

# GUVERNANȚA INTELIGENȚEI ARTIFICIALE

DE LA

DECIZIE

LA

CERTIFICARE

Metodologia de implementare a  
SR ISO/IEC 42001:2024



ION IORDACHE

# GUVERNANȚA INTELIGENȚEI ARTIFICIALE

## DE LA DECIZIE LA CERTIFICARE

### GHID PRACTIC

#### METODOLOGIA DE IMPLEMENTARE A SR ISO/IEC 42001:2024

Tehnologia informației - Inteligență artificială - Sistem de management

Autor

Ion Iordache

Consultant de securitate, Lead Implementer, Lead Auditor

Ediția 1, 2026

### Drepturi de autor și licență

© 2026 Ion Iordache. Acest document este distribuit sub licență Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Sunteți liberi să:

- **partajați**, copiați și redistribuiți materialul în orice mediu sau format;
- **adaptați**, reformulați, transformați și construiți pe baza acestui material.

În următoarele condiții:

- **Atribuire**, trebuie să indicați autorul, să furnizați un link către licență și să precizați dacă au fost făcute modificări.
- **Necomercial**, nu puteți utiliza materialul în scopuri comerciale fără acordul scris prealabil al autorului.

Textul integral al licenței este disponibil la: <https://creativecommons.org/licenses/by-nc/4.0/deed.ro>

### Disclaimer profesional

Documentul de față are caracter informativ și metodologic și nu constituie consultanță juridică sau de conformitate. Metodologia de implementare prezentată reflectă experiența și abordarea profesională a autorului și nu reprezintă o interpretare oficială a cerințelor SR ISO/IEC 42001:2024 sau ale Regulamentului (UE) 2024/1689. Pentru aplicarea concretă a acestor cerințe într-o organizație specifică, se recomandă consultarea textelor oficiale ale standardului și ale regulamentului, precum și apelul la consultanță de specialitate calificată.

Studiul de caz prezentat în Capitolul 6 descrie o companie ipotetică, Fortis Security Solutions S.R.L., construită pe un profil compozit reprezentativ pentru sectorul serviciilor de securitate fizică din România. Orice asemănare cu o organizație reală este neintenționată. Situațiile, deciziile și provocările descrise au scop exclusiv ilustrativ și nu constituie o reprezentare a unui angajament de consultanță real.

Standardele menționate în acest ghid sunt protejate prin drepturi de autor ale Asociației de Standardizare din România (ASRO) și se procură exclusiv de pe site-ul oficial [www.asro.ro](http://www.asro.ro). Citatele și referințele din ghid au scop informativ și nu substituie consultarea textelor integrale ale standardelor.

Informațiile privind calendarul de aplicare a AI Act și acordul politic provizoriu din mai 2026 reflectă situația la data redactării acestui ghid (iunie 2026) și pot fi modificate prin adoptarea formală a pachetului Digital Omnibus sau prin alte acte legislative ulterioare.

## Notă de transparență privind utilizarea inteligenței artificiale

Acest ebook a fost elaborat printr-o colaborare hibridă om-inteligență artificială, în care deciziile de conținut, structură și interpretare au rămas în permanență sub controlul autorului.

### Rolul instrumentului AI utilizat

În procesul de documentare și redactare au fost utilizate trei instrumente de inteligență artificială generativă. **Claude Sonnet 4.6**, dezvoltat de Anthropic, a fost utilizat pentru:

- redactarea inițială a textului fiecărui capitol, pe baza instrucțiunilor structurate ale autorului și a documentelor de referință din baza de cunoștințe a proiectului;
- structurarea conținutului în opt capitole, concluzie și trei anexe, conform planului editorial stabilit și validat de autor în etape succesive;
- elaborarea studiului de caz ipotetic din Capitolul 6, pe baza profilului de companie ales de autor, cu ancorare în situații tipice din sectorul serviciilor de securitate fizică;
- elaborarea formei tehnice a tabelelor, glosarului și a calendarului AI Act din anexe;
- generarea documentului Word cu machetare profesională, conform standardelor vizuale stabilite de autor pentru această serie editorială.

Instrumentul AI nu a avut acces la date cu caracter personal despre persoane identificabile și nici la informații confidențiale ale unor organizații cliente. Studiul de caz este în întregime ipotetic.

Suportul vizual a fost generat utilizând **Google Gemini**, **NotebookLM** și **ChatGPT** (OpenAI), strict pe baza instrucțiunilor și specificațiilor mele detaliate. Instrumentele AI nu au acționat autonom, ci au fost utilizate pentru a transpune indicațiile mele într-un format vizual coerent

### Proporția și natura contribuției AI

Modelul AI a contribuit semnificativ la producerea formei textuale finale a ebook-ului. Rolul autorului a fost cel de arhitect, validator și decident la fiecare etapă a procesului:

- toate deciziile de structură (numărul de capitole, ordinea lor, includerea și poziționarea studiului de caz, conținutul anexelor) au fost luate de autor în urma unei sesiuni de strategie editorială și validate explicit înainte de începerea redactării;
- toate deciziile de poziționare profesională (audiența țintă, adâncimea metodologică, relația cu volumul 1 al seriei, modul de prezentare a modelului de co-implementare) au fost stabilite de autor și transpuse în text de instrumentul AI;
- toate deciziile de conținut substanțial (profilul companiei din studiul de caz, formularea principiilor nenegociabile, conținutul întrebărilor de autoevaluare din Anexa 3, poziționarea calendarului AI Act față de acordul politic provizoriu din mai 2026) au fost validate sau ajustate explicit de autor;

- formularea concretă a paragrafelor a fost produsă de instrumentul AI și validată de autor la finalul fiecărui capitol, înainte de trecerea la capitolul următor.

Procesul a fost organizat secvențial: o sesiune de strategie editorială și clarificare a obiectivelor, urmată de o sesiune de definire și validare a structurii — care a inclus și selecția profilului de companie pentru studiul de caz — urmată de redactarea capitolelor în ordine, cu validare autor la finalul fiecăruia, și finalizată cu producerea rubricilor auxiliare și a fișierului DOCX.

### Designul vizual al ebook-ului

Versiunea publicată a ebook-ului include elemente grafice și de machetare profesională (copertă, elemente vizuale complementare) realizate independent de procesul de redactare a textului, sub coordonarea autorului.

### Responsabilitatea autorului

Responsabilitatea integrală pentru selecția și interpretarea surselor, verificarea veridicității informațiilor factuale, coerența conceptuală și arhitecturală a ghidului și opiniile, analizele și recomandările formulate revine exclusiv autorului. Utilizarea inteligenței artificiale ca instrument de redactare nu diminuează și nu transferă această responsabilitate.

### Controlul calității și verificarea surselor

Rezultatele furnizate de instrumentul AI au fost tratate ca propuneri de lucru, supuse unui proces sistematic de verificare. Informațiile factuale critice, în special referințele la articolele Regulamentului (UE) 2024/1689, la clauzele standardului SR ISO/IEC 42001:2024 și la controalele Anexei A, au fost verificate prin consultarea directă a textelor oficiale din baza de cunoștințe a proiectului.

O atenție specială a fost acordată acurateței numerelor de articol și de alineat din AI Act. Trei zone de verificare prioritară au fost: poziționarea cerinței privind riscul rezidual la Articolul 9 alineatul (5), poziționarea cerinței de notificare a persoanelor afectate la Articolul 26 alineatul (11) și domeniul de aplicabilitate strict al obligației privind evaluarea impactului asupra drepturilor fundamentale conform Articolului 27 alineatul (1), care se aplică exclusiv categoriilor de implementatori expres menționate, nu tuturor operatorilor de sisteme AI cu risc ridicat.

### Confidențialitate și etică

În interacțiunea cu instrumentul AI nu au fost introduse date cu caracter personal despre persoane identificabile și nici informații confidențiale ale unor organizații cliențe. Studiul de caz din Capitolul 6 a fost construit pe un profil compozit ipotetic, fără legătură cu vreun client real al autorului.

Această notă reflectă angajamentul autorului pentru o utilizare etică, transparentă și controlată a inteligenței artificiale în elaborarea de materiale aplicate în domeniul guvernanței inteligenței artificiale și al implementării SR ISO/IEC 42001:2024.

## Cuprins:

<b>PREAMBUL.....</b>	<b>6</b>
<b>CAPITOLUL 1: DE CE ACUM ȘI PENTRU CINE.....</b>	<b>7</b>
UNDE SE AFLĂ ORGANIZAȚIA DUMNEAVOASTRĂ PE HARTA OBLIGAȚIILOR.....	8
CE OBLIGAȚII REVIN IMPLEMENTATORULUI.....	9
UN CALENDAR CARE CERE O DECIZIE .....	10
<b>CAPITOLUL 2: CE FACE STANDARDUL ȘI UNDE SE ÎNTÂLNEȘTE CU AI ACT .....</b>	<b>11</b>
CE SPECIFICĂ STANDARDUL .....	12
ELEMENTUL CARE FACE 42001 DIFERIT DE ALTE STANDARDE .....	12
UNDE SE ÎNTÂLNESC, CONCRET, STANDARDUL ȘI REGULAMENTUL .....	13
CE NU ACOPERĂ STANDARDUL ÎN MOD EXPLICIT .....	14
BENEFICIILE DINCOLO DE CONFORMITATE .....	14
<b>CAPITOLUL 3: CE CONSTRUIEȘTI CONCRET .....</b>	<b>16</b>
ARHITECTURA UNUI SMIA: CUM ARATĂ ÎN PRACTICĂ.....	16
STRATUL MODULAR: CELE 49 DE DOCUMENTE ACTIVATE DE AI ACT .....	17
ÎNTEGRAREA CU SISTEMELE DE MANAGEMENT EXISTENTE .....	18
DE CE ȘABLOANELE GENERICI NU FUNCȚIONEAZĂ .....	18
<b>CAPITOLUL 4: CUM LUCRĂM ÎMPREUNĂ .....</b>	<b>20</b>
TREI MODELE, TREI FILOSOFII DIFERITE .....	20
CUM FUNCȚIONEAZĂ CO-IMPLEMENTAREA ÎN PRACTICĂ .....	21
TRANSFERUL DE COMPETENȚĂ CA OBIECTIV DELIBERAT .....	21
<b>CAPITOLUL 5: METODOLOGIA ÎN 7 FAZE .....</b>	<b>23</b>
FAZA 0: PREGĂTIRE ȘI CONTRACTARE .....	24
FAZA 1: DIAGNOSTICARE ȘI DEFINIRE SCOPE .....	25
FAZA 2: FUNDAMENTELE SISTEMULUI .....	27
FAZA 3: RISCURI ȘI EVALUĂRI DE IMPACT .....	28
FAZA 4: CONTROALE OPERAȚIONALE ȘI DECLARAȚIA DE APLICABILITATE .....	30
FAZA 5: OPERAȚIONALIZARE ȘI COMPETENȚE .....	31
FAZA 6: AUDIT INTERN ȘI PREGĂTIRE CERTIFICARE .....	33
SINTEZA PROIECTULUI .....	34
<b>CAPITOLUL 6: DE LA DECIZIE LA CERTIFICARE — STUDIU DE CAZ .....</b>	<b>35</b>
PROFILUL COMPANIEI ȘI SITUAȚIA DE PORNIRE .....	35
FAZA 0: PREGĂTIRE ȘI CONTRACTARE .....	36
FAZA 1: DIAGNOSTICARE ȘI DEFINIRE SCOPE .....	36
FAZA 2: FUNDAMENTELE SISTEMULUI .....	37
FAZA 3: RISCURI ȘI EVALUĂRI DE IMPACT .....	38
FAZA 4: CONTROALE OPERAȚIONALE ȘI DECLARAȚIA DE APLICABILITATE .....	40
FAZA 5: OPERAȚIONALIZARE ȘI COMPETENȚE .....	40
FAZA 6: AUDIT INTERN SIMULAT ȘI PREGĂTIRE CERTIFICARE .....	41
CE S-A SCHIMBAT ÎN FORTIS DUPĂ CERTIFICARE .....	41
SINTEZA PROIECTULUI FORTIS SECURITY SOLUTIONS.....	43

<b>CAPITOLUL 7: PROCESUL DE CERTIFICARE .....</b>	<b>44</b>
CINE POATE CERTIFICA .....	45
CELE DOUĂ ETAPE ALE AUDITULUI EXTERN.....	45
CE SE POATE ÎNTÂMPLA LA STAGE 2.....	46
CICLUL DE VIAȚĂ AL CERTIFICATULUI .....	46
<b>CAPITOLUL 8: CE DETERMINĂ SUCCESUL ȘI CE PRODUCE EȘECUL.....</b>	<b>47</b>
PRINCIPIILE PE CARE LE CONSIDER NENEGOCIABILE .....	48
FACTORII CRITICI DE SUCCES.....	48
CE PRODUCE EȘECUL .....	49
MATURITATE ORGANIZAȚIONALĂ, NU CONFORMITATE DOCUMENTARĂ .....	49
<b>CONCLUZIE .....</b>	<b>51</b>
<b>ANEXA 1: CALENDARUL AI ACT — JALOANE ȘI IMPLICAȚII PRACTICE .....</b>	<b>52</b>
<b>ANEXA 2: GLOSAR DE TERMENI CHEIE.....</b>	<b>53</b>
<b>ANEXA 3: ZECE ÎNTREBĂRI DE AUTOEVALUARE PENTRU CONDUCEREA ORGANIZAȚIEI .....</b>	<b>54</b>

## Preambul

De câte ori termin o primă discuție cu conducerea unei organizații despre SR ISO/IEC 42001:2024, primesc invariabil aceeași întrebare, formulată în cuvinte diferite, dar cu același conținut: „*Bun, am înțeles de ce avem nevoie de asta. Dar concret, ce urmează? Ce faceți voi, ce facem noi, cât durează și cu ce rămânem la final?*”

Răspunsul complet nu încapă într-o oră de conversație. Ghidul de față este acel răspuns, scris deliberat, pentru că am ajuns la concluzia că un factor de decizie informat este un partener mai bun în proiect, indiferent de sectorul din care provine.

Dacă ați citit primul volum din această serie, „**Managementul riscurilor inteligenței artificiale. Ghid practic**”, ați înțeles deja de ce riscul AI este diferit de alte categorii de risc și cum se construiește procesul de evaluare. Volumul de față este pasul următor: cum construiți, în organizația dumneavoastră sistemul care gestionează aceste riscuri, cum le documentează și le demonstrează față de orice parte interesată, de la auditorii externi la autoritățile de supraveghere și la clienții corporativi sofisticăți. Cele două volume se pot citi independent, dar împreună acoperă traseul complet de la înțelegere la acțiune.

### Cui se adresează acest ghid

L-am scris pentru directorii generali și CEO, directorii de operațiuni, directorii de tehnologie și/sau IT, responsabilii cu protecția datelor, responsabilii cu managementul riscurilor și responsabilii de conformitate care se confruntă cu o decizie practică: dacă și cum să pornească un proiect de implementare a SR ISO/IEC 42001:2024. Lectura nu cere cunoștințe tehnice despre inteligența artificială și nici experiență anterioară cu sisteme de management certificabile.

Nu se adresează consultanților sau auditorilor care caută o referință tehnică detaliată. Aceștia vor găsi nivelul de detaliu de care au nevoie în textul standardului, în documentele normative aferente și în literatura specializată.

### Ce nu conține acest ghid

- Nu conține **șabloane complete de documente**. Documentele unui SMIA se adaptează specific fiecărei organizații și sunt livrate ca parte a unui angajament contractual. Un șablon generic, fără adaptare la contextul operațional real al organizației, produce exact tipul de documentație care cade la auditul extern.
- Nu conține o **ofertă comercială sau o structură de prețuri**. Costul unui proiect de implementare depinde de prea mulți factori specifici pentru a putea fi prezentat ca un număr valid în afara unui diagnostic inițial.
- **Nu înlocuiește standardul**. Implementarea SR ISO/IEC 42001:2024 presupune procurarea și studierea textului integral al standardului de către organizație, alături de Regulamentul (UE) 2024/1689.

### Cum utilizați acest ghid

Citiți-l integral înainte de orice altă acțiune. Nu este un document de referință care se consultă punctual, ci un ghid de parcurs care are sens ca întreg. Capitolele sunt construite secvențial: fiecare îl pregătește pe cel următor. Studiul de caz din Capitolul 6 este cel mai practic instrument din acest ghid: puneți organizația dumneavoastră în locul companiei descrise și veți ieși din lectură cu o imagine clară despre ce vă așteaptă.



## Capitolul 1: De ce acum și pentru cine



Întâlnesc frecvent printre liderii organizațiilor din România ideea că normele europene privesc doar companiile tech care dezvoltă inteligență artificială. Cum separă, de fapt, legislația responsabilitățile?

**Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 stabilește norme armonizate privind inteligența artificială (denumit în continuare AI Act).** Acest document distinge clar între **furnizor** — *cel care proiectează și introduce pe piață sistemul* — și **implementator**, adică *organizația care îl utilizează în activitatea curentă*.

Dacă folosiți o soluție bazată pe inteligență artificială achiziționată de la un terț pentru a evalua oameni, a gestiona servicii sau a automatiza procese cu impact major, deveniți automat implementator. Obligațiile legale vă revin direct și sunt substanțiale, chiar dacă echipa dumneavoastră nu a scris niciodată o linie de cod.



## Unde se află organizația dumneavoastră pe harta obligațiilor

Articolul 113 din AI Act stabilește un **calendar eşalonat de aplicare**. Nu toate obligațiile au intrat în vigoare simultan, iar înțelegerea acestui calendar este esențială pentru a calibra urgența și prioritățile.

