Documentation - ISO 27001 Annex A

Documento di supporto allo Stage 1 - ISO/IEC 27001:2022 - Annex A Controls

Organizzazione	COMIN COSTRUZIONI GENERALI S.R.L.
Sede principale	Via Callalta 43, 31037 Loria (TV), Italia
Codice fiscale / P. IVA	03409330267
Settore IAF	IAF 28 - Costruzioni
Norma di riferimento	ISO/IEC 27001:2022 - Allegato A
Tipo documento	Documentation Annex A - elenco documenti, registrazioni ed evidenze attese per Stage 1
Stato	Bozza controllata per audit Stage 1 - da confermare con risk assessment, piano trattamento rischi e SoA

Nota di utilizzo

Il presente documento costituisce allegato documentale allo Stage 1 per la verifica della copertura dei controlli dell'Allegato A ISO/IEC 27001:2022. Non sostituisce la Dichiarazione di Applicabilita' richiesta dal punto 6.1.3, ma la supporta indicando, per ciascun controllo, la documentazione minima, le registrazioni e le evidenze normalmente attese in audit.

Per il settore costruzioni, particolare attenzione deve essere posta a documentazione tecnica e contrattuale di commessa, dati personali, PEC, archivi digitali, backup, dispositivi mobili, fornitori IT, accessi, continuita' operativa e riservatezza verso clienti, progettisti, direzione lavori, coordinatori e subappaltatori.

1. Scopo e criteri

Scopo del documento

Fornire una mappatura operativa della documentazione e delle evidenze richieste o attese per i controlli dell'Allegato A ISO/IEC 27001:2022, a supporto del riesame Stage 1 e della successiva pianificazione Stage 2.

Criteri di riferimento

- ISO/IEC 27001:2022, requisiti 4-10 e punto 6.1.3 - Information security risk treatment.
- ISO/IEC 27001:2022, Annex A - controlli organizzativi, persone, fisici e tecnologici.
- Risk assessment SGSI, piano di trattamento del rischio e Statement of Applicability dell'organizzazione.
- Requisiti cogenti e contrattuali: GDPR, D.Lgs. 196/2003, obblighi di riservatezza, contratti con clienti e fornitori, obblighi relativi a gare, commesse e cantieri.

Documentazione minima generale per SGSI

Governance SGSI	Campo di applicazione SGSI, politica sicurezza informazioni, ruoli e responsabilita, organigramma, procedura controllo informazioni documentate.
Risk management	Metodologia di risk assessment, registro rischi, criteri di accettazione del rischio, piano di trattamento del rischio, SoA aggiornata e approvata.
Asset e accessi	Inventario asset informativi, matrice profili/accessi, elenco utenti, gestione credenziali, autorizzazioni e revisioni periodiche.
Operativita IT	Procedure backup, log, antivirus/EDR, patching, configurazioni, gestione dispositivi, gestione fornitori IT, continuita operativa.
Persone	Accordi di riservatezza, istruzioni operative, formazione e consapevolezza, onboarding/offboarding, gestione segnalazioni.
Miglioramento	Audit interni, riesame direzione, indicatori, incidenti, non conformita, azioni correttive, verifiche di efficacia.

2. Annex A - Organizational controls (A.5)

Controlli organizzativi: governance, ruoli, processi, fornitori, incidenti, continuita, conformita e procedure operative.

