Risk Management - Scopo, Contesto e Valutazione dei Rischi

- Analisi del Contesto e Gestione dei Rischi ISO 27001
- REGISTRO DEI RISCHI (RISK REGISTER)
- PIANO DI TRATTAMENTO DEL RISCHIO (RISK TREATMENT PLAN - RTP)
- DICHIARAZIONE DI APPLICABILITÀ (STATEMENT OF APPLICABILITY - SoA)

Analisi del Contesto e Gestione dei Rischi ISO 27001

1. Definizione del Contesto e dei Portatori d'Interesse (Stakeholders)

1.1 Analisi del Contesto Organizzativo

Forma Farm S.r.l. sviluppa, mantiene ed eroga soluzioni software per la formazione, con particolare riferimento alla piattaforma e-learning Forma LMS, al servizio Forma Cloud LMS e ai relativi plugin e servizi integrati.

L'organizzazione opera in un contesto caratterizzato dall'evoluzione continua delle tecnologie, dalla dipendenza da fornitori e servizi digitali esterni e dalla necessità di garantire la sicurezza delle informazioni trattate nello sviluppo software e nell'erogazione dei servizi ai clienti.

Il modello operativo di Forma Farm si basa sulla collaborazione con soci e professionisti esterni, che svolgono le proprie attività interamente da remoto (full remote), senza una sede operativa aziendale presso cui si svolgano ordinariamente le attività lavorative. L'organizzazione si avvale inoltre di fornitori specializzati per l'infrastruttura tecnologica e per altri servizi necessari allo svolgimento delle attività aziendali.

I fattori interni ed esterni rilevanti per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sono individuati e riesaminati considerando le caratteristiche dell'organizzazione, i servizi erogati, le esigenze delle parti interessate e le variazioni del contesto operativo.

Fattori esterni

- **Quadro normativo e regolamentare:** applicabilità delle disposizioni in materia di protezione dei dati personali, sicurezza delle informazioni, proprietà intellettuale e diritto d'autore, nonché degli obblighi derivanti dai contratti stipulati con i clienti e dai relativi accordi sul trattamento dei dati.
- **Minacce informatiche:** esposizione a tentativi di accesso non autorizzato, compromissione delle credenziali, sfruttamento di vulnerabilità software, attacchi alla catena di fornitura, indisponibilità dei servizi e altre minacce che possono compromettere la riservatezza, l'integrità o la disponibilità delle informazioni.
- **Dipendenza da fornitori e servizi esterni:** utilizzo di infrastrutture cloud, strumenti software e servizi di terze parti necessari allo sviluppo, alla manutenzione e all'erogazione dei servizi aziendali. La disponibilità e la sicurezza di tali servizi costituiscono elementi rilevanti per il SGSI.
- **Aspettative del mercato e dei clienti:** richieste di protezione dei dati, continuità del servizio, affidabilità delle soluzioni, gestione degli incidenti e disponibilità di informazioni ed evidenze relative alle misure di sicurezza adottate.
- **Evoluzione tecnologica:** cambiamenti nelle tecnologie cloud, nei componenti open source, nelle dipendenze software e nelle modalità di sviluppo ed erogazione dei servizi, che possono introdurre nuovi rischi e richiedere l'aggiornamento delle misure di sicurezza.

Fattori interni

- **Modello organizzativo:** organizzazione basata sulla collaborazione con soci e professionisti esterni, con responsabilità e autorizzazioni da definire in funzione delle attività svolte e degli accessi necessari. Il ricorso a collaboratori esterni rende rilevanti la gestione degli accessi, la riservatezza delle informazioni e la chiarezza delle responsabilità.
- **Processi aziendali:** progettazione, sviluppo, manutenzione e distribuzione del software; gestione degli ambienti cloud; assistenza tecnica; gestione delle relazioni con i clienti e dei fornitori tecnologici.
- **Infrastruttura e strumenti tecnologici:** utilizzo di ambienti cloud, repository del codice sorgente, strumenti di sviluppo e gestione operativa; strumenti cloud di comunicazione, condivisione documentale e collaborazione; dispositivi utilizzati dai collaboratori per accedere ai sistemi aziendali;connessioni remote e strumenti di autenticazione. La configurazione e l'effettivo utilizzo di tali risorse sono considerati nell'individuazione e nella valutazione dei rischi.
- **Competenze e risorse:** disponibilità di competenze specialistiche in ambito software, e-learning e infrastrutture tecnologiche. La distribuzione delle conoscenze operative e la dipendenza da singole persone o fornitori sono considerate nella valutazione dei rischi per la continuità delle attività.
- **Informazioni e proprietà intellettuale:** necessità di proteggere i dati dei clienti e degli utenti, le credenziali, la documentazione tecnica, il codice sorgente e le altre informazioni aziendali da divulgazione, modifica, perdita o accesso non autorizzato.
- **Modalità di lavoro:** svolgimento interamente da remoto delle attività aziendali da parte dei soci e dei collaboratori autorizzati. Tale modello rende rilevanti la sicurezza degli accessi remoti, la protezione dei dispositivi utilizzati, la gestione delle credenziali, la riservatezza delle informazioni negli ambienti di lavoro individuali e l'utilizzo sicuro delle

reti e degli strumenti di comunicazione

Il contesto organizzativo viene riesaminato almeno annualmente e in occasione di cambiamenti significativi nei servizi erogati, nell'organizzazione, nelle tecnologie utilizzate, nei fornitori rilevanti o nei requisiti normativi e contrattuali applicabili.

1.2 Parti Interessate e relative Esigenze e Aspettative

Forma Farm individua le parti interessate rilevanti per il SGSI e determina quali esigenze e aspettative costituiscono requisiti applicabili alle attività comprese nel campo di applicazione del sistema.