**Două jaloane sunt deja depășite la data acestui ghid.**

- **Din 2 februarie 2025**, interdicțiile privind practicile AI cu risc inacceptabil, prevăzute de articolul 5, sunt aplicabile. Concret: dacă organizația dumneavoastră opera sau intenționa să opereze sisteme de scoring social generalizat, de manipulare subliminală sau de identificare biometrică în timp real în spații publice fără excepție legală, acestea sunt deja interzise. Tot din aceeași dată, a apărut obligația de a asigura alfabetizarea în domeniul AI pentru personalul care operează astfel de sisteme.
- **Din 2 august 2025**, regulile pentru modelele de inteligență artificială de uz general sunt aplicabile, iar statele membre trebuiau să fi desemnat deja autoritățile naționale competente.

**Jalonul critic** pentru majoritatea organizațiilor este cel **din data de 2 august 2026**, data la care, în calendarul de bază al AI Act, se aplică obligațiile pentru sistemele AI cu risc ridicat.

La această dată, în calendarul de bază al AI Act, se aplică obligațiile pentru sistemele AI cu risc ridicat clasificate în Anexa III a regulamentului.

Tot atunci intră în vigoare cerințele de transparență de la articolul 50 și măsurile de sprijin pentru inovare.

Trebuie să menționez că, în **mai 2026**, Consiliul UE și Parlamentul European au anunțat un acord politic provizoriu în cadrul pachetului Digital **Omnibus**, care ajustează aceste termene.

- Conform acestui acord, **obligațiile de conformitate pentru sistemele AI cu risc ridicat de tip stand-alone** din Anexa III ar urma să se aplice din **2 decembrie 2027**, nu din 2 august 2026.
- Pentru **sistemele AI cu risc ridicat integrate în produse reglementate de legislație sectorială de siguranță**, termenul s-ar muta la **2 august 2028**.
- De asemenea, **watermarking-ul pentru sisteme generative**, prevăzut de articolul 50 alineatul (2), ar deveni aplicabil din **2 decembrie 2026**.

Acordul politic provizoriu nu echivalează însă cu adoptarea formală a acestor modificări. Până la intrarea lor în vigoare, **recomandarea mea pentru orice organizație din România care operează sisteme AI cu risc ridicat este să trateze data de 2 august 2026 drept termenul-limită**.

Până atunci trebuie construite bazele guvernanței AI. Acest proces include realizarea inventarului sistemelor, clasificarea pe categorii de risc, evaluările de impact și implementarea unui sistem de management funcțional.

Eventualele amânări pentru perioada 2027-2028 reprezintă un spațiu de manevră pentru rafinare, iar nu un argument pentru a amâna startul.

**Regulamentul separă explicit două categorii de operatori:**

- **Furnizorul** este entitatea care proiectează un sistem AI, îl antrenează și îl introduce pe piață sau îl pune în funcțiune.
- **Implementatorul** este entitatea care utilizează un sistem AI cu risc ridicat în contextul propriilor activități profesionale.

Aceeași organizație poate cumula ambele calități dacă dezvoltă, dar și utilizează sisteme AI proprii.

Cele mai multe organizații din sectoarele financiar, medical, de resurse umane, de asigurări sau din administrație publică din România se află în poziția de implementator pur. Au achiziționat sau închiriat sisteme AI de la furnizori și le utilizează în procesele lor interne sau în relația cu clienții. Aceasta nu le exonerează de obligații, lci e conferă un set specific de obligații proprii.

**Ce obligații revin implementatorului**

**Articolul 26 din regulament concentrează obligațiile implementatorilor.** Principalele obligații sunt următoarele:

- Implementatorul **trebuie să asigure o supraveghere umană competentă a sistemului AI**. Concret, persoanele care utilizează sau monitorizează sistemul trebuie să înțeleagă ce face acesta, care îi sunt limitele și când trebuie să intervină. Această cerință implică o instruire documentată și proceduri clare de escaladare.
- Implementatorul **trebuie să utilizeze sistemul strict în conformitate cu instrucțiunile furnizorului**. Orice utilizare în afara scopului prevăzut, sau în contexte pentru care sistemul nu a fost evaluat, transferă responsabilitatea asupra implementatorului.
- Implementatorul **trebuie să monitorizeze funcționarea sistemului și să păstreze jurnalele de evenimente pe durata prevăzută**. Articolul 26 alineatul (6) stabilește că această obligație include și raportarea incidentelor grave sau a comportamentelor neașteptate către furnizor și, după caz, către autoritatea competentă.
- Articolul 26 alineatul (11) impune **obligația de a informa în prealabil persoanele fizice vizate de un sistem AI cu risc ridicat**, acolo unde această informare nu este realizată direct de către furnizor.
- Articolul 27 alineatul (1) prevede că **anumite categorii de implementatori trebuie să realizeze o evaluare a impactului asupra drepturilor fundamentale înainte de punerea în funcțiune**. Această regulă vizează, în principal, organismele de drept public și entitățile private care prestează servicii publice. Obligația nu se aplică tuturor implementatorilor, ci numai categoriilor expres menționate. Acolo unde nu există o obligație legală strictă, evaluarea de impact rămâne o practică recomandabilă și o componentă valoroasă a unui sistem de management matur.
- Implementatorul **trebuie să informeze lucrătorii și reprezentanții acestora înainte de introducerea unui sistem AI la locul de muncă**, în conformitate cu articolul 26 alineatul (7).

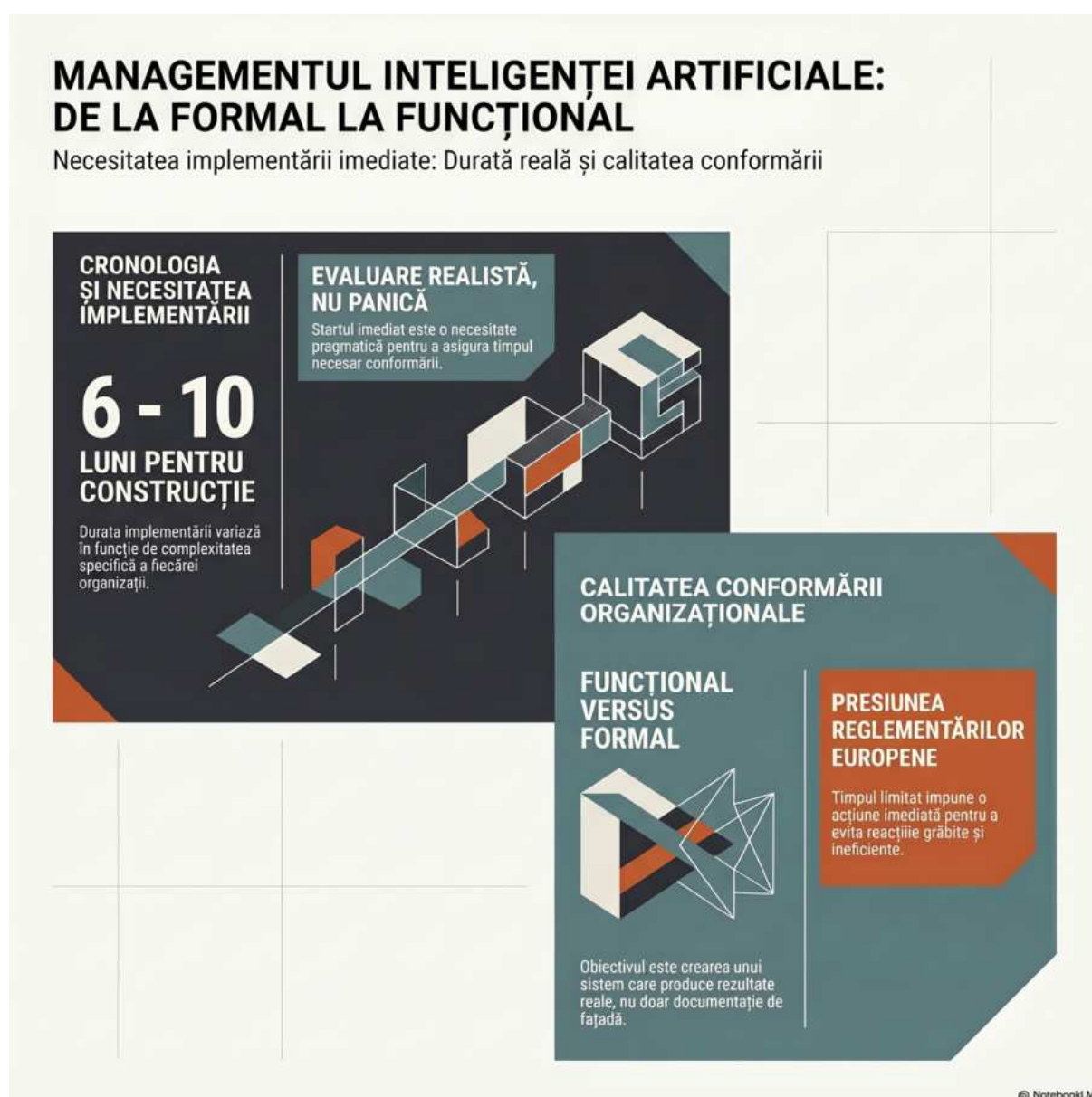
## Un calendar care cere o decizie

Toate obligațiile de mai sus presupun documentare, proceduri, instruire și o structură de guvernanță funcțională. Niciuna dintre ele nu se poate îndeplini cu câteva săptămâni înainte de termenul-limită.

**Un sistem de management al inteligenței artificiale construit corect se construiește în șase până la zece luni, în funcție de complexitatea organizației.**

Decizia de a începe astăzi nu ar trebui privită ca o reacție grăbită la presiunea reglementărilor europene. Nu este vorba despre panică, ci despre o evaluare realistă a timpului necesar pentru conformare.

Prin urmare, întrebarea nu este dacă organizația trebuie să înceapă „mai devreme” sau „mai târziu”, ci dacă mai are suficient timp pentru a construi ceva funcțional, nu doar formal.



## Capitolul 2: Ce face standardul și unde se întâlnește cu AI Act



Există o tentație de a trata **SR ISO/IEC 42001:2024** ca pe un document de conformitate, ceva ce procuri, implementezi și bifezi.

Această perspectivă produce sisteme care cad la audit și organizații care, după certificare, nu știu ce să facă cu ceea ce au construit.

O înțelegere corectă a standardului pornește de la altceva: de la întrebarea **ce problemă rezolvă**, nu ce cerință bifează.

Răspunsul scurt este că **standardul rezolvă problema demonstrabilității**. Orice organizație care utilizează sisteme AI cu impact semnificativ poate afirma că le gestionează responsabil. Standardul oferă cadrul prin care această afirmație devine verificabilă, repetabilă și auditabilă.

## Ce specifică standardul

SR ISO/IEC 42001:2024 este adoptarea română a standardului internațional ISO/IEC 42001:2023, publicat în decembrie 2023 de Organizația Internațională de Standardizare. Adoptarea este integrală, ceea ce înseamnă că **o certificare obținută în România pe baza acestui standard beneficiază de recunoaștere internațională**.

*"ISO/IEC 42001 este un standard internațional care specifică cerințele pentru stabilirea, implementarea, menținerea și îmbunătățirea continuă a unui sistem de management al inteligenței artificiale (AIMS) în cadrul organizațiilor. Acesta este conceput pentru entitățile care furnizează sau utilizează produse sau servicii bazate pe inteligență artificială, asigurând dezvoltarea și utilizarea responsabilă a sistemelor de inteligență artificială."* (ISO)

**Structura sa urmează logica High Level Structure**, comună tuturor standardelor moderne de management: ISO 9001 pentru calitate, ISO/IEC 27001 pentru securitatea informației, ISO 22301 pentru continuitatea afacerii folosesc același schelet. Dacă organizația dumneavoastră are deja unul dintre aceste sisteme implementat, o bună parte din infrastructura procedurală și documentară există deja și se poate integra, nu reconstrui.

**Cerințele de bază** sunt organizate în clauzele 4 până la 10. Clauza 4 cere înțelegerea contextului organizației și a părților interesate. Clauza 5 stabilește cerințele de leadership și angajament al conducerii. Clauza 6 acoperă planificarea, inclusiv evaluarea riscurilor și a impactului. Clauza 7 reglementează resursele, competențele și comunicarea. Clauza 8 tratează operarea efectivă a sistemelor AI. Clauza 9 acoperă evaluarea performanței prin audit intern și analiza efectuată de management. Clauza 10 se referă la îmbunătățirea continuă și tratarea neconformităților.

Dincolo de aceste cerințe generale, **standardul include Anexa A, cu 38 de controale de referință organizate în nouă domenii**. Acestea acoperă politicile AI, alocarea resurselor, evaluarea impactului sistemelor AI asupra persoanelor și societății, guvernanța datelor, documentarea sistemelor, relațiile cu furnizorii și terții, utilizarea responsabilă a AI și ciclul de viață al sistemelor.

## Elementul care face 42001 diferit de alte standarde

Față de alte standarde de management pe care le-am implementat de-a lungul anilor, SR ISO/IEC 42001:2024 introduce un element pe care îl consider definitoriu: **evaluarea impactului sistemului AI nu doar asupra organizației, ci asupra persoanelor fizice și a societății în ansamblu**.

ISO/IEC 27001, de exemplu, te întreabă ce riscuri există pentru organizație dacă securitatea informației este compromisă.

Standardul 42001 te întreabă și altceva: *ce se întâmplă cu oamenii care sunt afectați de deciziile sistemului tău AI? Ce impact are sistemul asupra grupurilor vulnerabile, asupra echității, asupra drepturilor fundamentale?*

Această schimbare de perspectivă este exact puntea care conectează logica standardului cu filosofia AI Act.



## Unde se întâlnesc, concret, standardul și regulamentul

Suprapunerea dintre SR ISO/IEC 42001:2024 și AI Act este substanțială în mai multe puncte. Cunoașterea acestor puncte de contact este utilă oricărui factor de decizie care evaluează utilitatea certificării.



**Articolul 17 din AI Act cere furnizorilor de sisteme cu risc ridicat un sistem de management al calității.** Standardul 42001 este exact un astfel de sistem, construit specific pentru inteligența artificială.

O organizație care operează în calitate de furnizor și care obține certificarea pe acest standard are o bază solidă pentru a demonstra conformitatea cu această cerință.

**Articolul 9 din regulament impune un sistem de gestionare a riscurilor pe tot ciclul de viață al sistemului AI.** Clauza 6.1 din standard, împreună cu controalele din Anexa A, construiesc exact acest mecanism, cu metodologie de evaluare, registru de riscuri, plan de tratare și monitorizare continuă.



**Articolul 10 solicită guvernanța datelor de antrenament, validare și testare.** Controalele din domeniul A.7 al Anexei A acoperă această cerință printr-un set de proceduri și înregistrări privind calitatea, proveniența și gestionarea datelor utilizate de sistemele AI.

**Articolul 14 cere supraveghere umană efectivă și documentată.** Controalele din domeniul A.9 stabilesc cadrul procedural prin care această supraveghere este definită, atribuită și verificabilă.

**Articolul 72 impune monitorizarea post-piață a sistemelor AI cu risc ridicat.** Clauza 9.1 din standard, care reglementează monitorizarea și măsurarea performanței sistemului de management, furnizează infrastructura prin care această monitorizare devine o activitate sistematică și înregistrată, nu ocazională.

## Ce nu acoperă standardul în mod explicit

O să fiu direct în această privință, pentru că am văzut prezentări ale standardului care sugerează o suprapunere completă cu cerințele AI Act, dar aceasta nu reflectă realitatea.

**Anumite cerințe specifice ale regulamentului nu sunt solicitate explicit de standard.** Declarația de conformitate UE, înregistrarea sistemului în baza de date europeană prevăzută de articolul 49, documentația tehnică conform Anexei IV a regulamentului și procedurile specifice de evaluare a conformității cerute furnizorilor de sisteme cu risc ridicat nu sunt generate automat de implementarea standardului.

Într-un proiect de implementare matur, **aceste documente se construiesc suplimentar, pe arhitectura de bază a sistemului de management.** Ele nu înlocuiesc SMIA, se adaugă peste el. Exact aceasta este funcția modulului AI Act din metodologia pe care o aplic, despre care voi vorbi în detaliu în capitolele următoare.

## Beneficiile dincolo de conformitate

Conformitatea cu AI Act și cu cerințele de certificare este motivul declarat al majorității proiectelor pe care le conduc. Nu este singurul beneficiu și, pe termen mediu, nici cel mai important.

**Un SMIA funcțional produce o imagine clară asupra sistemelor AI din organizație.** Mulți directori generali descoperă în faza de inventariere sisteme pe care le-au achiziționat departamentele operaționale fără o evaluare formală a riscurilor și pe care conducerea nu le cunoștea. Această vizibilitate, singură, justifică efortul.

Produce, de asemenea, **baza pentru decizii informate:** ce sisteme merită operate, care necesită modificări și care ar trebui retrase sau înlocuite. Fără un cadru de evaluare, aceste decizii se iau pe baza intuiției sau, mai rău, nu se iau deloc.

Produce **siguranță reputațională** prin reducerea probabilității incidentelor generate de comportamente neașteptate ale sistemelor AI, incidente care în mediul actual ajung rapid în spațiul public.

Produce un **avantaj competitiv** concret în relația cu clienții corporativi sau cu autoritățile contractante care cer dovezi de guvernanță AI în procesele de achiziție. Certificarea devine o dovadă verificabilă, nu o declarație de intenție.

Și, poate cel mai subtil beneficiu, **produce scalabilitate**: orice sistem AI nou achiziționat sau dezvoltat în viitor se integrează într-un cadru deja testat, fără a reconstrui procesele de la zero.

