

# MANAGEMENTUL RISCURILOR INTELIGENȚEI ARTIFICIALE

Standardele ISO pentru pregătirea conformității cu AI Act



ION IORDACHE

# MANAGEMENTUL RISCURILOR INTELIGENȚEI ARTIFICIALE

## GHID PRACTIC

SR EN ISO/IEC 23894:2024 și triada standardelor pentru pregătirea conformității cu AI Act

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 nu constituie consultanță juridică sau de conformitate. Pentru aplicarea concretă a prevederilor SR EN ISO/IEC 23894:2024, SR ISO/IEC 42001:2024 și ale Regulamentului (UE) 2024/1689 într-o organizație specifică, se recomandă consultarea textelor oficiale ale standardelor și ale regulamentului, precum și apelul la consultanță de specialitate calificată.

Standardele române 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.

### Contact autor

Email: [ion@ioniordache.com](mailto:ion@ioniordache.com)

Site: [ioniordache.com](http://ioniordache.com)

LinkedIn: [linkedin.com/in/ioniordache](https://www.linkedin.com/in/ioniordache)

Telefon: +40 725 631 096

## 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 a fost utilizat un singur instrument de inteligență artificială generativă: **Claude Opus 4.7**, dezvoltat de Anthropic.

Instrumentul a fost utilizat pentru:

- redactarea inițială a textului fiecărui capitol, pe baza instrucțiunilor structurate ale autorului și a materialelor de referință consultate;
- structurarea conținutului în capitole, subsecțiuni și anexe, conform planului editorial stabilit de autor;
- elaborarea formei tehnice a tabelelor, glosarului și a mapării dintre cerințele AI Act, controalele SR ISO/IEC 42001:2024 și componentele procesului SR EN ISO/IEC 23894:2024;
- generarea documentului Word cu machetare profesională, conform deciziilor de design comunicate de autor;
- formularea propunerilor pentru elementele auxiliare ale ebook-ului (cuvânt înainte, casete laterale, pagina „Despre autor”, secțiunea „Cum vă pot ajuta”).

Instrumentul AI nu a avut acces la documente confidențiale ale unor organizații cliente și nu a fost utilizat pentru a formula decizii normative independente. Toate sursele primare consultate au fost furnizate de autor sub formă de fișiere PDF aflate în spațiul de lucru.

### 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** (împărțirea în capitole, ordinea secțiunilor, prezența anexelor) au fost luate de autor și implementate de instrumentul AI;
- toate deciziile de **poziționare profesională** (audiența țintă, registrul tonului, proporția dintre conținutul didactic și conținutul metodologic, modul de prezentare a metodologiei proprii a autorului) au fost luate de autor și transpuse în text de instrumentul AI;
- toate deciziile de **conținut substanțial** (titlul, formularea recomandărilor, lista erorilor frecvente, structura glosarului, conținutul tabelului de mapare) au fost validate sau ajustate explicit de autor;
- formularea concretă a paragrafelor a fost produsă de instrumentul AI și revizuită de autor la fiecare secțiune înainte de a trece la următoarea;

Procesul a fost organizat în șapte sesiuni succesive, în care fiecare componentă a ebook-ului a fost discutată, redactată, prezentată autorului spre validare și ajustată în funcție de observațiile lui, înainte de a trece la componenta următoare.

### Designul vizual al ebook-ului

Versiunea publicată a ebook-ului include elemente grafice și de machetare profesională (copertă, scheme conceptuale, eventuale ilustrații complementare) realizate independent de procesul de redactare a textului.

Pentru această componentă a fost utilizat **ChatGPT**, dezvoltat de OpenAI, ca instrument de generare a propunerilor vizuale, sub coordonarea autorului. Selecția, ajustarea și integrarea finală a elementelor vizuale au fost realizate de autor.

## Responsabilitatea autorului

Responsabilitatea integrală pentru:

- selecția și interpretarea surselor;
- verificarea veridicității informațiilor factuale (referințe la articolele AI Act, clauzele standardelor, controalele Anexei A);
- coerența conceptuală și arhitecturală a ghidului;
- 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 standardelor ISO citate și la controalele Anexei A din SR ISO/IEC 42001:2024, au fost verificate prin consultarea directă a textelor oficiale.

O atenție specială a fost acordată acurateței numerelor de articol și de alineat din AI Act, având în vedere riscul cunoscut de erori sistematice în interpretările inițiale ale regulamentului. 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 FRIA conform Articolului 27.

Resursele citate în Anexa C au fost incluse exclusiv pe baza relevanței lor verificate de autor, nu pe baza menționării lor de către instrumentul AI.

## 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 clienți. Exemplele și scenariile prezentate în ghid au fost formulate astfel încât să respecte obligațiile profesionale de confidențialitate ale autorului și legislația privind protecția datelor cu caracter personal.

Această notă reflectă angajamentul autorului pentru o utilizare etică, transparentă și controlată a inteligenței artificiale în elaborarea de materiale aplicate în domeniul guvernantei inteligenței artificiale și al pregătirii conformității cu cadrul european.



# Cuprins

## Notă de transparență privind utilizarea inteligenței artificiale

### Cuvânt înainte

### Capitolul 1. De ce contează managementul riscurilor IA pentru o afacere din România

- 1.1. Contextul de afaceri
- 1.2. De ce riscurile IA sunt diferite
- 1.3. Argumentul de evitare a pierderilor
- 1.4. Argumentul de oportunitate

### Capitolul 2. SR EN ISO/IEC 23894:2024, prezentare detaliată

- 2.1. Identitate și statut
- 2.2. Structura standardului
- 2.3. Cele trei anexe
- 2.4. Ce aduce specific 23894 față de ISO 31000

### Capitolul 3. Triada standardelor IA: 22989, 23894 și 42001

- 3.1. Trei standarde, trei funcții
- 3.2. SR EN ISO/IEC 22989:2023, vocabularul comun
- 3.3. SR EN ISO/IEC 23894:2024, instrumentul de lucru
- 3.4. SR ISO/IEC 42001:2024, sistemul de management certificabil
- 3.5. AI Act, deasupra triadei