Le esigenze considerate comprendono gli obblighi normativi e regolamentari, i requisiti contrattuali, gli impegni assunti nei confronti dei clienti e le altre condizioni pertinenti alla sicurezza delle informazioni.

Portatore d'interesse (Stakeholder)	Esigenze e aspettative rilevanti	Requisiti di sicurezza collegati
Clienti (aziende e organizzazioni)	Protezione delle informazioni e dei dati trattati nei servizi erogati; affidabilità e continuità della piattaforma; rispetto degli impegni contrattuali.	Gestione degli accessi; protezione dei dati; disponibilità del servizio; gestione degli incidenti; rispetto dei DPA, degli SLA e degli eventuali requisiti di audit applicabili.
Utenti finali e corsisti	Riservatezza dei dati personali e delle attività formative; corretto funzionamento del servizio; protezione degli account.	Autenticazione; controllo degli accessi; protezione delle informazioni; gestione delle vulnerabilità e delle anomalie di sicurezza.
Soci e Direzione aziendale	Continuità delle attività, tutela della reputazione, protezione della proprietà intellettuale e sostenibilità dei servizi erogati.	Definizione delle responsabilità; approvazione delle politiche e dei criteri di sicurezza; valutazione e trattamento dei rischi; disponibilità delle risorse necessarie al SGSI.
Collaboratori e professionisti esterni	Chiarezza delle responsabilità e delle autorizzazioni; disponibilità degli strumenti necessari; tutela delle informazioni a cui accedono nello svolgimento delle attività.	Impegni di riservatezza; autorizzazioni coerenti con le attività assegnate; gestione degli accessi; rispetto delle regole e delle procedure di sicurezza applicabili.
Fornitori di infrastruttura cloud e servizi tecnologici	Rispetto degli accordi contrattuali e delle condizioni di utilizzo dei servizi; definizione delle responsabilità tra le parti.	Valutazione dei fornitori; verifica delle garanzie e degli impegni contrattuali pertinenti; gestione delle dipendenze esterne e dei rischi della catena di fornitura.

Portatore d'interesse (Stakeholder)	Esigenze e aspettative rilevanti	Requisiti di sicurezza collegati
Altri fornitori e partner operativi	Definizione delle condizioni di collaborazione e delle responsabilità; protezione delle informazioni condivise.	Riservatezza; gestione degli accessi, ove applicabile; definizione dei requisiti di sicurezza pertinenti al servizio fornito.
Autorità di controllo e organismi competenti	Rispetto degli obblighi legislativi e regolamentari applicabili; disponibilità delle informazioni richieste nell'ambito delle rispettive competenze.	Conformità normativa; conservazione delle evidenze pertinenti; gestione delle violazioni e degli incidenti secondo gli obblighi applicabili.
Organismi di certificazione e auditor	Disponibilità di evidenze attendibili relative al SGSI e alla conformità ai requisiti applicabili.	Documentazione controllata; registrazioni delle attività svolte; tracciabilità delle valutazioni e delle decisioni; disponibilità delle evidenze necessarie agli audit.

Le parti interessate e i relativi requisiti vengono riesaminati almeno annualmente e quando intervengono cambiamenti significativi nei rapporti contrattuali, nei servizi, nell'organizzazione o nel quadro normativo applicabile.

I requisiti individuati sono considerati nella definizione del campo di applicazione del SGSI, nell'individuazione dei rischi per la sicurezza delle informazioni e nella determinazione delle misure di sicurezza pertinenti. I dettagli relativi agli obblighi contrattuali, normativi e alle specifiche misure adottate sono mantenuti nella documentazione di riferimento del SGSI.

---

2. Campo di Applicazione (Scope) del SGSI

2.1 Perimetro di certificazione

Il Campo di Applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Forma Farm S.r.l. comprende:

«La progettazione, lo sviluppo, la manutenzione, l'erogazione in modalità SaaS e l'assistenza tecnica della piattaforma e-learning Forma Cloud LMS, dei relativi plugin, dei servizi cloud integrati e delle infrastrutture tecnologiche correlate, in conformità alle politiche aziendali e ai requisiti applicabili.»

Il perimetro comprende i processi, le risorse, gli strumenti e le informazioni necessari alla progettazione, allo sviluppo, alla manutenzione e all'erogazione dei servizi inclusi, nonché le attività di gestione tecnica e supporto connesse.

Le attività e i servizi di terze parti da cui dipende l'erogazione dei servizi inclusi nel perimetro sono considerati nell'ambito del SGSI per gli aspetti pertinenti alla sicurezza delle informazioni.

2.2 Delimitazione operativa, logica e fisica

- **Processi aziendali inclusi:**
  - Sviluppo e manutenzione del codice sorgente (*Secure SDLC* e gestione dei plugin).
  - Gestione e provisioning dell'infrastruttura Cloud Hosting, inclusi i servizi utilizzati per l'erogazione della piattaforma, i database e i servizi di backup.
  - Servizi di Helpdesk, supporto tecnico e monitoraggio dei sistemi.
  - Gestione dei contratti e delle relazioni con i clienti SaaS ed Enterprise.
- **Sedi fisiche e ambienti operativi:**
  - Le attività aziendali sono svolte interamente da remoto (*full remote*) dai soci e dai collaboratori autorizzati; non è prevista una sede operativa presso cui si svolgano ordinariamente le attività lavorative.
  - La sede legale della società, ove distinta dagli ambienti operativi, è indicata nei dati societari e non costituisce di per sé un luogo di svolgimento ordinario delle attività.
  - Le attività da remoto e i relativi rischi per la sicurezza delle informazioni rientrano nel SGSI, con particolare riferimento alla protezione dei dispositivi utilizzati, alla gestione delle credenziali, agli accessi remoti e alla riservatezza delle informazioni.
- **Asset e confini logici:**
  - Piattaforme di produzione e test di *Forma Cloud LMS* e ambienti e strumenti tecnologici utilizzati per la gestione e l'erogazione del servizio, inclusa *Forma Factory* ove pertinente.
  - Repository del codice sorgente, sistemi di gestione delle identità e degli accessi (*IAM*), strumenti di comunicazione, collaborazione e ticketing.
  - Dispositivi utilizzati dai soci e dai collaboratori autorizzati per accedere ai sistemi e trattare informazioni comprese nel perimetro.
  - Infrastrutture cloud e servizi tecnologici forniti da terze parti, per le componenti e le responsabilità rilevanti ai fini della sicurezza delle informazioni.

