					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P33					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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clauses 9.2, 9.3, 10	
ISO/IEC 27002:2022	Controls 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
EU GDPR	Articles 24, 32, 33	
EU NIS2	Article 21(2)(g), 27	
EU DORA	Articles 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Finalità

1.1 La presente politica ha la finalità di definire e disciplinare il programma di audit e monitoraggio della conformità dell'organizzazione al fine di:

1.1.1 convalidare l'efficacia dei controlli di sicurezza e privacy

1.1.2 garantire l'allineamento ai requisiti applicabili, ai quadri di riferimento normativi e agli obblighi contrattuali

1.1.3 rilevare tempestivamente non conformità, inefficienze e rischi di conformità

1.1.4 supportare il miglioramento continuo e la preparazione a certificazioni, valutazioni e riesami normativi

1.2 La presente politica supporta l'integrità e il livello di maturità del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), integrando pratiche di audit e monitoraggio strutturate, basate sul rischio e fondate su evidenze.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i seguenti elementi:

2.1.1 unità organizzative interne, funzioni e dipartimenti

2.1.2 sedi fisiche, ambienti cloud, piattaforme SaaS e servizi esternalizzati

2.1.3 sistemi informativi, applicazioni, infrastrutture e asset informativi disciplinati dal SGSI

2.1.4 dipendenti, collaboratori esterni e fornitori terzi soggetti a obblighi di audit o di conformità

2.2 La politica copre:

2.2.1 audit interni

2.2.2 audit esterni e di certificazione

2.2.3 monitoraggio tecnico della conformità

2.2.4 audit dei fornitori e delle terze parti

2.2.5 azioni correttive e preventive (CAPA)

2.2.6 metriche, dashboard e processi di rendicontazione

2.3 Si applica a tutti i quadri di riferimento rilevanti cui l'organizzazione è soggetta, inclusi, a titolo esemplificativo, ISO/IEC 27001, GDPR, NIS2, DORA e SOC 2.

3. Obiettivi

3.1 Verificare l’adeguatezza e l’efficacia dei controlli, delle politiche e delle procedure attuate nell’ambito del SGSI e degli ambienti correlati.

3.2 Identificare e correggere eventuali carenze, non conformità o lacune di conformità prima che si trasformino in incidenti o violazioni.

3.3 Garantire una preparazione continua ai riesami di governance interni, agli audit esterni e alle certificazioni indipendenti.

3.4 Generare evidenze sostenibili e tracce di audit a supporto di richieste delle autorità di regolamentazione, procedimenti legali o richieste di assurance dei clienti.

3.5 Integrare gli esiti degli audit nelle più ampie attività dell’organizzazione relative alla gestione del rischio, alle metriche di sicurezza e al miglioramento continuo.

4. Ruoli e responsabilità

4.1 Responsabile dell’audit interno / Compliance Manager

4.1.1 Pianifica, programma ed esegue gli audit interni in base alle priorità di rischio.

4.1.2 Mantiene il Registro degli audit, coordina le attività di audit e monitora le azioni correttive.

4.2 Responsabile della sicurezza delle informazioni (CISO)

4.2.1 Garantisce che l’ambito dell’audit comprenda tutti gli elementi rilevanti del SGSI e i controlli dell’Allegato A.

4.2.2 Supervisiona la verifica delle CAPA e integra gli esiti degli audit nel programma di sicurezza.

[... 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 La presente politica deve essere riesaminata almeno annualmente dal Compliance Manager e dal CISO, o prima in risposta a:

9.1.1 modifiche dei quadri normativi, contrattuali o di certificazione

9.1.2 risultanze di audit significative o ripetuti fallimenti dei controlli

9.1.3 riorganizzazioni aziendali o modifiche del sistema GRC

9.1.4 raccomandazioni degli auditor esterni o rilievi delle autorità di regolamentazione

9.2 Il processo di riesame deve valutare:

9.2.1 metodologia e frequenza della pianificazione degli audit

9.2.2 modifiche al campo di applicazione del SGSI o all’infrastruttura

9.2.3 aggiornamenti al catalogo dei controlli o al registro normativo

9.2.4 coerenza e qualità delle evidenze di audit e dei processi CAPA

9.3 Tutte le modifiche alle politiche devono essere:

9.3.1 documentate in un repository soggetto a controllo delle versioni

9.3.2 approvate dalla Direzione aziendale

9.3.3 comunicate a tutto il personale interessato e integrate nelle procedure aggiornate e nei programmi di sensibilizzazione

9.4 La convalida successiva al riesame deve confermare che i requisiti aggiornati siano recepiti nel Registro degli audit, negli strumenti di conformità e nelle dashboard di monitoraggio interne.

