitori critici, aggiornamento competenze, verifica documenti, analisi reclami e chiusura delle azioni correttive.

La sorveglianza deve poter trovare un sistema vivo. Per questo il manuale prevede scadenze semplici: KPI almeno trimestrali o semestrali per processi critici, riesame annuale, audit interno annuale, valutazione fornitori critici annuale, aggiornamento formazione annuale, revisione rischi annuale o al verificarsi di eventi significativi. Le evidenze devono essere archiviate in modo ordinato.

La Direzione deve garantire che nuove attivita, nuovi clienti, nuovi servizi, cambi infrastrutturali e nuove tecnologie siano valutati rispetto al campo di applicazione. Se CLOUD3 S.R.L. introduce servizi con rischi o requisiti diversi, il SGQ deve essere aggiornato prima che tali servizi diventino consolidati.

Attivita	Frequenza	Responsabile	Output
Monitoraggio KPI	Trimestrale/semestrale	Responsabile SGQ/Direzione	Report KPI e azioni
Audit interno completo	Annuale	Auditor interno qualificato	Rapporto audit e rilievi
Riesame Direzione	Annuale	Direzione	Verbale riesame e piano azioni
Valutazione fornitori critici	Annuale o per evento	Direzione/SGQ	Schede valutazione
Aggiornamento rischi	Annuale o per cambiamento	Direzione/SGQ	Registro rischi aggiornato
Verifica documenti SGQ	Annuale	Responsabile SGQ	Lista documenti aggiornata
Formazione e competenze	Annuale o per nuova esigenza	Direzione	Matrice e registri formazione
Analisi reclami/NC	Continuo e riesame	Responsabile processo	Registro NC e azioni

26. Appendice A - Registro rischi e opportunita

ID	Rischio/ opportunita	Effetto	Prob.	Impatto	Controllo/ azione	Resp.	Stato
R01	Requisiti cliente incompleti	Rilavorazione, ritardi, contestazioni	Media	Alta	Checklist requisiti, conferma cliente, verbale	Responsabile tecnico	Aperto/ monitorato
R02	Difetti applicativi in produzione	Disservizio e reclamo	Media	Alta	Test, staging, release note, rollback	Responsabile tecnico	Aperto/ monitorato
R03	Perdita o indisponibilita dati	Interruzione servizio	Bassa/media	Alta	Backup, controllo accessi, fornitori affidabili	Responsabile tecnico	Monitorato
R04	Fornitore hosting critico non performante	Downtime e ritardi	Media	Alta	Qualifica, SLA, monitoraggio, piano alternativo	Direzione	Monitorato
R05	Competenza tecnica non aggiornata	Errore tecnico o inefficienza	Media	Media	Formazione, studio, affiancamento	Direzione	Monitorato
R06	Change request non formalizzate	Conflitti economici e di scopo	Media	Media/alta	Registro modifiche, approvazione cliente	Direzione/ tecnico	Monitorato
R07	Accessi non revocati o non controllati	Rischio sicurezza/privacy	Bassa/media	Alta	Account nominali, revoca, limitazione privilegi	Responsabile tecnico	Monitorato
R08	Documentazione tecnica insufficiente	Difficolta manutenzione	Media	Media	Checklist documentale, note progetto	Responsabile tecnico	Monitorato
R09	Sovraccarico operativo	Ritardi e calo qualita	Media	Media	Pianificazione priorita, monitoraggio carico	Direzione	Monitorato
R10	Opportunita automazione test	Riduzione difetti e tempi verifica	Media	Positivo	Valutare strumenti e casi ripetitivi	Responsabile tecnico	Da valutare
R11	Opportunita standardizzazione offerte	Riduzione ambiguita requisiti	Alta	Positivo	Template offerte e scheda requisiti	Direzione	Da attuare
R12	Opportunita knowledge base supporto	Riduzione tempi risposta	Media	Positivo	FAQ interne e procedure ricorrenti	Responsabile supporto	Da attuare

27. Appendice B - Obiettivi e KPI

Obiettivo	Indicatore	Formula	Target	Fonte	Azione se non raggiunto
Qualita sviluppo	Difetti post-rilascio	Numero difetti post-rilascio per release	<= 2 non bloccanti per release significativa	Ticket e report test	Analisi causa e miglioramento test
Puntualita	Consegne nei tempi	Consegne puntuali / consegne pianificate	>= 90%	Piani progetto	Riesame stime e carico
Supporto	Tempo prima risposta	Tempo medio tra richiesta e prima presa in carico	<= 1 giorno lavorativo per critici	Ticket/email	Rivedere priorita e reperibilita
Soddisfazione	Feedback cliente	Media valutazioni raccolte	>= 4/5	Questionari/ feedback	Analisi commenti e reclami
Fornitori	Fornitori critici valutati	Fornitori valutati / fornitori critici	100% annuale	Schede fornitori	Rivalutazione o piani alternativi
Competenze	Aggiornamento tecnico	Ore formazione o aggiornamento per addetto	>= 8 ore/anno	Registro formazione	Piano formazione integrativo
SGQ	Azioni correttive chiuse	Azioni chiuse entro scadenza / azioni pianificate	>= 90%	Registro azioni	Riesame scadenze e responsabilita