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
5.1	Policies for information security	Politica SGSI approvata, comunicazione al personale, riesame periodico, registro distribuzione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.2	Information security roles and responsibilities	Matrice ruoli e responsabilita', nomine interne, job description, deleghe operative.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.3	Segregation of duties	Matrice segregazione compiti critici, controlli compensativi, autorizzazioni per funzioni amministrative e IT.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.4	Management responsibilities	Istruzioni alla direzione e ai responsabili, evidenze di comunicazione, verbali riunioni, obiettivi assegnati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.5	Contact with authorities	Elenco contatti autorita' rilevanti: Garante Privacy, CSIRT/ACN se applicabile, forze dell'ordine, consulenti privacy/legali.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.6	Contact with special interest groups	Elenco fonti informative: associazioni di settore, consulenti IT/privacy, provider, newsletter sicurezza, organismi tecnici.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.7	Threat intelligence	Procedura o istruzione per monitorare minacce informatiche, vulnerabilita', phishing, avvisi del fornitore IT, registro azioni.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.8	Information security in project management	Template progetto/commessa con requisiti di sicurezza informazioni, responsabilita', accessi e scambio documentale.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.9	Inventory of information and associated assets	Inventario asset informativi: server, PC, notebook, smartphone, PEC, gestionali, repository, archivi commessa, backup.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.10	Acceptable use of information and assets	Regolamento uso strumenti informatici, posta, internet, dispositivi mobili, supporti rimovibili e archivi documentali.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.11	Return of assets	Checklist offboarding, restituzione PC, smartphone, chiavi, badge, supporti, documentazione aziendale e credenziali.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.12	Classification of information	Schema classificazione informazioni: pubblico, interno, riservato, confidenziale; criteri per commesse, dati personali e contratti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.13	Labelling of information	Regole di etichettatura documenti e cartelle digitali, nomenclatura file, gestione documenti riservati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.14	Information transfer	Procedura trasferimento informazioni: email, PEC, cloud, portali clienti, cifratura, autorizzazioni, tracciabilita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.15	Access control	Politica accessi, matrice autorizzazioni, criteri need-to-know, review periodiche, autorizzazioni a dati di commessa.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.16	Identity management	Procedura creazione/modifica/disabilitazione utenze, elenco utenti, gestione account condivisi, account fornitori.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.17	Authentication information	Regole password, MFA ove disponibile, gestione credenziali, divieto condivisione, reset controllato.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.18	Access rights	Richieste accesso approvate, revisioni accessi, revoche, evidenza disabilitazione utenti cessati o cambi ruolo.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.19	Information security in supplier relationships	Elenco fornitori rilevanti, valutazione fornitori IT/cloud/consulenti, requisiti minimi di sicurezza e privacy.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.20	Information security in supplier agreements	Contratti/ordini con clausole sicurezza, riservatezza, backup, incident reporting, trattamento dati, subfornitura.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.21	Managing information security in ICT supply chain	Valutazione catena ICT, servizi cloud, hosting, manutentori, responsabilita' condivise, SLA e controlli terze parti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.22	Monitoring, review and change management of supplier services	Riesame periodico fornitori, ticket, SLA, report servizi IT, gestione modifiche contrattuali e tecniche.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

Documentation - ISO/IEC 27001:2022 Annex A

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
5.23	Information security for use of cloud services	Elenco servizi cloud, configurazioni, contratti, ubicazione dati, accessi, backup, MFA, ownership dati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.24	Information security incident management planning and preparation	Procedura incidenti, ruoli, canali di segnalazione, classificazione eventi, escalation e template report.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.25	Assessment and decision on information security events	Registro eventi, criteri per qualificare incidente, decisioni documentate, triage e responsabilita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.26	Response to information security incidents	Piano risposta incidenti, evidenze test/esercitazioni, azioni correttive, comunicazioni interne/esterne.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.27	Learning from information security incidents	Analisi cause, lesson learned, aggiornamento controlli, formazione, riesame eventi e near miss.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.28	Collection of evidence	Istruzione raccolta evidenze digitali, conservazione log, catena di custodia semplificata, supporto legale/forense.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.29	Information security during disruption	Piano continuita' operativa per informazioni critiche, ruoli emergenza, scenari indisponibilita' sistemi/PEC/dati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.30	ICT readiness for business continuity	Backup, restore test, ridondanze essenziali, contatti fornitori, RTO/RPO, prove di ripristino.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.31	Legal, statutory, regulatory and contractual requirements	Registro obblighi: GDPR, contratti, riservatezza, gare, requisiti clienti, conservazione documentale, licenze software.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.32	Intellectual property rights	Inventario licenze software, regole uso elaborati tecnici, copyright, divieto software non autorizzato.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.33	Protection of records	Procedura gestione registrazioni, tempi conservazione, protezione da perdita/modifica, backup e archiviazione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.34	Privacy and protection of PII	Registro trattamenti, informative, nomine autorizzati/responsabili, DPIA se applicabile, data breach procedure.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.35	Independent review of information security	Piano audit interni/esterni SGSI, verbali riesame indipendente, azioni di miglioramento.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.36	Compliance with policies, rules and standards	Verifiche compliance interne, checklist controlli, report non conformita', azioni correttive.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
5.37	Documented operating procedures	Procedure operative IT/SGSI: backup, accessi, incidenti, asset, dispositivi, fornitori, cambiamenti, archiviazione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

3. Annex A - People controls (A.6)

Controlli relativi alle persone: selezione, condizioni contrattuali, consapevolezza, riservatezza, lavoro remoto e segnalazione eventi.