Le attività eventualmente affidate a fornitori esterni non sono considerate estranee al SGSI per il solo fatto di essere esternalizzate: le relative dipendenze e i rischi connessi sono valutati in funzione del loro impatto sui servizi e sulle informazioni comprese nel perimetro.

---

3. Metodologia di Valutazione del Rischio (Risk Assessment Methodology)

3.1 Criteri di Valutazione

Forma Farm S.r.l. adotta un approccio basato sul rischio (*Risk-Based Approach*) coerente con le linee guida della norma ISO/IEC 27005. Il rischio (R) viene calcolato in funzione della **Probabilità** (P) che una minaccia sfrutti una vulnerabilità di un asset e dell'**Impatto** (I) derivante dalla perdita di Confidenzialità, Integrità o Disponibilità.

$$R = P \times I$$

3.2 Scale di Valutazione

- **Scala della Probabilità (P):**
  1. **Bassa (1):** Evento raro o con basse possibilità di verificarsi, richiedente condizioni o competenze complesse.
  2. **Media (2):** Evento possibile che si è verificato o potrebbe verificarsi occasionalmente nel settore.
  3. **Alta (3):** Evento molto probabile o frequente, legato a vulnerabilità note o attacchi diffusi.
- **Scala dell'Impatto (I):**
  1. **Lieve (1):** Disservizio minimo, nessun impatto significativo sui clienti o sulla reputazione, violazione di dati non critici.
  2. **Moderato (2):** Interruzione temporanea di alcuni servizi, impatto economico limitato, potenziale violazione di dati senza conseguenze gravi.
  3. **Grave (3):** Interruzione prolungata del servizio SaaS LMS, violazione di dati personali (Data Breach), danno reputazionale rilevante o sanzioni normative.

3.3 Matrice del Rischio e Soglie di Accettabilità

Probabilità / Impatto	Impatto Lieve (1)	Impatto Moderato (2)	Impatto Grave (3)
Alta (3)	**3 (Medio)**	**6 (Alto)**	**9 (Critico)**

Probabilità / Impatto	Impatto Lieve (1)	Impatto Moderato (2)	Impatto Grave (3)
Media (2)	**2 (Basso)**	**4 (Medio)**	**6 (Alto)**
Bassa (1)	**1 (Basso)**	**2 (Basso)**	**3 (Medio)**

- **Valori 1–2 (Rischio Basso):** *Accettabile.* Non richiede azioni immediate, ma è soggetto a monitoraggio periodico.
- **Valori 3–4 (Rischio Medio):** *Tollerabile.* Richiede la pianificazione di contromisure nel Piano di Trattamento del Rischio (RTP) entro tempi definiti.
- **Valori 6–9 (Rischio Alto / Critico):** *Inaccettabile.* Richiede un intervento prioritario immediato tramite l'implementazione dei controlli previsti dall'Allegato A (Annex A) della ISO/IEC 27001.

REGISTRO DEI RISCHI (RISK REGISTER)

Documento: Registro dei Rischi (Risk Register)
Organizzazione: Forma Farm S.r.l. (Via Savona 10, Milano)
Standard di Riferimento: ISO/IEC 27001:2022 / ISO/IEC 27005
Ambito (Scope): Sviluppo, gestione, manutenzione ed erogazione SaaS della piattaforma *Forma Cloud LMS*, plugin e servizi cloud correlati.

---

1. Metodologia e Formula di Calcolo

Il calcolo del **Rischio Lordo (R)** e del **Rischio Residuo** viene effettuato moltiplicando la **Probabilità (P)** che una minaccia sfrutti una vulnerabilità dell'asset per l'**Impatto (I)** registrato su Confidenzialità, Integrità o Disponibilità:

$$R = P \times I$$

Scale di Valutazione:

- **Probabilità (P):** `1` (Bassa), `2` (Media), `3` (Alta)
- **Impatto (I):** `1` (Lieve), `2` (Moderato), `3` (Grave)

Matrice di Rischio e Soglie di Trattamento:

- **Rischio 1–2 (Basso):** Accettabile. Richiede monitoraggio ordinario.
- **Rischio 3–4 (Medio):** Tollerabile. Richiede la pianificazione di contromisure nel Piano di Trattamento del Rischio (RTP).
- **Rischio 6–9 (Alto / Critico):** Inaccettabile. Richiede interventi correttivi prioritari immediati tramite i controlli dell'Annex A (ISO/IEC 27001).

