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).

Revision #3
Created 2026-10-17 07:41:40 UTC by Alberto Pastorelli
Updated 2026-10-17 07:42:58 UTC by Alberto Pastorelli