Certificarea pe SR ISO/IEC 42001:2024 nu este, în opinia mea, o investiție care se justifică prin evitarea unei amenzi. Este o investiție care produce valoare indiferent de evoluția calendarului reglementărilor.

## DINCOLO DE CONFORMITATE: VALOAREA STRATEGICĂ A ISO/IEC 42001

Implementarea standardului SR ISO/IEC 42001:2024 nu este doar o măsură de conformitate cu AI Act, ci o investiție strategică. Un SMIA funcțional transformă incertitudinea în vizibilitate, oferind un cadru solid pentru decizii informate, siguranță reputațională și scalabilitate pe termen lung.



### VIZIBILITATE ȘI DECIZII INFORMATE

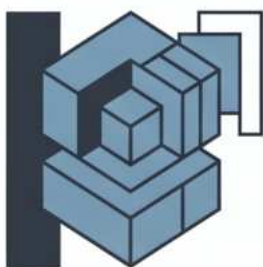
Permite inventarierea sistemelor AI achiziționate informal și oferă o bază obiectivă pentru menținerea sau înlocuirea lor.

Permite inventarierea sistemelor AI achiziționate informal și oferă o bază obiectivă pentru menținerea sau înlocuirea lor.



### SCALABILITATE INTEGRATĂ

Orice sistem AI viitor se integrează într-un cadru deja testat, fără a reconstrui procesele de la zero.



### VALOARE EXTERNĂ ȘI SIGURANȚĂ



### PROTECȚIA REPUTAȚIEI

Reduce probabilitatea incidentelor generate de comportamentele neașteptate ale AI care pot ajunge rapid în spațiul public.



### AVANTAJ COMPETITIV VERIFICABIL

Certificarea oferă dovezi de guvernanță solicitate de clienții corporate, transformând intenția în dovadă verificabilă.

### INVESTIȚIE ÎN VALOARE CONTINUĂ

Reprezintă o investiție care produce valoare indiferent de evoluția reglementărilor, nu doar o metodă de a evita amenzi.



# NotebookLM

## Capitolul 3: Ce construiești concret



Când conducerea unei organizații decide să implementeze SR ISO/IEC 42001:2024, prima întrebare practică este, de regulă, una dintre acestea: *câte documente trebuie să producem sau cât de mult durează*. Întrebările sunt legitime, dar puse în ordinea greșită. Întrebarea corectă este alta: *ce tip de guvernanță construim și cum o facem să reflecte realitatea organizației noastre?*

**Documentele nu sunt guvernanța.** Sunt dovada că guvernanța există și funcționează. Această distincție poate părea subtilă, dar ea separă sistemele care rezistă la auditul extern de cele care cad la prima verificare serioasă.

### Arhitectura unui SMIA: cum arată în practică

Un sistem de management al inteligenței artificiale este, structural, o arhitectură de politici, proceduri, registre, rapoarte și înregistrări operaționale, organizate în jurul ciclului Plan-Do-Check-Act comun tuturor sistemelor de management certificabile. Nucleul

**unui SMIA acoperă aproximativ 60 de documente** aplicabile oricărei organizații care dezvoltă, integrează sau utilizează sisteme AI, indiferent de dimensiune sau sector.

Aceste 60 de documente nu sunt un catalog uniform. Se grupează funcțional în mai multe categorii, fiecare cu un scop distinct în arhitectura sistemului.

**Prima categorie acoperă contextul și inventarul.** Organizația trebuie să știe ce sisteme AI operează, în ce rol, cu ce categorie de risc și cu ce impact potențial. Registrul sistemelor AI, analiza contextului, registrul părților interesate și raportul de gap analysis față de cerințele standardului formează fundația pe care se construiește tot restul. Fără un inventar complet și corect, orice document ulterior este construit pe presupuneri, iar presupunerile cad la audit.

**A doua categorie acoperă guvernanța și angajamentul conducerii.** Politica de inteligență artificială, documentul care exprimă poziția strategică a organizației față de AI, rolurile și responsabilitățile formalizate, obiectivele SMIA cu planul de realizare și procedurile de comunicare internă și externă formează scheletul de guvernanță. Aceste documente sunt, de regulă, cele care cer cel mai mult timp din partea conducerii executive, pentru că reflectă decizii strategice asumate, nu proceduri tehnice.

**A treia categorie este cea mai densă și acoperă managementul riscurilor și al impactului.** Criteriile de risc, procedura de evaluare, registrul riscurilor, rapoartele de evaluare per sistem AI, evaluările de impact asupra persoanelor și societății, procedura și planul de tratare a riscurilor formează împreună mecanismul central al standardului. Calitatea acestor documente determină în proporție decisivă credibilitatea întregului SMIA. Un auditor cu experiență petrece cea mai mare parte a timpului său din Stage 2 în această zonă.

**A patra categorie acoperă controalele operaționale din Anexa A a standardului,** 38 la număr, grupate în nouă domenii. Nu toate cele 38 de controale generează câte un document separat, dar toate trebuie să fie adresate fie prin documente dedicate, fie prin justificarea explicită a excluderii lor în Declarația de Aplicabilitate. Această declarație, documentul-ogindă al sistemului, consemnează pentru fiecare control dacă este aplicabil, de ce și cum este implementat. Este documentul pe care orice auditor extern îl citește primul.

**A cincea categorie acoperă evaluarea performanței și îmbunătățirea continuă:** programul și procedura de audit intern, rapoartele de audit, procesul-verbal al analizei efectuate de management și planul de îmbunătățire continuă. Aceste documente nu se produc o singură dată: ele se generează periodic și constituie dovada că sistemul este viu, nu o arhivă statică.

## Stratul modular: cele 49 de documente activate de AI Act

Peste nucleul generic de **60 de documente**, metodologia pe care o aplic include un **strat modular de 49 de documente suplimentare, activate condiționat în funcție de doi factori:** rolul organizației în lanțul valoric AI și categoria de risc a sistemelor operate.

**Organizațiile care acționează exclusiv ca implementatori de sisteme cu risc limitat sau minim nu vor activa cea mai mare parte a acestor documente.** Organizațiile care cumulează calitățile de furnizor și implementator pentru sisteme cu risc ridicat le vor activa pe aproape toate. Între aceste două extreme există un spectru larg de configurații, iar calibrarea exactă se face în faza de diagnosticare, nu anterior.

**Documentele din stratul modular** acoperă, printre altele, documentația tehnică cerută furnizorilor de sisteme cu risc ridicat, procedurile de înregistrare în baza de date UE, dosarul de evaluare a conformității, procedura de raportare a incidentelor grave la autoritățile competente, evaluarea de impact asupra drepturilor fundamentale pentru categoriile de implementatori cărora li se aplică articolul 27 din regulament și documentele specifice de supraveghere umană pentru sisteme cu risc ridicat.

**Această structură modulară are o consecință practică importantă pentru un factor de decizie:** costul și durata proiectului nu sunt fixe. Ele depind direct de complexitatea portofoliului de sisteme AI și de rolul asumat în lanțul valoric. O organizație mică, cu un singur sistem AI cu risc limitat, în rol de implementator pur, construiește un SMIA semnificativ mai restrâns decât o organizație care dezvoltă și utilizează mai multe sisteme clasificate ca risc ridicat. Diagnosticul inițial stabilește cu precizie această configurație.

## Integrarea cu sistemele de management existente

**Dacă organizația dumneavoastră are deja implementate sisteme de management certificabile, ISO 9001, ISO/IEC 27001, ISO 22301 sau altele,** o parte semnificativă din infrastructura procedurală a SMIA există deja.

Procedura de control al documentelor și înregistrărilor, procedura de audit intern, procedura de tratare a neconformităților și acțiunilor corective, procedura de analiză efectuată de management: toate acestea sunt cerute de standardul 42001, dar dacă există deja versiuni funcționale în organizație, **nu se rescriu. Se extind sau se adaptează** pentru a acoperi și cerințele specifice sistemului de management AI.

**Politicile tematice rămân distincte:** o organizație nu va unifica politica de securitate a informației cu politica de inteligență artificială într-un singur document, pentru că au logici și audiențe diferite. Dar ambele se aliniază cu politica-umbrelă a organizației și cu structura de guvernanță generală.

**Integrarea bine realizată reduce volumul de muncă în construcția SMIA cu 20 până la 35 la sută** față de un proiect pornit de la zero, în funcție de maturitatea sistemelor existente. Este unul dintre factorii pe care îi verific explicit în diagnosticul inițial.

## De ce șabloanele generice nu funcționează

Aceasta este o discuție pe care o port frecvent și pe care o consider necesară înainte de orice angajament. În România, încă nu există pe piață pachete de documente SMIA gata produse, descărcabile imediat, uneori la prețuri atractive, dar nu cred că va dura prea mult până să apară. Avem exemple de șabloane și kit-uri pentru toate sistemele de management care promit să rezolve problemele, așa că sunt convins că se vor găsi furnizori și de kit-uri SMIA.

Problema nu este că aceste documente arată rău. Unele arată foarte bine. Problema este că un auditor cu experiență din domeniul sistemelor de management le identifică în primele minute ale auditului. Politica AI a organizației trebuie să reflecte deciziile strategice asumate de conducere, nu fraze generice despre responsabilitate și inovare. Registrul riscurilor trebuie să conțină riscurile reale ale sistemelor reale din organizație, nu categorii abstracte din literatura de specialitate. Rapoartele de evaluare a impactului trebuie să descrie impactul concret al sistemelor concrete asupra persoanelor concrete, nu scenarii ipotetice.

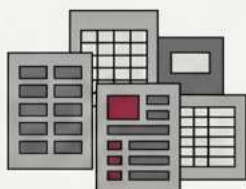


Un SMIA construit pe șabloane generice bifează cerințele la suprafață și cedează la prima verificare serioasă. Organizațiile care au trecut prin această experiență au plătit de două ori: o dată pentru pachetul de șabloane și o dată pentru reconstrucția sistemului după auditul care nu a mers bine.

Documentele unui SMIA nu pot fi mai bune decât cunoașterea pe care o reflectă. Construirea lor corectă cere timp, dialog și acces la realitatea operațională a organizației. Este exact ce nu poate oferi nicio platformă automată și exact ce aduce un angajament de consultanță condus corect.

# SMIA: Capcana Șabloanelor vs. Realitatea Operațională

## Eșecul Sistemelor Generice



### Detectabilitate imediată la audit

Auditorii identifică documentele tipizate în primele minute, deoarece nu reflectă specificul organizației.



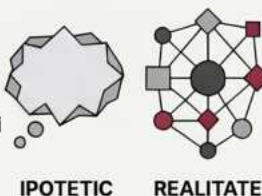
### Riscul costurilor duble

Organizațiile plătesc inițial pentru șabloane și ulterior pentru reconstrucția completă a sistemului.



### Conținut abstract vs. realitate

Șabloanele folosesc scenarii ipotetice și categorii din literatură în locul riscurilor reale.



## Pilonii unui SMIA Autentic

### Politici bazate pe decizii strategice

Documentația trebuie să reflecte asumările conducerii, nu fraze generice despre inovație.



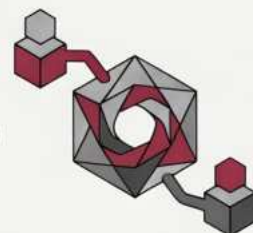
### Evaluarea impactului concret

Analiza trebuie să vizeze efectele sistemelor reale asupra persoanelor reale din organizație.



### Valoarea dialogului și a timpului

Construcția corectă necesită acces direct la realitatea operațională prin consultanță dedicată.



© NotebookLM



## Capitolul 4: Cum lucrăm împreună



Un proiect de implementare a unui sistem de management poate fi structurat în mai multe moduri, iar **alegerea modelului de lucru** are consecințe care se văd nu la semnarea contractului, ci la doi ani după certificare.

Am văzut organizații care au obținut certificarea și nu au putut menține sistemul pentru că nu știau cum funcționează. Am văzut altele care au construit sisteme atât de complexe încât le era imposibil să le opereze cu resursele interne disponibile. Ambele situații erau consecința unui model de lucru ales greșit, nu a unui standard greu sau a unui consultant incompetent.

### Trei modele, trei filosofii diferite

**Există trei abordări fundamentale pentru un proiect de implementare SMIA**, fiecare cu logica ei și cu un profil de organizație căruia îi este potrivită.

**Primul model este consultanța completă.** Consultantul construiește integral sistemul: proiectează arhitectura documentară, redactează toate documentele, conduce toate sesiunile, realizează auditul intern și predă un pachet finalizat. Clientul aprobă și semnează. Este cel mai rapid din perspectiva efortului intern al organizației și cel mai scump. Produce, de asemenea, cel mai fragil rezultat: o organizație care nu a construit sistemul nu știe să îl mențină și devine dependentă de consultant ori de câte ori apare o neconformitate, o schimbare de scope sau un audit de supraveghere.

**Al doilea model este coaching-ul.** Consultantul ghidează, explică și revizuieste, dar echipa internă construiește efectiv toate documentele. Este cel mai accesibil financiar și produce cea mai puternică internalizare a sistemului. Are o condiție prealabilă pe care multe organizații nu o îndeplinesc: o echipă internă cu timp disponibil, motivație și o minimă familiarizare cu logica sistemelor de management. Când această condiție există, coaching-ul este excelent. Când nu există, produce întârzieri, frustrări și, uneori, proiecte abandonate la jumătate.

**Al treilea model este co-implementarea.** Este abordarea pe care o recomand și o aplic în toate proiectele mele și pe care o consider, pentru profilul majorității organizațiilor cu care lucrez, alegerea corectă din trei motive concrete. Costul total este semnificativ mai mic decât la consultanța completă, fără pierderi de calitate, pentru că efortul meu se concentrează pe construcția cadrului și pe conținutul tehnic și normativ, nu pe completarea datelor operaționale. Echipa internă învață sistemul în timp ce îl construiește, ceea ce elimină sindromul sistemului care moare la plecarea consultantului. Documentele reflectă realitatea operațională a organizației, pentru că sunt completate de oameni care știu ce se întâmplă efectiv în procesele lor.

## Cum funcționează co-implementarea în practică

Împărțirea responsabilităților în modelul de co-implementare urmează o logică simplă: **consultantul aduce expertiza metodologică și normativă, organizația aduce cunoașterea operațională și datele reale.** Niciunul dintre cei doi nu poate face treaba celuilalt fără pierderi semnificative de calitate.

Concret, **eu construiesc structura** și cadrul fiecărui document, completez secțiunile tehnice și normative, definesc metodologiile de evaluare a riscurilor și a impactului, conduc instruirile și workshop-urile, revizuiesc și validez variantele finale și realizez auditul intern simulat.

**Echipa organizației validează structura** și o adaptează specificului intern, furnizează datele reale din operațiuni, completează secțiunile operaționale și contextuale ale documentelor, asigură participarea la instruirile și ia deciziile de conținut politic și strategic: ce exprimă politica AI a organizației, care este apetitul la risc, ce obiective SMIA sunt realiste.

Această responsabilitate nu este delegabilă. Politica de inteligență artificială a organizației trebuie să exprime convingeri și decizii asumate de conducere, nu formulări redactate de consultant. **Auditorii externi verifică explicit dacă conducerea cunoaște și susține conținutul documentelor pe care le-a semnat.**

## Transferul de competență ca obiectiv deliberat

**Există o diferență fundamentală între un proiect care se încheie cu o certificare și un proiect care se încheie cu o organizație capabilă.** Urmăresc al doilea rezultat în toate

angajamentele mele, pentru că primul fără al doilea are o durată de viață de maximum trei ani, adică exact până la primul audit de reînnoire a certificării.

**Transferul de competență** nu este un bonus, **este un obiectiv explicit al proiectului**. Se realizează prin modul în care lucrăm, nu printr-o sesiune de instruire la final.

**Coordonatorul SMIA** desemnat de conducere **participă activ la construcția fiecărui document** și înțelege nu doar ce conțin, ci de ce sunt construite astfel. **Auditorii interni** pe care îi formează în cursul proiectului **sunt capabili să conducă audituri interne reale** după certificare, nu să bifeze proceduri.

**Echipa care a participat la evaluările de risc** știe să actualizeze registrul când apare un sistem AI nou, fără să aștepte o intervenție externă.

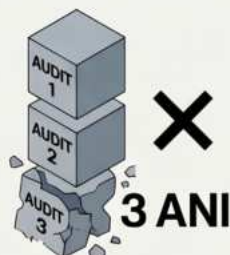
La finalul proiectului, organizația primește un sistem de management funcțional și o echipă care știe să îl mențină. Aceasta este, în opinia mea, singura definiție acceptabilă a unui proiect de implementare reușit.

## Transferul de Competență: Fundația unei Organizații Sustenabile

### Certificare vs. Organizație Capabilă

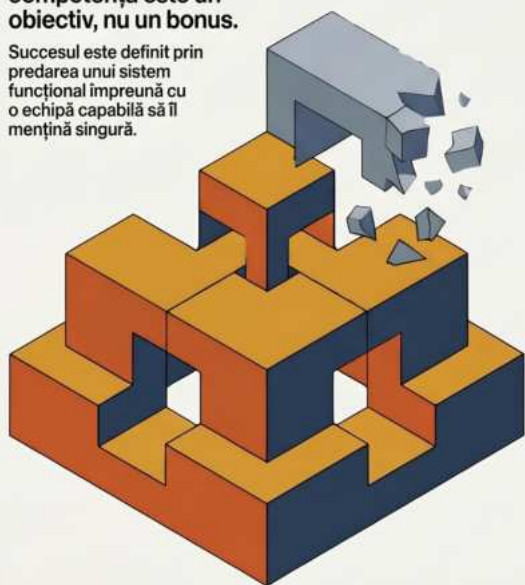
**Certificarea fără competență expiră în 3 ani.**

Proiectele care vizează doar documentul de certificare își pierd relevanța imediat după primul audit de reînnoire dacă echipa nu înțelege sistemul.