---

2. Tabella Inventario Minacce, Vulnerabilità e Rischi

ID Rischio	Asset Coinvolto	Minaccia (Threat)	Vulnerabilità Sfruttata	P	I	Rischio Lordo (R)	Controlli ISO 27001 / Trattamento Consigliato	Rischio Residuo
RSK-01	Codice sorgente (Forma Lms / Plugin)	Iniezione di codice malevolo o sfruttamento di vulnerabilità (0-day / CVE) nei componenti Open Source o nei plugin	Presenza di librerie di terze parti non aggiornate o difetti nel ciclo di sviluppo (Secure SDLC)	3	3	**9 (Critico)**	**A.8.8 Gestione delle vulnerabilità tecniche / A.8.25 Sviluppo sicuro:** Scansioni periodiche di codice (SAST/DAST), patch management tempestivo e isolamento ambienti.	**2 (Basso)**
RSK-02	Infrastruttura Cloud Hosting (AWS) & Database	Accesso non autorizzato ai server di produzione o esfiltrazione di dati dei corsisti/clienti	Credenziali di accesso deboli, assenza di autenticazione a due fattori (MFA) o errata configurazione dei permessi IAM	2	3	**6 (Alto)**	**A.5.15 Controllo degli accessi / A.8.5 Autenticazione sicura:** Obbligo di MFA per tutti gli amministratori, principio del minimo privilegio e revoca immediata delle utenze cessate.	**2 (Basso)**

ID Rischio	Asset Coinvolto	Minaccia (Threat)	Vulnerabilità Sfruttata	P	I	Rischio Lordo (R)	Controlli ISO 27001 / Trattamento Consigliato	Rischio Residuo
RSK-03	Piattaforma SaaS (Forma Cloud LMS)	Interruzione prolungata del servizio (DDoS, guasto infrastrutturale del Cloud Provider)	Mancanza di ridondanza geografica o procedure di disaster recovery non testate regolarmente	2	3	**6 (Alto)**	**A.5.30 Prontezza dell'ICT per la continuità operativa / A.8.14 Ridondanza:** Accordi di servizio (SLA) stringenti con il Cloud Provider, backup automatici e test di ripristino periodici (DRP).	**2 (Basso)**
RSK-04	Dati dei Clienti / Aziendali	Violazione dei dati personali (Data Breach) o perdita di dati critici per errore umano o attacco ransomware	Mancanza di cifratura dei dati a riposo/transito o errate policy di conservazione/cancellazione dei dati	2	3	**6 (Alto)**	**A.8.24 Uso della crittografia / A.5.12 Classificazione delle informazioni:** Cifratura end-to-end (HTTPS/TLS) e cifratura dei database cloud, sottoscrizione di DPA con i clienti.	**2 (Basso)**

ID Rischio	Asset Coinvolto	Minaccia (Threat)	Vulnerabilità Sfruttata	P	I	Rischio Lordo (R)	Controlli ISO 27001 / Trattamento Consigliato	Rischio Residuo
RSK-05	Dispositivi dei dipendenti (Smart Working / Notebook)	Perdita, furto o accesso abusivo a un dispositivo aziendale fuori sede (es. lavoro da remoto)	Mancanza di cifratura del disco (BitLocker/FileVault) o assenza di blocchi schermo automatici	2	2	**4 (Medio)**	**A.7.9 Sicurezza dei dispositivi / A.8.1 Attrezzature degli utenti:** Cifratura obbligatoria dei dispositivi, blocco schermo automatico e policy di pulizia dello schermo (Clean Screen).	**1 (Basso)**
RSK-06	Supply Chain Software / Fornitori Terzi	Compromissione della catena di fornitura software o disservizio da parte di un fornitore critico	Assenza di verifiche preventive di sicurezza sui fornitori terzi o dipendenze software esterne	2	2	**4 (Medio)**	**A.5.19 Sicurezza nelle relazioni con i fornitori:** Due diligence preventiva sui fornitori cloud/servizi e inserimento di clausole di sicurezza nei contratti di fornitura.	**1 (Basso)**

ID Rischio	Asset Coinvolto	Minaccia (Threat)	Vulnerabilità Sfruttata	P	I	Rischio Lordo (R)	Controlli ISO 27001 / Trattamento Consigliato	Rischio Residuo
RSK-07	Reputazione e Proprietà Intellettuale	Perdita o corruzione del codice sorgente proprietario (Forma Factory / Plugin)	Mancanza di backup isolati (versioning sicuro) o permessi di scrittura non controllati sui repository	1	3	**3 (Medio)**	**A.8.12 Prevenzione della fuga di dati / A.8.28 Code signing:** Utilizzo di repository cloud sicuri (es. GitHub/GitLab Enterprise) con controllo accessi granulare e backup immutabili.	**1 (Basso)**
RSK-08	Personale interno e Collaboratori	Errori operativi o disattenzione nella gestione della sicurezza (es. phishing, condivisione credenziali)	Bassa consapevolezza dei rischi informatici (*Security Awareness*) da parte del personale	2	2	**4 (Medio)**	**A.6.3 Formazione e consapevolezza sulla sicurezza:** Esecuzione di piani di formazione periodici sulla sicurezza e simulazioni di phishing per i dipendenti.	**1 (Basso)**

3. Riesame e Valutazione Continua

Il presente Registro dei Rischi è soggetto a revisione periodica con cadenza almeno **semestrale** o in coincidenza con:

1. Rilasci di importanti aggiornamenti di versione della piattaforma *Forma Cloud LMS*.
2. Modifiche sostanziali all'infrastruttura cloud o all'architettura di rete.
3. Rilevazione di nuovi incidenti di sicurezza o vulnerabilità critiche (CVE/0-day).

PIANO DI TRATTAMENTO DEL RISCHIO (RISK TREATMENT PLAN - RTP)

Il presente documento definisce le azioni correttive, i controlli di sicurezza implementati o pianificati, i ruoli di responsabilità e le tempistiche per mitigare, trasferire o accettare i rischi emersi durante la valutazione del rischio (*Risk Assessment*) relativa alla piattaforma *Forma Cloud LMS* e ai servizi correlati.

