					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: PII18					Titolo del documento: **Politica di monitoraggio, audit e miglioramento del PIMS**							
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**

Allineamento a standard e normative applicabili

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Misurazione degli obiettivi privacy
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informazioni documentate relative a monitoraggio, audit e miglioramento
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitoraggio della pianificazione operativa e del controllo
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitoraggio, misurazione, analisi e valutazione
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audit interno
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Riesame della direzione
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Miglioramento continuo
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Non conformità e azione correttiva
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registrazioni dei trattamenti del titolare del trattamento utilizzate per l'audit
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Accordo del responsabile del trattamento ed evidenze di cooperazione per l'audit
GDPR	Article 5(2)	Controller	Supporting	Evidenze di responsabilizzazione
GDPR	Article 24	Controller	Supporting	Misure del titolare del trattamento e riesame dell'efficacia
GDPR	Article 28	Both	Supporting	Governance degli audit e della cooperazione del

				responsabile del trattamento
GDPR	Article 30	Both	Supporting	Registrazioni dei trattamenti utilizzate per l'audit
GDPR	Article 32	Both	Supporting	Test e valutazione delle misure di sicurezza
GDPR	Article 39	Conditional	Supporting	Monitoraggio e consulenza sugli audit da parte del DPO, ove applicabile
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Conformità privacy, audit e supervisione indipendente
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Riesame della protezione dei PII e verifiche di conformità
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitoraggio e valutazione della sicurezza delle informazioni
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Supporto all'audit interno ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Supporto al riesame della direzione ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Supporto al miglioramento continuo ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Supporto alle non conformità e alle azioni correttive ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Riesame indipendente della sicurezza delle informazioni
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Riesame della conformità di politiche e standard
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Principi, programma, conduzione e competenza per gli

				audit dei sistemi di gestione

1. Ambito di applicazione

1.1 La presente politica definisce i requisiti dell'organizzazione per il monitoraggio, la misurazione, l'analisi, la valutazione, l'audit interno, il riesame della direzione, la gestione delle non conformità, le azioni correttive e il miglioramento continuo del PIMS.

1.2 La presente politica si applica a quanto segue:

1.2.1 tutti i processi, i controlli, le politiche, i registri, gli elementi di evidenza, i sistemi, i fornitori, i responsabili del trattamento, i sub-responsabili e gli accordi di condivisione dei dati compresi nell'ambito di applicazione del PIMS;

1.2.2 i contesti dell'organizzazione quale titolare del trattamento, contitolare del trattamento, responsabile del trattamento e sub-responsabile;

1.2.3 il monitoraggio consolidato delle prestazioni del PIMS, degli obiettivi privacy, dello stato di attuazione dei controlli, delle risultanze dell'audit, delle non conformità, delle azioni correttive, delle azioni derivanti dal riesame della direzione e delle azioni di miglioramento;

1.2.4 le evidenze conservate in REG12 e le evidenze di origine a supporto conservate in REG01 fino a REG11.

1.3 La presente politica non sostituisce i requisiti di monitoraggio operativo definiti in altre politiche PIMS. Essa stabilisce il ciclo consolidato di valutazione delle prestazioni, audit, riesame e miglioramento per il PIMS.

1.4 Ai fini della presente politica, una non conformità del PIMS maggiore indica un mancato adempimento che incide in modo sostanziale sull'ambito di applicazione del PIMS, sugli obiettivi privacy, sulla responsabilizzazione del trattamento dei PII, sul trattamento del rischio privacy, sui diritti degli interessati, sulla sicurezza del trattamento, sulla governance dei responsabili del trattamento o dei sub-responsabili, sulla preparazione alla gestione delle violazioni, sull'integrità delle evidenze documentate, sull'ambito della certificazione o sulla ripetizione del mancato rispetto dello stesso requisito nell'arco di 12 mesi.

1.5 Ai fini della presente politica, una modifica sostanziale indica qualsiasi modifica che incida sull'ambito di applicazione del PIMS, sulle finalità del trattamento dei PII, sulle categorie di PII, sulle categorie di interessati, sui luoghi di trattamento, sull'allocazione dei ruoli di titolare del trattamento o responsabile del trattamento, sull'architettura di sistema, sugli accordi con fornitori o sub-responsabili, sul profilo di rischio privacy, sugli obblighi legali o contrattuali applicabili, sull'ambito dell'audit, sul metodo di monitoraggio o sull'ambito della certificazione.