10. Politiche correlate e collegamenti

10.1 La presente politica è allineata alle seguenti politiche organizzative correlate:

10.1.1 P1 – Politica per la sicurezza delle informazioni: definisce il SGSI e stabilisce la responsabilità per la conformità e il miglioramento continuo

10.1.2 P5 – Politica di gestione delle modifiche: garantisce la visibilità di audit sulle modifiche all'infrastruttura e alla configurazione che incidono sugli ambienti di controllo

10.1.3 P6 – Politica di gestione del rischio: integra gli esiti degli audit nelle attività aziendali di valutazione e trattamento del rischio

10.1.4 P14 – Politica di conservazione e smaltimento dei dati: disciplina la conservazione delle evidenze di audit, dei log e delle registrazioni di conformità

10.1.5 P18 – Politica sui controlli crittografici: supporta l'archiviazione e il trasferimento sicuri dei dati di audit sensibili

10.1.6 P26 – Politica di sicurezza delle terze parti e dei fornitori: disciplina i diritti di audit, la documentazione di assurance e la supervisione della conformità dei fornitori

10.1.7 P30 – Politica di risposta agli incidenti (P30): allinea gli audit dei processi di gestione degli incidenti agli obiettivi di assurance del SGSI

10.1.8 P32 – Politica di continuità operativa e ripristino di emergenza: richiede la verifica dei test di continuità e della conformità al DRP durante i cicli di audit

11. Standard e quadri di riferimento

11.1 La presente politica è allineata agli standard globali e ai requisiti legali in materia di audit e convalida continua della conformità.

11.2 ISO/IEC 27001:

11.2.1 Clausola 9.2 – Audit interno: richiede audit periodici del SGSI basati sul rischio per valutarne efficacia e conformità.

11.2.2 Clausola 9.3 – Riesame della direzione: gli esiti degli audit devono confluire nel riesame strategico e nel miglioramento.

11.2.3 Clausola 10.1 – Non conformità e azione correttiva: le risultanze di audit devono essere trattate tramite procedure CAPA documentate.

11.3 ISO/IEC 27002:2022 – Controlli 5.35–5.37:

11.3.1 Controlli dell'Allegato A 5.35–5.37: coprono il riesame indipendente, la conformità ai requisiti legali e contrattuali e la registrazione di audit.

11.3.2 Forniscono indicazioni di attuazione per pianificare, eseguire e migliorare i programmi di audit e conformità.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Valutazioni dei controlli: richiede il riesame periodico dei controlli di sicurezza attuati.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): è allineato al tracciamento e alla remediation delle risultanze di audit.

11.4.3 CA-7 – Monitoraggio continuo: supporta valutazioni proattive e automatizzate della conformità.

11.5 GDPR UE (2016/679):

11.5.1 Articoli 24 e 32: richiedono evidenze dell'attuazione e dell'efficacia dei controlli di sicurezza attraverso adeguati assetti di governance.

11.5.2 Articolo 33: supporta la necessità di tracce di audit verificate per la risposta a una violazione e la relativa notifica.

11.6 Direttiva NIS2 UE (2022/2555):

11.6.1 Articolo 21(2)(g): richiede l'audit di politiche e procedure come parte delle misure minime di gestione del rischio di cibersicurezza.

11.6.2 Articolo 27: le autorità nazionali possono effettuare o richiedere audit per i soggetti essenziali e importanti.

11.7 DORA UE (2022/2554):

11.7.1 Articolo 10(2)(e): i soggetti devono effettuare audit interni ed esterni delle pratiche di gestione del rischio ICT.

11.7.2 Articolo 25 – Requisiti di audit: richiede audit periodici da parte di auditor interni o auditor esterni indipendenti con visibilità regolamentare.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: garantisce che l'efficacia dei controlli sia verificata e riportata agli organi di governance.

11.8.2 MEA03 – Monitor, Evaluate and Assess Compliance: richiede l'allineamento delle prassi organizzative ai requisiti legali, contrattuali e basati su standard.