**Transferul de competență este un obiectiv, nu un bonus.**

Succesul este definit prin predarea unui sistem funcțional împreună cu o echipă capabilă să îl mențină singură.



### Metodologia Transferului Activ & Autonomie în Era AI

**Co-construcția documentelor în timp real.**

Coordonatorul SMIA participă activ la crearea fiecărei proceduri pentru a înțelege nu doar conținutul, ci și logica din spatele structurii acestora.



**Audituri interne reale, nu doar proceduri bifate.**

Formarea auditorilor interni se concentrează pe capacitatea de a conduce evaluări autentice după finalizarea proiectului.



**Autonomie și Reziliență în Era AI**

**Gestionarea independentă a noilor sisteme AI.**

O echipă competentă știe să actualizeze registrul de riscuri atunci când apare un sistem AI nou, fără a depinde de consultanți externi.



**Sistem de management funcțional și menținut.**

Singura definiție acceptabilă a unui proiect reușit este simbioza dintre un sistem bine structurat și o echipă care deține controlul total asupra lui.



© NotebookLM

## Capitolul 5: Metodologia în 7 faze



**Standardul** spune **ce trebuie să construiești**. **Regulamentul** spune **ce ești obligat să construiești**. Niciunul dintre ele nu spune în ce ordine, cu ce dependențe, unde sunt blocajele tipice și ce decizii pot fi amânate fără consecințe asupra întregului calendar. Aceasta este funcția metodologiei.

Cele **șapte faze** descrise în continuare **sunt consecutive și dependente unele de altele**. **Fiecare fază generează intrările necesare pentru faza următoare**.

Tentația de a comprima calendarul prin execuția paralelă a fazelor produce, invariabil, o refacere costisitoare a lucrărilor. Mai mult, în cazurile pe care le-am văzut, această abordare a generat sisteme care a trebuit să fie reconstruite parțial înainte de auditul extern.

**Durata de referință este de șase luni** (*situație pe care o exemplific inclusiv în studiul de caz*) pentru o organizație de dimensiune medie, cu un portofoliu de sisteme AI de complexitate moderată. Pentru organizații mai mici, cu scope restrâns, proiectul se poate finaliza în trei



până la patru luni. Pentru organizații mari, cu portofolii extinse și fără sisteme de management anterioare, durata poate ajunge la opt până la zece luni. Calibrarea exactă se face în faza de diagnosticare, nu înainte.

## Faza 0: Pregătire și contractare



**Durata: una până la două săptămâni**, înainte de startul oficial al proiectului.

Această fază este scurtă, dar **uneori tratată superficial**, ceea ce o transformă în sursa principală a problemelor din lunile care urmează. Tot ceea ce nu este clarificat acum devine subiect de negociere în mijlocul unui milestone critic, când presiunea este maximă și marja de manevră minimă.

În această fază **se constituie echipa internă a proiectului**: sponsorul executiv, coordonatorul SMIA și membrii grupului de lucru care vor fi implicați activ în construcția documentelor. **Se semnează contractul de consultanță și acordul de confidențialitate. Se calibrează așteptările reciproce**: ce livrează consultantul, ce livrează organizația, care sunt termenele

și ce se întâmplă dacă unul dintre jaloane nu este respectat. Se fixează calendarul complet, cu datele blocate ale workshop-urilor și ale ședințelor de status.

**Livrabilul principal** al acestei faze **nu este un document SMIA**, este un acord de lucru clar și un calendar asumat de ambele părți.

**Riscul principal** este subestimarea efortului intern. Conducerea desemnează un coordonator SMIA, dar nu îi eliberează efectiv timp în calendar. Tratarea lui se face în această fază, nu după ce primele întârzieri devin vizibile: efortul mediu cerut echipei interne în modelul de co-implementare este de trei până la cinci zile-om pe lună, concentrate în jurul workshop-urilor și al milestone-urilor. Dacă această resursă nu poate fi garantată, calendarul se reconstruiește înainte de start, nu pe parcurs.

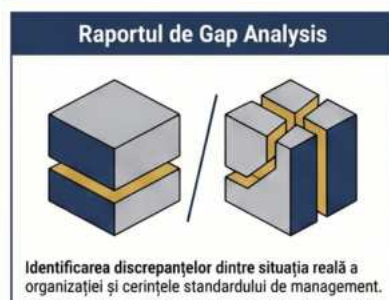
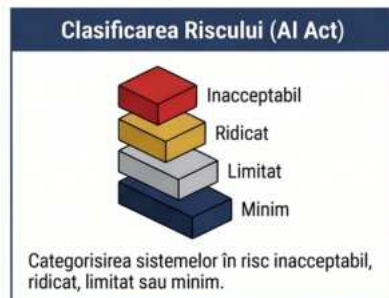
**Milestone:** contractul semnat, echipa constituită, calendarul agreat și blocat în agendele tuturor participanților.

## Faza 1: Diagnosticare și definire scope

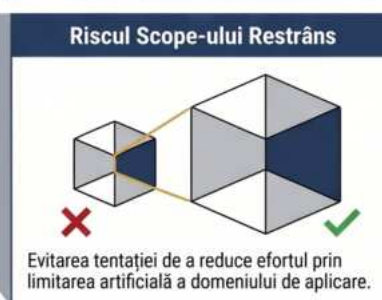
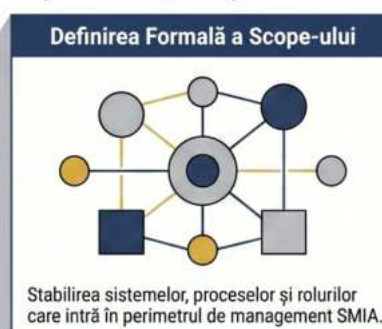
### SMIA: Faza 1 – Fundația Guvernanței AI

Faza 1: Diagnosticare și Definire Scope (Luna 1) - Identificarea sistemelor AI și stabilirea limitelor strategice de aplicare a guvernanței.

#### Procesul de Evaluare și Analiză



#### Direcția Strategică și Rezultate



#### Livrabile Principale & Importanță Strategică



© NotebookLM



### **Durata: Prima lună a proiectului.**

Aceasta este faza în care organizația se privește în oglindă. Din experiența mea, este și faza cu cele mai multe surprize, nu neapărat neplăcute, ci revelatoare.

**Activitatea centrală** a acestei faze este **inventarierea tuturor sistemelor AI din organizație**. Prin acest demers se clarifică: ce sisteme există, cine le operează, în ce procese sunt integrate, cine este furnizorul, care este scopul declarat și care este impactul real asupra deciziilor care afectează persoane.

Multe organizații descoperă în acest pas sisteme pe care departamentele operaționale le-au achiziționat sau implementat fără o aprobare formală din partea conducerii și fără o evaluare prealabilă a riscurilor.

**Inventarul este, totodată, primul document obligatoriu al SMIA și baza oricărui raționament ulterior.**

Pe baza inventarului, **fiecare sistem AI este clasificat** conform logicii de risc din AI Act: **risc inacceptabil, risc ridicat, risc limitat sau risc minim**. Această clasificare determină ce obligații se aplică organizației și ce documente din stratul modular AI Act se activează.

Urmează **analiza diferențelor față de cerințele standardului**, respectiv „**gap analysis-ul**”.

Acest raport este primul document pe care conducerea executivă trebuie să îl citească cu atenție, deoarece reflectă situația reală, nu pe cea dorită. În cadrul acestuia, se identifică elementele de guvernanță AI care pot fi deja valorificate, precum și lacunele existente și amplexarea acestora.

Faza se încheie cu **definirea formală a domeniului de aplicare al SMIA**. Aceasta presupune stabilirea sistemelor AI, a proceselor organizaționale, a locațiilor și a rolurilor care intră în perimetrul sistemului de management.

**Această decizie este strategică și aparține exclusiv conducerii, nu consultantului.**

**Livrabilele principale sunt:** registrul sistemelor AI cu clasificare pe categorii de risc, raportul de analiză a contextului organizației, registrul părților interesate și al cerințelor, raportul de gap analysis și documentul de scope al SMIA.

**Un risc tipic este tentația de a defini un scope prea restrâns pentru a reduce efortul aparent.** Totuși, un scope insuficient produce un SMIA care nu acoperă sistemele cu adevărat relevante și nu demonstrează ceea ce este necesar. Auditorii externi verifică adecvarea scope-ului explicit.

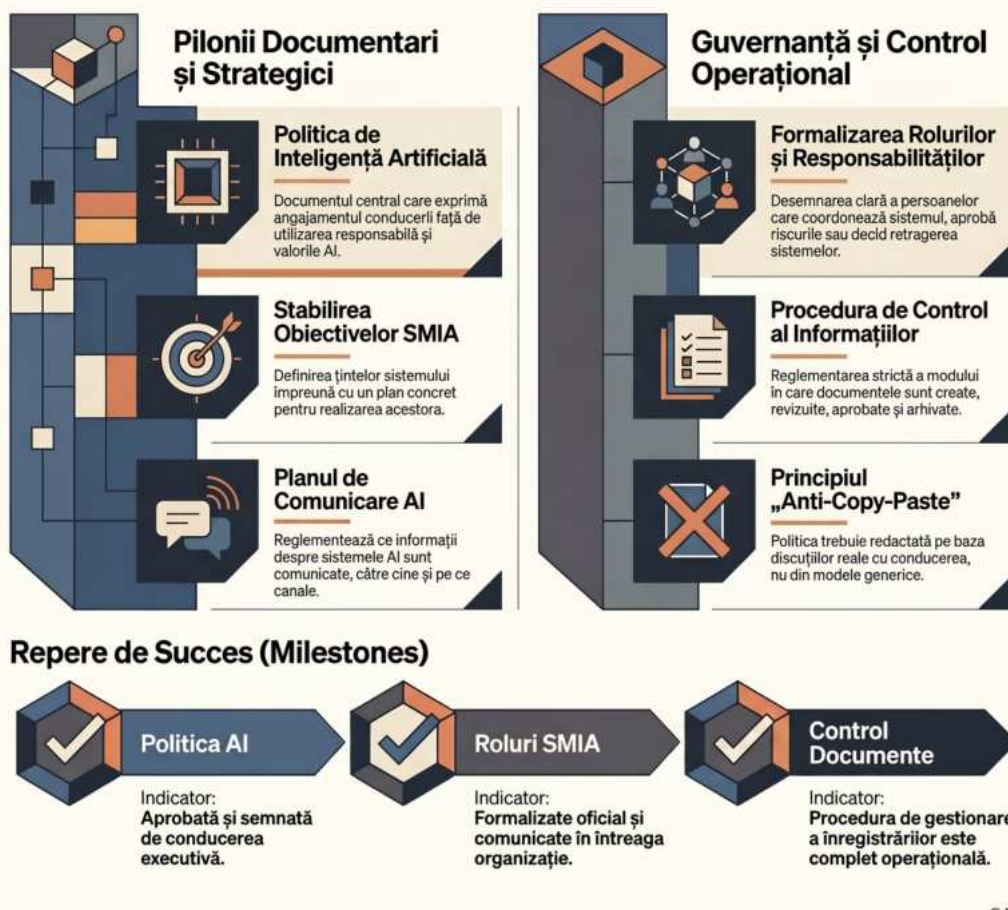
Tratarea acestui risc constituie o discuție deschisă în faza 1, în care explic concret ce înseamnă un scope insuficient în contextul unui audit extern.

**Milestone:** inventarul complet și clasificat, gap analysis aprobat de conducere, scope definit și documentat formal.

## Faza 2: Fundamentele sistemului

### Guvernanța AI: Construirea Fundamentului (Faza 2)

Trecerea de la limite la stabilirea pilonilor de guvernanță. Cristalizează viziunea prin documente normative ce transformă angajamentul teoretic în reguli obligatorii.



**Durata:** A doua lună a proiectului.

**Dacă faza 1 trasează limitele intervenției, faza 2 stabilește pilonii de guvernanță.** Documentele generate în această etapă nu vizează funcționarea operațională, evaluarea riscurilor sau monitorizarea sistemelor, ci cristalizează viziunea organizației privind utilizarea inteligenței artificiale, oferind cadrul normativ necesar dezvoltărilor viitoare.

**Documentul central** al acestei faze este **politica de inteligență artificială**. Nu este o declarație de intenții. Este documentul în care conducerea exprimă angajamentul față de utilizarea responsabilă a AI, principiile care ghidează deciziile despre sisteme AI, limitele acceptabile și valorile care primează când apar conflicte între eficiență și impact. **Redactarea lui cere cel puțin o ședință de lucru cu conducerea executivă**, în care discutăm concret ce vrea organizația să afirme și ce este dispusă să respecte în practică.

Tot în această fază **se formalizează rolurile și responsabilitățile legate de SMIA**: cine coordonează sistemul, cine aprobă evaluările de risc, cine are autoritatea de a decide retragerea unui sistem AI din funcțiune, cine raportează incidentele. Aceste decizii de guvernanță, odată documentate, devin obligatorii și auditabile.

**Se stabilesc obiectivele SMIA cu planul de realizare**, procedura de control al informațiilor documentate care reglementează cum sunt create, revizuite, aprobate și arhivate documentele sistemului, și planul de comunicare AI, care specifică ce informații despre sistemele AI se comunică intern și extern, cui, când și pe ce canale.

**Livrabile principale:** politica de inteligență artificială, documentul de roluri și responsabilități, obiectivele SMIA și planul de realizare, procedura de control al documentelor și înregistrărilor, planul de comunicare AI.

**Riscul tipic în această fază este redactarea unei politici AI generice**, construite pe fraze preluate din alte organizații sau din modele descărcate de pe internet. Tratarea lui este una dintre aplicațiile directe ale principiului anti-copy-paste discutat în capitolul anterior: politica se redactează pe baza discuțiilor cu conducerea, nu înaintea lor.

**Milestone:** politica AI aprobată și semnată de conducere, rolurile formalizate și comunicate intern, procedura de control al documentelor operațională.

Faza 3: Riscuri și evaluări de impact

Faza 3: Evaluarea Riscurilor și Impactului AI

Aceasta este etapa decisivă care separă un sistem de management AI decorativ de unul funcțional. Pe parcursul lunii a treia, organizația trece de la cadrul teoretic la evaluarea concretă a riscurilor tehnice și a impactului asupra societății.



Livrabile Principale	Importanță Strategică
Registrul Riscurilor AI	Documentul central pentru monitorizarea continuă a sistemelor.
Rapoarte de Impact (A.5.2)	Elementul diferențiator cheie pentru succesul auditului extern.
Planul de Tratare	Documentul care transformă analiza riscurilor în acțiuni operaționale.

© NotebookLM

**Durata: A treia lună a proiectului.**

Aceasta este **faza care separă SMIA-urile credibile de cele decorative**. Tot ce s-a construit până acum este cadrul. Acum se face munca reală: **evaluarea riscurilor** fiecărui sistem AI din inventar și evaluarea impactului acestor sisteme asupra persoanelor și societății.

**Faza debutează cu stabilirea criteriilor de risc:** ce înseamnă risc mare, mediu sau mic în contextul specific al organizației, care sunt sursele de risc relevante pentru tipurile de sisteme operate (bias algoritmic, drift al modelului, date de antrenament deficitare, utilizare în afara scopului declarat, dependență de furnizor, vulnerabilități de securitate cibernetică) și care este nivelul de risc rezidual acceptabil după aplicarea măsurilor de tratare. Aceste criterii sunt decizii ale conducerii.

**Urmează prima rundă de evaluări de risc pentru fiecare sistem AI din scope.** Fiecare evaluare produce un raport care identifică riscurile specifice, le cuantifică conform criteriilor stabilite și propune măsuri de tratare.

**Registrul riscurilor AI centralizează toate aceste evaluări și devine documentul de referință pentru monitorizarea continuă.**

**Paralel cu evaluările de risc,** se realizează **evaluările de impact ale sistemelor AI**. Aceasta este, în terminologia standardului, procedura de la clauza 6.1.4 și controlul A.5.2: ce impact are fiecare sistem AI asupra persoanelor afectate de deciziile sale, asupra grupurilor vulnerabile, asupra echității și, acolo unde este relevant, asupra societății în ansamblu.

Calitatea acestor rapoarte de impact determină în proporție semnificativă impresia pe care o face SMIA-ul la auditul extern.

**Faza se încheie cu procedura și planul de tratare a riscurilor,** care transformă riscurile identificate în acțiuni concrete cu responsabili și termene.

**Livrabile principale:** criteriile de risc aprobate, procedura de evaluare a riscurilor, procedura de evaluare a impactului, registrul riscurilor AI, rapoartele de evaluare a riscurilor per sistem, rapoartele de evaluare a impactului per sistem, procedura și planul de tratare a riscurilor.

**Riscul tipic este scurtarea evaluărilor de impact pentru a economisi timp.** Este cea mai scumpă greșeală pe care o poate face o organizație în proiectul de implementare.

Auditorii externi acordă o atenție deosebită tocmai acestei componente, pentru că evaluarea impactului este elementul diferențiator al standardului 42001.

Un raport de impact superficial, cu scenarii generice și fără ancorare în operațiunile reale, comunică auditorului că organizația nu a înțeles ce construiește.