28. Appendice C - Piano audit interno

Area audit	Clausole	Criteri	Metodo	Frequenza

Direzione e contesto	4.1, 4.2, 5.1, 6.1, 9.3	Analisi contesto, rischi, obiettivi, riesame	Intervista Direzione e verifica documenti	Annuale
Commerciale e requisiti	8.2	Offerte, ordini, comunicazioni, requisiti	Campione 2 commesse/ticket	Annuale
Progettazione e sviluppo	8.3, 8.5, 8.6	Requisiti, sviluppo, test, rilascio	Campione progetto software o web	Annuale
Hosting e supporto	8.5, 8.7, 9.1	Ticket, incidenti, monitoraggio, reclami	Campione ticket e report	Annuale
Fornitori	8.4	Qualifica, ordini, valutazioni	Campione fornitori critici	Annuale
Risorse e competenze	7.1, 7.2, 7.3	Matrice competenze, formazione, consapevolezza	Intervista e registri	Annuale
Documenti e registrazioni	7.5	Versioni, archivi, conservazione	Verifica lista documenti	Annuale
NC e miglioramento	10.2, 10.3	NC, reclami, azioni, efficacia	Campione azioni	Annuale

29. Appendice D - Riesame della Direzione

Il riesame deve contenere una valutazione completa degli input richiesti dalla ISO 9001:2015. Il verbale non deve limitarsi a dichiarare conformita: deve riportare dati, tendenze, criticita, decisioni, risorse e responsabilita. La tabella seguente puo essere utilizzata come indice operativo del verbale.

Input	Contenuto da valutare	Fonte	Output atteso
Stato azioni precedenti	Azioni aperte/chiuse, ritardi, efficacia	Registro azioni	Confermare chiusura o ripianificare
Cambiamenti contesto	Mercato, tecnologia, normativa, risorse, clienti	Analisi contesto	Aggiornare rischi e obiettivi
Prestazioni processi	KPI e scostamenti	Dashboard KPI	Definire azioni miglioramento
Soddisfazione clienti	Feedback, reclami, rinnovi	Questionari, ticket	Azioni su criticita
NC e azioni correttive	Numero, cause, stato, efficacia	Registro NC	Azioni e risorse
Audit interni/esterni	Rilievi, osservazioni, buone pratiche	Rapporti audit	Piano azioni
Fornitori	Performance e criticita	Schede valutazione	Conferma/rivalutazione
Risorse e competenze	Adeguatezza persone, strumenti, infrastruttura	Matrice competenze	Piano formazione/acquisti
Rischi e opportunita	Livelli, nuovi rischi, opportunita	Registro rischi	Azioni preventive/migliorative
Output riesame	Decisioni, obiettivi, modifiche SGQ, risorse	Verbale riesame	Piano approvato

30. Appendice E - Moduli e registrazioni audit-ready

La presente appendice riporta esempi di contenuti minimi che devono comparire nelle registrazioni. I moduli possono essere implementati in file digitali, fogli di calcolo, sistema ticket, repository o applicativi interni, purche siano controllati, rintracciabili e protetti.

Scheda requisiti cliente

Campo minimo	Descrizione/criterio di compilazione
ID commessa/ticket	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Cliente e referente	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Descrizione esigenza	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Requisiti funzionali	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Requisiti non funzionali	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Vincoli tecnici e normativi	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Esclusioni	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Criteri accettazione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Approvazione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

Checklist rilascio

Campo minimo	Descrizione/criterio di compilazione
Versione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Ambiente	Compilare in modo completo, con dato oggettivo, data,

	responsabile o riferimento documentale quando applicabile.
Backup eseguito	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Test superati	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Difetti aperti accettati	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Autorizzazione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Piano rollback	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Comunicazione cliente	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Esito post-rilascio	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

Registro reclami

Campo minimo	Descrizione/criterio di compilazione
ID reclamo	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Cliente	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Data	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Descrizione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Impatto	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Correzione immediata	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Causa	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Azione correttiva	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Responsabile	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Efficacia	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

Scheda formazione

Campo minimo	Descrizione/criterio di compilazione
Partecipante	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Competenza richiesta	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Attivita formativa	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Data	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Durata	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Docente/fonte	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Evidenza	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Valutazione efficacia	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

Valutazione fornitore

Campo minimo	Descrizione/criterio di compilazione
Fornitore	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Servizio	Compilare in modo completo, con dato oggettivo, data,

	responsabile o riferimento documentale quando applicabile.
Criticita	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Puntualita	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Qualita	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Supporto	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Sicurezza	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Problemi	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Decisione	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Azioni	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

Rapporto audit

Campo minimo	Descrizione/criterio di compilazione
Data	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Auditor	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Criteri	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Campo	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Persone intervistate	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Campioni	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Evidenze	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Rilievi	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Conclusioni	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.
Piano azioni	Compilare in modo completo, con dato oggettivo, data, responsabile o riferimento documentale quando applicabile.

Il modulo deve essere archiviato nel repository o nel sistema applicativo definito. La registrazione e valida ai fini audit se consente di dimostrare requisito, responsabilita, data, decisione e risultato. In caso di registrazioni digitali, screenshot, esportazioni o riferimenti a ticket possono essere utilizzati come evidenza se sono rintracciabili e protetti.