### Capitolul 4. Maparea SR EN ISO/IEC 23894:2024 pe cerințele AI Act

- 4.1. Premisa de mapare
- 4.2. Articolul 9: Sistemul de gestionare a riscurilor
- 4.3. Articolul 27: Evaluarea impactului asupra drepturilor fundamentale (FRIA)
- 4.4. Articolul 17: Sistemul de management al calității
- 4.5. Articolul 10: Guvernanța datelor
- 4.6. Articole conexe
- 4.7. Sinteza relației 23894 cu AI Act

### Capitolul 5. Implementarea practică a standardului

- 5.1. Punctul de intrare: inventarul sistemelor IA
- 5.2. Etapele procesului, conform Clauzei 6 din 23894
- 5.3. Integrarea procesului 23894 în arhitectura SMIA
- 5.4. Surse tipice de risc IA, conform Anexei B
- 5.5. Integrarea cu sistemele de management existente
- 5.6. Formatul livrabilelor

### Capitolul 6. Erori frecvente și ce să eviți

### Capitolul 7. Recomandări operaționale și concluzii

### Anexa A. Glosar de termeni

### Anexa B. Tabel sintetic de mapare AI Act → 42001 → 23894

### Anexa C. Resurse bibliografice și de aprofundare

### Despre autor

### Cum vă pot ajuta

### Lista casetelor

## Cuvânt înainte

Pe 2 august 2026, **Regulamentul (UE) 2024/1689 privind inteligența artificială**, cunoscut drept **AI Act**, devine pe deplin aplicabil. Pentru organizațiile europene care dezvoltă sau utilizează sisteme de inteligență artificială, această dată marchează tranziția de la o etapă de pregătire opțională la o conformitate cu obligații legale verificabile.

Articolul 9 al regulamentului cere instituirea unui sistem de gestionare a riscurilor pentru sistemele IA cu grad ridicat de risc, descris ca un proces iterativ continuu, derulat pe tot ciclul de viață al sistemului. Cerința este clară. Metoda de implementare nu este precizată în textul regulamentului.

Acest spațiu metodologic este acoperit de **SR EN ISO/IEC 23894:2024 - Tehnologia informației - Inteligența artificială - Ghid privind managementul riscurilor**, aprobat de Asociația de Standardizare din România în septembrie 2024.

Standardul preia logica deja consolidată a **SR ISO 31000:2018 Managementul riscurilor - Linii directe** și o specializează pe particularitățile sistemelor de inteligență artificială: bias algoritmic, opacitate decizională, drift al modelelor, dependență de date și de furnizori terți, vulnerabilități față de atacuri adversariale.

SR EN ISO/IEC 23894:2024 face parte dintr-o triadă de standarde care, împreună, oferă cadrul cel mai complet de astăzi pentru guvernanta inteligenței artificiale: SR EN ISO/IEC 22989:2023 stabilește vocabularul comun, SR EN ISO/IEC 23894:2024 oferă metoda de management al riscurilor, SR ISO/IEC 42001:2024 oferă sistemul de management certificabil. Deasupra acestei triade, AI Act stabilește obligațiile legale.

**Ghidul de față prezintă SR EN ISO/IEC 23894:2024, locul lui în triada de standarde IA și modul în care se mapează concret pe cerințele AI Act.** Documentul se adresează în primul rând membrilor conducerii executive care iau decizii privind alinierea organizației la AI Act, responsabililor de conformitate și de managementul riscurilor (CISO, DPO, manageri de risc, ofițeri de conformitate) și consultanților care însoțesc organizațiile în pregătirea pentru certificare.

Pentru fiecare dintre aceste categorii, **ghidul oferă un parcurs adaptat**: secțiunile inițiale prezintă miza și contextul, capitolele tehnice descriu standardul și aplicarea lui, anexele oferă instrumente directe de lucru.

**Documentul nu se substituie textului oficial al standardelor sau al regulamentului.** Pentru o implementare riguroasă, consultarea textelor oficiale este obligatorie. SR EN ISO/IEC 23894:2024 este disponibil pentru achiziție de pe site-ul Asociației de Standardizare din România. Regulamentul (UE) 2024/1689 este disponibil gratuit pe portalul EUR-Lex al Uniunii Europene.

Structura ghidului este construită astfel încât fiecare capitol să poată fi consultat independent. Cititorul care urmărește o decizie strategică privind implementarea SMIA poate parcurge capitolele 1, 2 și 7.

Cititorul care construiește un proces de management al riscurilor IA va găsi în capitolele 3, 4 și 5 instrumentele operaționale. Cititorul care evaluează un proiect existent va găsi în capitolul 6 lista erorilor frecvente.

**Ion Iordache**

# Capitolul 1. De ce contează managementul riscurilor IA pentru o afacere din România

## 1.1. Contextul de afaceri

Trei realități fac din managementul riscurilor inteligenței artificiale o discuție pe care nicio conducere de companie nu o mai poate amâna.

**Prima realitate: inteligența artificială este deja în organizație, indiferent dacă a fost adoptată conștient sau nu.** Sistemele de analiză video inteligentă, filtrele antifraudă, motoarele de scoring de credit, instrumentele de selecție a candidaților, asistenții generativi integrați în suitele de productivitate, modulele de mentenanță predictivă, chatbotii pentru clienți, toate operează pe componente IA furnizate de terți.

Inventarul inițial realizat în proiectele de implementare SMIA scoate la iveală, în mod constant, sisteme IA pe care conducerea nu le declarase formal: funcționalități integrate în suitele de productivitate, module de analiză predictivă din ERP-uri, asistenți generativi folosiți individual de angajați, scriptări de automatizare cu componentă IA în zonele operaționale. Această necunoaștere este o vulnerabilitate documentată.

**A doua realitate: expunerea contractuală crește accelerat.** Clienții instituționali, mai ales cei din sectoarele financiar, sănătate, energie și sectorul public, încep să introducă în caietele de sarcini și în due diligence-ul de furnizor cerințe explicite privind guvernanta IA.

