					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P33					Titlul documentului: **Politica de audit și monitorizare a conformității**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 9.2, 9.3, 10	
ISO/IEC 27002:2022	Controalele 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
RGPD al UE	Articolele 24, 32, 33	
Directiva NIS2 a UE	Articolul 21(2)(g), 27	
Regulamentul DORA al UE	Articolele 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Scop

1.1 Scopul acestei politici este de a stabili și guverna programul de audit și monitorizare a conformității al organizației, pentru a:

1.1.1 valida eficacitatea controalelor de securitate și de protecție a datelor

1.1.2 asigura alinierea la standardele aplicabile, cadrele juridice și obligațiile contractuale

1.1.3 identifica în timp util neconformitățile, ineficiențele și riscurile de conformitate

1.1.4 sprijini îmbunătățirea continuă și pregătirea pentru certificări, evaluări și revizuiri de reglementare

1.2 Această politică susține integritatea și maturitatea Sistemului de management al securității informației (SMSI) prin integrarea unor practici de audit și monitorizare structurate, bazate pe risc și pe dovezi documentate.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor:

2.1.1 liniilor de activitate, funcțiilor și departamentelor interne

2.1.2 locațiilor fizice, mediilor cloud, platformelor SaaS și serviciilor externalizate

2.1.3 sistemelor informatice, aplicațiilor, infrastructurii și activelor de date guvernate de SMSI

2.1.4 angajaților, contractorilor și furnizorilor terți de servicii care au obligații de audit sau de conformitate

2.2 Politica acoperă:

2.2.1 auditurile interne

2.2.2 auditurile externe/de certificare

2.2.3 monitorizarea tehnică a conformității

2.2.4 auditurile furnizorilor și terților

2.2.5 acțiunile corective și preventive (CAPA)

2.2.6 indicatorii, tablourile de bord și procesele de raportare

2.3 Se aplică tuturor cadrelor relevante la care este supusă organizația, inclusiv ISO/IEC 27001, RGPD, NIS2, DORA și SOC 2, precum și altora.

3. Obiective

3.1 Verificarea adecvării și eficacității controalelor, politicilor și procedurilor implementate în cadrul SMSI și al mediilor asociate.

3.2 Identificarea și remedierea oricăror deficiențe, neconformități sau lacune de control înainte ca acestea să se transforme în incidente sau încălcări.

3.3 Asigurarea unei stări susținute de pregătire pentru audit în vederea revizuirilor interne de guvernanță, a auditurilor externe și a certificărilor independente.

3.4 Generarea de dovezi documentate și piste de audit care să susțină solicitările autorităților de reglementare, procedurile judiciare sau cerințele clienților privind asigurarea controalelor.

3.5 Integrarea rezultatelor auditului în activitățile mai ample ale organizației privind managementul riscurilor, indicatorii de securitate și îmbunătățirea continuă.

4. Roluri și responsabilități

4.1 Responsabilul cu auditul intern / Managerul de conformitate

4.1.1 Planifică, programează și efectuează auditurile interne pe baza priorităților de risc.

4.1.2 Menține Registrul de audit, coordonează activitățile de audit și urmărește acțiunile corective.

4.2 Directorul de securitate a informațiilor (CISO)

4.2.1 Se asigură că domeniul de audit acoperă toate elementele relevante ale SMSI și controalele din Anexa A.

4.2.2 Asigură supravegherea verificării CAPA și integrează rezultatele auditului în programul de securitate.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1 Această politică trebuie revizuită cel puțin anual de Managerul de conformitate și de CISO sau mai devreme, ca răspuns la:

9.1.1 schimbări ale cadrelor de reglementare, contractuale sau de certificare

9.1.2 constatări semnificative de audit sau eșecuri repetate ale controalelor

9.1.3 restructurări organizaționale sau modificări ale sistemului GRC

9.1.4 recomandări ale auditorilor externi sau feedback din partea autorităților de reglementare

9.2 Procesul de revizuire trebuie să evalueze:

9.2.1 metodologia și frecvența planificării auditului

9.2.2 schimbările privind domeniul de aplicare al SMSI sau infrastructura

9.2.3 actualizările aduse catalogului de controale sau registrului cerințelor legale

9.2.4 consecvența și calitatea dovezilor de audit și a proceselor CAPA

9.3 Toate modificările politicii trebuie să fie:

9.3.1 documentate într-un depozit supus controlului versiunilor

9.3.2 aprobate de managementul executiv

9.3.3 comunicate întregului personal afectat și integrate în procedurile actualizate și în programele de conștientizare

9.4 Validarea ulterioară revizuirii trebuie să confirme că cerințele actualizate sunt reflectate în Registrul de audit, instrumentele de conformitate și tablourile de bord interne de monitorizare.