Tabella Operativa di Trattamento del Rischio

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-01	Codice sorgente (Forma LMS / Plugin)	**9 (Critico)**	**Mitigazione**	Analisi automatizzata SAST/DAST integrata nella pipeline CI/CD (Secure SDLC) e patch management automatizzato.	**Già attiva**	Lead Developer / DevOps	Monitoraggio continuo (Patch entro 48h per falle critiche)	**2 (Basso)**

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-02	Cloud Hosting (AWS) & Database	**6 (Alto)**	**Mitigazione**	Autenticazione a Due Fattori (MFA) obbligatoria per amministratori, politica del minimo privilegio IAM e cifratura dati.	**Già applicata**	System Administrator	Revisione permessi semestrale	**2 (Basso)**
RSK-03	Piattaforma SaaS (Forma Cloud LMS)	**6 (Alto)**	**Mitigazione / Trasferimento**	Accordi SLA con provider AWS, backup automatici multi-regione e test DRP.	**Già attive**	IT Operations Manager	**Test DRP Annuale** (e al cambio di architettura)	**2 (Basso)**
RSK-04	Dati dei Clienti / GDPR	**6 (Alto)**	**Mitigazione**	Cifratura end-to-end in transito (HTTPS/TLS) e a riposo per DB cloud. Sottoscrizione DPA (IT/EN).	**Già attive**	DPO / Legal	Operativo permanente / Aggiornamento contratti	**2 (Basso)**
RSK-05	Dispositivi Dipendenti / Workstation	**4 (Medio)**	**Mitigazione**	Cifratura dischi (BitLocker/FileVault), blocco schermo e policy Clean Screen.	**Già applicata**	IT Helpdesk	Verifiche periodiche sui dispositivi	**1 (Basso)**

ID Rischio	Asset / Processo	Rischio Iniziale	Opzione di Trattamento	Controlli ISO 27001 / Azioni di Mitigazione	Stato Attuazione	Responsabile Attuazione	Tempistiche / Frequenza	Rischio Residuo
RSK-06	Supply Chain / Fornitori Terzi	**4 (Medio)**	**Mitigazione**	Processo di Due Diligence preventiva e clausole contrattuali di sicurezza nei contratti.	**In corso di formalizzazione**	Management / Legal	Completamento entro 90 giorni	**1 (Basso)**
RSK-07	Reputazione e Proprietà Intellettuale	**3 (Medio)**	**Mitigazione**	Repository Git privati con branch protection, gestione ruoli granulare e backup immutabili.	**Già applicata**	Lead Developer	Operativo permanente	**1 (Basso)**
RSK-08	Personale interno e Collaboratori	**4 (Medio)**	**Mitigazione**	Piano annuale di Security Awareness, formazione e sicurezza e simulazioni di phishing.	**In corso / Pianificato**	HR / Responsabile SGSI	Avvio entro 60 giorni (cadenza annuale)	**1 (Basso)**

Modalità di Riesame e Monitoraggio

1. **Verifica dell'attuazione:** Il Responsabile della Sicurezza verifica lo stato di avanzamento delle azioni correttive definite nell'RTP con cadenza trimestrale.
2. **Aggiornamento del Piano:** Il Piano di Trattamento del Rischio viene riesaminato e aggiornato formalmente almeno una volta all'anno in occasione del *Riesame della Direzione*, oppure a seguito di incidenti di sicurezza significativi o modifiche rilevanti dell'infrastruttura tecnologica.

DICHIARAZIONE DI APPLICABILITÀ (STATEMENT OF APPLICABILITY - SoA)

Conforme alla Norma ISO/IEC 27001:2022

Organizzazione: Forma Farm S.r.l.
Sede Legale: Via Savona 10, 20144 Milano (MI)
Modello Operativo: 100% Full Remote / Distributed Organization
Infrastruttura: Cloud Hosting AWS (Amazon Web Services) & Servizi Managed SaaS
Versione Documento: 1.0
Data del Documento: Ottobre 2026

---

1. INTRODUZIONE E CRITERI DI SELEZIONE

Il presente documento costituisce la **Dichiarazione di Applicabilità (SoA)** del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di **Forma Farm S.r.l.**, redatta in conformità ai requisiti della norma **ISO/IEC 27001:2022** (Allegato A).

1.1 Contesto e Specificità Operative

Forma Farm S.r.l. sviluppa, eroga e gestisce in modalità SaaS la piattaforma e-learning *Forma Cloud LMS*, i relativi plugin e servizi integrati. L'organizzazione adotta un modello **100% Full Remote**, privo di server o data center fisici di proprietà; l'intera infrastruttura applicativa e di memorizzazione dati è ospitata presso il Cloud Provider **AWS (Amazon Web Services)**.

1.2 Criteri di Inclusione ed Esclusione dei Controlli

I controlli dell'Allegato A della norma ISO/IEC 27001:2022 sono stati valutati e selezionati in base a:

1. Risultati della valutazione dei rischi (Risk Assessment) declinati nel *Registro dei Rischi* e nel *Piano di Trattamento del Rischio (RTP)*.

2. Requisiti cogenti e normativi (es. Regolamento UE 2016/679 - GDPR, normative sul diritto d'autore e proprietà intellettuale).
3. Obblighi contrattuali stipulati con i clienti (SLA, Data Processing Agreement - DPA).
4. Esigenze operative del modello di business SaaS/Cloud e lavoro da remoto.