Apar tot mai des: declarații de conformitate cu AI Act, dovezi privind procesele de management al riscurilor, raportarea biasului în sistemele de selecție automată, mecanisme de supraveghere umană. O companie care nu poate produce aceste dovezi pierde licitații pe care, tehnic, le-ar fi câștigat.

**Avantajul competitiv, cel puțin în următoarele 18 luni, va aparține organizațiilor care intră în negociere cu un sistem deja construit, nu cu promisiunea că îl vor avea curând.**

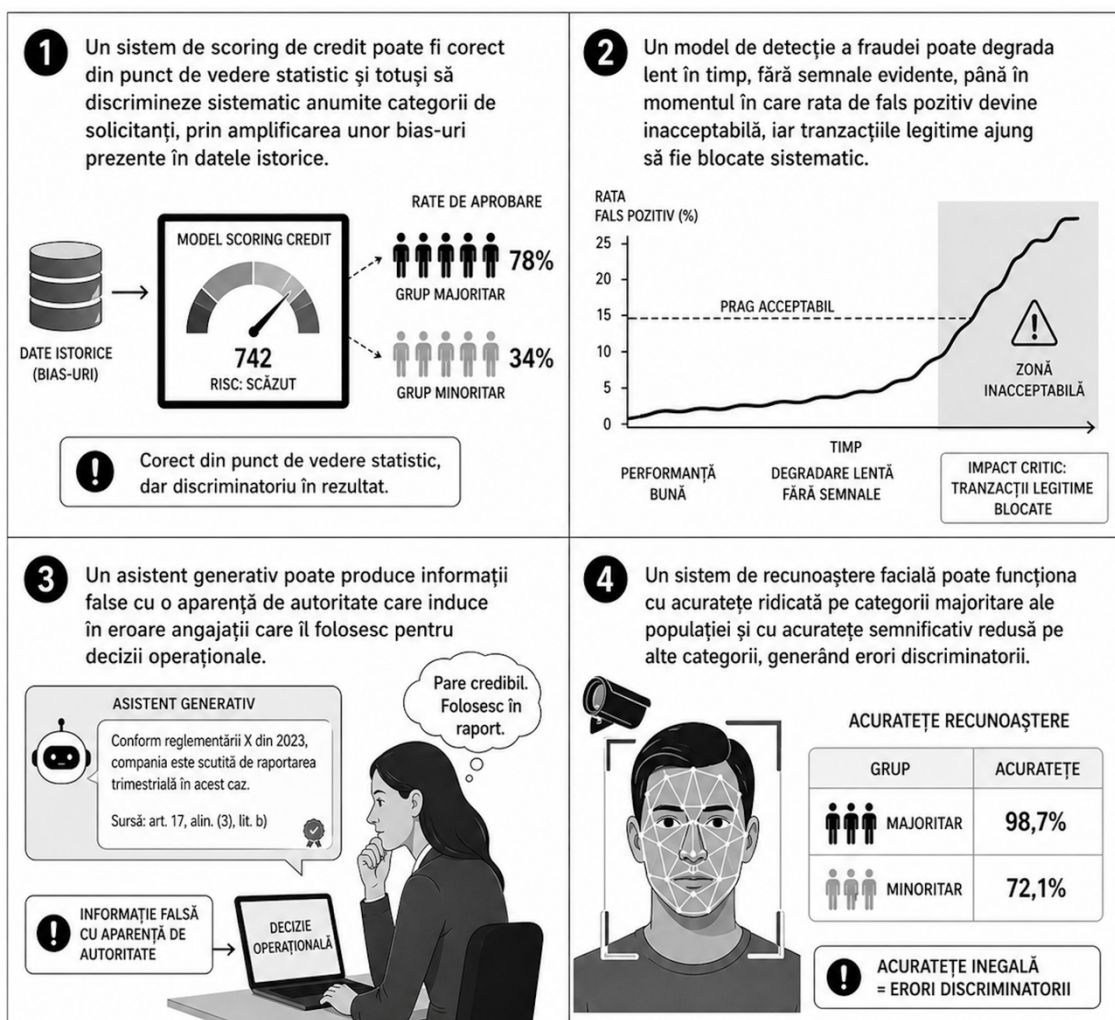
**A treia realitate: efectul Bruxelles se transmite în întreg lanțul valoric.** Chiar și companiile care nu intră direct sub Articolul 9 din AI Act, pentru că nu operează sisteme cu grad ridicat de risc, ajung să răspundă unor cerințe similare prin contracte cu parteneri europeni, prin obligațiile de transparență de la Articolul 50 sau prin cerințele sectoriale care încep să integreze terminologia regulamentului.

Un IMM care livrează componente software unui producător de dispozitive medicale sau unei bănci comerciale va primi, în următorul an, întrebări concrete despre modul în care gestionează riscurile sistemelor IA pe care le include în propriile produse.

## 1.2. De ce riscurile IA sunt diferite

În paralel cu aceste presiuni externe, riscurile sistemelor de inteligență artificială sunt structural diferite de cele acoperite de cadrele clasice de management al riscurilor.

Un sistem de scoring de credit poate fi corect din punct de vedere statistic și totuși să discrimineze sistematic anumite categorii de solicitanți, prin amplificarea unor bias-uri prezente în datele istorice. Un model de detecție a fraudei poate degrada lent în timp, fără semnale evidente, până în momentul în care rata de fals pozitiv devine inacceptabilă, iar tranzacțiile legitime ajung să fie blocate sistematic. Un asistent generativ poate produce informații false cu o aparență de autoritate care induce în eroare angajații care îl folosesc pentru decizii operaționale. Un sistem de recunoaștere facială poate funcționa cu acuratețe ridicată pe categorii majoritare ale populației și cu acuratețe semnificativ redusă pe alte categorii, generând erori discriminatorii.



**Aceste riscuri nu se identifică prin metodologiile tradiționale de risc operațional, securitate cibernetică sau conformitate.** Au nevoie de un cadru specializat, capabil să surprindă particularitățile sistemelor care învață din date, care iau decizii probabilistice și care pot avea comportamente emergente neprevăzute la momentul proiectării.