10. Politici conexe și interdependențe

10.1 Această politică este aliniată cu următoarele politici organizaționale conexe:

10.1.1 P1 – Politica de securitate a informației: definește SMSI și stabilește responsabilitatea pentru conformitate și îmbunătățire continuă

10.1.2 P5 – Politica de management al schimbărilor: asigură vizibilitatea în audit asupra schimbărilor de infrastructură și configurație care afectează mediile de control

10.1.3 P6 – Politica de management al riscurilor: integrează rezultatele auditului în activitățile de evaluare și tratament al riscurilor la nivelul organizației

10.1.4 P14 – Politica de păstrare și eliminare a datelor: guvernează păstrarea dovezilor de audit, a jurnalelor și a înregistrărilor de conformitate

10.1.5 P18 – Politica privind controalele criptografice: sprijină stocarea și transferul securizat al datelor de audit sensibile

10.1.6 P26 – Politica de securitate privind terții și furnizorii: acoperă drepturile de audit, documentația de asigurare și supravegherea conformității furnizorilor

10.1.7 P30 – Politica de răspuns la incidente: aliniază auditurile proceselor de gestionare a incidentelor cu obiectivele de asigurare ale SMSI

10.1.8 P32 – Politica de continuitate a activității și recuperare în caz de dezastru: impune verificarea testării continuității și a conformității planului de recuperare în caz de dezastru (DRP) în cadrul ciclurilor de audit

11. Standarde și cadre de referință

11.1 Această politică este aliniată cu standardele globale și cerințele legale privind auditul și validarea continuă a conformității.

11.2 ISO/IEC 27001:

11.2.1 Clauza 9.2 – Audit intern: impune audituri regulate, bazate pe risc, ale SMSI pentru evaluarea eficacității și a conformității.

11.2.2 Clauza 9.3 – Revizuirea de management: rezultatele auditului trebuie integrate în revizuirea strategică și în îmbunătățire.

11.2.3 Clauza 10.1 – Neconformitate și acțiune corectivă: constatările auditului trebuie tratate prin proceduri CAPA documentate.

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

11.3.1 Controalele din Anexa A 5.35–5.37: acoperă revizuirea independentă, conformitatea cu cerințele legale/contractuale și jurnalizarea auditului.

11.3.2 Oferă îndrumări de implementare pentru planificarea, desfășurarea și îmbunătățirea programelor de audit și conformitate.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Evaluări ale controalelor: impune revizuirea de rutină a controalelor de securitate implementate.

11.4.2 CA-5 – Plan de acțiune și etape (POA&M): este aliniat cu urmărirea și remedierea constatărilor de audit.

11.4.3 CA-7 – Monitorizare continuă: susține evaluări proactive și automatizate ale conformității.

11.5 RGPD al UE (2016/679):

11.5.1 Articolele 24 și 32: impun existența unor dovezi privind implementarea și eficacitatea controalelor de securitate prin structuri de guvernanță adecvate.

11.5.2 Articolul 33: susține necesitatea unor piste de audit verificate pentru răspunsul la încălcări și notificarea acestora.

11.6 Directiva NIS2 a UE (2022/2555):

11.6.1 Articolul 21(2)(g): impune auditarea politicilor și procedurilor ca parte a măsurilor minime de management al riscurilor de securitate cibernetică.

11.6.2 Articolul 27: autoritățile naționale pot efectua sau solicita audituri pentru entitățile esențiale și importante.

11.7 Regulamentul DORA al UE (2022/2554):

11.7.1 Articolul 10(2)(e): entitățile trebuie să efectueze audituri interne și externe ale practicilor de management al riscurilor TIC.

11.7.2 Articolul 25 – Cerințe de audit: impune audituri periodice realizate de auditori interni sau auditori externi independenți, cu vizibilitate pentru autoritățile de reglementare.

11.8 COBIT 2019:

11.8.1 MEA01 – Măsurare, evaluare și analiză a performanței și conformității: asigură verificarea eficacității controalelor și raportarea acesteia către organismele de guvernanță.

11.8.2 MEA03 – Măsurare, evaluare și analiză a conformității: impune alinierea practicilor organizației la cerințele legale, contractuale și bazate pe standarde.