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
6.1	Screening	Procedura selezione e controlli pre-assunzione proporzionati al ruolo, nel rispetto della normativa privacy e lavoro.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.2	Terms and conditions of employment	Lettere di incarico, mansionari, clausole riservatezza, istruzioni su uso sistemi e dati aziendali.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.3	Information security awareness, education and training	Piano formazione SGSI, registri presenze, test apprendimento, campagne phishing/awareness ove applicabili.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.4	Disciplinary process	Procedura disciplinare o richiamo a CCNL/regolamento interno per violazioni di sicurezza informazioni.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.5	Responsibilities after termination or change of employment	Checklist cessazione/cambio ruolo, revoca accessi, obblighi di riservatezza post rapporto, restituzione asset.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.6	Confidentiality or non-disclosure agreements	NDA, clausole riservatezza dipendenti/fornitori/subappaltatori/consulenti, evidenza sottoscrizione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.7	Remote working	Regole smart working/accesso remoto, VPN/MFA ove presenti, protezione dispositivi, divieto uso improprio reti pubbliche.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
6.8	Information security event reporting	Canali segnalazione, istruzioni al personale, registro eventi, tempi e responsabilita' di escalation.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

4. Annex A - Physical controls (A.7)

Controlli fisici: accessi, aree, attrezzature, supporti, locali, minacce fisiche e dismissione sicura.

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
7.1	Physical security perimeters	Planimetria/descrizione aree, accessi uffici, archivi, locali tecnici, separazione aree riservate.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.2	Physical entry controls	Gestione chiavi/badge, registro visitatori ove applicabile, autorizzazioni accesso uffici e archivi.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.3	Securing offices, rooms and facilities	Regole chiusura uffici, armadi, archivi, locali tecnici, custodia documenti di commessa.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.4	Physical security monitoring	Sistemi allarme/videosorveglianza se presenti, informative privacy, verifiche, manutenzione, responsabilita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.5	Protecting against physical and environmental threats	Valutazione rischi incendio/allagamento/furto, protezione server/archivi, estintori, UPS se presenti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.6	Working in secure areas	Istruzioni per locali/aree riservate, presenza accompagnata visitatori, divieto foto/accessi non autorizzati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.7	Clear desk and clear screen	Regolamento scrivania e schermo puliti, blocco sessione, custodia documenti e stampe riservate.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.8	Equipment siting and protection	Posizionamento PC/server/router, protezione furto/danni, armadi chiusi, protezione dispositivi mobili.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.9	Security of assets off-premises	Regole notebook/smartphone fuori sede e in cantiere, cifratura se disponibile, custodia e segnalazione smarrimenti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.10	Storage media	Inventario e gestione USB/dischi, autorizzazioni uso supporti, conservazione sicura e tracciabilita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.11	Supporting utilities	UPS, alimentazione, connettivita', climatizzazione locali IT se applicabile, contratti manutenzione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.12	Cabling security	Protezione cablaggi di rete/elettrici, accesso a rack/router, verifiche fisiche periodiche.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.13	Equipment maintenance	Registro manutenzioni apparati IT, interventi fornitori, autorizzazioni, protezione dati durante manutenzione.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
7.14	Secure disposal or re-use of equipment	Procedura cancellazione dati e dismissione, verbali wipe/distruzione, riassegnazione dispositivi.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

5. Annex A - Technological controls (A.8)

Controlli tecnologici: endpoint, accessi, backup, reti, logging, vulnerabilita, cloud, cambiamenti, sviluppo e test.

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
8.1	User endpoint devices	Elenco endpoint, configurazione minima, antivirus/EDR, cifratura ove disponibile, aggiornamenti, regole uso.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.2	Privileged access rights	Elenco amministratori, autorizzazioni privilegiate, account separati, review periodica, logging amministrativo.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.3	Information access restriction	Restrizioni a cartelle, gestionali, cloud, commesse e dati personali; gruppi autorizzativi.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.4	Access to source code	Applicabile solo se l'organizzazione gestisce codice sorgente o script critici; in tal caso repository, accessi e versioning.	Non applicabile se non vi e' sviluppo software o gestione codice; esclusione da motivare nella SoA.
8.5	Secure authentication	MFA ove disponibile, policy password, blocco account, gestione reset e autenticazione a servizi cloud/PEC/VPN.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.6	Capacity management	Monitoraggio spazio storage, mailbox, backup, sistemi gestionali, soglie e azioni preventive.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.7	Protection against malware	Antivirus/EDR, aggiornamenti, scansioni, gestione allegati email, formazione phishing, report minacce.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.8	Management of technical vulnerabilities	Patching, scansioni/verifiche vulnerabilita', bollettini fornitori, registro azioni correttive.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.9	Configuration management	Baseline configurazioni PC/server/router/cloud, modifiche approvate, inventario software installato.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.10	Information deletion	Regole cancellazione sicura dati, retention, dismissione cartelle/progetti, eliminazione dati non necessari.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.11	Data masking	Applicabile per test, condivisioni o report contenenti dati personali/riservati; regole oscuramento/anonymization.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.12	Data leakage prevention	Misure DLP proporzionate: restrizioni invio dati, cloud sharing controllato, USB limitate, autorizzazioni su cartelle.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.13	Information backup	Piano backup, frequenze, retention, supporti, protezione, test restore, responsabilita' e report esiti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.14	Redundancy of information processing facilities	Ridondanza o alternative per sistemi critici, connettivita', backup cloud/locali, procedure manuali temporanee.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.15	Logging	Log sistemi critici, accessi, backup, amministrazione, conservazione minima, protezione da modifica.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.16	Monitoring activities	Monitoraggio eventi IT, alert antivirus, log accessi, incidenti, disponibilita' servizi, review periodica.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.17	Clock synchronization	Sincronizzazione orari PC/server/router/NAS/cloud per coerenza log e tracciabilita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.18	Use of privileged utility programs	Elenco strumenti amministrativi, restrizioni uso, autorizzazioni, logging, uso solo da personale incaricato.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.19	Installation of software on operational systems	Regole installazione software, autorizzazioni, licenze, blocco software non approvato, inventario applicazioni.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.20	Networks security	Schema rete, firewall/router, Wi-Fi, VPN, segmentazione minima, password Wi-Fi, accessi ospiti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.21	Security of network services	Contratti/provider rete, SLA, configurazioni sicurezza, responsabilita' manutenzione, review servizi.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.22	Segregation of networks	Separazione rete aziendale/ospiti/impianti o dispositivi non gestiti, ove tecnicamente applicabile.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