31. Manuale operativo dettagliato per la conduzione del SGQ

La presente sezione sviluppa in modo esteso le istruzioni operative necessarie per rendere il sistema effettivamente applicabile e sostenibile. Ogni istruzione e progettata per una struttura aziendale snella, ma mantiene un livello di presidio sufficiente a dimostrare la conformita in audit di certificazione e sorveglianza. Le istruzioni non devono essere interpretate come burocrazia aggiuntiva: esse definiscono il modo ordinato con cui trasformare le attivita tecniche quotidiane in evidenze affidabili.

Quando una istruzione viene applicata a una commessa semplice, e ammesso utilizzare registrazioni minime, ad esempio un ticket completo, una email di approvazione o una checklist sintetica. Quando la commessa e complessa, critica o continuativa, e necessario produrre evidenze piu strutturate: piano progetto, analisi requisiti, registro modifiche, test, verbali, report e riesame finale. La proporzionalita non elimina il controllo, ma adatta il controllo al rischio.

IO-01 - Ricezione richiesta cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di assicurare che ogni richiesta sia identificata, compresa e indirizzata al processo corretto. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: email, telefonata, richiesta web, contatto diretto, referral, segnalazione cliente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non

realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: richieste perse, interpretazioni incomplete, mancanza di tracciabilita iniziale. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: ticket iniziale, email archiviata, nota contatto, registro opportunita. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	ticket iniziale, email archiviata, nota contatto, registro opportunita
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-02 - Valutazione preliminare di fattibilita

Scopo e campo di applicazione. L istruzione ha lo scopo di valutare se CLOUD3 S.R.L. dispone di competenze, tempi, strumenti e condizioni per assumere l incarico. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: richiesta cliente, dati tecnici preliminari, disponibilita risorse, vincoli tecnologici. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: accettazione di lavori non sostenibili, sovraccarico, sottostima tecnica. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: scheda fattibilita, note interne, riesame offerta. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.

Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	scheda fattibilita, note interne, riesame offerta
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-03 - Formalizzazione dell offerta

Scopo e campo di applicazione. L istruzione ha lo scopo di predisporre offerte chiare, complete e coerenti con requisiti e limiti del servizio. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: requisiti preliminari, stima impegno, listini, condizioni contrattuali. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: ambiguita economiche, contestazioni, inclusioni implicite non gestite. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: offerta firmata, email conferma, revisione commerciale. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	offerta firmata, email conferma, revisione commerciale
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-04 - Riesame del contratto e dell ordine

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare che ordine o accettazione siano coerenti con offerta e requisiti concordati. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: offerta, ordine, comunicazioni cliente, condizioni particolari. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La

sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: discordanze tra offerta e ordine, requisiti modificati senza riesame. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: ordine approvato, email accettazione, checklist contratto. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	ordine approvato, email accettazione, checklist contratto
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-05 - Kick-off operativo della commessa

Scopo e campo di applicazione. L istruzione ha lo scopo di avviare la commessa con ruoli, tempi, canali e responsabilita definiti. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: ordine approvato, requisiti, risorse assegnate, contatti cliente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: avvio disordinato, assenza di referente, priorita non chiare. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: verbale kick-off, piano progetto, comunicazione iniziale. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	verbale kick-off, piano progetto, comunicazione iniziale
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-06 - Raccolta requisiti funzionali

Scopo e campo di applicazione. L istruzione ha lo scopo di raccogliere e strutturare funzioni attese, comportamenti, vincoli e priorita del cliente. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: interviste, documenti cliente, sistemi esistenti, esempi, prototipi. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: requisiti impliciti non chiariti, sviluppo non allineato. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: scheda requisiti, backlog, verbale approvato. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	scheda requisiti, backlog, verbale approvato
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-07 - Requisiti non funzionali e livelli di servizio

Scopo e campo di applicazione. L istruzione ha lo scopo di determinare requisiti di performance, sicurezza, disponibilita, usabilita e compatibilita. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: necessita cliente, infrastruttura, utenti, dati, SLA attesi. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: servizio tecnicamente funzionante ma non adeguato all uso reale. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: specifiche non funzionali, SLA, checklist tecnica. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	specifiche non funzionali, SLA, checklist tecnica
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-08 - Gestione backlog e priorita

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere un elenco ordinato di funzionalita, anomalie, modifiche e priorita. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: requisiti, ticket, feedback cliente, vincoli di progetto. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: perdita di priorita, lavoro non autorizzato, confusione su stato avanzamento. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: backlog, ticket, piano sprint o piano attivita. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	backlog, ticket, piano sprint o piano attivita
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono

state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-09 - Pianificazione tempi e risorse

Scopo e campo di applicazione. L istruzione ha lo scopo di assegnare attivita e risorse in modo compatibile con impegni, competenze e criticita. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: backlog, disponibilita personale, scadenze cliente, rischi. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: ritardi, sovrapposizioni, scarsa visibilita carico lavoro. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: piano commessa, calendario, assegnazioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	piano commessa, calendario, assegnazioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-10 - Analisi privacy e dati cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di identificare dati personali o informazioni riservate trattate durante il servizio. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: sistemi cliente, accessi, database, flussi dati, contratti. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: accessi non regolati, trattamento non autorizzato, perdita riservatezza. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: istruzioni privacy, accordi, registro accessi. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	istruzioni privacy, accordi, registro accessi
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-11 - Analisi sicurezza tecnica preliminare

