					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P33S					Titolo del documento: **Politica di audit e monitoraggio della conformità**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineata a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 9.2, 10	Audit interni, miglioramento continuo e azioni correttive per le non conformità
ISO/IEC 27002:2022	Controlli 5.35, 5.37	Riesami interni pianificati, riesami indipendenti per i processi esternalizzati
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Valutazioni di sicurezza, monitoraggio continuo, riesame/analisi/reporting dell'audit
GDPR UE	Articoli 24 e 32	Audit delle misure tecniche e organizzative, evidenze dell'efficacia dei controlli
NIS2 UE	Articolo 21(2)(f)	Riesame proattivo e conformità basata su evidenze
DORA UE	Articolo 10	Gestione del rischio ICT, monitoraggio e reporting
COBIT 2019	MEA01, MEA03	Monitoraggio/valutazione della conformità, conformità, preparazione ai riesami di terze parti

1. Finalità

1.1 La presente politica definisce l'approccio dell'organizzazione alla conduzione degli audit interni, delle verifiche dei controlli di sicurezza e del monitoraggio della conformità normativa. Garantisce che tutti i controlli, le politiche, i sistemi e i fornitori di servizi siano sottoposti a un riesame regolare e strutturato.

1.2 La finalità è individuare i malfunzionamenti dei controlli, prevenire la non conformità e dimostrare la due diligence ai sensi della ISO/IEC 27001, del GDPR e dei relativi quadri di riferimento.

1.3 Essa consente alle piccole e medie imprese (PMI) di mantenere il controllo operativo e la preparazione alle certificazioni, anche in assenza di una funzione dedicata alla conformità, mediante checklist semplici e ripetibili e risultanze prioritarizzate in base al rischio.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutte le funzioni interne e i fornitori esterni di servizi con responsabilità relative ai sistemi IT, ai dati personali e ai servizi critici per l'operatività aziendale

2.1.2 Tutti i controlli e i sistemi compresi nel campo di applicazione del Sistema di gestione della sicurezza delle informazioni (SGSI)

2.1.3 Tutti gli audit interni, i riesami dei controlli di sicurezza e le verifiche di conformità, sia svolti internamente sia eseguiti da un consulente esterno, da un cliente o da un'autorità di regolamentazione

2.2 La presente politica si applica inoltre alla raccolta delle evidenze e al reporting per:

2.2.1 Audit di certificazione e ricertificazione ISO/IEC 27001

2.2.2 Audit in materia di protezione dei dati ai sensi del GDPR o di clausole contrattuali

2.2.3 Questionari di sicurezza richiesti dai clienti o verifiche di due diligence

2.2.4 Qualsiasi riesame normativo o indipendente ai sensi di NIS2 o DORA, ove applicabile

3. Obiettivi

3.1 Garantire che tutti i controlli e le politiche chiave siano sottoposti a riesame regolare sotto il profilo dell'efficacia e della conformità.

3.2 Mantenere tracce di audit e registrazioni delle azioni correttive per dimostrare accountability e miglioramento.

3.3 Preparare l'organizzazione alla certificazione, alla ricertificazione e ai programmi di assurance richiesti dai clienti (ad es. ISO 27001, onboarding dei fornitori).

3.4 Individuare tempestivamente le lacune per consentire azioni correttive prima che i problemi si aggravino o comportino violazioni di obblighi.

3.5 Consentire al Direttore generale (GM) e al Fornitore di supporto IT di coordinare i riesami con complessità minima, assicurando al contempo esiti sostenibili e difendibili.

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Sovraintende al programma di audit

4.1.2 Approva i piani di riesame interno e le risultanze

4.1.3 Assegna e monitora le azioni correttive

4.1.4 Autorizza il coinvolgimento di auditor esterni o consulenti

4.2 Fornitore di supporto IT / Amministratore

4.2.1 Fornisce evidenze durante gli audit interni ed esterni (ad es. log, configurazioni, registrazioni del controllo degli accessi)

4.2.2 Supporta le verifiche tecniche (ad es. stato dei backup, stato di conformità delle patch)

4.2.3 Mantiene il repository delle evidenze di audit

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Riesame annuale della politica e del piano di audit

9.1.1 Il Direttore generale (GM) deve riesaminare la presente politica e la pianificazione degli audit almeno una volta all'anno.