Ctrl	Control topic	Documentazione / evidenze attese	Applicabilita / note Stage 1
8.23	Web filtering	Filtri navigazione ove disponibili, blocco siti malevoli, proxy/DNS security, formazione uso internet.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.24	Use of cryptography	Regole cifratura dati, VPN, HTTPS, PEC, password manager, cifratura dispositivi/supporti se disponibile.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.25	Secure development life cycle	Applicabile solo in presenza di sviluppo software interno/commissionato; procedure SDLC sicuro.	Non applicabile se non vi e' sviluppo software; valutare applicabilita' per siti web o personalizzazioni gestionali.
8.26	Application security requirements	Requisiti sicurezza per applicazioni acquisite o sviluppate, gestione credenziali, ruoli, backup, log.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.27	Secure system architecture and engineering principles	Principi architettura sicura per rete, cloud, gestionali, condivisioni file, backup e accessi remoti.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.28	Secure coding	Applicabile solo se si sviluppa codice; linee guida coding sicuro, review e test.	Non applicabile se non vi e' sviluppo software; esclusione da motivare nella SoA.
8.29	Security testing in development and acceptance	Test sicurezza per nuovi sistemi/applicativi prima del go-live, collaudi, hardening, verifica accessi.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.30	Outsourced development	Applicabile se sviluppo siti/applicazioni e' affidato a terzi; contratti con requisiti sicurezza, test e ownership codice.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.31	Separation of development, test and production environments	Applicabile per sistemi sviluppati/configurati; separazione ambienti o controlli compensativi documentati.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.32	Change management	Procedura modifiche IT, richieste, approvazioni, test, rollback, comunicazione e registrazione modifiche.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.33	Test information	Regole uso dati in test, anonimizzazione, divieto dati personali reali se non autorizzato/protetto.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.
8.34	Protection of information systems during audit testing	Regole per audit/test su sistemi, autorizzazioni, finestre operative, protezione dati e continuita'.	Applicabile salvo diversa giustificazione nel risk assessment e nella SoA.

6. Checklist di accettabilita' per Stage 1

Campo SGSI	Definito con confini organizzativi, sedi, processi, asset, persone e tecnologie incluse/escluse. Scope approvato e coerente con Stage 1.
Risk assessment	Metodologia definita, criteri di probabilita/impatto, asset/rischi/minacce/vulnerabilita valutati. Registro rischi disponibile.
Piano trattamento rischi	Trattamenti assegnati, responsabilita, scadenze, controlli Annex A collegati ai rischi. Piano approvato dalla direzione.
SoA	Tutti i 93 controlli valutati come applicabili/non applicabili con motivazione, stato ed evidenze. Dichiarazione approvata.
Documenti operativi	Procedure e istruzioni minime disponibili per accessi, asset, backup, incidenti, fornitori, dispositivi, conservazione e privacy.
Evidenze	Registrazioni almeno iniziali: elenco asset, utenti, backup, formazione, fornitori, audit interno, riesame direzione. Evidenze campionabili in Stage 2.

Conclusione Stage 1

La documentazione elencata nel presente allegato e' ritenuta idonea come base per dimostrare la copertura documentale dei controlli Annex A in sede di Stage 1. La conformita effettiva e l'implementazione operativa dovranno essere verificate in Stage 2 mediante campionamento di evidenze, interviste, riesame dei sistemi informativi, analisi dei processi di commessa e verifica della coerenza tra risk assessment, piano di trattamento, SoA e controlli implementati.

Preparato da	Lead Auditor Senior Data: ____ / ____ / _____
Riesaminato da	Direzione / Responsabile SGSI Firma: _____