---

2. MATRICE DEI CONTROLLI ISO/IEC 27001:2022

Sezione A.5 — Controlli Organizzativi (Organizational Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.1	Politiche per la sicurezza delle informazioni	**Sì**	Implementato	Politica di Sicurezza delle Informazioni definita e approvata dalla Direzione.
A.5.2	Ruoli e responsabilità per la sicurezza	**Sì**	Implementato	Assegnazione formale delle responsabilità SGSI (Direzione, Lead Dev, Admin, DPO).
A.5.3	Segregazione dei compiti	**Sì**	Implementato	Separazione dei ruoli tra ambienti di dev/test e produzione cloud AWS.
A.5.4	Responsabilità della direzione	**Sì**	Implementato	Coinvolgimento attivo nei Riesami della Direzione e nell'allocazione delle risorse SGSI.
A.5.5	Contatto con le autorità	**Sì**	Implementato	Procedure di contatto per Data Breach con il Garante Privacy e CSIRT Italia.
A.5.6	Contatto con gruppi di interesse speciale	**Sì**	Implementato	Partecipazione a community Open Source (Forma LMS) e forum sulla sicurezza cloud.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.7	Threat intelligence	**Sì**	Implementato	Monitoraggio di bollettini CVE, feed di sicurezza AWS e dipendenze software.
A.5.8	Sicurezza delle informazioni nella gestione dei progetti	**Sì**	Implementato	Integrazione della sicurezza nella roadmap di prodotto e nello sviluppo plugin.
A.5.9	Inventario delle informazioni e degli altri asset associati	**Sì**	Implementato	Inventario formale degli asset (codice, account cloud, dati clienti, laptop aziendali).
A.5.10	Uso ammissibile delle informazioni e degli asset	**Sì**	Implementato	Definizione dell'Acceptable Use Policy nell'Information Security Policy e contratti.
A.5.11	Restituzione degli asset	**Sì**	Implementato	Procedura di offboarding con revoca utenze e restituzione/wipe dei dispositivi.
A.5.12	Classificazione delle informazioni	**Sì**	Implementato	Definizione di 4 livelli di riservatezza (Pubblico, Interno, Confidenziale, Dati Personali).
A.5.13	Etichettatura delle informazioni	**Sì**	Implementato	Applicazione di tag e criteri logici sui repository Git, DB e bucket S3.
A.5.14	Trasferimento di informazioni	**Sì**	Implementato	Utilizzo esclusivo di canali cifrati (TLS/HTTPS, SSH) e clausole contrattuali DPA.
A.5.15	Controllo degli accessi	**Sì**	Implementato	Principio del minimo privilegio gestito via IAM policy e ruoli ruotati.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.16	Gestione delle identità	**Sì**	Implementato	Processo formalizzato di provisioning e de-provisioning delle utenze aziendali.
A.5.17	Informazioni per l'autenticazione	**Sì**	Implementato	Gestione credenziali tramite Password Manager aziendale e obbligo di password complesse.
A.5.18	Diritti di accesso	**Sì**	Implementato	Revisione periodica (semestrale) delle ACL e delle policy IAM su AWS e GitHub.
A.5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	**Sì**	Implementato	Valutazione della sicurezza dei fornitori critici (AWS, SaaS terzi).
A.5.20	Indirizzamento della sicurezza nei contratti con i fornitori	**Sì**	Implementato	Clausole di sicurezza e riservatezza nei contratti e sottoscrizione DPA.
A.5.21	Gestione della sicurezza nella catena di fornitura ICT	**Sì**	In corso	Procedura di due diligence e verifica della sicurezza delle librerie Open Source.
A.5.22	Monitoraggio, riesame e gestione dei servizi dei fornitori	**Sì**	Implementato	Verifiche continue sugli SLA dei Cloud Provider e sui report di conformità SOC/ISO.
A.5.23	Sicurezza delle informazioni per l'uso dei servizi cloud	**Sì**	Implementato	Configurazione conforme alle best-practice di sicurezza cloud AWS (CIS Benchmark).
A.5.24	Gestione degli incidenti per la sicurezza delle informazioni	**Sì**	Implementato	Procedura formale per rilevazione, escalation e notifica di incidenti/Data Breach.
A.5.25	Valutazione e decisione sugli eventi di sicurezza	**Sì**	Implementato	Criteri di classificazione della gravità degli eventi correlati alle risorse Cloud.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.26	Risposta agli incidenti di sicurezza	**Sì**	Implementato	Piani di risposta rapida per isolamento istanze, ripristino backup e patch emergenti.
A.5.27	Apprendimento dagli incidenti di sicurezza	**Sì**	Implementato	Post-mortem analysis e aggiornamento dei controlli a seguito di anomalie/incidenti.
A.5.28	Raccolta di prove	**Sì**	Implementato	Tracciabilità dei log di audit AWS CloudTrail e audit log di sistema per uso forense.
A.5.29	Sicurezza delle informazioni durante l'interruzione	**Sì**	Implementato	Piano di Continuità Operativa e Disaster Recovery per la piattaforma LMS.
A.5.30	PR di ICT per la continuità operativa	**Sì**	Implementato	Replicazione multi-AZ dei dati e procedure automatizzate di failover su AWS.
A.5.31	Requisiti legali, statutari, normativi e contrattuali	**Sì**	Implementato	Registro di conformità normativa (GDPR, Proprietà Intellettuale, Contratti Clienti).
A.5.32	Diritti di proprietà intellettuale	**Sì**	Implementato	Tutela del codice proprietario (Forma Factory/Plugin) e rispetto licenze Open Source.
A.5.33	Protezione dei registri (records)	**Sì**	Implementato	Conservazione sicura e immutabile dei log e dei documenti fiscali/legali.
A.5.34	Privacy e protezione dei dati personali (PII)	**Sì**	Implementato	Nomina a Responsabile del Trattamento (DPA), nomina DPO e rispetto del GDPR.
A.5.35	Riesame indipendente della sicurezza	**Sì**	Implementato	Audit interni programmati e verifiche da parte di enti di certificazione terzi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.5.36	Conformità con politiche e standard di sicurezza	**Sì**	Implementato	Verifiche periodiche sull'applicazione delle policy da parte del personale.
A.5.37	Procedure operative documentate	**Sì**	Implementato	Documentazione tecnica di deploy, gestione server, backup e manutenzione LMS.