### 1.3. Argumentul de evitare a pierderilor

Sanctiunile prevăzute de AI Act pentru încălcarea cerințelor aplicabile sistemelor cu grad ridicat de risc ajung la 15 milioane de euro sau 3% din cifra de afaceri globală anuală, alegându-se valoarea cea mai mare. Pentru încălcarea interdicțiilor privind practicile interzise (Articolul 5), sancțiunile pot ajunge la 35 milioane de euro sau 7% din cifra de afaceri globală anuală. La acestea se adaugă costuri care nu apar în textul regulamentului: expunerea reputațională, expunerea în litigii civile pentru prejudicii cauzate de decizii automate eronate, pierderea oportunităților comerciale cu clienți care cer dovezi de guvernare, costurile de remediere accelerată în cazul unui control al autorității de supraveghere.

Costul implementării unui sistem de management al riscurilor IA, fie prin abordare voluntară pe baza standardului 23894, fie integrat într-un SMIA conform 42001, este de ordin de mărime semnificativ inferior expunerii potențiale. Această disparitate face din decizia de implementare nu o cheltuială discreționară, ci o investiție de protecție cu raport cost-beneficiu favorabil.

### 1.4. Argumentul de oportunitate

Dincolo de evitarea pierderilor, implementarea timpurie a unui sistem de management al riscurilor IA produce avantaje competitive concrete:

- **Vizibilitate strategică:** un inventar complet al sistemelor IA permite conducerii să ia decizii informate despre care sisteme merită extinse, care trebuie modificate și care ar trebui retrase.
- **Diferențiere comercială:** capacitatea de a produce, la cerere, dovezi de guvernare pentru clienții corporativi sofisticati devine criteriu de departajare în licitații.
- **Reziliență operațională:** sistemele IA monitorizate sistematic, conform unui proces de management al riscurilor, au o probabilitate mult mai redusă de a genera incidente operaționale majore.
- **Pregătire pentru viitor:** structura de risc construită acum se va extinde natural pe sistemele IA viitoare, fără rescriere de procese.

Întrebarea pentru o conducere matură nu mai este dacă organizația trebuie să se ocupe de managementul riscurilor IA, ci cu ce instrument o face. Răspunsul este oferit de SR EN ISO/IEC 23894:2024.

#### Caseta 1. De la inventar la decizie

În proiectele de implementare SMIA, primul document construit este **Registrul sistemelor IA**. Importanța lui depășește funcția documentară: un sistem IA neinventariat este un sistem necontrolat, care nu a trecut prin evaluare de risc, care nu are documentație tehnică și care, în cazul unui control, expune organizația ca neconformă. Recomand sweep-uri periodice pe departamente (IT, marketing, resurse umane, operațional), pentru a identifica sistemele IA introduse informal, fără validare formală a conducerii.



## Capitolul 2. SR EN ISO/IEC 23894:2024, prezentare detaliată

### 2.1. Identitate și statut

**SR EN ISO/IEC 23894:2024 Tehnologia informației. Inteligența artificială. Ghid privind managementul riscurilor** a fost aprobat de Asociația de Standardizare din România la data de 30 septembrie 2024. Standardul român este identic cu standardul european EN ISO/IEC 23894:2024, care, la rândul său, preia ediția internațională ISO/IEC 23894:2023, publicată în februarie 2023.

**Două precizări sunt esențiale** pentru a evita confuziile pe care le întâlnim frecvent în discuțiile de specialitate.

**Prima precizare: este un ghid, nu un standard certificabil.** Spre deosebire de SR ISO/IEC 42001:2024, organizația nu poate obține un certificat de conformitate cu 23894 de la un organism acreditat. Ghidul oferă recomandări, descrie procese și ilustrează cu exemple, dar nu stabilește cerințe auditabile în sensul certificării. Acest statut nu îi reduce utilitatea, dimpotrivă, îi conferă flexibilitatea necesară pentru a fi adaptat la realitatea specifică a fiecărei organizații.

**A doua precizare: este o specializare a ISO 31000:2018 pe domeniul IA, nu un cadru independent.** Standardul declară explicit, în introducere, că este destinat utilizării împreună cu ISO 31000:2018, Managementul riscurilor. Linii directoare. Acolo unde extinde îndrumările din ISO 31000, face trimitere la clauza relevantă a acestuia și adaugă considerațiile specifice IA. Pentru o organizație care are deja un cadru de management al riscurilor construit pe ISO 31000, indiferent dacă pentru riscuri operaționale, financiare sau de securitate, 23894 nu cere o reconstrucție, ci o extensie.

### 2.2. Structura standardului

**Ghidul preia structura ISO 31000 și o organizează în trei părți principale, plus trei anexe.**

#### 2.2.1. Clauza 4. Principiile managementului riscurilor IA

Clauza 4 reia cele opt principii din ISO 31000 și pentru fiecare descrie considerațiile specifice care apar atunci când subiectul este un sistem de inteligență artificială:

1. **Integrare**, managementul riscurilor IA este parte integrantă a tuturor activităților organizației.
2. **Abordare structurată și cuprinzătoare**, procesul produce rezultate consistente și comparabile.
3. **Personalizare**, cadrul și procesul se adaptează la contextul specific al organizației.
4. **Includere**, implicarea adecvată a părților interesate în procesul de management al riscurilor.
5. **Dinamism**, procesul anticipează, detectează, recunoaște și reacționează la schimbări.
6. **Cea mai bună informație disponibilă**, intrările sunt bazate pe informații istorice și actuale.

7. **Factori umani și culturali**, influența semnificativă a comportamentului uman și a culturii organizaționale.
8. **Îmbunătățire continuă**, procesul se rafinează permanent prin învățare și experiență.