2. Finalità

2.1 La finalità della presente politica è garantire che l'organizzazione valuti le prestazioni del PIMS, verifichi la conformità del PIMS, identifichi le non conformità, corregga le debolezze dei controlli e migliori continuamente il PIMS mediante evidenze oggettive.

2.2 La presente politica consente all'organizzazione di dimostrare che le attività di monitoraggio, audit, riesame della direzione e miglioramento del PIMS sono pianificate, indipendenti ove richiesto, basate su evidenze, tempestive e tracciabili a ruoli responsabili e a elementi di evidenza canonici.

3. Obiettivi

3.1 Gli obiettivi della presente politica sono:

3.1.1 definire un processo consolidato di monitoraggio e misurazione del PIMS;

3.1.2 garantire che gli obiettivi privacy e le prestazioni dei controlli PIMS siano misurati mediante evidenze documentate;

3.1.3 istituire un programma di audit interno del PIMS basato sul rischio;

3.1.4 preservare l'indipendenza e l'obiettività nelle attività di audit del PIMS;

3.1.5 garantire che il riesame della direzione riceva input completi e aggiornati sulle prestazioni del PIMS;

3.1.6 garantire che le non conformità siano registrate, valutate, corrette e verificate;

3.1.7 garantire che le azioni correttive siano tracciate fino alla chiusura e riesaminate per verificarne l'efficacia;

3.1.8 identificare debolezze ricorrenti e opportunità di miglioramento;

3.1.9 supportare la preparazione alle certificazioni e la gestione responsabile delle evidenze;

3.1.10 evitare duplicazioni delle metriche operative già definite nelle politiche PIMS correlate.

4. Dichiarazioni della politica

4.1 Quadro di monitoraggio e misurazione del PIMS

4.1.1 [Both] Il Privacy Lead / PIMS Manager DEVE definire il programma di monitoraggio del PIMS consolidato in REG12 prima dell'operatività iniziale del PIMS e successivamente con cadenza annuale.

4.1.2 [Both] Il Privacy Lead / PIMS Manager DEVE definire in REG12 il metodo di misurazione, la frequenza, la fonte delle evidenze, l'obiettivo e il ruolo responsabile per ciascuna metrica PIMS prima dell'avvio del ciclo di misurazione.

4.1.3 [Both] Il Process Owner / Business Owner DEVE fornire trimestralmente al Privacy Lead / PIMS Manager gli input di monitoraggio delle attività di trattamento dei PII provenienti da REG02.

4.1.4 [Both] L'Information Security Lead DEVE fornire trimestralmente al Privacy Lead / PIMS Manager gli input sullo stato dei controlli di sicurezza dei PII provenienti da REG03.

4.1.5 [Both] Il Vendor / Procurement Owner DEVE fornire trimestralmente al Privacy Lead / PIMS Manager gli input sullo stato di assurance relativi a responsabili del trattamento, sub-responsabili, condivisione con terze parti e fornitori provenienti da REG08.

4.1.6 [All] L'Incident Response Coordinator DEVE fornire al Privacy Lead / PIMS Manager gli input sulle tendenze relative agli incidenti privacy e alle violazioni provenienti da REG10 mensilmente ed entro 10 giorni lavorativi dalla chiusura di un incidente maggiore.

4.1.7 [Both] Il Privacy Lead / PIMS Manager DEVE consolidare trimestralmente in REG12 i risultati del monitoraggio del PIMS.

4.2 Programma di audit interno del PIMS

4.2.1 [All] L'Internal Audit / Compliance Reviewer DEVE predisporre annualmente in REG12 un programma di audit interno del PIMS basato sul rischio prima del primo ciclo di audit PIMS pianificato.

4.2.2 [All] L'Internal Audit / Compliance Reviewer DEVE definire in REG12 l'obiettivo, i criteri, l'ambito, il metodo, la base di campionamento e il termine di rendicontazione per ciascun audit PIMS prima dell'avvio delle attività di audit sul campo.