Sezione A.6 — Controlli sulle Persone (People Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.6.1	Screening	**Sì**	Implementato	Verifiche pre-assunzione (curriculum, referenze, assenza di condanne) per nuovi assunti.
A.6.2	Termini e condizioni di impiego	**Sì**	Implementato	Clausole di riservatezza (NDA) ed etica professionale integrate nei contratti di lavoro.
A.6.3	Consapevolezza, istruzione e formazione	**Sì**	In corso	Piano di formazione annuale in *Security Awareness* e simulazioni di phishing.
A.6.4	Processo disciplinare	**Sì**	Implementato	Richiamo al CCNL applicabile per le violazioni delle politiche di sicurezza.
A.6.5	Responsabilità post-impiego	**Sì**	Implementato	Obbligo di riservatezza permanente e revoca totale degli accessi al termine del rapporto.
A.6.6	Accordi di riservatezza o non divulgazione	**Sì**	Implementato	Sottoscrizione di NDA con tutti i dipendenti, collaboratori esterni e fornitori terzi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.6.7	Lavoro da remoto (Remote working)	**Sì**	Implementato	**Controllo critico:** Regolamento di Telelavoro/Smart Working, uso VPN/TLS e dispositivi protetti.
A.6.8	Segnalazione di eventi di sicurezza	**Sì**	Implementato	Canale di segnalazione interno tempestivo per anomalie, phishing o smarrimento dispositivi.

Sezione A.7 — Controlli Fisici (Physical Controls)

> **Nota metodologica sul modello Full Remote:** Poiché Forma Farm S.r.l. non gestisce server o perimetri fisici di data center (interamente in outsourcing ad AWS), i controlli fisici perimetrali tradizionali sono dichiarati **Non Applicabili (Esclusi)** o adattati esclusivamente alla sicurezza delle postazioni di lavoro domiciliari/nomadi.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.1	Perimetri di sicurezza fisica	**No**	Escluso	**Non applicabile:** Assenza di perimetri fisici aziendali o server locali (infrastruttura 100% AWS).
A.7.2	Ingresso fisico	**No**	Escluso	**Non applicabile:** Inesistenti aree ad accesso controllato o sale server proprie.
A.7.3	Mantenimento di uffici, stanze e strutture	**No**	Escluso	**Non applicabile:** Organizzazione operativamente 100% distribuita in remote working.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.4	Monitoraggio della sicurezza fisica	**No**	Escluso	**Non applicabile:** Gestito autonomamente da AWS per i propri Data Center (certificati ISO 27001).
A.7.5	Protezione contro minacce fisiche e ambientali	**No**	Escluso	**Non applicabile:** Delega della sicurezza fisica dei server al Cloud Provider (AWS).
A.7.6	Lavoro in aree sicure	**No**	Escluso	**Non applicabile:** Nessuna area ad alto rischio fisico o di produzione gestita in sede.
A.7.7	Scrivania pulita e schermo pulito (Clean desk/screen)	**Sì**	Implementato	Applicabile alle postazioni di lavoro dei remotisti: blocco schermo automatico e no stampe.
A.7.8	Posizionamento e protezione delle apparecchiature	**Sì**	Implementato	Obbligo di custodia fisica e non abbandono dei laptop/dispositivi aziendali in luoghi pubblici.
A.7.9	Sicurezza degli asset fuori dalle sedi	**Sì**	Implementato	Regolamentazione dell'uso dei computer portatili durante trasferte o spostamenti.
A.7.10	Supporti di memorizzazione (Storage media)	**Sì**	Implementato	Divieto d'uso di pendrive/hard-disk USB non cifrati per il trasferimento di dati riservati.
A.7.11	Utenze di servizio (Utilities)	**No**	Escluso	**Non applicabile:** Gestione di energia/climatizzazione affidata interamente al provider AWS.
A.7.12	Sicurezza del cablaggio	**No**	Escluso	**Non applicabile:** Assenza di infrastruttura di rete cablata proprietaria.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.7.13	Manutenzione delle apparecchiature	**Sì**	Implementato	Manutenzione e sostituzione ordinaria dei laptop di lavoro gestita via Helpdesk/IT.
A.7.14	Smaltimento o riutilizzo sicuro degli asset	**Sì**	Implementato	Wipe crittografico/distruzione sicura dei dischi prima della dismissione dei notebook.

Sezione A.8 — Controlli Tecnologici (Technological Controls)