**Milestone:** toate evaluările de risc și de impact finalizate și aprobate, planul de tratare a riscurilor aprobat de conducere.

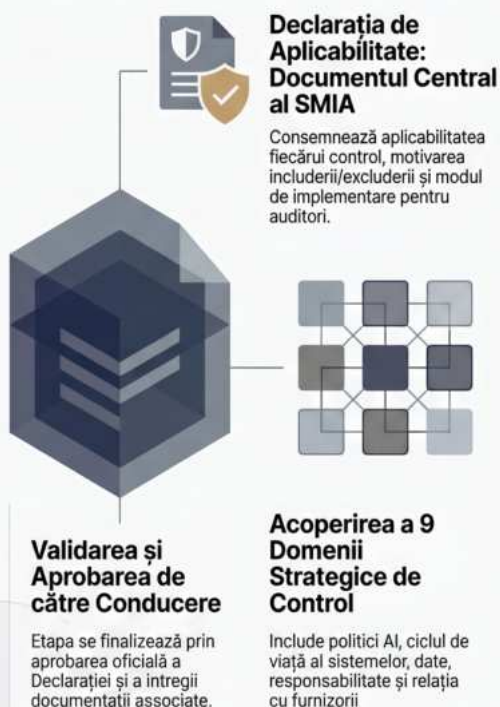


## Faza 4: Controale operaționale și declarația de aplicabilitate

### Faza 4: Controale Operaționale și Declarația de Aplicabilitate în Managementul AI

Transformarea planificării în documentație verificabilă, cu accent pe Declarația de Aplicabilitate și conformitatea AI Act pentru audit extern.

#### Declarația de Aplicabilitate și Pilonii Anexei A



#### Conformitate AI Act și Trasabilitate

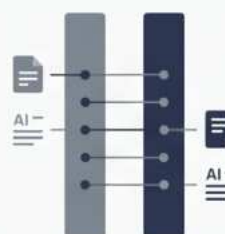
##### Activarea Stratului Modular AI Act

Generarea documentației tehnice, a evaluărilor de impact (FRIA) și a procedurilor de supraveghere umană.



##### Sistemul de Trasabilitate Dublă

Fiecare document se referă explicit la clauza standardului și la articolul corespunzător din AI Act.



##### Livrabile Critice pentru Auditul Stage 1

Include Declarația de Aplicabilitate, dosarul de evaluare a conformității și procedurile specifice de risc.



AI NotebookLM

**Durata: A patra lună a proiectului.**

Tot ceea ce fazele anterioare au definit, evaluat și aprobat devine în faza a patra **documentație concretă și verificabilă**: documentele asociate celor 38 de controale din Anexa A a standardului și, acolo unde sunt aplicabile, documentele din stratul modular AI Act.

**Documentul central al acestei faze este Declarația de Aplicabilitate.** Pentru fiecare dintre cele 38 de controale din Anexa A, declarația consemnează dacă controlul este aplicabil organizației, motivul includerii sau excluderii și modul în care este implementat. Este **documentul care pune în relație directă arhitectura SMIA cu cerințele standardului** și este primul pe care îl solicită orice auditor extern la deschiderea Stage 1.

**Construcția controalelor din Anexa A acoperă nouă domenii:** politicile AI ale organizației, organizarea internă și responsabilitatea, resursele pentru sistemele AI, evaluarea impactului sistemelor AI, ciclul de viață al sistemelor AI, datele pentru sistemele AI, informațiile pentru părțile interesate, utilizarea responsabilă a sistemelor AI și relațiile cu furnizorii, terții și clienții.

**Fiecare domeniu generează un set de proceduri, politici sectoriale și înregistrări.** Nu toate organizațiile le construiesc pe toate: Declarația de Aplicabilitate consemnează explicit ce se exclude și de ce, iar o excludere motivată corect este complet acceptabilă la audit.

**Tot în această fază se activează, acolo unde sunt aplicabile, documentele din stratul modular AI Act:** documentația tehnică cerută furnizorilor, dosarul de evaluare a conformității, procedurile specifice de supraveghere umană pentru sisteme cu risc ridicat și evaluările de impact asupra drepturilor fundamentale pentru categoriile de implementatori cărora li se aplică articolul 27 din regulament.

**Livrabile principale:** Declarația de Aplicabilitate, documentele asociate tuturor controalelor din Anexa A aplicabile, documentele din modulul AI Act activate conform profilului organizației.

**Riscul tipic este pierderea coerenței pe volumul mare de documente:** fiecare document este construit izolat și nu se conectează corect cu celelalte. Tratarea lui este sistemul de trasabilitate dublă: fiecare document se referă explicit la clauza standardului și la articolul AI Act pe care le acoperă, astfel încât auditorul poate naviga rapid în sistem.

**Milestone:** Declarația de Aplicabilitate finalizată și aprobată de conducere, toate documentele controalelor aplicabile finalizate și validate.

Faza 5: Operaționalizare și competențe

# SMIA Faza 5: De la Proiect la Realitate Operațională

Tranziția organizațiilor de la documentația teoretică a Sistemului de Management al Inteligenței Artificiale la funcționarea reală, conformă legal. Faza 5 (luna 5) mută accentul pe dezvoltarea competențelor umane și activarea sistemelor de monitorizare pentru conformitatea cu AI Act.

Alfabetizarea și Competența AI (Conformitate Legală)

## Matricea de Competențe AI

Identificarea cunoștințelor necesare și a lacunelor pentru fiecare rol implicat.

## Termen Limită AI Act: 2 Februarie 2025

Alfabetizarea AI documentată devine o obligație legală obligatorie pentru furnizori și implementatori.

## Evitarea Formalismului în Instruiri

Instruirile trebuie adaptate rolului, nu doar bifate ca o formalitate administrativă.

Rol Vizat	Focus Instruirea
Conducere Executivă	Orientare strategică și responsabilitate
Utilizatori Operativi	Utilizarea sigură și eficientă a sistemelor
Auditori Interni	Verificarea conformității și a proceselor

Monitorizare și Supraveghere Umană

## Activarea Jurnalelor de Evenimente

Înregistrarea sistematică a comportamentelor AI și a tuturor intervențiilor umane decizionale.

## Supravegherea Umană ca Practică

Sistemul produce înregistrări reale, demonstrând că supravegherea nu este doar pe hârtie.

## Milestone-ul Operaționalizării

Toate instruirile documentate și primele înregistrări operaționale generate cu succes.



**Durata: A cincea lună a proiectului.**

Până la finalul lunii a patra, SMIA există pe hârtie. Faza a cincea îl face să existe în realitate. Este **faza în care sistemul trece din starea de proiect în starea de funcționare și în care organizația începe să producă primele înregistrări operaționale reale.**

**Prima componentă a acestei faze este construcția matricei de competențe AI:** ce cunoștințe și abilități sunt necesare pentru fiecare rol care interacționează cu sistemele AI din scope, ce competențe există deja și ce lacune trebuie acoperite.

Pe baza acestei matrice, se planifică și se desfășoară instruirile: sesiuni pentru conducerea executivă, sesiuni pentru coordonatorul SMIA, sesiuni pentru utilizatorii operaționali ai sistemelor AI și sesiuni pentru auditorii interni.

**Atenție!** Articolul 4 din AI Act impune tuturor furnizorilor și implementatorilor să asigure alfabetizare AI documentată pentru personalul relevant, obligație aplicabilă din 2 februarie 2025. Articolul 26 alin. (2) adaugă că persoanele desemnate pentru supravegherea umană a sistemelor cu risc ridicat trebuie să dispună de competența, instruirea și autoritatea necesare.

**Dovada acestor cerințe sunt înregistrările instruirilor, nu declarațiile de intenție.**

**A doua componentă este punerea în funcțiune a jurnalelor de evenimente și a procedurilor de monitorizare:** înregistrarea sistematică a funcționării sistemelor AI, a incidentelor și comportamentelor neașteptate, a intervențiilor umane și a deciziilor care derogă de la recomandările sistemului. Aceste înregistrări sunt dovada că supravegherea umană nu este o procedură pe hârtie, ci o practică operațională.

**Faza se încheie cu primele înregistrări operaționale reale ale sistemului,** care dovedesc că SMIA nu a produs doar documente, ci a produs și comportamente organizaționale verificabile.

**Livrabile principale:** matricea de competențe AI, planul de instruire și înregistrările instruirilor realizate, procedurile de monitorizare operațională, jurnalele de evenimente activate și primele înregistrări generate.

**Riscul tipic este tratarea instruirilor ca pe o formalitate de parcurs rapid.** Un angajat care a semnat o condică de prezență la o sesiune de două ore nu îndeplinește cerințele de alfabetizare AI impuse de articolul 4 și nici competența de supraveghere umană cerută de articolul 26 alin. (2) din AI Act. Tratarea lui este calibrarea instruirilor pe roluri concrete, cu conținut relevant pentru ce face efectiv fiecare participant cu sistemele AI din scope.

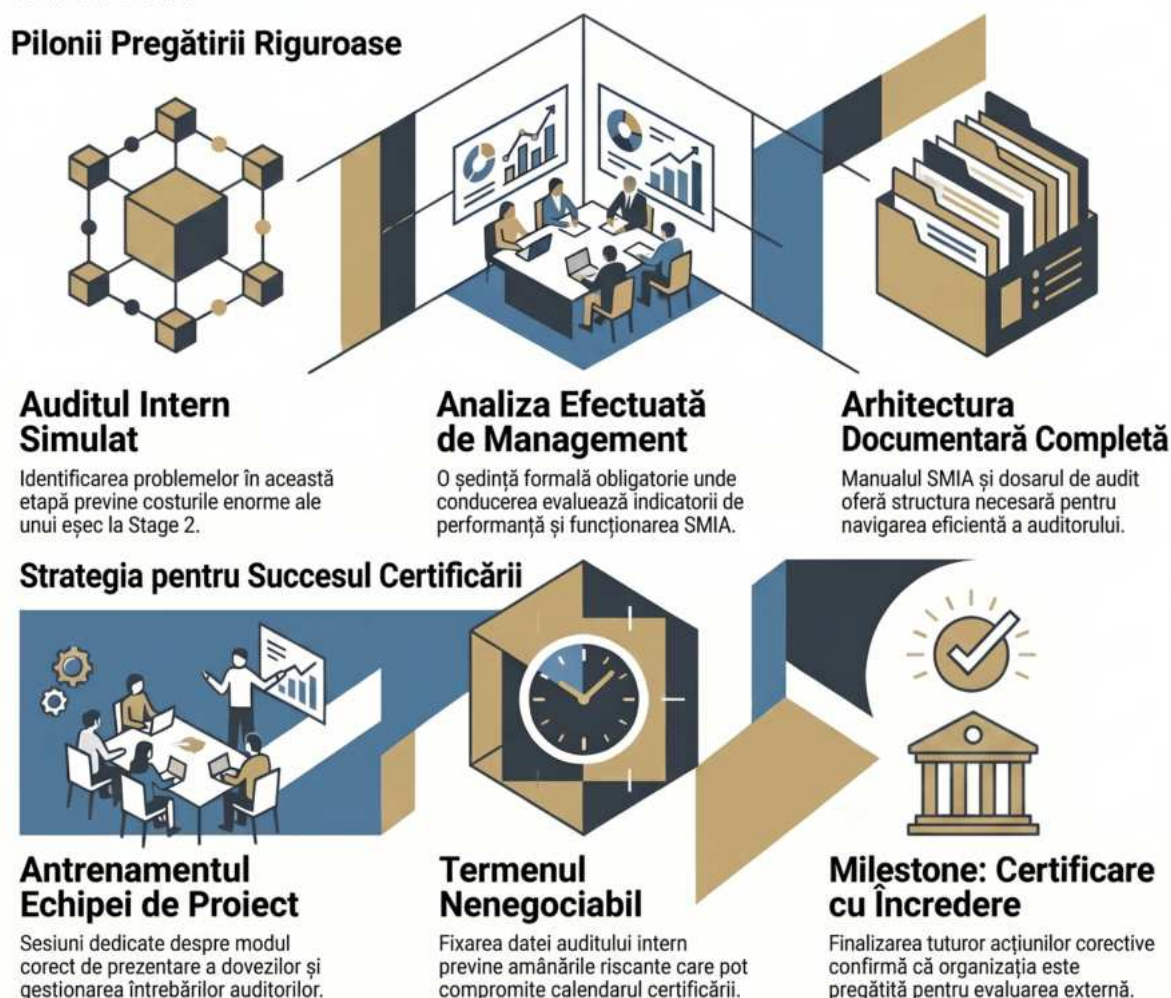
**Milestone:** toate instruirile planificate realizate și documentate, jurnalele operaționale active și primele înregistrări generate.

## Faza 6: Audit intern și pregătire certificare

### SMIA: Pregătirea Finală pentru Certificarea AI

Faza a șasea a proiectului transformă speranța în certitudine printr-o simulare riguroasă a auditului extern. Această etapă finală se concentrează pe identificarea timpurie a erorilor și alinierea strategică a echipei pentru succesul certificării oficiale.

#### Pilonii Pregătirii Riguroase



#3 NotebookLM

**Durata:** A șasea lună a proiectului.

Ultima fază a proiectului are un singur obiectiv: organizația iese din ea pregătită să facă față auditului extern cu încredere, nu cu speranța că totul va fi în ordine.

**Activitatea centrală este auditul intern**, pe care îl conduc personal și îl tratez cu aceeași rigoare pe care o aplică un auditor extern. Verific completitudinea și coerența documentației, trasabilitatea cerințelor standardului și a AI Act, funcționarea efectivă a procedurilor și dovezile operaționale generate în faza anterioară. **Fiecare neconformitate identificată este documentată și urmată de un plan de acțiune corectivă cu termen și responsabil.**

**Auditul intern este cel mai valoros instrument de pregătire pentru certificare**, nu pentru că identifică probleme, ci pentru că le identifică la momentul potrivit, când mai există timp pentru remediere. Organizațiile care sar peste acest pas sau îl realizează superficial descoperă problemele la Stage 2, unde consecințele sunt incomparabil mai costisitoare.

Urmează **analiza efectuată de management**, prima ședință formală în care conducerea executivă evaluează funcționarea SMIA pe baza rezultatelor auditului intern, a indicatorilor de performanță și a constatărilor din faza operațională. **Procesul-verbal al acestei ședințe este un document obligatoriu și auditabil.**

Se redactează **manualul SMIA**, documentul-umbrelă care descrie sistemul în ansamblu și servește ca ghid de navigare prin întreaga arhitectură documentară, și se organizează dosarul de audit extern: toate documentele și înregistrările aranjate în ordinea în care le va solicita auditorul extern.

**Ultima activitate a acestei faze este sesiunea de pregătire a echipei pentru interacțiunea cu auditorii externi:** cum se răspunde la întrebările de audit, ce dovezi se prezintă, ce nu se spune din proprie inițiativă și cum se gestionează o constatare pe parcursul Stage 2.

**Livrabile principale:** raportul complet de audit intern simulat, planul de acțiuni corective cu evidența implementării, procesul-verbal al analizei efectuate de management, planul de îmbunătățire continuă, manualul SMIA, dosarul de audit extern organizat și echipa pregătită pentru interacțiunea cu auditorii externi.

**Riscul tipic este amânarea auditului intern simulat pentru a câștiga timp pe restanțe din fazele anterioare.** Aceasta este o decizie care costă: fiecare zi câștigată prin scurtarea fazei 6 se poate transforma în săptămâni de remedieri după Stage 2. Tratarea lui este fixarea datei auditului intern simulat la startul proiectului și tratarea ei ca un termen nenegociabil.

**Milestone:** auditul intern simulat finalizat, toate neconformitățile identificate tratate și verificate, dosarul de audit extern predat conducerii, cererea de audit transmisă organismului de certificare ales.

## Sinteza proiectului

Fază	Durată	Livrabilul central	Milestone
<b>0 - Pregătire și contractare</b>	1-2 săptămâni	Contractul și calendarul proiectului	Echipă constituită, calendar agreat
<b>1 - Diagnosticare și scope</b>	Prima lună	Registrul sistemelor AI, gap analysis	Scope definit și aprobat de conducere
<b>2 - Fundamentele sistemului</b>	A doua lună	Politica AI, roluri, obiective	Politica AI semnată de conducere
<b>3 - Riscuri și impact</b>	A treia lună	Registrul riscurilor, rapoarte de impact	Plan de tratare aprobat de conducere
<b>4 - Controale și SoA</b>	A patra lună	Declarația de Aplicabilitate, controalele Anexei A	SoA aprobată, documentele finalizate
<b>5 - Operaționalizare</b>	A cincea lună	Instruiri, jurnale, prime înregistrări	Primele înregistrări operaționale generate
<b>6 - Audit și certificare</b>	A șasea lună	Raport audit intern, dosar certificare	Dosar predat, cerere de audit transmisă

## Capitolul 6: De la decizie la certificare — studiu de caz



**Fortis Security Solutions S.R.L. este o companie ipotetică**, construită pe un profil compozit reprezentativ pentru sectorul serviciilor de securitate fizică din România. **Orice asemănare cu o organizație reală este neintenționată.** Situațiile, deciziile și provocările descrise sunt, în schimb, tipice pentru proiectele din acest sector.

### Profilul companiei și situația de pornire

**Fortis Security Solutions S.R.L.** este o companie de securitate cu 340 de angajați, cu sediul în Cluj-Napoca și cu sucursale operaționale în București, Timișoara și Iași. Activitatea sa acoperă trei linii de servicii: paza umană cu 275 de agenți de securitate, securitate electronică prin proiectarea, instalarea și mentenanța sistemelor VSS, control acces, detecție efracție și detecție incendiu, și servicii integrate de securitate prin intermediul unui centru de monitorizare propriu, activ 24 de ore din 24.



