

**S.R.L “CloudSentinel”**

**PROCEDURA AUDITULUI INTERN**

|  |  |
| --- | --- |
| Cod: | PAI-01 |
| Versiune: | 0.4.1a |
| Date of version: | Jun 5, 2024 |
| Created by: | Chirita Stanislav |
| Approved by: | Boboc Sandu |
| Nivelul de confidențialitate: | Secret |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2024-01-01 | 0.1 | Chihai Andrian | Crearea procedurii auditului intern |
| 2024-02-15 | 0.2 | Vozian Vladimir | Adăugarea cerințelor privind selectarea auditorilor interni |
| 2024-04-10 | 0.3 | Vozian Vladimir | Clarificarea criteriilor de numire a auditorilor interni |
| 2024-06-20 | 0.4 | Chirita Stanislav | Actualizarea descrierii procesului de audit intern |
| 2024-09-05 | 0.4.1a | Boboc Sandu | Revizuire generală a întregului document |

**Cuprins**

[1. Scop, domeniu de aplicare și utilizatoriPurpose, scope and users 3](#__RefHeading___Toc1880_1449849499)

[2. Documente de referință 3](#__RefHeading___Toc1882_1449849499)

[3. Auditul intern 3](#__RefHeading___Toc1884_1449849499)

[3.1. Scopul auditului intern 3](#__RefHeading___Toc1886_1449849499)

[3.2. Planificarea auditului intern 3](#__RefHeading___Toc1888_1449849499)

[3.3. Desemnarea auditorilor interni 4](#__RefHeading___Toc1890_1449849499)

[3.4. Efectuarea auditurilor interne individuale 5](#__RefHeading___Toc1892_1449849499)

[4. Gestionarea înregistrărilor păstrate pe baza acestui document 6](#__RefHeading___Toc1894_1449849499)

[5. Valabilitatea și managementul documentelor 7](#__RefHeading___Toc1896_1449849499)

[6. Anexe 7](#__RefHeading___Toc1898_1449849499)

# Scop, domeniu de aplicare și utilizatoriPurpose, scope and users

Scopul acestei proceduri este de a descrie toate activitățile legate de audit – redactarea programului de audit, selectarea unui auditor, efectuarea auditurilor individuale și raportarea.

Această procedură se aplică tuturor activităților desfășurate în cadrul Sistemului de Management al Securității Informației (ISMS). Utilizatorii acestui document sunt membrii managementului de vârf ai CloudSentinel, precum și auditorii interni.

# Documente de referință

* Standardul ISO/IEC 27001, clauza 9.2
* Standardul ISO 22301, clauza 9.2
* Standardul BS 25999-2, clauza 5.1
* Politica Sistemului de Management al Securității
* Politica de Management al Continuității în Afaceri
* Procedură pentru Acţiune Corectivă şi Preventivă
* ISO 19011 standard
* ISO 9001 standard, clause 9.2
* **Business Continuity Management Policy**: Politica internă privind continuitatea afacerii va furniza îndrumări pentru auditul BCMS.

# Auditul intern

## Scopul auditului intern

Scopul auditului intern este de a determina dacă procedurile, controalele, procesele, aranjamentele și alte activități din cadrul ISMS [BCMS] sunt în conformitate cu standardele ISO 27001 și ISO 22301/BS 25999-2, reglementările aplicabile și documentația internă a organizației, dacă sunt implementate și menținute eficient și dacă îndeplinesc cerințele politicii și obiectivele stabilite.

## Planificarea auditului intern

Chief Information Security Officer (CISO) aprobă un program anual pentru auditurile interne, redactat conform formularului din Anexa 1.

Unul sau mai multe audituri interne ar trebui să fie efectuate pe parcursul unui an, asigurând acoperirea cumulativă a întregului domeniu ISMS [BCMS]. Auditurile interne sunt planificate pe baza evaluării riscurilor, precum și a rezultatelor auditărilor anterioare; acestea sunt de obicei efectuate înainte de revizuirea managementului. Programul anual de audit intern trebuie să conțină următoarele informații despre fiecare audit intern individual:

• perioada auditului (specificând datele sau luna în care este planificat auditul)

• domeniul de aplicare al auditului (departamente, procese, clauze ale standardului etc.)

• criteriile auditului (standarde, legislație și reglementări, documentație internă, standarde corporative și/sau obligații contractuale)

• metodele de auditare (revizuirea documentației, interviuri cu angajații, revizuirea înregistrărilor, revizuirea sistemelor informatice etc.)