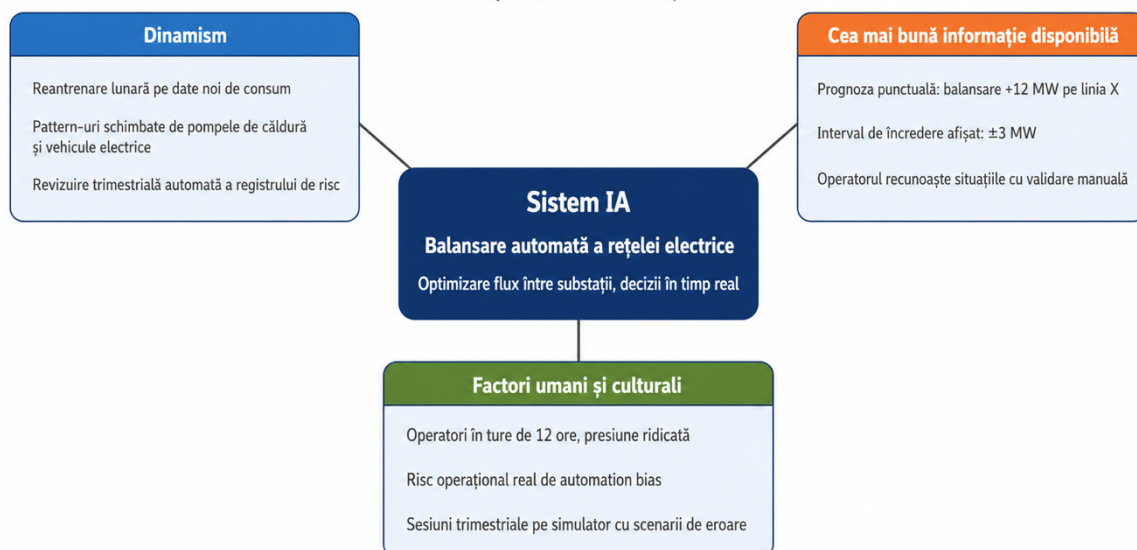
Pentru sistemele IA, mai multe principii capătă o dimensiune nouă. Cea mai bună informație disponibilă devine o cerință neobișnuit de complexă în contextul modelelor probabilistice, unde incertitudinea este intrinsecă, nu accidentală, iar performanța modelului poate degrada în moduri greu de detectat în timp real. Factorii umani și culturali capătă o importanță sporită, pentru că deciziile sistemelor IA sunt mediate de încrederea și înțelegerea operatorilor umani.

### Exemplu: cum se aplică principiile la un sistem IA de balansare a rețelei de energie electrică

*Un distribuitor integrat de energie electrică și gaze naturale operează un sistem IA de balansare automată a rețelei, care optimizează fluxurile între substații în funcție de consumul prognozat. Trei dintre cele opt principii din Clauza 4 capătă, în acest caz, o dimensiune specifică.*

#### Principiile managementului riscurilor IA aplicate unui sistem de balansare automată a rețelei

SR EN ISO/IEC 23894:2024, Clauza 4



**Dinamism.** *Procesul de management al riscurilor nu se oprește la evaluarea inițială. Modelul de prognoză este reantrenat lunar pe date noi de consum, iar pattern-urile se schimbă vizibil odată cu adopția pompelor de căldură și a stațiilor de încărcare pentru vehicule electrice. Ce a fost un risc marginal în 2024 (consum sezonier atipic) devine în 2026 un risc principal. Cadrul include o procedură de revizuire trimestrială a registrului de risc, declanșată automat de modificări ale distribuției datelor de intrare.*

**Cea mai bună informație disponibilă.** *Pentru un model probabilistic care decide în timp real, „cea mai bună informație” nu înseamnă doar date precise, ci și informație despre incertitudinea predicției. Echipa adaugă în tabloul de bord operațional, alături de prognoza punctuală, intervalul de încredere al fiecărei decizii. Operatorul de dispecerat vede simultan „balansare recomandată:*

+12 MW pe linia X” și „incertitudine:  $\pm 3$  MW”, astfel încât să poată recunoaște situațiile în care decizia automată trebuie validată manual.

**Factori umani și culturali.** Operatorii de dispecerat lucrează în ture de 12 ore într-un mediu cu presiune ridicată. Automation bias-ul nu este o ipoteză academică, ci un risc operațional real. Cadrul include sesiuni trimestriale de exerciții pe simulator, în care operatorii sunt expuși la scenarii cu erori intenționate ale sistemului, pentru a păstra capacitatea de detecție și de intervenție umană în condiții reale.

### 2.2.2. Clauza 5. Cadrul de management al riscurilor

Clauza 5 descrie modul în care managementul riscurilor IA se integrează în structura organizației, prin cinci componente:

- **Leadership și angajament**, rolul conducerii în asigurarea unui cadru efectiv.
- **Integrare**, corelarea cu structura, procesele și cultura organizației.
- **Proiectarea cadrului**, înțelegerea organizației și contextului, articularea angajamentului, definirea rolurilor și responsabilităților, alocarea resurselor, stabilirea modalităților de comunicare și consultare.
- **Implementarea cadrului**, executarea concretă a proiectului.
- **Evaluarea și îmbunătățirea cadrului**, monitorizarea performanței și adaptarea continuă.

Aceste componente acoperă temele pe care un organism de certificare 42001 le verifică în clauza 5 (Leadership) și clauza 7 (Suport) ale Sistemului de Management al Inteligenței Artificiale.

#### Exemplu: cum se construiește cadrul de management al riscurilor IA într-o companie distribuitor integrat de energie electrică și gaze naturale

*Un operator distribuitor integrat de energie electrică și gaze naturale din România decide să adopte SR ISO/IEC 42001:2024 în pregătirea pentru AI Act, având în vedere că rețeaua de distribuție intră sub categoria infrastructurii critice (Anexa III pct. 2 din regulament). Pentru procesul de management al riscurilor IA aplică SR EN ISO/IEC 23894:2024. Aplicarea Clauzei 5 se materializează astfel.*

**Leadership și angajament.** Directorul general semnează personal Politica AI și o prezintă în Consiliul Director. Consiliul aprobă un buget anual dedicat și include un indicator de risc IA în raportul trimestrial către acționari și în raportarea către ANRE. Angajamentul nu rămâne declarativ.

**Integrare.** Procesul de management al riscurilor IA nu se construiește separat. Se conectează cu cadrul existent ISO/IEC 27001 prin proceduri comune (control al documentelor, audit intern, acțiuni corective) și cu cadrul de reziliență construit pe Directiva NIS2. Registrul riscurilor IA devine extensia registrului de risc operațional și de securitate cibernetică, nu un document paralel.