**Fortis nu deținea nicio certificare ISO la momentul startului proiectului.** Directorul general avusese în vedere ISO 9001 cu câțiva ani în urmă, dar proiectul nu se materializase.

**Factorul declanșator** nu a fost un termen din AI Act. **A fost o solicitare comercială.** Unul dintre clienții corporativi majori ai companiei, o instituție financiară, a transmis un chestionar de evaluare a furnizorilor care includea, pentru prima dată, întrebări despre guvernanța AI și conformitatea cu Regulamentul (UE) 2024/1689. Fără un răspuns credibil, Fortis risca descalificarea dintr-un proces de reînnoire contractuală cu o valoare anuală semnificativă. Directorul general a contactat serviciile mele la două săptămâni după primirea chestionarului.

## Faza 0: Pregătire și contractare

**Prima discuție cu conducerea Fortis a durat trei ore și jumătate.** Nu pentru că documentele de contractare ar fi cerut atât, ci pentru că directorul general și directorul de operațiuni aveau viziuni diferite despre ce presupune proiectul.

**Directorul de operațiuni considera că cerințele AI Act nu se aplică Fortis, deoarece compania nu dezvoltă software AI, ci doar îl instalează și îl configurează.** Această convingere, corectă parțial și incorectă în aspectele esențiale, a trebuit clarificată direct și documentată înainte de semnarea contractului.

**Am clarificat că rolul de integrator, adică instalarea și configurarea unui sistem AI la un client, nu exonerează automat Fortis de obligații.** Când același sistem este utilizat în centrul de monitorizare propriu al companiei pentru a lua decizii operaționale, Fortis este implementator în sensul AI Act și are obligații proprii. Când sistemul este instalat la un client, Fortis are obligații de informare și documentare față de acel client, care devine la rândul lui implementator.

Această clarificare a schimbat complet perspectiva directorului de operațiuni. Proiectul a primit susținerea lui activă de la acel moment, nu doar acordul formal. Contractul a fost semnat la două săptămâni după prima discuție.

**Echipa internă a inclus un coordonator SMIA desemnat din departamentul tehnic, doi membri din operațiuni și un reprezentant HR.** Calendarul a fost fixat pentru șase luni, cu workshop-urile blocate în agendele tuturor participanților.

## Faza 1: Diagnosticare și definire scope

**Inventarierea sistemelor AI din Fortis a produs patru descoperiri,** dintre care una complet neașteptată pentru conducere.

- **Primul sistem identificat a fost platforma VMS cu analiză video AI,** utilizată atât în centrul de monitorizare propriu, cât și instalată la aproximativ 60 de clienți activi. Platforma include module de detecție a anomaliilor comportamentale, detecție a efracției de perimetru, numărare persoane și analiză a densității mulțimilor. Furnizorul este o companie internațională care livrează sistemul ca produs finit, fără modificări de cod din partea Fortis. Rolul Fortis este dublu: integrator pentru instalările la clienți și implementator pentru utilizarea în centrul propriu de monitorizare.
- **AI doilea sistem a fost un sistem de control acces cu verificare biometrică facială,** instalat la 23 de clienți. Sistemul realizează verificarea identității, adică confirmă că persoana care solicită accesul este cine susține că este, fără a construi o



bază de date de identificare a persoanelor necunoscute. Această distincție este esențială din perspectiva AI Act: sistemele de verificare biometrică destinate exclusiv confirmării identității și acordării accesului într-o incintă nu se încadrează în categoria sistemelor cu risc ridicat. Clasificarea corectă a acestui sistem a eliminat un volum documentar semnificativ pe care Fortis îl anticipase incorect ca obligatoriu.

- **AI treilea sistem a fost o platformă de management și predicție a incidentelor**, utilizată intern de dispeceratul din centrul de monitorizare. Platforma analizează datele istorice ale incidentelor și generează recomandări de redistribuire a agenților de pază și de prioritizare a intervențiilor. Clasificarea: risc limitat, cu obligații de transparență.
- **AI patrulea sistem a fost descoperit în cursul interviului cu directorul de resurse umane**, nu al celui cu directorul tehnic. Fortis utiliza de aproximativ doi ani un modul AI integrat în platforma de HR pentru planificarea schimburilor agenților de pază, optimizarea alocărilor pe baza performanței istorice și generarea de scoruri de eficiență individuală per agent. Directorul general nu știa că acel modul are componente AI. Credea că este vorba despre un instrument de planificare cu automatizări simple.

Acesta a fost momentul cel mai tensionat din faza de diagnosticare. **Modulul de planificare și evaluare a personalului se încadrează în Anexa III a AI Act**, punctul 4 litera (b), categoria sistemelor utilizate pentru alocarea sarcinilor pe baza comportamentului individual și pentru monitorizarea și evaluarea performanței persoanelor aflate în relații contractuale de muncă. **Clasificarea ca risc ridicat este în acest caz certă și necontestabilă**: modulul generează scoruri de eficiență individuală per agent, adică creează profiluri ale persoanelor fizice, iar articolul 6 alineatul (3) din regulament prevede explicit că un astfel de sistem este întotdeauna considerat cu risc ridicat, indiferent de alte circumstanțe. **Este un sistem cu risc ridicat**. Fortis îl utiliza fără nicio documentație de guvernanță, fără o evaluare formală a riscurilor și fără să fi informat agenții că deciziile de alocare și scorurile de performanță sunt generate cu suport AI.

**Această descoperire a recalibrat complet profilul de risc al Fortis față de AI Act și a extins documentarul necesar.**

**Gap analysis-ul a confirmat ce era de așteptat**: nicio structură de guvernanță AI nu exista, nicio procedură de evaluare a riscurilor AI nu era în vigoare și nicio documentare a sistemelor nu fusese produsă anterior. **Punctul de pornire era zero**, ceea ce, paradoxal, simplifică proiectul față de organizațiile care au documentație inconsistentă pe care trebuie mai întâi să o dezasambleze.

**Scope-ul SMIA a fost definit pentru toate cele patru sisteme AI identificate**, pentru toate locațiile Fortis și pentru activitățile de integrare la clienți, în măsura în care Fortis operează sisteme AI în cadrul acestor activități, concret centrul de monitorizare.

## Faza 2: Fundamentele sistemului

**Redactarea politicii de inteligență artificială a Fortis a necesitat două sesiuni de lucru cu directorul general**. Motivul a fost convingerea fermă a acestuia că documentul trebuie să afirme că Fortis nu utilizează sisteme AI proprii, ci doar instalează sisteme ale furnizorilor, o

premisă infirmată clar de constatările primei etape, dar adânc înrădăcinată în percepția managementului.

- **Prima sesiune a servit exclusiv pentru a discuta ce semnifică operarea unui sistem AI în centrul de monitorizare**, indiferent că software-ul aparține furnizorului.
- **A doua sesiune a produs textul efectiv al politicii**, care a reflectat în final o poziție clară și asumată: **Fortis recunoaște că utilizează sisteme AI în operațiunile sale, se angajează să le guverneze responsabil și stabilește principiile care ghidează deciziile despre adoptarea, utilizarea și retragerea sistemelor AI.**

Directorul general a semnat politica la finalul celei de-a doua sesiuni, ceea ce este, din experiența mea, un indicator bun al nivelului real de angajament al conducerii față de proiect.

Formalizarea rolurilor a evidențiat o **lacună organizațională tipică pentru companiile de securitate**: responsabilitatea pentru sistemele AI era distribuită informal între directorul tehnic, care gestiona VMS-ul și sistemele de control acces, directorul de operațiuni, care superviza centrul de monitorizare, și directorul HR, care utiliza modulul de planificare. Nimeni nu deținea responsabilitatea de ansamblu. SMIA a creat această responsabilitate prin desemnarea formală a coordonatorului SMIA cu atribuții clare și autoritate de escaladare.

### Faza 3: Riscuri și evaluări de impact

**Prima rundă de evaluări de risc a produs rezultate predictibile pentru trei dintre cele patru sisteme și un rezultat surprinzător pentru al patrulea.**

**Înainte de a demara evaluările efective**, echipa de proiect **a transmis furnizorilor principalelor platforme AI solicitări formale de documentație tehnică.**

**Obligația furnizorilor** de a transmite aceste informații implementatorilor derivă din Art. 13 din AI Act, care reglementează transparența și furnizarea de informații, iar Anexa IV definește conținutul minim al documentației tehnice care poate fi utilizat ca referință la solicitare.

Controlul A.6.2.7 din standard, aplicabil Fortis în rolul de integrator, impune păstrarea documentației tehnice a sistemelor AI instalate. **Furnizorul platformei VMS nu dispunea de documentația structurată conform cerințelor regulamentului**, fapt consemnat ca risc suplimentar: dependența de un furnizor care nu poate demonstra conformitatea propriului produs.

**Platforma VMS cu analiză video a generat riscurile tehnice așteptate**: fals pozitive în detecția anomaliilor comportamentale cu potențial de intervenție nejustificată, erori de numărare în condiții de iluminare deficitară și dependență de actualizările algoritmice ale furnizorului fără notificare prealabilă.

**O decizie de clasificare a trebuit luată explicit în această fază.** Funcționalitățile platformei descrise în inventar, detecția anomaliilor comportamentale, detecția efracției de perimetru, numărarea persoanelor și analiza densității mulțimilor, nu se încadrează automat în nicio categorie din Anexa III a AI Act.

**Clasificarea ca sistem cu risc ridicat** ar presupune că algoritmi procesează date biometrice și constituie categorisire biometrică în sensul regulamentului, aspect pe care documentația tehnică incompletă a furnizorului nu îl lămură definitiv. **Fortis a decis să trateze platforma**

**VMS ca sistem cu risc ridicat în scopul construcției SMIA**, aplicând principiul prudenței, și a documentat această decizie explicit în registrul sistemelor AI.

**Măsurile de tratare au inclus proceduri de verificare umană obligatorie** înainte de orice intervenție și un protocol de escaladare pentru situațiile în care recomandarea sistemului este depășită de dispecer.

**Baza juridică a acestor obligații pentru Fortis ca implementator** este Art. 14 și Art. 26 alin. (1) din AI Act, care impun implementatorilor să activeze și să mențină măsurile de supraveghere umană și să utilizeze sistemul conform instrucțiunilor furnizorului. **Obligația de a proiecta sistemul astfel încât riscul rezidual să fie acceptabil revine furnizorului**, conform Art. 9 alin. (5), care reglementează exclusiv obligații de proiectare și dezvoltare. Fortis trebuia să primească informarea privind riscul rezidual de la furnizor, informare care nu fusese furnizată, generând o acțiune corectivă formală adresată acestuia.

**Evaluarea de impact a platformei VMS a fost cel mai complex document din faza 3.** Sistemul este utilizat pentru supravegherea spațiilor clienților, care includ atât angajați ai clienților, cât și vizitatori și, în unele instalații, clienți ai clienților.

**Impactul potențial al unui fals pozitiv** poate include, de exemplu, reținerea nejustificată a unei persoane de către agenții de pază, cu consecințe juridice și reputaționale pentru Fortis și pentru clientul său. La acest lanț de consecințe s-a adăugat **riscul de bias algoritmic față de anumite categorii de persoane**, ca urmare a datelor de antrenament nereprezentative, risc imposibil de cuantificat precis din cauza documentației tehnice incomplete a furnizorului. Ambele dimensiuni au fost documentate explicit în raportul de impact.

**Modulul AI de planificare și evaluare a personalului a produs evaluarea de risc cu cele mai mari implicații operaționale și juridice.** Spre deosebire de platforma VMS, a cărei clasificare a necesitat o decizie de prudență, modulul HR este un sistem cu risc ridicat cert și necontestabil.

Se încadrează în Anexa III, punctul 4 litera (b), **categoria sistemelor utilizate pentru alocarea sarcinilor pe baza comportamentului individual și pentru monitorizarea și evaluarea performanței persoanelor aflate în relații contractuale de muncă.**

Clasificarea este consolidată suplimentar de Art. 6 alin. (3) din regulament, care prevede că **un sistem din Anexa III este întotdeauna considerat cu risc ridicat dacă creează profiluri ale persoanelor fizice**: modulul generează scoruri de eficiență individuală per agent, eliminând orice excepție posibilă.

Analiza a identificat că algoritmul de scoring utiliza ca input principal numărul de intervenții confirmate per agent, fără să pondereze complexitatea intervențiilor sau contextul operațional.

Agenții de securitate alocați în zone cu activitate redusă primeau scoruri mai mici nu pentru că performau mai slab, ci pentru că circumstanțele îi expuneau la mai puține evenimente. Acest bias sistematic afecta direct deciziile de alocare preferențială și, indirect, evaluările de performanță care intrau în calculul primelor.

**Niciunul dintre cei aproximativ 275 de agenți de securitate afectați nu fusese informat că un sistem AI contribuia la aceste decizii**, ceea ce genera o neconformitate directă cu Art. 26 alin. (11) din AI Act, care impune informarea persoanelor fizice supuse deciziilor unui sistem AI cu risc ridicat.

**Remediarea a necesitat atât o măsură tehnică**, ajustarea metodologiei de scoring din platforma HR împreună cu furnizorul, **cât și o măsură organizațională urgentă**: informarea formală a tuturor agenților despre existența și rolul sistemului AI în deciziile de planificare și evaluare.

Această comunicare a fost redactată cu atenție, pentru a fi clară, nediscriminatorie și conformă cu cerințele de transparență din Art. 26 alin. (11), și a fost transmisă înainte de finalizarea fazei 3.

## Faza 4: Controale operaționale și declarația de aplicabilitate

**Din cele 38 de controale ale Anexei A, Declarația de Aplicabilitate a Fortis a marcat 31 ca aplicabile și 7 ca excluse cu justificare.** Excluderile au vizat în principal controalele referitoare la dezvoltarea și antrenarea modelelor AI, irelevante pentru o organizație care nu dezvoltă sisteme AI proprii.

**Construcția documentelor pentru controalele din domeniul A.7, guvernanța datelor**, a generat o discuție importantă cu directorul tehnic despre datele video stocate în VMS-ul din centrul de monitorizare. Datele erau reținute pe durate variabile, în funcție de cerințele contractuale ale fiecărui client, fără o politică unitară de guvernanță. **Construcția controlului A.7 a produs prima politică unitară de gestionare a datelor AI din istoria companiei**, acoperind retenția, accesul, ștergerea și trasabilitatea.

Documentele din stratul modular AI Act au inclus **procedura de raportare a incidentelor grave la autoritățile competente, procedura de supraveghere umană specifică pentru platforma VMS și modulul HR, și instrucțiunile de utilizare** pe care Fortis le furnizează clienților la instalarea sistemelor cu componente AI, pentru a le permite acestora să își exercite la rândul lor obligațiile de implementator.

Acest din urmă document a rezolvat și problema comercială care declanșase proiectul: chestionarul clientului financiar a putut fi completat cu referință la documentele formalizate și la procedurile implementate, nu cu asigurări verbale.

## Faza 5: Operaționalizare și competențe

**Matricea de competențe AI a Fortis a identificat trei grupuri cu nevoi de instruire distincte: dispecerii din centrul de monitorizare**, care utilizează zilnic platforma VMS cu analiză AI și trebuie să înțeleagă limitele sistemului și obligația de verificare umană înainte de orice intervenție; **agenții de securitate**, care supervizează intervențiile și trebuie să știe când și cum să depășească recomandările sistemului; și **departamentul HR**, care utilizează modulul de planificare și trebuie să înțeleagă cum se interpretează scorurile generate și care sunt limitele lor.

**Sesiunea de instruire cu dispecerii a produs cea mai valoroasă conversație din întreaga fază.** Unul dintre dispeceri a adus în discuție o situație reală: platforma generase în trecut o alertă de comportament suspect pentru o persoană care, la verificarea înregistrării, se dovedise a fi un angajat al clientului cu un mers specific din cauza unui handicap locomotor. Intervenția fusese declanșată, iar situația fusese stânjenitoare pentru toate părțile. Sistemul nu fusese antrenat pe date suficient de diverse.

Această situație a intrat în raportul de evaluare a impactului ca exemplu real documentat și a generat o cerință suplimentară față de furnizorul platformei VMS: furnizarea de informații



despre diversitatea datelor de antrenament ale algoritmului de detecție comportamentală. Este exact tipul de informație pe care controlul A.6.2.7 al standardului o cere documentată.

## Faza 6: Audit intern simulat și pregătire certificare

**Auditul intern simulat a identificat trei neconformități și șase observații.**

- **Prima neconformitate:** Declarația de Aplicabilitate fusese aprobată de directorul tehnic, nu de directorul general, contrar procedurii de aprobare stabilite în faza 2. Tratare: reaprobare formală cu semnătura corectă în termen de trei zile.
- **A doua neconformitate:** jurnalul de evenimente al platformei VMS din centrul de monitorizare nu înregistra sistematic motivul depășirii recomandării sistemului, adică cazurile în care dispecerul decidea să nu declanșeze intervenția în ciuda alertei AI. Această înregistrare este esențială pentru demonstrarea supravegherii umane efective. Tratare: modificarea formularului de jurnal și instruire suplimentară de 30 de minute cu echipa de dispeceri.
- **A treia neconformitate:** procedura de evaluare a riscurilor nu includea un mecanism explicit de reevaluare automată la actualizarea majoră a algoritmilor de către furnizori. Un furnizor actualizase algoritmul de detecție comportamentală cu trei luni anterior fără ca Fortis să fi realizat o reevaluare a riscurilor. Tratare: adăugarea unui punct explicit în procedura de gestionare a relației cu furnizorii AI, care obligă la reevaluarea riscurilor la orice actualizare majoră de algoritm.