• cine va efectua auditul (dacă există mai mulți auditori, specificați liderul echipei de audit)

Auditurile efectuate trebuie să fie înregistrate în programul anual de audit intern.

## Desemnarea auditorilor interni

**Managerul de Securitate Informațională** va desemna auditori interni.

Un auditor intern poate fi cineva din organizație sau o persoană din afara organizației. Criteriile pentru desemnarea auditorilor interni sunt:

* cunoștințe despre standardele ISO/IEC 27001 și ISO 22301/BS 25999-2
* familiaritatea cu tehnicile de auditare a sistemelor de management
* cunoștințe despre modul de funcționare a tehnologiilor informației și comunicațiilor, în măsura în care acesta/aceasta este familiarizat(ă) cu scopul sistemelor individuale, precum și cu impacturile asupra proceselor de securitate și/sau asupra continuității afacerii

Auditorii interni trebuie să fie selectați astfel încât să se asigure obiectivitatea și imparțialitatea, adică pentru a evita conflictul de interese, deoarece auditorilor nu le este permis să-și auditeze propriul lucru.

Se recomandă ca auditorii interni să completeze un curs pentru auditori interni conform ISO/IEC 27001.

## Efectuarea auditurilor interne individuale

**Persoanele responsabile pentru auditurile interne individuale sunt identificate în Programul Anual de Audit Intern.** Dacă un audit este realizat de o echipă formată din mai mulți auditori, persoana responsabilă pentru audit este cea desemnată ca Lider al Echipei de Audit.

În timpul unui audit intern, trebuie luate în considerare următoarele:

* criteriile stabilite în Programul Anual de Audit Intern
* rezultatele auditurilor interne sau externe anterioare
* rezultatele evaluării riscurilor, implementarea controalelor, analiza impactului asupra afacerii, etc.
* Lista de verificare a auditului intern – vezi Anexa 3

Rezultatele auditului intern trebuie documentate astfel:

* Raportul de Audit Intern – acesta trebuie trimis către **Managerul de Securitate Informațională**
* acțiunile corective posibile trebuie documentate în Formularul de Acțiuni Corective, conform Procedurii pentru Acțiuni Corective

# Gestionarea înregistrărilor păstrate pe baza acestui document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nume înregistrare** | **Locație de stocare** | **Persoana responsabilă pentru stocare** | **Controale pentru protecția înregistrărilor** | **Perioada de retenție** |
| Programul Anual de Audit Intern (în format electronic) | Calculatorul Managerului de Securitate Informațională | Managerul de Securitate Informațională | Doar Managerul de Securitate Informațională și auditorul intern au dreptul să facă înscrieri și modificări în programul anual de audit intern. | 3 ani |
| Raportul de Audit Intern (în format electronic) | Calculatoarele auditorului intern și Managerului de Securitate Informațională | Auditorul intern | Rapoartele sunt stocate în versiuni doar pentru citire | 3 ani |
| Lista de Verificare a Auditului Intern (formular completat în timpul auditului intern) | Calculatorul auditorului intern | Auditorul intern | Lista de verificare este stocată în versiune doar pentru citire | 3 ani |

Doar Responsabilul de Audit Intern(Managerul de Securitate Informațională) poate acorda altor angajați dreptul de acces la Programul Anual de Audit Intern, Raportul de Audit Intern și Lista de Verificare a Auditului Intern.

# Valabilitatea și managementul documentelor

Acest document este valabil începând cu 01.01.2025.

Proprietarul acestui document este Managerul de Securitate Informațională, care trebuie să verifice și, dacă este necesar, să actualizeze documentul cel puțin o dată pe an.

Atunci când se evaluează eficacitatea și caracterul adecvat al acestui document, trebuie luate în considerare următoarele criterii:

• numărul de acțiuni corective identificate în timpul auditului

• numărul de acțiuni corective identificate în cursul auditului de certificare efectuat după auditul intern

• Întrebarea dacă frecvența auditului intern este în concordanță cu Programul Anual de Audit Intern

# Anexe

* Anexa 1 – Programul anual de audit intern
* Anexa 2 – Raportul de audit intern
* Anexa 3 – Lista de verificare pentru auditul intern

Responsabilul de Securitate a Informațiilor

Boboc Sandu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Semnătura