Scopo e campo di applicazione. L istruzione ha lo scopo di valutare controlli minimi di sicurezza applicabili a soluzioni, ambienti e accessi. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: architettura, hosting, credenziali, librerie, ruoli utente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: vulnerabilita, privilegi eccessivi, esposizione servizi. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: checklist sicurezza, note tecniche, piano mitigazioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	checklist sicurezza, note tecniche, piano mitigazioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono

state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-12 - Definizione architettura software

Scopo e campo di applicazione. L istruzione ha lo scopo di stabilire struttura logica, componenti, interfacce e vincoli della soluzione. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: requisiti, tecnologie disponibili, standard interni, infrastruttura. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: architettura fragile, debito tecnico, dipendenze non gestite. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: specifica architetturale, decision log, diagrammi. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	specifica architetturale, decision log, diagrammi
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-13 - Gestione database e dati applicativi

Scopo e campo di applicazione. L istruzione ha lo scopo di progettare, modificare e mantenere dati con attenzione a integrita, backup e tracciabilita. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: modello dati, requisiti, migrazioni, vincoli, dati esistenti. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: perdita dati, inconsistenza, query non controllate. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output,

registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: schema DB, script, backup, log migrazione. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	schema DB, script, backup, log migrazione
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-14 - Integrazioni API e sistemi terzi

Scopo e campo di applicazione. L istruzione ha lo scopo di governare requisiti, responsabilita, test e limiti delle integrazioni. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: specifiche API, credenziali, ambienti test, documentazione fornitore. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: rottura integrazione, dipendenza esterna, errori dati. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: documentazione API, test integrazione, ticket fornitore. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	documentazione API, test integrazione, ticket fornitore
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-15 - Standard di codifica

Scopo e campo di applicazione. L istruzione ha lo scopo di favorire manutenibilita, leggibilita, sicurezza e uniformita del codice. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua

applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: linguaggi, framework, convenzioni, repository. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: codice non mantenibile, difetti ricorrenti, difficolta di trasferimento know-how. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: linee guida, commit, review, note tecniche. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	linee guida, commit, review, note tecniche
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-16 - Versionamento e controllo repository

Scopo e campo di applicazione. L istruzione ha lo scopo di garantire tracciabilita delle modifiche e possibilita di ripristino. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: codice, configurazioni, branch, commit, rilasci. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: modifiche non tracciate, perdita versione stabile, conflitti. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: repository, commit log, tag release. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	repository, commit log, tag release
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-17 - Code review proporzionata

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare aspetti critici del codice prima di rilascio o merge. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: pull request, modifiche critiche, checklist sviluppo. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: difetti non rilevati, vulnerabilita, non conformita a standard. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: commenti review, approvazione merge, checklist. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	commenti review, approvazione merge, checklist
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-18 - Gestione ambienti sviluppo-test-produzione

Scopo e campo di applicazione. L istruzione ha lo scopo di separare ambienti e ridurre rischi di modifiche non controllate in produzione. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: server, cloud, database, credenziali, configurazioni. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: test su produzione, contaminazione dati, downtime. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: inventario ambienti, accessi, procedure deployment. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	inventario ambienti, accessi, procedure deployment
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-19 - Piano di test

Scopo e campo di applicazione. L istruzione ha lo scopo di definire prove necessarie in base a requisiti e rischio della modifica. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: requisiti, casi d uso, difetti storici, criteri accettazione. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: test insufficienti o non ripetibili. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: piano test, casi test, esiti. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti

	applicabili.
Registrazione minima	piano test, casi test, esiti
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-20 - Test funzionale

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare che le funzioni realizzate soddisfino requisiti definiti. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: software, requisiti, dati prova, ambiente test. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: funzioni incomplete, comportamenti inattesi. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: checklist test, screenshot, report difetti. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	checklist test, screenshot, report difetti
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-21 - Test di regressione

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare che modifiche nuove non compromettano funzioni esistenti. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: versioni precedenti, aree impattate, casi critici. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: introduzione difetti in aree non modificate. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: report regressione, ticket difetti. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	report regressione, ticket difetti
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-22 - Validazione cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di ottenere conferma che output risponde all uso previsto o alle attese concordate. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: demo, ambiente staging, requisiti, criteri accettazione. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: rilascio non accettato o non utilizzabile. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: verbale collaudo, email approvazione, feedback. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	verbale collaudo, email approvazione, feedback
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o

	azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-23 - Preparazione rilascio

Scopo e campo di applicazione. L istruzione ha lo scopo di assicurare che prerequisiti, backup, autorizzazioni e comunicazioni siano completi. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: release candidate, test, piano deployment, finestra intervento. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: rilascio incompleto, mancato backup, cliente non informato. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: checklist rilascio, release note, backup report. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	checklist rilascio, release note, backup report
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-24 - Esecuzione deployment

Scopo e campo di applicazione. L istruzione ha lo scopo di mettere in produzione in modo controllato e verificato. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: pacchetto rilascio, credenziali autorizzate, piano rollback. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: downtime non pianificato, errori configurazione. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: log deployment, conferma verifica, ticket rilascio. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	log deployment, conferma verifica, ticket rilascio
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-25 - Verifica post-rilascio