4.2.3 [All] L'Internal Audit / Compliance Reviewer DEVE registrare in REG12 i controlli di indipendenza dell'auditor e di conflitto di interessi prima di ogni incarico di audit.

4.2.4 [All] Il Privacy Lead / PIMS Manager DEVE rendere disponibili tramite REG12 le informazioni documentate del PIMS controllate e le evidenze dei registri richieste entro 10 giorni lavorativi da una richiesta di audit approvata.

4.2.5 [Both] L'Internal Audit / Compliance Reviewer DEVE testare lo stato di attuazione dei controlli PIMS applicabili rispetto a REG03 durante ciascun audit PIMS.

4.2.6 [Both] L'Internal Audit / Compliance Reviewer DEVE registrare in REG12 il campione selezionato di evidenze relative al trattamento dei PII durante ciascun audit PIMS.

4.2.7 [All] L'Internal Audit / Compliance Reviewer DEVE registrare in REG12 i risultati dell'audit PIMS entro 15 giorni lavorativi dal completamento dell'audit.

4.2.8 [All] Il Privacy Lead / PIMS Manager DEVE assegnare in REG12 i titolari delle azioni correttive per le risultanze di audit PIMS accettate entro 10 giorni lavorativi dall'accettazione dei risultati dell'audit.

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

9. Eccezioni

9.1 Eccezioni al monitoraggio, all'audit e al miglioramento

9.1.1 [All] Il Process Owner / Business Owner DEVE richiedere in REG12 qualsiasi eccezione alla presente politica prima che si verifichi lo scostamento.

9.1.2 [All] Il Privacy Lead / PIMS Manager DEVE valutare in REG12 l'impatto privacy, di certificazione, di audit e sulle azioni correttive di ciascuna eccezione richiesta entro 10 giorni lavorativi dalla richiesta.

9.1.3 [All] Il Data Protection Officer / Privacy Advisor DEVE registrare il proprio parere in REG12 prima dell'approvazione di qualsiasi eccezione che incida su obblighi legali, diritti degli interessati, impegni DPIA, obblighi di audit dei clienti o trattamenti ad alto rischio.

9.1.4 [All] Top Management DEVE approvare in REG12 le eccezioni che incidono sul completamento del piano di audit, sul riesame della direzione, sulle non conformità maggiori, sull'ambito della certificazione o sui trattamenti ad alto rischio prima che l'eccezione abbia effetto.

9.1.5 [All] Il Privacy Lead / PIMS Manager DEVE impostare in REG12 una data di scadenza non superiore a 90 giorni per ciascuna eccezione approvata relativa a monitoraggio, audit o miglioramento.

9.1.6 [All] Il Privacy Lead / PIMS Manager DEVE chiudere o rivalutare in REG12 ciascuna eccezione relativa a monitoraggio, audit o miglioramento entro cinque giorni lavorativi dalla scadenza.

10. Applicazione

10.1 Applicazione dei requisiti di monitoraggio, audit e miglioramento

10.1.1 [All] Il Privacy Lead / PIMS Manager DEVE registrare in REG12 un ciclo di monitoraggio mancato, un audit PIMS mancato, un riesame della direzione scaduto, evidenze di audit mancanti, un'azione correttiva scaduta o un'azione di miglioramento scaduta come non conformità entro cinque giorni lavorativi dall'identificazione.

10.1.2 [All] L'Internal Audit / Compliance Reviewer DEVE registrare in REG12 la gravità della risultanza di audit prima dell'emissione del rapporto di audit.

10.1.3 [All] Top Management DEVE richiedere in REG12 un'azione correttiva per ciascuna non conformità del PIMS maggiore entro 10 giorni lavorativi dall'escalation.

10.1.4 [All] Il Process Owner / Business Owner DEVE impedire la messa in esercizio o la presentazione di assurance esterna per trattamenti ad alto rischio quando le evidenze richieste delle azioni correttive mancano da REG12 prima della messa in esercizio o della presentazione.