9.1.2 Il riesame deve valutare:

9.1.2.1 L'efficacia degli audit nell'individuazione delle lacune

9.1.2.2 Il tasso di completamento degli audit e delle azioni correttive

9.1.2.3 Le modifiche ai requisiti legali, normativi o di certificazione applicabili

9.2 Aggiornamenti basati su eventi attivatori

9.2.1 La politica deve essere riesaminata e aggiornata quando:

9.2.2 Un audit di certificazione o di sorveglianza produce una non conformità maggiore

9.2.3 I quadri normativi o regolatori cambiano (ad es. nuove linee guida GDPR, recepimento nazionale della NIS2)

9.2.4 Cambiamenti aziendali incidono su sistemi, processi o fornitori inclusi nell'ambito di audit

9.2.5 Un incidente critico o una violazione rivelano lacune nei controlli precedentemente non individuate

9.3 Documentazione degli aggiornamenti

9.3.1 Tutte le revisioni devono essere tracciate in un registro di controllo delle versioni della politica

9.3.2 Gli aggiornamenti devono essere distribuiti a tutti i membri del team coinvolti negli audit

9.3.3 Alla politica aggiornata deve essere allegata una sintesi delle modifiche per garantirne la comprensione

10. Politiche correlate e collegamenti

10.1 La presente politica è supportata da diverse altre politiche SME e ne rafforza l'applicazione:

10.1.1 P1S – Politica per la sicurezza delle informazioni: definisce la baseline di tutte le aspettative di controllo e ne richiede la verifica tramite audit.

10.1.2 P2S – Politica sui ruoli e sulle responsabilità di governance: stabilisce la responsabilità per la pianificazione degli audit, l'esecuzione e la titolarità delle azioni correttive.

10.1.3 P6S – Politica di gestione del rischio: individua le debolezze dei controlli emerse dagli audit e garantisce che le risultanze siano documentate nel Registro dei rischi.

10.1.4 P17S – Politica di protezione dei dati e privacy: definisce i controlli GDPR da sottoporre ad audit, inclusi gestione dei dati, risposta alle violazioni e informative privacy.

10.1.5 P22S – Politica di registrazione e monitoraggio: fornisce i log di audit e i dati forensi utilizzati durante i riesami di conformità e dei controlli.

10.1.6 P30S – Politica di risposta agli incidenti (P30): richiede l'audit periodico delle registrazioni degli incidenti e dei riesami successivi all'evento per verificare l'efficacia della risposta.

10.1.7 P31S – Politica di raccolta delle evidenze e forense: fornisce le procedure per raccogliere evidenze verificabili in catena di custodia durante gli audit.

10.2 Nel loro insieme, queste politiche creano un ambiente di controllo a ciclo chiuso che consente verifica interna, assurance esterna e governance allineata agli standard.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001:

11.1.1 Clausola 9.2 – Richiede audit interni per valutare le prestazioni del SGSI e il suo allineamento ai requisiti.

11.1.2 Clausola 10.1 – Impone il miglioramento continuo sulla base dei risultati dell'audit e delle azioni correttive per le non conformità.

11.2 ISO/IEC 27002:

11.2.1 Controllo 5.35 – Richiede riesami interni pianificati dei controlli e dei processi.

11.2.2 Controllo 5.37 – Sottolinea l'importanza di riesami indipendenti, in particolare per i processi esternalizzati.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Valutazioni di sicurezza: richiede audit dei controlli implementati per verificarne l'efficacia.

11.3.2 CA-7 – Monitoraggio continuo: sottolinea l'individuazione proattiva e il riesame delle debolezze dei controlli.

11.3.3 AU-6 – Riesame, analisi e reporting dell'audit: richiede l'analisi regolare e la risoluzione dei log di audit e delle risultanze.

11.4 GDPR UE:

11.4.1 Articoli 24 e 32 – Richiedono l'attuazione e l'audit delle misure tecniche e organizzative, incluse evidenze dell'efficacia dei controlli e del miglioramento nel tempo.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articoli 20–21 – Impongono il riesame proattivo dei controlli, la conformità basata su evidenze e la verificabilità per i soggetti essenziali e importanti.

11.6 COBIT 2019:

11.6.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: richiede la valutazione periodica delle prestazioni dei processi e dei controlli rispetto a standard e obiettivi.

11.6.2 MEA03 – Ensure Compliance with External Requirements: si concentra sul monitoraggio interno e sulla preparazione per audit di terze parti e riesami normativi.