**Toate trei neconformitățile au fost tratate și verificate în două săptămâni.** Analiza efectuată de management a avut loc în săptămâna a treia a lunii 6 și a produs procesul-verbal obligatoriu. Dosarul de audit extern a fost predat conducerii la finalul lunii, iar cererea de audit a fost transmisă organismului de certificare acreditat RENAR ales de Fortis.

**Stage 1 și Stage 2 s-au desfășurat în lunile 7 și 8 față de startul proiectului.** Auditorul extern a identificat două observații, fără neconformități majore sau minore. **Certificatul ISO/IEC 42001 a fost emis la finalul lunii a 8-a.**

## Ce s-a schimbat în Fortis după certificare

Răspunsul evident este că Fortis deține acum un certificat și a câștigat reînnoirea contractului cu clientul financiar. Răspunsul mai puțin evident, dar mai important, este că directorul general știe acum ce sisteme AI operează compania sa, ce riscuri produc și cine este responsabil pentru fiecare decizie legată de ele. Directorul de operațiuni conduce trimestrial o ședință de revizuire a registrului riscurilor AI. Departamentul HR a modificat metodologia de scoring a personalului și a comunicat transparent cu agenții. Când un client nou a solicitat instalarea unui sistem de analiză video cu modul de recunoaștere a emoțiilor, Fortis a refuzat oferta furnizorului pe baza unei evaluări de risc, nu a unei intuiții.

**Acesta este, în opinia mea, semnul că sistemul funcționează.**

# Drumul spre Certificarea ISO 42001: Studiul de Caz Fortis Security Solutions

## 1. Profilul Companiei și Factorul Declanșator



### Fortis Security Solutions: 340 angajați

Companie cu sediul în Cluj-Napoca și sucursale în București, Timișoara și Iași, activând în paza umană, securitate electronică și monitorizare.



### Riscul pierderii unui contract major

O instituție financiară a solicitat dovezi de guvernanță AI și conformitate cu Regulamentul (UE) 2024/1689 (AI Act) pentru reînnoirea contractului.



### Clarificarea rolului: Integrator vs. Implementator

Fortis este **integrator** când instalează sisteme AI la clienți și **implementator** când utilizează AI în propriul centru de monitorizare pentru decizii operaționale.

## 2. Inventarul Sistemelor AI (Faza 1)



### Platforma VMS (Analiză Video)

Utilizată pentru detecția anomaliilor și densitatea mulțimilor; clasificată preventiv ca „Risc Ridicat” din cauza documentației incomplete a furnizorului.

### Control Acces Biometric vs.

Verificarea biometrică pentru acces a fost clasificată sub pragul de risc ridicat, în timp ce platforma de predicție a incidentelor a fost marcată cu „Risc Limitat”.

### Management Incidente

platforma de predicție a incidentelor a fost marcată cu „Risc Limitat”.



### Descoperirea critică: Modulul HR

Un sistem de planificare a schimburilor care generează scoruri de eficiență individuală, clasificat direct ca „Risc Ridicat” conform AI Act (Anexa III).

## 3. Drumul spre Certificare (Fazele 2-6)

### Faza 2 & 3: Politică și Evaluare de Impact

Asumarea responsabilității de către conducere și documentarea riscurilor de bias algoritmic și a necesității supravegherii umane.

### Faza 4 & 5: Controale și Competențe

Implementarea a 31 de controale operaționale și instruirea dispocerilor pentru a înțelege limitele algoritmilor (ex: evitarea falselor alerte cauzate de dizabilități motorii).



### Luna 8: Certificarea ISO/IEC 42001

După un audit intern cu 3 neconformități remediate rapid, Fortis obține certificarea acreditată RENAR la finalul lunii a opta.

## Clasificarea Sistemelor AI identificate

Sistem AI	Rol Fortis	Clasificare Risc	Baza Legală (AI Act)
Platforma VMS (Video)	Implementator / Integrator	Risc Ridicat (Prudență)	Art. 14 & 26 (Supraveghere umană)
Control Acces Biometric	Integrator	Sub pragul de risc ridicat	Verificare identitate (nu identificare)
Predicție Incidente	Implementator	Risc Limitat	Obligații de transparență
Planificare/ Scoring HR	Implementator	Risc Ridicat (Cert)	Anexa III, pct. 4 lit. (b) / Art. 6(3)

## 4. Rezultate și Schimbări Organizaționale

### Succes Comercial Imediat

Reînnoirea contractului cu clientul financiar prin demonstrarea unei guvernanțe AI solide.



### Maturitate Decizională

Managementul a început să refuze tehnologii invazive (ex: recunoașterea emoțiilor) pe baza evaluărilor de risc, nu a intuiției.

Sinteza proiectului Fortis Security Solutions

Fază	Durață	Livrabilul central	Milestone
0 - Pregătire și contractare	1-2 săptămâni	Contractul și calendarul proiectului	Echipă constituită, calendar agreed
1 - Diagnosticare și scope	Prima lună	Registrul sistemelor AI, gap analysis	Scope definit și aprobat de conducere
2 - Fundamentele sistemului	A doua lună	Politica AI, roluri, obiective	Politica AI semnată de conducere
3 - Riscuri și impact	A treia lună	Registrul riscurilor, rapoarte de impact	Plan de tratare aprobat de conducere
4 - Controale și SoA	A patra lună	Declarația de Aplicabilitate, controalele Anexei A	SoA aprobată, documentele finalizate
5 - Operaționalizare	A cincea lună	Instruiri, jurnale, prime înregistrări	Primele înregistrări operaționale generate
6 - Audit și certificare	A șasea lună	Raport audit intern, dosar certificare	Dosar predat, cerere de audit transmisă

## Capitolul 7: Procesul de certificare



Certificarea nu este concluzia firească și automată a implementării. Este **rezultatul unui audit extern independent**, realizat de o entitate complet separată de consultantul care a condus proiectul.

**Această separare este o cerință de imparțialitate fără de care certificarea nu ar valora nimic.** O organizație certificată de propriul consultant ar fi echivalentul unui student care își corectează singur examenul.

Înțelegerea acestui mecanism înainte de startul proiectului evită o **confuzie frecventă**: conducerea nu trebuie să aștepte finalul implementării pentru a contacta un organism de certificare.

**Contractarea organismului se face de regulă în faza 5 sau la începutul fazei 6**, pentru a sincroniza disponibilitatea auditorilor cu calendarul proiectului.



## Cine poate certifica

**Organismul de certificare trebuie să fie acreditat pentru schema ISO/IEC 42001 de către un organism de acreditare recunoscut internațional.** În România, organismul național de acreditare este **RENAR**. O certificare emisă de un organism acreditat RENAR sau de un organism dintr-o altă țară membră a rețelei internaționale IAF are recunoaștere internațională deplină prin acordurile de recunoaștere multilaterală.

Criteriile practice de selecție a organismului de certificare includ dovada acreditării specifice pentru ISO/IEC 42001, disponibilitatea auditorilor cu experiență în domeniul inteligenței artificiale și al sistemelor de management, reputația pe piața din România și transparența ofertei financiare.

**Costul auditului extern nu este fix:** variază în funcție de dimensiunea organizației, de complexitatea scope-ului, de numărul de locații și de efortul estimat în zile-om de audit. Este întotdeauna separat de costul consultanței și se achită direct organismului de certificare.

**Ofer suport în selecția organismului, în interpretarea documentelor de acreditare și în compararea ofertelor. Această asistență face parte din faza 6 a proiectului și nu generează costuri suplimentare.**

## Cele două etape ale auditului extern

**Auditul extern se desfășoară în două etape consecutive, cu un interval de regulă de câteva săptămâni între ele.**

- **Stage 1 este auditul de pregătire.** Auditorul extern evaluează documentația SMIA și gradul de pregătire a organizației pentru auditul complet. Verifică dacă scope-ul este adecvat, dacă documentele obligatorii există și sunt coerente, dacă Declarația de Aplicabilitate este completă și dacă există dovezi că sistemul a început să funcționeze, adică înregistrări operaționale, cel puțin un ciclu de monitorizare, dovada că politica AI a fost comunicată. Stage 1 se încheie cu un raport care identifică ce trebuie remediat înainte de Stage 2. Neconformitățile identificate în Stage 1 sunt un semnal util, nu un eșec: organizația are timp să le trateze înainte ca auditul propriu-zis să înceapă.
- **Stage 2 este auditul complet pe teren.** Auditorul verifică implementarea efectivă a sistemului prin interviuri cu membrii echipei, analiza înregistrărilor operaționale, examinarea rapoartelor de evaluare a riscurilor și a impactului și evaluarea funcționării reale a procedurilor. Nu verifică doar dacă documentele există, verifică dacă oamenii din organizație știu ce fac și de ce.
- Aceasta este distincția care contează cel mai mult pentru un factor de decizie: Stage 2 nu este un audit de documente. Este un audit al realității organizaționale. Un coordonator SMIA care nu poate explica cu propriile cuvinte cum funcționează metodologia de evaluare a riscurilor, sau un dispecer care nu știe ce face cu o alertă AI înainte de a declanșa o intervenție, vor produce constatări la audit indiferent câte pagini de proceduri există în dosar.

Exact aceasta este rațiunea pentru care sesiunea de pregătire a echipei pentru interacțiunea cu auditorii externi, inclusă în faza 6 a metodologiei, nu este o formalitate. Oamenii nu trebuie să memoreze răspunsuri corecte. Trebuie să înțeleagă ce au construit.

## Ce se poate întâmpla la Stage 2

**Auditorul extern poate concluziona că nu există neconformități și recomandă certificarea direct.**

**Poate identifica neconformități minore**, care se pot trata printr-un plan de acțiuni corective acceptat de organism fără un nou audit pe teren.

**Poate identifica neconformități majore**, care necesită un audit suplimentar înainte de emiterea certificatului. Sau **poate constata că sistemul nu este suficient de matur pentru certificare**, situație rară dacă implementarea a fost condusă corect și dacă auditul intern simulat din faza 6 și-a făcut treaba.

**Subliniez un lucru** pe care îl menționez în orice prim contact cu un client: **nu garantez obținerea certificării**. Decizia aparține exclusiv organismului de certificare.

**Garantez un proiect condus profesionist, o documentație adaptată realității organizației și o echipă pregătită să facă față auditului.** Acestea sunt condițiile necesare pentru certificare. Nu sunt, prin ele însele, suficiente dacă organizația nu și-a respectat angajamentele de co-implementare pe durata proiectului.

## Ciclul de viață al certificatului

**Certificatul ISO/IEC 42001 emis după Stage 2 are o valabilitate de trei ani.** Pe durata acestor trei ani, organismul de certificare realizează anual audituri de supraveghere, mai scurte decât auditul inițial, care verifică că sistemul rămâne funcțional și că neconformitățile identificate anterior au fost tratate. La finalul celor trei ani, un audit de reînnoire revaluează sistemul în ansamblu.

Implicația practică pentru o organizație care a parcurs un proiect de implementare corect este că auditul de supraveghere nu este o surpriză.

Este o verificare periodică a unui sistem pe care organizația îl operează continuu. Diferența dintre organizațiile care trec lejer prin auditurile de supraveghere și cele care le trăiesc cu anxietate este exact diferența dintre un sistem viu și o arhivă.

## Capitolul 8: Ce determină succesul și ce produce eșecul



Am văzut destule proiecte de implementare ca să știu că **standardul nu este niciodată problema**. Standardul este clar, logic și bine structurat.

**Problemele vin din altă parte:** din modul în care organizația se raportează la propriul proiect, din deciziile care se amână, din angajamentele care se iau la semnarea contractului și se uită la prima presiune operațională, din tentația de a produce documente în locul guvernanței.

**Capitolul acesta nu este o listă de bune practici.** Este o colecție de lecții pe care le-am învățat din proiecte care au mers bine și din altele care nu au mers, și pe care le consider relevante pentru orice factor de decizie care pornește sau intenționează să pornească un proiect de implementare SMIA.

## Principiile pe care le consider nenegociabile

- **Dubla trasabilitate este primul dintre ele.** Fiecare document din SMIA trebuie să fie trasabil explicit la clauza standardului care îl cere și, acolo unde există corespondență, la articolul din AI Act pe care îl acoperă. Un auditor extern care poate naviga rapid între un raport de evaluare a riscurilor și clauza 6.1 a standardului și articolul 9 din AI Act are imediat o impresie despre calitatea sistemului. Un auditor care trebuie să descifreze singur aceste relații are o impresie diferită. Dubla trasabilitate nu îngreunează construcția documentelor, o disciplinează.
- **Refuzul șabloanelor generice este al doilea principiu.** Am văzut sisteme SMIA construite integral din documente descărcate de pe internet sau generate automat de platforme specializate. Arată impecabil. Cad la audit pentru că auditorul pune o singură întrebare persoanei care a semnat politica AI: **ce a vrut să exprime organizația în paragraful trei al politicii, cel despre principiile utilizării responsabile?** Dacă persoana nu știe, dacă citește din document sau dacă recunoaște că textul a venit de la consultant fără o discuție reală, auditul devine dificil. Politica AI trebuie să conțină decizii asumate de conducere, nu formulări preluate din modele generice.
- **Calitatea evaluărilor de impact este al treilea principiu.** Este, din experiența mea, elementul cel mai subestimat din întreaga implementare și cel mai verificat de auditorii cu experiență. Un raport de evaluare a impactului sistemului AI care descrie scenarii ipotetice abstracte, fără ancorare în operațiunile reale ale organizației și fără o analiză concretă a grupurilor afectate, comunică auditorului că organizația a parcurs un exercițiu formal, nu că a înțeles ce face cu sistemele sale AI. Scurtarea acestui pas este cea mai scumpă greșală pe care o poate face o organizație în proiectul de implementare, indiferent cât de bine arată restul documentației.

## Factorii critici de succes

**Sponsorul executiv activ este, fără nicio îndoială, factorul cu cel mai mare impact asupra succesului unui proiect SMIA.** Nu sponsorul nominal, cel care semnează contractul și dispare. Sponsorul care participă la analiza efectuată de management, care citește rapoartele de risc și care ia decizii de conținut, adică ce exprimă politica AI, care este apetitul la risc al organizației, ce sisteme se mențin și care se reconfigurează.

**Proiectele în care conducerea executivă este efectiv prezentă, produc sisteme mai bune.** Nu pentru că directorul general știe mai mult despre SR ISO/IEC 42001:2024 decât coordonatorul SMIA, ci pentru că deciziile care contează cu adevărat sunt decizii strategice, nu tehnice, și nimeni altcineva din organizație nu le poate lua în locul conducerii.

Am oprit un proiect (altul decât 42001) după trei luni, cu acordul clientului, pentru că sponsorul executiv fusese înlocuit pe parcurs și succesorul său nu considera proiectul o prioritate. Continuarea ar fi produs un dosar voluminos și un sistem nefuncțional. Decizia de oprire a fost, în acel caz, mai responsabilă decât continuarea.

Disponibilitatea reală a echipei interne este al doilea factor critic. **Modelul de co-implementare funcționează dacă echipa organizației participă efectiv la construcția documentelor, nu dacă aprobă ceea ce consultantul a produs în totalitate.** Trei până la cinci zile-om pe lună din partea echipei interne nu este o estimare conservatoare, este minimul



necesar pentru ca transferul de competență să aibă loc. Organizațiile care declară că au echipa disponibilă și nu livrează disponibilitatea reală produc proiecte care durează mai mult, costă mai mult și generează sisteme pe care nimeni din interior nu le înțelege la final.

**Viteza deciziilor la milestone-uri este al treilea factor.** Un proiect SMIA are o logică secvențială: fiecare fază produce inputurile pentru faza următoare. Dacă aprobarea livrabilelor unei faze se amână cu două săptămâni pentru că directorul general este ocupat sau pentru că documentele stau pe e-mail fără să fie citite, tot calendarul ulterior se decalează.

Am văzut proiecte de șase luni care au durat zece luni exclusiv din cauza întârzierilor la aprobare, fără nicio problemă de conținut. Blocarea calendaristică a ședințelor de aprobare de la startul proiectului și tratarea milestone-urilor ca termene nenegociabile reduce semnificativ acest risc.

## Ce produce eșecul

**Cel mai frecvent tip de eșec pe care l-am văzut nu este eșecul la auditul extern. Este eșecul silențios:** organizația obține certificarea, iar sistemul moare în primele douăsprezece luni după aceea, înainte de primul audit de supraveghere. Coordonatorul SMIA pleacă din organizație și nimeni altcineva nu știe să preia. Rapoartele de evaluare a riscurilor nu mai sunt actualizate la achiziția unor sisteme AI noi. Jurnalele de evenimente devin formalitate. La auditul de supraveghere, auditorul găsește un dosar impecabil și o realitate operațională care nu mai corespunde cu el.

Acest tip de eșec este consecința directă a unui proiect în care **transferul de competență nu a fost un obiectiv real, ci o declarație din contractul de consultanță.** Sistemul a fost construit de consultant, livrat organizației și adoptat formal. Nu a fost niciodată înțeles.

**Al doilea tip de eșec pe care îl consider la fel de semnificativ este construcția unui scope insuficient deliberat,** pentru a reduce volumul de muncă și costul proiectului. Organizații care exclud sisteme AI relevante din scope pentru că clasificarea lor ca risc ridicat ar implica mai multă documentație, sau care definesc un perimetru atât de restrâns încât sistemul nu acoperă activitățile cu adevărat expuse.