10.1.5 [All] Il Privacy Lead / PIMS Manager DEVE effettuare escalation a Top Management in REG12 in caso di ripetuto mancato rispetto delle scadenze di monitoraggio o delle azioni correttive entro cinque giorni lavorativi dal secondo evento in un periodo di 12 mesi.

10.1.6 [All] L'Internal Audit / Compliance Reviewer DEVE verificare in REG12 la chiusura dell'azione di applicazione al successivo audit pianificato o entro 60 giorni dalla chiusura dichiarata, a seconda di quale evento si verifichi per primo.

11. Riesame e manutenzione

11.1 Riesame e manutenzione della politica

11.1.1 [All] Il Privacy Lead / PIMS Manager DEVE riesaminare la presente politica in REG12 annualmente e entro 30 giorni da una modifica sostanziale ai requisiti di monitoraggio, audit, riesame della direzione, azione correttiva o certificazione del PIMS.

11.1.2 [All] L'Internal Audit / Compliance Reviewer DEVE riesaminare annualmente in REG12 l'efficacia del programma di audit PIMS dopo l'ultimo audit pianificato dell'anno operativo del PIMS.

11.1.3 [All] Il Data Protection Officer / Privacy Advisor DEVE riesaminare in REG12 le modifiche alla presente politica significative per la privacy prima dell'approvazione.

11.1.4 [All] Top Management DEVE approvare in REG12 le modifiche sostanziali alla presente politica prima della pubblicazione.

11.1.5 [All] Il Privacy Lead / PIMS Manager DEVE aggiornare REG01 e REG03 entro 15 giorni lavorativi dalle modifiche approvate alla presente politica che alterino l'ambito di applicazione del PIMS o l'applicabilità dei controlli.

11.1.6 [All] Il Privacy Lead / PIMS Manager DEVE registrare in REG11 la comunicazione delle modifiche approvate alla presente politica entro 30 giorni dalla pubblicazione.