Scopo e campo di applicazione. L istruzione ha lo scopo di controllare funzionamento effettivo e chiudere il rilascio solo dopo esiti positivi. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: ambiente produzione, funzioni critiche, feedback iniziale. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: rilascio apparentemente concluso ma non stabile. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: check post-rilascio, email chiusura. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	check post-rilascio, email chiusura
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione

valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-26 - Gestione rollback o patch urgente

Scopo e campo di applicazione. L istruzione ha lo scopo di ripristinare o correggere rapidamente in caso di difetti critici post-rilascio. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: incidenti, log, backup, versione precedente, priorita cliente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: prolungamento disservizio, perdita dati, decisioni non autorizzate. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: ticket incidente, log rollback, analisi causa. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	ticket incidente, log rollback, analisi causa
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-27 - Gestione incidenti di servizio

Scopo e campo di applicazione. L istruzione ha lo scopo di classificare, contenere, risolvere e analizzare incidenti che impattano servizi o clienti. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: segnalazioni, monitoraggio, log, fornitori, utenti. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: risoluzione non tracciata, ricorrenza, comunicazione insufficiente. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output,

registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro incidenti, comunicazioni, azioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro incidenti, comunicazioni, azioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-28 - Backup e ripristino

Scopo e campo di applicazione. L istruzione ha lo scopo di assicurare disponibilita di copie di sicurezza e capacita di recupero proporzionata. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: sistemi, database, hosting, configurazioni, requisiti cliente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: perdita dati, backup non recuperabili, tempi ripristino elevati. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: piano backup, log, test ripristino. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	piano backup, log, test ripristino
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-29 - Gestione accessi e credenziali

Scopo e campo di applicazione. L istruzione ha lo scopo di limitare accessi a dati e sistemi secondo necessita operative. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve

essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: utenti, ruoli, sistemi cliente, repository, hosting. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: accessi eccessivi, credenziali condivise, mancata revoca. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro accessi, autorizzazioni, revoche. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro accessi, autorizzazioni, revoche
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-30 - Gestione asset e strumenti ICT interni

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere controllo su strumenti, dispositivi, software e ambienti utilizzati. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: PC, licenze, repository, tool, account, servizi cloud. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: strumenti non aggiornati, licenze non chiare, perdita configurazioni. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: inventario, elenco licenze, note configurazione. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	inventario, elenco licenze, note configurazione
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-31 - Gestione licenze software e componenti

Scopo e campo di applicazione. L istruzione ha lo scopo di utilizzare software e componenti nel rispetto di condizioni contrattuali e licenze. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: tool, librerie, framework, componenti terzi, ordini. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: uso improprio di licenze, vincoli non rilevati, rischio legale. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: elenco licenze, approvazioni, documentazione componenti. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	elenco licenze, approvazioni, documentazione componenti
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-32 - Gestione fornitori critici

Scopo e campo di applicazione. L istruzione ha lo scopo di monitorare fornitori che possono incidere su qualita, continuita e sicurezza. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: hosting, cloud, licenze, connettivita, consulenti, hardware. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: dipendenza non gestita, disservizi ricorrenti, mancanza SLA. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: schede qualifica, valutazioni, ordini. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	schede qualifica, valutazioni, ordini
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-33 - Gestione subfornitori e collaboratori

Scopo e campo di applicazione. L istruzione ha lo scopo di definire requisiti, riservatezza, competenza e controllo degli output esterni. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: attivita delegate, accordi, accessi, requisiti cliente. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: output non conforme, riservatezza non tutelata, ruoli non chiari. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: accordi, NDA, report attivita, verifiche. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti

	applicabili.
Registrazione minima	accordi, NDA, report attivita, verifiche
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-34 - Comunicazione con il cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere comunicazioni tempestive, chiare e rintracciabili. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: richieste, stati progetto, ritardi, anomalie, rilasci. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: malintesi, aspettative non allineate, contestazioni. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: email, verbali, ticket, report stato. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	email, verbali, ticket, report stato
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-35 - Gestione modifiche richieste dal cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di valutare impatto tecnico, economico e temporale di ogni change request. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: richiesta modifica, requisiti esistenti, piano progetto. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: scope creep, ritardi, costi non riconosciuti. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro modifiche, approvazione cliente. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro modifiche, approvazione cliente
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-36 - Gestione reclami

Scopo e campo di applicazione. L istruzione ha lo scopo di trattare reclami in modo tempestivo e orientato a causa ed efficacia. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: comunicazioni cliente, ticket, anomalie, insoddisfazione. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: reclamo ignorato, causa non eliminata, ripetizione problema. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro reclami, risposta, azione correttiva. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro reclami, risposta, azione correttiva
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.

Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-37 - Raccolta soddisfazione cliente

Scopo e campo di applicazione. L istruzione ha lo scopo di ottenere informazioni utilizzabili per valutare percezione del cliente. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: feedback, questionari, rinnovi, ticket, colloqui. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: assenza di dati per migliorare, percezioni non documentate. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: feedback, questionari, analisi riesame. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	feedback, questionari, analisi riesame
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-38 - Gestione formazione interna

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere aggiornate competenze tecniche, gestionali e SGQ. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: matrice competenze, tecnologie, esiti audit, nuovi servizi. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: obsolescenza tecnica, errori operativi, dipendenza da singole persone. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la

conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro formazione, prove efficacia. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro formazione, prove efficacia
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-39 - Qualificazione docenti e contenuti formativi

Scopo e campo di applicazione. L istruzione ha lo scopo di garantire che i corsi informatici siano coerenti con bisogni e competenze richieste. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: programma, obiettivi, docente, materiali, partecipanti. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: contenuti non adeguati, aspettative non soddisfatte. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: programma corso, registri, feedback. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	programma corso, registri, feedback
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-40 - Gestione documenti SGQ

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere documenti aggiornati, approvati, disponibili e protetti. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: manuale, procedure, moduli, istruzioni, registrazioni. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: uso documenti obsoleti, perdita informazioni, versioni incoerenti. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: lista documenti, registro revisioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	lista documenti, registro revisioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-41 - Conservazione registrazioni

Scopo e campo di applicazione. L istruzione ha lo scopo di definire tempi, luoghi e responsabilita di conservazione delle evidenze. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: ticket, contratti, test, audit, formazioni, fornitori. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: evidenze non recuperabili durante audit o reclamo. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: piano conservazione, archivi digitali. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	piano conservazione, archivi digitali
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-42 - Raccolta KPI e analisi dati

Scopo e campo di applicazione. L istruzione ha lo scopo di trasformare registrazioni operative in dati per decisioni e miglioramento. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: ticket, progetti, test, feedback, fornitori, audit. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: indicatori non affidabili, decisioni non basate su dati. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: dashboard KPI, report riesame. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	dashboard KPI, report riesame
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-43 - Esecuzione audit interno

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare applicazione effettiva del sistema e non solo presenza documentale. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti,

progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: piano audit, criteri, campioni, persone, registrazioni. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: audit superficiale, mancata rilevazione problemi. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: checklist audit, rapporto, rilievi. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	checklist audit, rapporto, rilievi
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-44 - Trattamento non conformita

Scopo e campo di applicazione. L istruzione ha lo scopo di assicurare contenimento, analisi causa, azione e verifica efficacia. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: rilievi audit, reclami, difetti, incidenti, errori. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: correzioni senza causa, problemi ricorrenti. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro NC, piano azioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro NC, piano azioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-45 - Riesame della Direzione operativo

Scopo e campo di applicazione. L istruzione ha lo scopo di assicurare che dati e risultanze generino decisioni, risorse e obiettivi. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: KPI, audit, reclami, rischi, fornitori, formazione. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: riesame formale ma non decisionale. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: verbale riesame, piano azioni. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	verbale riesame, piano azioni
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

IO-46 - Gestione lezioni apprese

Scopo e campo di applicazione. L istruzione ha lo scopo di capitalizzare errori, successi e criticita per ridurre ricorrenze. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: progetti conclusi, incidenti, reclami, feedback, audit. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: perdita know-how, ripetizione degli stessi errori. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro lesson learned, aggiornamenti procedura. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro lesson learned, aggiornamenti procedura
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-47 - Chiusura commessa

Scopo e campo di applicazione. L istruzione ha lo scopo di verificare completamento tecnico, amministrativo e documentale della commessa. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: deliverable, test, accettazione, fatturazione, ticket. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: commesse formalmente aperte, evidenze incomplete. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: checklist chiusura, conferma cliente. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti

	applicabili.
Registrazione minima	checklist chiusura, conferma cliente
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-48 - Gestione continuita operativa essenziale

Scopo e campo di applicazione. L istruzione ha lo scopo di mantenere capacita minima di risposta in caso di indisponibilita persone, strumenti o fornitori. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: persone chiave, strumenti, fornitori, backup, accessi. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: blocco operativo, dipendenza non presidiata. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: piano continuita, contatti, backup, deleghe. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	piano continuita, contatti, backup, deleghe
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-49 - Monitoraggio conformita cogente

Scopo e campo di applicazione. L istruzione ha lo scopo di identificare requisiti legali e contrattuali che impattano i servizi ICT. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: privacy, sicurezza lavoro, licenze, contratti, norme societarie. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: non conformita legale o contrattuale. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: registro requisiti, check riesame. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	registro requisiti, check riesame
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

IO-50 - Preparazione audit esterno

Scopo e campo di applicazione. L istruzione ha lo scopo di organizzare evidenze e persone per dimostrare efficacia del SGQ. Si applica alle attivita pertinenti svolte da CLOUD3 S.R.L. nella gestione di clienti, progetti software, servizi web, hosting, consulenza informatica, configurazioni, formazione e supporto. La sua applicazione deve essere proporzionata al rischio: maggiore e la criticita per cliente, dati, continuita o requisiti contrattuali, maggiore deve essere la profondita della registrazione.

Input e condizioni di avvio. Gli input tipici comprendono: manuale, procedure, registrazioni, KPI, audit, riesame. Prima di procedere il responsabile verifica che tali input siano sufficientemente chiari, aggiornati e approvati quando necessario. Se emergono informazioni mancanti, contraddittorie o non realistiche, l attivita deve essere sospesa o limitata alla sola analisi fino al chiarimento con la parte interessata pertinente.

Sequenza operativa. Il responsabile assegna la priorita, identifica eventuali parti coinvolte, determina vincoli e rischi, seleziona strumenti e registrazioni, esegue o coordina le attivita, verifica l output e comunica l esito. La sequenza puo essere integrata in un ticket, in un piano progetto, in una email strutturata o in un verbale, purche siano conservate le informazioni minime richieste per dimostrare controllo e decisione.