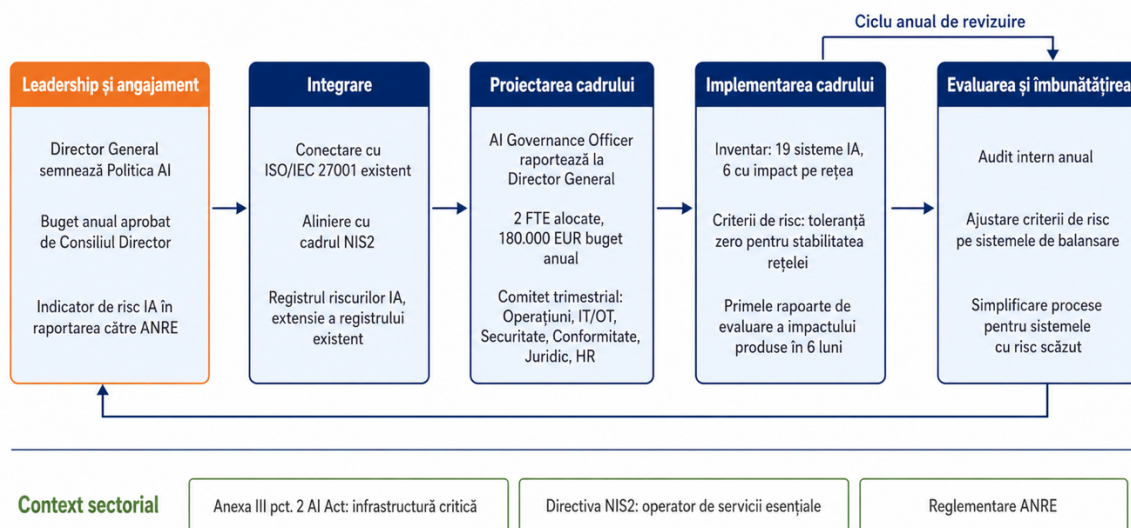
**Proiectarea cadrului.** Se desemnează un AI Governance Officer care raportează direct directorului general și colaborează cu CISO-ul și cu directorul de operațiuni. Se alocă două FTE-uri din echipele de risc și operațiuni și un buget de 180.000 EUR pentru primul an. Se stabilește un comitet trimestrial cu reprezentanți din Operațiuni Rețea, IT/OT, Securitate Cibernetică, Conformitate, Juridic și Resurse Umane.

**Implementarea cadrului.** În primele șase luni, comitetul finalizează inventarul sistemelor IA (identifică 19 sisteme operate intern sau prin furnizori, dintre care 6 cu impact direct asupra rețelei: predicție de consum, balansare automată, mentenanță predictivă pe transformatoare, detecție pierderi necomerciale pe gaze, optimizare rute pentru echipele de intervenție, scoring de risc pentru racordări noi), definește criteriile de risc cu prag de toleranță zero pentru sistemele care influențează stabilitatea rețelei, construiește registrul și produce primele rapoarte de evaluare a impactului pentru sistemele cu risc ridicat.

**Evaluarea și îmbunătățirea cadrului.** După un an, auditul intern compară performanța indicatorilor cu țintele stabilite și identifică două zone de ajustare: criteriile de risc erau prea permissive pentru sistemele de balansare automată (un sistem care optimizează încărcarea rețelei poate genera, în condiții extreme, decizii care contribuie la propagarea unui blackout) și procesul de aprobare era prea greoi pentru sistemele administrative cu risc scăzut. Cadrul se rafinează în consecință.

#### Cadrul de management al riscurilor IA. Aplicare la un distribuitor integrat de energie electrică și gaze naturale

SR EN ISO/IEC 23894:2024, Clauza 5



### 2.2.3. Clauza 6. Procesul de management al riscurilor IA

Clauza 6 este partea cu cea mai mare valoare operațională a ghidului. Descrie procesul iterativ de management al riscurilor IA pe **șase componente**:

- **Comunicare și consultare (Clauza 6.2)**, implicarea părților interesate pe tot parcursul procesului.
- **Stabilirea scopului, contextului și criteriilor (Clauza 6.3)**, definirea limitelor, contextului extern și intern, criteriilor de risc.
- **Evaluarea riscului (Clauza 6.4)**, identificarea, analiza și evaluarea propriu-zisă a riscurilor.
- **Tratarea riscului (Clauza 6.5)**, selectarea și implementarea opțiunilor de tratare.
- **Monitorizare și revizuire (Clauza 6.6)**, urmărirea continuă a procesului și a riscurilor.
- **Înregistrare și raportare (Clauza 6.7)**, documentarea procesului și comunicarea rezultatelor.

Fiecare componentă conține îndrumări specifice IA: cum se identifică riscurile pentru un sistem care învață continuu, cum se analizează probabilitatea în absența datelor istorice relevante, cum se evaluează riscul rezidual atunci când explicabilitatea modelului este limitată, cum se monitorizează un sistem după implementare pentru detectarea driftului datelor sau a performanței.

#### **Exemplu: cum se aplică procesul de management al riscurilor IA la sistemul de balansare automată a rețelei**

*Distribuitorul integrat aplică cele șase componente ale procesului din Clauza 6 sistemului de balansare automată a rețelei electrice introdus în exemplele anterioare.*

**Comunicare și consultare (Clauza 6.2).** *Părțile interesate sunt identificate la începutul procesului: dispeceri, ingineri de rețea, IT/OT, securitate cibernetică, juridic, ANRE și, pentru anumite scenarii, autoritatea de protecție civilă. Comunicarea este programată trimestrial, cu interfețe ad-hoc pentru incidente.*

**Stabilirea scopului, contextului și criteriilor (Clauza 6.3).** *Scopul evaluării: toate deciziile automate ale sistemului care pot afecta stabilitatea rețelei. Contextul: infrastructură critică sub Anexa III pct. 2 din AI Act, reglementări ANRE, obligații NIS2. Criteriile de risc: toleranță zero pentru orice eveniment care poate declanșa cascadă de deconectări.*