Problema acestei abordări nu este că eșuează neapărat la auditul de certificare: un auditor de Stage 1 poate valida un scope restrâns dacă este justificat corect. Problema este că organizația iese din proiect cu o certificare reală și o guvernanță fictivă, pentru că sistemele care contează nu sunt acoperite.

**Al treilea tip de eșec este mai rar, dar mai spectaculos:** organizații care intră în proiect cu convingerea că implementarea este un exercițiu documentar și descoperă la Stage 2 că auditorul vorbește cu oamenii, nu cu dosarele. Un director de operațiuni care nu știe ce este o Declarație de Aplicabilitate, deși a semnat-o, sau un responsabil HR care nu poate explica ce face sistemul AI pe care îl utilizează zilnic în evaluarea performanței sunt constatări de audit care produc neconformități majore indiferent de calitatea documentelor.

## Maturitate organizațională, nu conformitate documentară

**Există o tendință în piața de consultanță de a prezenta implementarea SR ISO/IEC 42001:2024 ca un proiect de conformitate.** Termenele din AI Act, amenziile, obligațiile regulatorii: toate acestea sunt argumente reale și legitime pentru a porni un proiect, dar nu sunt, în opinia mea, argumentele care produc sisteme bune.

**Organizațiile care construiesc SMIA-uri care funcționează sunt cele care tratează proiectul ca pe un proiect de maturitate organizațională:** o oportunitate de a înțelege ce sisteme AI operează și ce fac acestea cu adevărat, de a lua decizii explicite despre ce riscuri acceptă și ce nu, de a construi o cultură internă în care oamenii care lucrează cu sisteme AI înțeleg responsabilitatea pe care o poartă și au instrumentele să o exercite.

**Conformitatea este un rezultat al maturității, nu invers.** Un sistem de management matur produce conformitate ca efect secundar natural, nu ca obiectiv primar. Un sistem construit exclusiv pentru conformitate produce un dosar corect și o organizație care nu s-a schimbat cu nimic față de ziua de dinaintea proiectului.

**Inteligența artificială nu este o tendință care se gestionează cu documente.** Este o tehnologie cu consecințe reale, uneori cu consecințe ireversibile, asupra oamenilor pe care deciziile sale îi afectează. A o guverna serios, cu un sistem funcțional și cu oameni care înțeleg ce fac, nu este un exercițiu de conformitate. Este, pur și simplu, o decizie de conducere responsabilă.



## Concluzie

Există un moment în fiecare proiect de implementare pe care îl aștept și pe care îl recunosc de fiecare dată când apare. Nu este momentul semnării contractului, nici cel al emiterii certificatului. Este momentul din faza de diagnosticare în care directorul general privește lista sistemelor AI din organizația sa și spune, uneori cu surprindere, uneori cu îngrijorare: „*Nu știam că avem atât.*” Acel moment este, în opinia mea, valoarea reală a unui proiect SMIA, indiferent de ce urmează.

**Un sistem de management al inteligenței artificiale bine construit** nu rezolvă toate problemele pe care le aduce AI în organizație.

- **Rezolvă problema vizibilității:** conducerea știe ce operează.
- **Rezolvă problema responsabilității:** cineva este desemnat și instruit pentru fiecare decizie legată de sistemele AI.
- **Rezolvă problema demonstrabilității:** organizația poate arăta, oricui și oricând, că guvernează AI în mod serios.

Acestea sunt rezultatele unui proiect condus corect, cu sau fără presiunea unui termen regulatoriu.

**Dacă ați ajuns la finalul acestui ghid cu o imagine mai clară despre ce implică un proiect de implementare a SR ISO/IEC 42001:2024 și despre cum arată el din interior, atunci ghidul și-a îndeplinit scopul.**

Pasul următor, dacă îl considerați oportun, este o discuție directă despre situația organizației dumneavoastră.

**Ofer un diagnostic inițial gratuit, fără obligații contractuale.** În cadrul lui, identificăm împreună sistemele AI relevante, le clasificăm pe categorii de risc, evaluăm distanța față de cerințele standardului și stabilim ce efort ar implica un proiect de implementare calibrat pe realitatea organizației dumneavoastră. Diagnosticul durează de regulă două până la trei ore și produce o imagine clară, nu o ofertă comercială deghezată.

Mă puteți contacta la [ion@ioniordache.com](mailto:ion@ioniordache.com) sau prin intermediul site-ului [ioniordache.com](https://ioniordache.com).

## Anexa 1: Calendarul AI Act — jaloane și implicații practice

Tabelul de mai jos sintetizează jaloanele relevante din Regulamentul (UE) 2024/1689 pentru organizațiile din România care utilizează sau integrează sisteme de inteligență artificială.

Datele marcate cu asterisc (\*) reflectă acordul politic provizoriu anunțat în mai 2026 în cadrul pachetului Digital Omnibus și nu sunt încă adoptate formal. Până la adoptarea formală, termenele din calendarul de bază rămân reperul juridic în vigoare.

Dată	Ce intră în aplicare	Implicații practice pentru organizațiile din România
1 august 2024	Intrarea în vigoare a AI Act	Regulamentul produce efecte juridice. Perioada de tranziție începe.
2 februarie 2025	Interdicțiile privind practicile AI cu risc inacceptabil (art. 5). Obligația de alfabetizare AI pentru personalul care operează sisteme AI.	Practicile interzise devin ilegale. Personalul operațional trebuie instruit documentat. Aplicabil oricărei organizații care utilizează AI, indiferent de categorie de risc.
2 august 2025	Regulile pentru modelele AI de uz general (GPAI). Structura de guvernanță UE operațională. Autorități naționale competente desemnate.	Furnizorii de GPAI au obligații active. Organizațiile din România au interlocutori instituționali identificați.
2 august 2026	Obligațiile pentru sistemele AI cu risc ridicat din Anexa III (calendar de bază). Cerințele de transparență din art. 50. Regulatory sandboxes.	Pivot de conformitate recomandat: inventarul sistemelor, clasificarea riscurilor, evaluările de impact și sistemul de management trebuie să fie funcționale la această dată.
2 decembrie 2026 *	Cerințele de watermarking machine-readable pentru sisteme generative (art. 50 alin. 2), conform pachetului Digital Omnibus.	Furnizorii de sisteme generative au un termen extins pentru marcarea tehnică a conținutului sintetic.
2 decembrie 2027 *	Obligațiile de conformitate pentru sistemele AI cu risc ridicat de tip stand-alone din Anexa III, conform pachetului Digital Omnibus.	Termen extins față de 2 august 2026 dacă pachetul Omnibus este adoptat formal. Nu tratați această amânare ca motiv de întârziere a proiectului.
2 august 2027	Obligațiile pentru sistemele AI cu risc ridicat integrate în produse reglementate sectorial (calendar de bază).	Operatorii din România care utilizează produse cu componente AI high-risk trebuie să adauge obligațiile AI Act peste regimul sectorial existent.
2 august 2028 *	Același perimetru ca 2 august 2027, cu termen extins conform pachetului Digital Omnibus.	Termen extins dacă pachetul Omnibus este adoptat formal.

**Notă de utilizare:** *Tratați datele fără asterisc ca termene ferme. Datele cu asterisc sunt orizonturi probabile, nu certitudini juridice. Recomandarea operațională rămâne nemodificată: 2 august 2026 este termenul pentru a avea bazele guvernanței AI construite. Orice amânare ulterioară este spațiu de rafinare, nu argument pentru amânarea startului.*

Anexa 2: Glosar de termeni cheie

Termen	Definiție
AI Act	Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024, primul cadru legal complet care reglementează inteligența artificială la nivelul Uniunii Europene, pe baza unei abordări bazate pe risc.
Declarație de Aplicabilitate (SoA)	Document central al SMIA care inventariază toate cele 38 de controale din Anexa A a SR ISO/IEC 42001:2024, consemnând pentru fiecare dacă este aplicabil organizației, motivul includerii sau excluderii și modul de implementare. Primul document solicitat de orice auditor extern la Stage 1.
Evaluare de impact al sistemului AI	Procedura prin care organizația analizează efectele potențiale ale unui sistem AI asupra persoanelor fizice, grupurilor vulnerabile și societății în ansamblu. Element diferențiator al standardului 42001 față de alte sisteme de management. Reglementată de clauza 6.1.4 și controlul A.5.2 din standard.
Furnizor (AI Act)	Entitatea care proiectează un sistem AI, îl antrenează și îl introduce pe piață sau îl pune în funcțiune sub propria marcă sau denumire. Poartă obligațiile cele mai substanțiale din regulament pentru sistemele cu risc ridicat.
Implementator (AI Act)	Entitatea care utilizează un sistem AI cu risc ridicat în contextul propriilor activități profesionale. Poartă obligații proprii, distincte de cele ale furnizorului, inclusiv supravegherea umană, monitorizarea funcționării, informarea persoanelor vizate conform art. 26 alin. (11) și, pentru categoriile prevăzute de art. 27 alin. (1), realizarea evaluării de impact asupra drepturilor fundamentale.
Organism de certificare acreditat	Entitate terță independentă, acreditată de RENAR sau de un alt organism de acreditare recunoscut internațional prin acordurile IAF, autorizată să realizeze auditul extern și să emită certificatul ISO/IEC 42001. Separarea dintre consultant și organism de certificare este o cerință de imparțialitate nenegociabilă.
Risc rezidual	Riscul care rămâne după aplicarea măsurilor de tratare stabilite în planul de tratare a riscurilor. Conform art. 9 alin. (5) din AI Act, furnizorii de sisteme cu risc ridicat trebuie să demonstreze că riscul rezidual se menține în limite acceptabile.
SMIA	Sistem de Management al Inteligenței Artificiale — denumirea în limba română a ceea ce standardul internațional numește AIMS (Artificial Intelligence Management System). Ansamblul de politici, proceduri, registre, rapoarte și înregistrări operaționale prin care o organizație stabilește, implementează, menține și îmbunătățește continuu guvernanța sistemelor sale AI, conform cerințelor SR ISO/IEC 42001:2024.
SR ISO/IEC 42001:2024	Adoptarea română a standardului internațional ISO/IEC 42001:2023, publicat în decembrie 2023 și adoptat de ASRO în iulie 2024. Adoptarea este integrală: standardul român este identic cu cel internațional, iar certificarea obținută în România beneficiază de recunoaștere internațională.
Supraveghere umană	Mecanismul prin care persoanele care operează sau monitorizează un sistem AI înțeleg funcționarea acestuia, îi recunosc limitele și pot interveni, corecta sau opri sistemul atunci când este necesar. Cerută de art. 14 din AI Act pentru sistemele cu risc ridicat și reglementată procedural prin controalele din domeniul A.9 al standardului.
VSS (Video Surveillance System)	Termenul tehnic utilizat conform standardului EN IEC 62676-4:2025 pentru sistemele de supraveghere video, înlocuind denumirea CCTV (TVCI) în documentele tehnice și de conformitate. Sistemele VSS cu componente de analiză AI pot intra sub incidența AI Act în funcție de funcționalitățile activate și de contextul de utilizare.



## Anexa 3: Zece întrebări de autoevaluare pentru conducerea organizației

Întrebările de mai jos nu formează un chestionar de conformitate. Sunt instrumente de reflecție pentru directorii generali și CEO, directorii de operațiuni, directorii de tehnologie și/sau IT, responsabilii cu protecția datelor, responsabilii cu managementul riscurilor și responsabilii de conformitate care vor să evalueze, cu mijloace proprii, cât de pregătită este organizația lor pentru un proiect de implementare SMIA.

Fiecare dintre aceste roluri aduce o perspectivă diferită asupra acelorași sisteme. De exemplu: **directorul de operațiuni** știe care sisteme AI sunt folosite zilnic și de cine; **directorul de tehnologie** are imaginea tehnică reală a sistemelor operate, dincolo de descrierile comerciale ale furnizorilor; **responsabilul cu protecția datelor** cunoaște deja intersecțiile cu GDPR și are, de regulă, o imagine mai completă decât restul echipei despre riscurile generate de prelucrarea automată a datelor cu caracter personal.

Nicio perspectivă singulară nu este suficientă pentru un răspuns onest la întrebările care urmează. Nu există răspunsuri corecte universale. Există răspunsuri oneste și răspunsuri care spun ce ar trebui să fie, nu ce este.

### 1. Puteți lista acum, fără să consultați pe nimeni, toate sistemele care utilizează componente de inteligență artificială în organizația dumneavoastră?

*Dacă răspunsul necesită o verificare cu directorul tehnic sau cu departamentul IT, aveți deja prima concluzie utilă despre starea guvernanței AI din organizație. Un inventar complet și actualizat al sistemelor AI este primul document obligatoriu al unui SMIA și prima surpriză din orice proiect de implementare.*

### 2. Știți, fiecare sistem AI din organizație, șidacă se încadrează în categoria sistemelor cu risc ridicat conform Anexei III a AI Act?

*Clasificarea corectă a sistemelor determină ce obligații se aplică organizației dumneavoastră. Un sistem de evaluare a performanței angajaților cu componente AI, de exemplu, este probabil sistem cu risc ridicat, indiferent că l-ați achiziționat ca modul al unui software HR mai larg.*

### 3. Există în organizație o persoană cu responsabilitate formală pentru guvernanța sistemelor AI, cu timp efectiv alocat acestei funcții?

*Responsabilitatea distribuită informal între directorul tehnic, departamentul juridic și managementul operațional produce, în practică, responsabilitate nulă. Un SMIA funcțional cere un coordonator desemnat cu autoritate clară și cu un număr realist de ore dedicate acestei funcții.*

### 4. Angajații care lucrează zilnic cu sisteme AI știu că le utilizează, înțeleg ce face sistemul și știu când și cum să depășească recomandările lui?

*Articolul 4 din AI Act impune tuturor furnizorilor și implementatorilor să asigure un nivel adecvat de alfabetizare AI pentru întregul personal relevant, indiferent de categoria de risc a sistemelor operate, obligație aplicabilă din 2 februarie 2025. Pentru personalul care operează sisteme cu risc ridicat, cerințele sunt mai stricte: articolul 14 din AI Act impune o supraveghere umană efectivă, care nu se traduce printr-o procedură documentată, ci printr-o competență reală a oamenilor care operează acele sisteme. Dacă răspunsul la această întrebare necesită o verificare cu managerii de linie, există o probabilitate ridicată că supravegherea umană există pe hârtie, nu în realitate.*

**5. Persoanele fizice afectate de deciziile sistemelor dumneavoastră AI știu că un sistem AI contribuie la acele decizii?**

*Pentru sistemele cu risc ridicat, obligația de informare prevăzută de articolul 26 alineatul (11) din AI Act este una dintre cele mai frecvent omise în organizațiile care utilizează sisteme AI achiziționate de la terți. Angajații ale căror evaluări de performanță sunt influențate de un algoritm, clienții ale căror cereri sunt procesate cu suport AI sau persoanele supuse unor decizii generate cu contribuția unui sistem AI cu risc ridicat trebuie informate în prealabil, acolo unde această informare nu este realizată direct de furnizor. Chiar și în absența unei obligații legale stricte pentru sistemele cu risc limitat sau minim, transparența față de persoanele afectate rămâne un indicator relevant al maturității guvernanței AI.*

**6. Contractele dumneavoastră cu furnizorii de sisteme AI includ clauze care vă asigură accesul la informații despre funcționarea algoritmilor, actualizările majore și limitele documentate ale sistemului?**

*Fără acces la aceste informații, organizația nu poate realiza evaluări de risc corecte, nu poate documenta supravegherea umană și nu poate demonstra conformitatea față de un auditor extern. Un furnizor care refuză să furnizeze informații minime despre sistemul pe care vi-l vinde ridică o problemă de guvernanță înainte de orice considerație de conformitate.*

**7. Dacă un sistem AI din organizația dumneavoastră ar produce mâine un rezultat greșit cu impact semnificativ asupra unei persoane, știți exact ce procedură urmați, cui raportați și în ce termen?**

*Procedura de raportare a incidentelor grave este cerută explicit de AI Act și de standard. Absența ei este o neconformitate majoră la orice audit extern. Dar dincolo de audit, absența ei înseamnă că organizația reacționează la incidente prin improvizație, nu prin protocol.*

**8. Dacă organizația dumneavoastră achiziționează mâine un sistem AI nou, există un proces formal de evaluare a riscurilor și de aprobare înainte de punerea în funcțiune?**

*Sistemele AI nu ar trebui să intre în operare pentru că un departament a găsit o soluție convenabilă și a semnat un abonament. Procesul de selecție, evaluare și aprobare a sistemelor AI noi este un control explicit al standardului și un indicator al maturității guvernanței.*

**9. Dacă organizația dumneavoastră are deja sisteme de management certificabile, conducerea a evaluat în ce măsură infrastructura existentă poate fi valorificată pentru SMIA?**

*Răspunsul la această întrebare determină direct durata și costul unui proiect de implementare. O organizație cu sisteme de management mature poate reduce efortul de construcție a SMIA cu 20 până la 35 la sută față de un start de la zero.*

**10. Conducerea organizației ar putea explica astăzi, în fața unui client corporativ sau a unei autorități de supraveghere, cum guvernează sistemele AI pe care le operează?**

*Aceasta este, în final, întrebarea care contează. Nu dacă există un dosar de documente, ci dacă conducerea înțelege și poate articula propria poziție față de sistemele AI pe care organizația le operează. Un SMIA bine implementat face această explicație naturală și credibilă. Un SMIA construit exclusiv pentru conformitate o face imposibilă.*

---

GUVERNANȚA INTELIGENȚEI ARTIFICIALE

**GHID PRACTIC**

---

ION IORDACHE  
[www.ioniordache.com](http://www.ioniordache.com)