Rischi da presidiare. I rischi principali sono: audit non supportato da evidenze, risposte incoerenti. Tali rischi devono essere valutati non solo in termini tecnici, ma anche rispetto a soddisfazione cliente, ritardi, costi, reputazione, sicurezza, privacy, ripetibilita del processo e possibilita di dimostrare la conformita in audit. Quando il rischio e elevato, la Direzione deve essere informata e deve approvare l approccio operativo.

Controlli di qualita. I controlli minimi comprendono verifica della completezza degli input, tracciabilita della decisione, coerenza con requisiti cliente, revisione tecnica quando appropriato, conferma dell output, registrazione delle anomalie e aggiornamento delle evidenze. Nei processi tecnici, il controllo puo includere test, backup, review, validazione, confronto con requisiti, verifica accessi e conferma del cliente.

Registrazioni e prova audit. Le evidenze attese sono: dossier audit, lista evidenze, agenda. Una registrazione e considerata adeguata quando consente a un auditor di ricostruire requisito, data, responsabile, attivita, decisione, output e verifica. L evidenza deve essere conservata in modo rintracciabile nel repository, nel sistema ticket, nella cartella commessa o nell archivio documentale definito.

Elemento di controllo	Applicazione pratica
Responsabile	Direzione o responsabile di processo designato, con supporto tecnico quando necessario.
Criterio di accettazione	Output completo, verificato, comunicato e coerente con requisiti applicabili.
Registrazione minima	dossier audit, lista evidenze, agenda
Indicatore possibile	Tempo di completamento, errori, riaperture, reclami, scostamenti o stato azioni.
Reazione a scostamento	Correzione immediata; se ricorrente o critica, apertura NC o azione correttiva.

Criterio di audit interno. Durante l audit il campione deve essere scelto su un caso realmente gestito e deve dimostrare applicazione dell istruzione. L auditor deve verificare se gli input erano chiari, se le decisioni sono

state registrate, se le responsabilita erano note, se l output e stato verificato e se eventuali anomalie sono state trattate in modo coerente con le procedure del SGQ.

Nota di consolidamento. Le cinque istruzioni precedenti devono essere considerate come parte di una catena integrata: una carenza in una fase puo generare non conformita o inefficienze nelle fasi successive. La Direzione valuta periodicamente se tali istruzioni richiedano semplificazione, automazione, maggiore formazione o integrazione con strumenti digitali.

32. Checklist audit-ready ISO 9001:2015 per CLOUD3 S.R.L.

La presente checklist e predisposta per supportare audit interno, Stage 2 e sorveglianza. Per ogni clausola sono indicati criteri di verifica, domande guida, evidenze oggettive attese e attenzione specifica per una societa ICT di piccole dimensioni. La checklist deve essere usata in modo dinamico: l auditor deve selezionare campioni reali e collegare dichiarazioni, documenti e registrazioni operative.

La verifica efficace non si limita alla presenza del manuale. Ogni requisito deve essere dimostrato con evidenze vive: un offerta, una commessa, un ticket, un rilascio, un test, una valutazione fornitore, una formazione, un reclamo, una non conformita o un riesame. La qualita del sistema si vede nella coerenza tra processi, dati e decisioni.

Clausola 4.1 - Comprendere organizzazione e contesto

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a fattori interni ed esterni, mercato ICT, tecnologie, rischi e direzione strategica sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: analisi contesto, riesame, registro rischi, obiettivi. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 4.2 - Parti interessate

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a clienti, utenti, fornitori, personale, autorita, organismo certificazione, requisiti pertinenti sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: matrice parti interessate, contratti, requisiti, feedback. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 4.3 - Campo di applicazione

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a coerenza tra attivita effettive, servizi ICT, sviluppo, hosting, formazione e sede sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: manuale, campo SGQ, visura, offerte e procedure. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 4.4 - Processi del SGQ

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a input, output, sequenza, responsabilita, criteri, KPI e registrazioni sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: mappa processi, schede processo, KPI, campioni commessa. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 5.1 - Leadership e impegno

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a coinvolgimento della Direzione, risorse, orientamento cliente, integrazione SGQ sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: politica, obiettivi, riesame, comunicazioni, decisioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 5.2 - Politica qualita

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a coerenza, comunicazione, disponibilita, quadro per obiettivi sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: politica approvata, evidenza comunicazione, riesame. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 5.3 - Ruoli e responsabilita

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a responsabilita per processi, output, report, miglioramento e cliente sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: organigramma, RACI, mansionari, interviste. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 6.1 - Rischi e opportunita

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a identificazione, valutazione, azioni, integrazione nei processi e verifica efficacia sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: registro rischi, piani azione, KPI, riesame. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 6.2 - Obiettivi qualita

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a obiettivi misurabili, coerenti, monitorati e comunicati sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: piano obiettivi, dashboard KPI, azioni su scostamenti. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 6.3 - Pianificazione cambiamenti

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a modifiche organizzative, tecniche, di processo, di strumenti o campo SGQ sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: registro modifiche, verbali, change request. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 7.1 - Risorse

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a persone, strumenti, infrastrutture, ambienti, repository, hosting e supporto sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: inventario, piani risorse, backup, tool, budget. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 7.2 - Competenza