**Evaluarea riscului (Clauza 6.4).** *Identificarea folosește Anexa B din standard: drift al datelor, comportament emergent, atacuri adversariale pe semnalele de intrare, dependență de furnizori SCADA. Analiza estimează probabilități pe scenarii (uzual, vârf de consum, condiții meteo extreme). Evaluarea clasifică riscurile în registrul prioritar.*

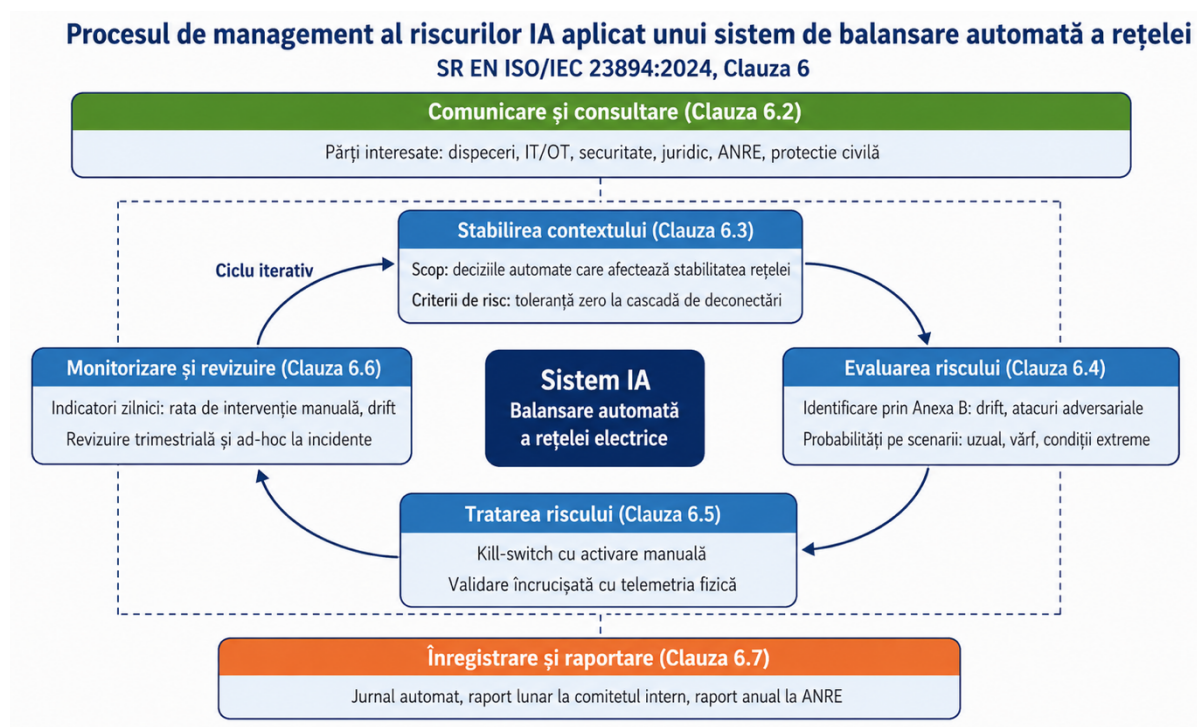
**Tratarea riscului (Clauza 6.5).** *Pentru riscul de propagare a deciziilor eronate se introduce un dispozitiv de oprire de urgență (kill-switch) cu activare manuală. Pentru drift al datelor se*



implementează monitorizare automată cu prag de alertă. Pentru atacuri adversariale se aplică validarea încrucișată cu telemetria fizică.

**Monitorizare și revizuire (Clauza 6.6).** Indicatori urmăriți zilnic: rata de intervenție manuală a dispecerilor, abateri ale predicției față de consumul real, tentative de manipulare a datelor de intrare. Revizuire formală trimestrială și ad-hoc la incidente.

**Înregistrare și raportare (Clauza 6.7).** Toate deciziile și incidentele se documentează în jurnal automat, accesibil la audit. Raport lunar către comitetul de risc IA, raport anual către ANRE.



## 2.3. Cele trei anexe

### 2.3.1. Anexa A. Obiective organizaționale tipice legate de IA

Anexa A listează obiectivele pe care organizațiile le formulează frecvent în legătură cu sistemele de inteligență artificială: corectitudine (fairness), transparență, explicabilitate, robustețe, securitate, protecția vieții private, siguranță, responsabilitate. Pentru fiecare obiectiv, anexa sugerează tipuri de riscuri care îl pot compromite. Anexa este informativă, dar este materialul de referință pentru structurarea discuției cu conducerea în faza de stabilire a criteriilor de risc.

### 2.3.2. Anexa B. Surse de risc IA

Anexa B este, în opinia consultanților care lucrează direct pe implementarea standardului, cea mai dens utilă parte a ghidului și, paradoxal, cea mai des ignorată în implementări. Identifică sursele de risc grupate pe categorii:

- **Probleme de date**, calitatea, reprezentativitatea, biasul, drift-ul, integritatea, sursa și licența.

- **Probleme de model**, alegerea inadecvată a algoritmului, supraînvățarea, lipsa robusteții, vulnerabilitatea la atacuri adversariale, opacitatea, lipsa explicabilității.
- **Complexitate și opacitate**, dificultatea de înțelegere și verificare a deciziilor sistemului.
- **Autonomie și nivel de automatizare**, comportamente emergente, lipsa controlului uman efectiv.
- **Hardware**, limitări ale infrastructurii de calcul, vulnerabilități fizice.
- **Factor uman și de sistem**, automation bias, încredere insuficientă, lacune de competență.
- **Ciclu de viață**, riscuri specifice fiecărei etape, de la concepție la retragere.

Pentru o organizație care construiește pentru prima dată un registru de riscuri IA, Anexa B funcționează ca o checklist de identificare ce reduce semnificativ riscul de a omite categorii întregi.