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.1	Dispositivi degli utenti finali (User endpoint devices)	**Sì**	Implementato	Cifratura integrale del disco (BitLocker/FileVault), antivirus e OS sempre aggiornato.
A.8.2	Diritti di accesso privilegiato	**Sì**	Implementato	Restrizione rigorosa dell'accesso Root/Admin su AWS e sistemi di produzione.
A.8.3	Restrizione dell'accesso alle informazioni	**Sì**	Implementato	Isolamento dei DB per cliente e segregazione dell'accesso ai dati di produzione LMS.
A.8.4	Accesso al codice sorgente	**Sì**	Implementato	Accesso ai repository GitHub/GitLab regolato da ruoli, MFA e branch protection.
A.8.5	Autenticazione sicura	**Sì**	Implementato	Obbligo tassativo di Autenticazione a Due Fattori (MFA) su tutte le risorse cloud/SaaS.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.6	Capacity management	**Sì**	Implementato	Autoscaling e monitoraggio risorse via AWS CloudWatch per prevenire saturazioni.
A.8.7	Protezione contro i malware	**Sì**	Implementato	Soluzioni Endpoint Protection (EDR/Antivirus) sulle workstation e scansioni container.
A.8.8	Gestione delle vulnerabilità tecniche	**Sì**	Implementato	Scansione automatizzata di codice e librerie (SAST/DAST) in pipeline CI/CD; patch in 48h.
A.8.9	Gestione della configurazione	**Sì**	Implementato	Infrastruttura definita come codice (IaC) e configurazioni di sicurezza standardizzate.
A.8.10	Cancellazione delle informazioni	**Sì**	Implementato	Script automatizzati per la cancellazione sicura dei dati al termine dei contratti (DPA).
A.8.11	Mascheramento dei dati (Data masking)	**Sì**	Implementato	Anonomizzazione/Pseudonimizzazione dei dati di produzione usati in ambienti di test.
A.8.12	Prevenzione della fuga di dati (DLP)	**Sì**	Implementato	Restrizione dei download, blocco condivisioni pubbliche di bucket S3 e monitoraggio log.
A.8.13	Backup delle informazioni	**Sì**	Implementato	Backup automatici giornalieri multi-regione AWS con test di ripristino periodici.
A.8.14	Ridondanza delle strutture di elaborazione	**Sì**	Implementato	Architettura Cloud distribuita su più Multi-Availability Zone (Multi-AZ AWS).

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.15	Logging	**Sì**	Implementato	Abilitazione di log centralizzati su AWS CloudWatch/CloudTrail e conservazione protetta.
A.8.16	Attività di monitoraggio	**Sì**	Implementato	Allarmi in tempo reale per accessi anomali, errori di sistema o picchi di traffico.
A.8.17	Sincronizzazione dell'ora	**Sì**	Implementato	Sincronizzazione automatica del tempo su server e container tramite NTP (AWS Time Sync).
A.8.18	Uso di programmi di utilità privilegiati	**Sì**	Implementato	Restrizione dell'uso di tool di sistema e tracciamento dei comandi amministrativi.
A.8.19	Installazione di software sui sistemi operativi	**Sì**	Implementato	Blocco dell'installazione di software non autorizzato sulle postazioni di lavoro.
A.8.20	Sicurezza delle reti	**Sì**	Implementato	Utilizzo di VPC (Virtual Private Cloud), subnet private e Security Group su AWS.
A.8.21	Sicurezza dei servizi di rete	**Sì**	Implementato	Utilizzo di HTTPS, firewall applicativi (WAF) e protezione anti-DDoS (AWS Shield).
A.8.22	Segregazione delle reti	**Sì**	Implementato	Separazione logica tra ambienti aziendali, ambienti Dev/Staging e Production Cloud.
A.8.23	Filtraggio web	**Sì**	Implementato	Protezione DNS/Endpoint per prevenire la navigazione su siti malevoli o di phishing.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.24	Uso della crittografia	**Sì**	Implementato	Cifratura dei dati in transito (TLS 1.2/1.3) e a riposo (AES-256 su database e storage).
A.8.25	Ciclo di vita dello sviluppo sicuro (Secure SDLC)	**Sì**	Implementato	Linee guida per lo sviluppo sicuro, code review obbligatoria e test di sicurezza.
A.8.26	Requisiti di sicurezza delle applicazioni	**Sì**	Implementato	Analisi dei requisiti di sicurezza per tutti i nuovi moduli o plugin di Forma LMS.
A.8.27	Architettura dei sistemi sicuri e principi di ingegneria	**Sì**	Implementato	Progettazione basata su principi di *Defense in Depth* e *Zero Trust* .
A.8.28	Coding sicuro	**Sì**	Implementato	Adozione degli standard OWASP Top 10 nelle prassi di programmazione del team Dev.
A.8.29	Test di sicurezza nello sviluppo e nell'accettazione	**Sì**	Implementato	Scansioni SAST/DAST e test di collaudo prima di ogni release in produzione.
A.8.30	Sviluppo esternalizzato	**Sì**	Implementato	Controllo del codice e review rigorosa per i plugin forniti da terzi/freelance.
A.8.31	Separazione degli ambienti di sviluppo, test e produzione	**Sì**	Implementato	Ambienti cloud separati e isolati; nessun dato reale di produzione in dev/test.
A.8.32	Gestione del cambiamento (Change management)	**Sì**	Implementato	Flusso di approvazione e tracciamento delle modifiche al codice e all'infrastruttura.
A.8.33	Informazioni di test	**Sì**	Implementato	Utilizzo esclusivo di dati sintetici o pseudonimizzati per gli ambienti di test.

Rif. ISO 27001	Nome Controllo	Applicabile (Sì/No)	Stato di Attuazione	Giustificazione / Modalità di Implementazione
A.8.34	Protezione dei sistemi di informazione durante i test	**Sì**	Implementato	Limitazione e monitoraggio degli accessi agli ambienti di staging e collaudo.

3. SINTESI E APPROVAZIONE

- **Totale controlli ISO/IEC 27001:2022:** 93
- **Controlli Dichiarati Applicabili:** 86
- **Controlli Esclusi (Non Applicabili):** 7 (tutti relativi alla sicurezza fisica perimetrale, motivati dall'architettura 100% Cloud e dal modello organizzativo Full Remote).

La presente Dichiarazione di Applicabilità è approvata dalla Direzione di **Forma Farm S.r.l.** ed è soggetta a riesame almeno annuale o in coincidenza con modifiche rilevanti dell'infrastruttura tecnologica e dei processi di business.

Milano, Ottobre 2026
Forma Farm S.r.l. — La Direzione