12. Politiche correlate

12.1 La presente politica è supportata dalle seguenti politiche correlate:

12.2 PII01 - Politica del sistema di gestione delle informazioni sulla privacy

12.3 PII02 - Politica sui ruoli, le responsabilità e la responsabilizzazione privacy

12.4 PII03 - Politica sull'inventario dei trattamenti PII e sulla base giuridica

12.5 PII04 - Politica sull'informativa privacy e sulla trasparenza

12.6 PII05 - Politica di gestione del consenso e delle preferenze

12.7 PII06 - Politica di gestione dei diritti degli interessati

12.8 PII07 - Politica di valutazione del rischio privacy e DPIA

12.9 PII08 - Politica privacy by design e by default

12.10 PII09 - Politica sulla raccolta, l'uso, la comunicazione e la condivisione dei PII

12.11 PII10 - Politica di conservazione, cancellazione e smaltimento dei PII

12.12 PII11 - Politica di accuratezza e qualità dei PII

12.13 PII12 - Politica di gestione privacy di responsabili del trattamento, sub-responsabili e terze parti

12.14 PII13 - Politica sui trasferimenti internazionali di PII

12.15 PII14 - Politica di sicurezza dei PII e controllo degli accessi

12.16 PII15 - Politica di gestione degli incidenti e delle violazioni dei PII

12.17 PII16 - Politica di formazione, sensibilizzazione e competenza privacy

12.18 PII17 - Politica di gestione delle informazioni documentate e delle evidenze del PIMS

13. Standard e quadri di riferimento

13.1 La presente politica è mappata ai seguenti standard e regolamenti. La mappatura spiega in che modo la politica supporta i requisiti citati e identifica le clausole interne che li attuano o li supportano.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Mappata alla definizione, misurazione, rendicontazione e riesame degli obiettivi PIMS e delle metriche di prestazione del PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Mappata al mantenimento di informazioni documentate per risultati del monitoraggio, programmi di audit, risultati degli audit, evidenze del riesame della direzione, non conformità, azioni correttive e azioni di miglioramento. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Mappata all'esecuzione del ciclo pianificato di monitoraggio PIMS, audit, azione correttiva e miglioramento quale parte del controllo operativo del PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Mappata alla definizione di ciò che è monitorato e misurato, al consolidamento dei risultati del monitoraggio, alla valutazione delle prestazioni del PIMS e al mantenimento delle evidenze di misurazione. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Mappata al mantenimento del programma di audit interno, alla pianificazione degli audit, ai controlli di indipendenza dell'auditor, al campionamento delle evidenze, ai risultati degli audit e al follow-up delle risultanze di audit. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Mappata alla pianificazione del riesame della direzione, al riesame delle prestazioni del PIMS, al riesame delle tendenze relative ad audit e azioni correttive, all'approvazione degli output e alle decisioni sulle risorse. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Mappata all'identificazione, approvazione, attuazione e tracciamento delle opportunità di miglioramento continuo per l'idoneità, l'adeguatezza e l'efficacia del PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Mappata alla registrazione delle non conformità, all'analisi della causa radice, alla pianificazione delle azioni correttive, all'attuazione delle azioni correttive, alla verifica dell'efficacia, all'escalation e all'applicazione. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Mappata alle registrazioni dei trattamenti del titolare del trattamento utilizzate come fonti di evidenza per monitoraggio, campionamento di audit e metriche di aggiornamento dell'inventario dei trattamenti. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Mappata all'accordo del responsabile del trattamento, all'audit del cliente, alla risposta di assurance e alle evidenze di cooperazione del responsabile del trattamento tracciate tramite i processi di assurance dei fornitori e dei clienti. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Mappata alle evidenze di responsabilizzazione per monitoraggio, audit, riesame della direzione, azione correttiva e miglioramento continuo. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Mappata alle misure di governance del titolare del trattamento, al riesame dell'efficacia, al riesame della direzione, all'azione correttiva e alle evidenze documentate di miglioramento. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Mappata alle evidenze relative a responsabili del trattamento, sub-responsabili, audit dei clienti, assurance delle terze parti e cooperazione dei fornitori. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Mappata alle registrazioni dei trattamenti utilizzate come evidenze per monitoraggio, campionamento di audit, completezza degli elementi di evidenza e aggiornamento dell'inventario dei trattamenti. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Mappata al monitoraggio e alla valutazione dello stato dei controlli di sicurezza dei PII, delle evidenze dei controlli tecnici e delle evidenze di efficacia relative alla sicurezza. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Mappata alla consulenza privacy, alle osservazioni di monitoraggio, al supporto agli audit e al riesame delle tendenze di conformità privacy da parte del Data Protection Officer / Privacy Advisor ove applicabile. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mappata alla verifica della conformità privacy, agli audit interni o indipendenti, ai controlli interni, ai meccanismi di supervisione e alle evidenze di valutazione del rischio privacy. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Mappata al riesame indipendente della sicurezza delle informazioni relativa ai PII, alla conformità a politiche e standard e al riesame della conformità tecnica per la protezione dei PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Mappata agli input di monitoraggio e valutazione della sicurezza delle informazioni che supportano la misurazione delle prestazioni del PIMS e lo stato dei controlli di sicurezza dei PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Mappata al supporto all'audit interno ISMS per la pianificazione degli audit PIMS, le evidenze di audit, i risultati degli audit e il completamento del programma di audit. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Mappata agli input e agli output del riesame della direzione per la supervisione integrata delle prestazioni del PIMS e della sicurezza delle informazioni. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Mappata al miglioramento continuo del PIMS e dell'ambiente di controllo della sicurezza delle informazioni a supporto. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Mappata alla gestione delle non conformità, alla pianificazione delle azioni correttive, all'attuazione delle azioni correttive e alla verifica dell'efficacia. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Mappata al riesame indipendente, ai controlli di indipendenza dell'auditor, ai test delle evidenze di audit e alla verifica indipendente dell'efficacia delle azioni correttive. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Mappata al riesame di conformità delle politiche PIMS e di sicurezza delle informazioni, dello stato di attuazione dei controlli e delle evidenze di conformità agli standard. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Mappata ai principi di audit, alla gestione del programma di audit, alla conduzione degli audit, alla rendicontazione di audit basata su evidenze, al follow-up degli audit e alle aspettative di competenza degli auditor per gli audit PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].