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.

Revision #3
Created 2026-10-14 06:49:37 UTC by Alberto Pastorelli
Updated 2026-10-21 11:09:35 UTC by Alberto Pastorelli