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a competenze necessarie, evidenze, formazione, efficacia sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: matrice competenze, CV, formazione, affiancamento. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 7.3 - Consapevolezza

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a politica, obiettivi, contributo personale, effetti NC sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: interviste, comunicazioni, riunioni, registrazioni formazione. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 7.4 - Comunicazione

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a cosa, quando, con chi e come comunicare internamente ed esternamente sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: email, ticket, verbali, piani comunicazione cliente. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 7.5 - Informazioni documentate

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a creazione, aggiornamento, controllo, protezione, conservazione sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: lista documenti, versioni, archivi, campioni registrazioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.1 - Pianificazione operativa

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a criteri di processo, risorse, requisiti, controlli e registrazioni sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: piani progetto, ticket, checklist, ordini. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.2 - Requisiti prodotti e servizi

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a comunicazione cliente, determinazione requisiti, riesame e modifiche sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: offerte, ordini, requisiti, approvazioni, change request. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.3 - Progettazione e sviluppo

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a input, controlli, output, modifiche, validazione software sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: specifiche, repository, test, release note, verbali. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.4 - Fornitori esterni

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a qualifica, controllo, requisiti comunicati, monitoraggio performance sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: elenco fornitori, ordini, SLA, valutazioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.5 - Erogazione servizio

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a condizioni controllate, identificazione, proprieta cliente, preservazione, post-delivery sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: ticket, report intervento, log, email cliente. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.6 - Rilascio prodotti e servizi

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a evidenza criteri accettazione e autorizzazione al rilascio sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: report test, collaudo, release note, approvazione. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 8.7 - Output non conformi

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a identificazione, controllo, correzione, comunicazione e autorita decisionale sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: registro NC, ticket difetti, reclami, concessioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 9.1 - Monitoraggio e analisi

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a cosa monitorare, metodi, frequenze, analisi e valutazione risultati sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: KPI, report, dashboard, riesame. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 9.1.2 - Soddisfazione cliente

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a metodi di raccolta e analisi feedback, reclami e percezione sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: questionari, feedback, ticket, rinnovi, reclami. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 9.2 - Audit interno

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a programma, criteri, campo, imparzialita, rapporto e azioni sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: piano audit, checklist, rapporto, azioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 9.3 - Riesame Direzione

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a input completi, output decisionali, risorse, modifiche e miglioramento sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: verbale riesame, KPI, piano azioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 10.1 - Miglioramento generale

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a opportunita, esigenze future, prevenzione effetti indesiderati sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: piano miglioramento, lesson learned, azioni. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente

Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 10.2 - NC e azioni correttive

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a reazione, causa, azione, efficacia, aggiornamento rischi sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: registro NC, RCA, piani azione, verifica. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Clausola 10.3 - Miglioramento continuo

Obiettivo della verifica. L auditor deve accertare che il requisito relativo a uso di dati, audit, riesame e KPI per migliorare sistema sia compreso, applicato e mantenuto nel tempo. La verifica deve tenere conto della dimensione aziendale, della natura ICT dei servizi e della necessita di dimostrare controllo senza appesantimenti non proporzionati. La semplice dichiarazione di conformita non e sufficiente: occorre cercare evidenze coerenti e recenti.

Evidenze attese. Per questa clausola le evidenze piu rilevanti includono: trend KPI, riesami, progetti migliorativi. L auditor deve verificare almeno un campione operativo quando la clausola incide sul servizio: ad esempio una commessa software, un ticket, un rilascio, un fornitore critico, una formazione o una non conformita. Il campione deve mostrare collegamento tra requisito, responsabilita, attivita e risultato.

Domanda audit	Criterio di accettazione	Possibile rilievo se assente
Il requisito e stato determinato e documentato in modo proporzionato?	Esiste evidenza chiara, aggiornata e coerente con il processo.	Osservazione o NC per assenza/incompletezza evidenza.
Le persone coinvolte conoscono responsabilita e modalita operative?	Interviste coerenti con manuale, procedure e registrazioni.	Osservazione per consapevolezza insufficiente o ruoli non chiari.
La registrazione dimostra applicazione reale e non solo formale?	Campione operativo completo e rintracciabile.	NC se processo applicato ma non tracciato su requisito critico.
Sono stati valutati rischi, impatti o scostamenti pertinenti?	Rischi e azioni collegati a dati o casi reali.	Osservazione/NC se rischi ignorati su processi critici.

Nota per la sorveglianza. Nelle verifiche successive alla certificazione, l attenzione deve spostarsi dalla costruzione del sistema alla sua efficacia nel tempo. Pertanto saranno particolarmente importanti trend KPI, chiusura azioni, coerenza dei campioni, miglioramenti introdotti e capacita della Direzione di spiegare le decisioni assunte sulla base dei dati.

Dichiarazione finale di approvazione

Il presente manuale e approvato dalla Direzione di CLOUD3 S.R.L. come riferimento interno per la gestione del Sistema di Gestione per la Qualita secondo ISO 9001:2015. Le procedure, le schede processo e gli allegati sono applicati con criterio di proporzionalita rispetto alla dimensione aziendale, alla complessita dei servizi e ai rischi associati. Ogni funzione e tenuta a mantenere le evidenze necessarie e a contribuire al miglioramento continuo del sistema.

Ruolo	Nome/Funzione	Firma/Data
Direzione	Simone Cola	
Responsabile SGQ	Funzione interna designata	