### 2.3.3. Anexa C. Maparea procesului pe ciclul de viață al sistemului IA

Anexa C arată, sub forma unui tabel, cum se aplică componentele procesului de management al riscurilor (din Clauza 6) la fiecare etapă a ciclului de viață al unui sistem IA: concepție, proiectare și dezvoltare, verificare și validare, implementare, operare și monitorizare, reevaluare continuă, retragere. Este puntea practică între metodologia de risc și cerințele Articolului 9 din AI Act, care impune procesul iterativ pe tot ciclul de viață.

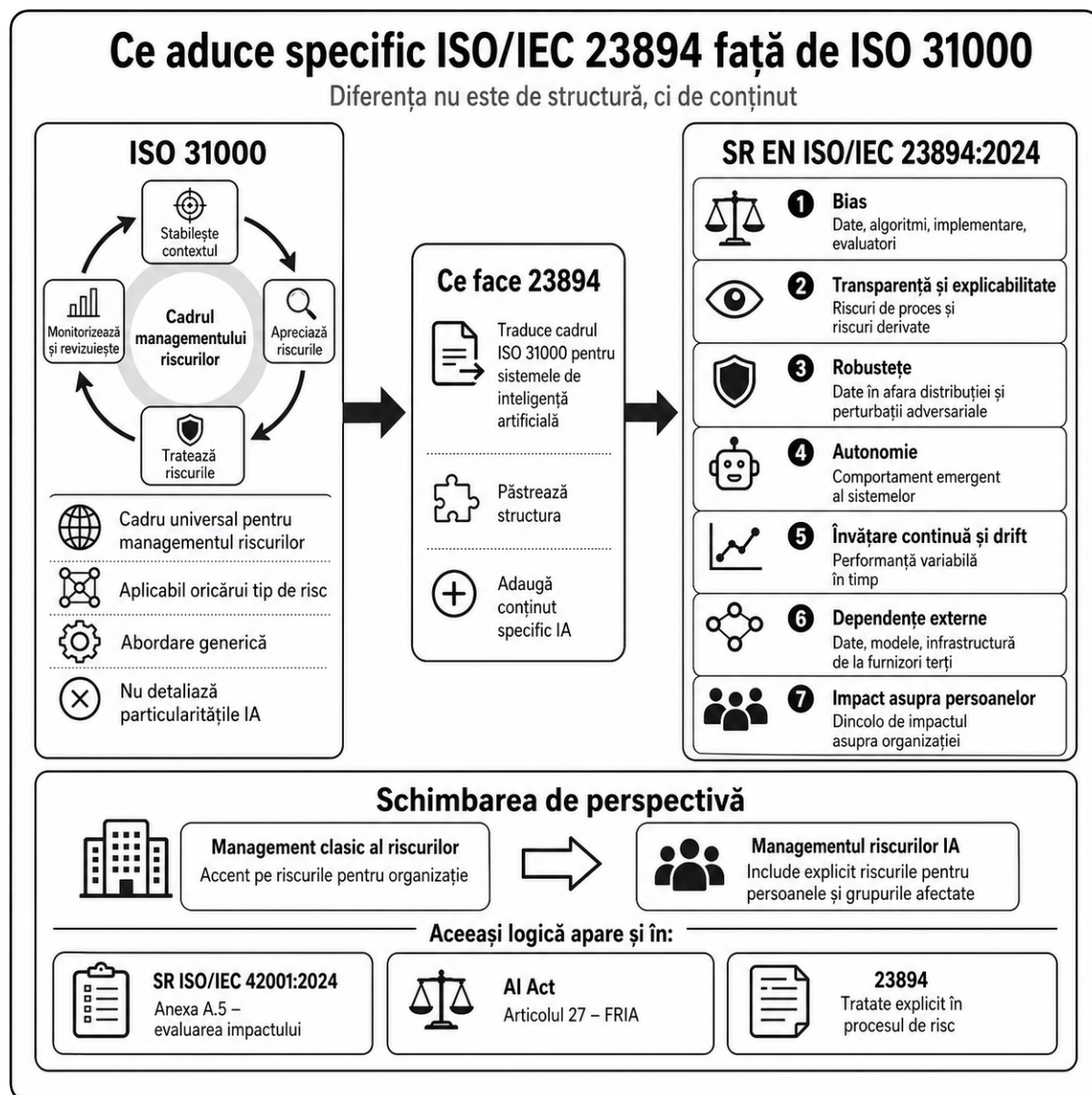
## 2.4. Ce aduce specific ISO/IEC 23894 față de ISO 31000

Diferența dintre cele două standarde nu este de structură, ci de conținut. ISO 31000 oferă cadrul universal, aplicabil oricărui tip de risc. SR EN ISO/IEC 23894:2024 traduce acel cadru pentru particularitățile sistemelor de inteligență artificială și introduce atenție explicită pentru zone pe care un proces generic de management al riscurilor le-ar putea trata superficial sau le-ar putea omite complet:

- **biasul**, sub toate formele sale, de date, algoritmic, de implementare, cognitiv al evaluatorilor;
- **transparența și explicabilitatea** modelelor, ca riscuri de proces și ca surse de risc derivate;
- **robustețea** în fața datelor în afara distribuției de antrenament și a perturbațiilor adversariale;
- **comportamentul emergent** al sistemelor cu autonomie crescută;
- **riscurile asociate ciclului continuu de învățare** și ale driftului datelor sau performanței;
- **dependența de furnizori terți** pentru date, modele sau infrastructură de calcul;
- **impactul asupra persoanelor și grupurilor** afectate de deciziile sistemului, dincolo de impactul asupra organizației.

Această ultimă componentă reprezintă una dintre cele mai importante schimbări de perspectivă față de un management clasic al riscurilor. Un sistem IA nu generează riscuri doar pentru organizația care îl operează, ci și pentru persoanele asupra cărora deciziile lui se aplică. SR EN ISO/IEC 23894:2024 cere ca această dimensiune să fie tratată explicit, ca parte a procesului.

Aceeași logică se regăsește în Anexa A din SR ISO/IEC 42001:2024, în domeniul A.5 dedicat evaluării impactului, și în obligațiile de evaluare a impactului asupra drepturilor fundamentale (FRIA) din Articolul 27 al AI Act.



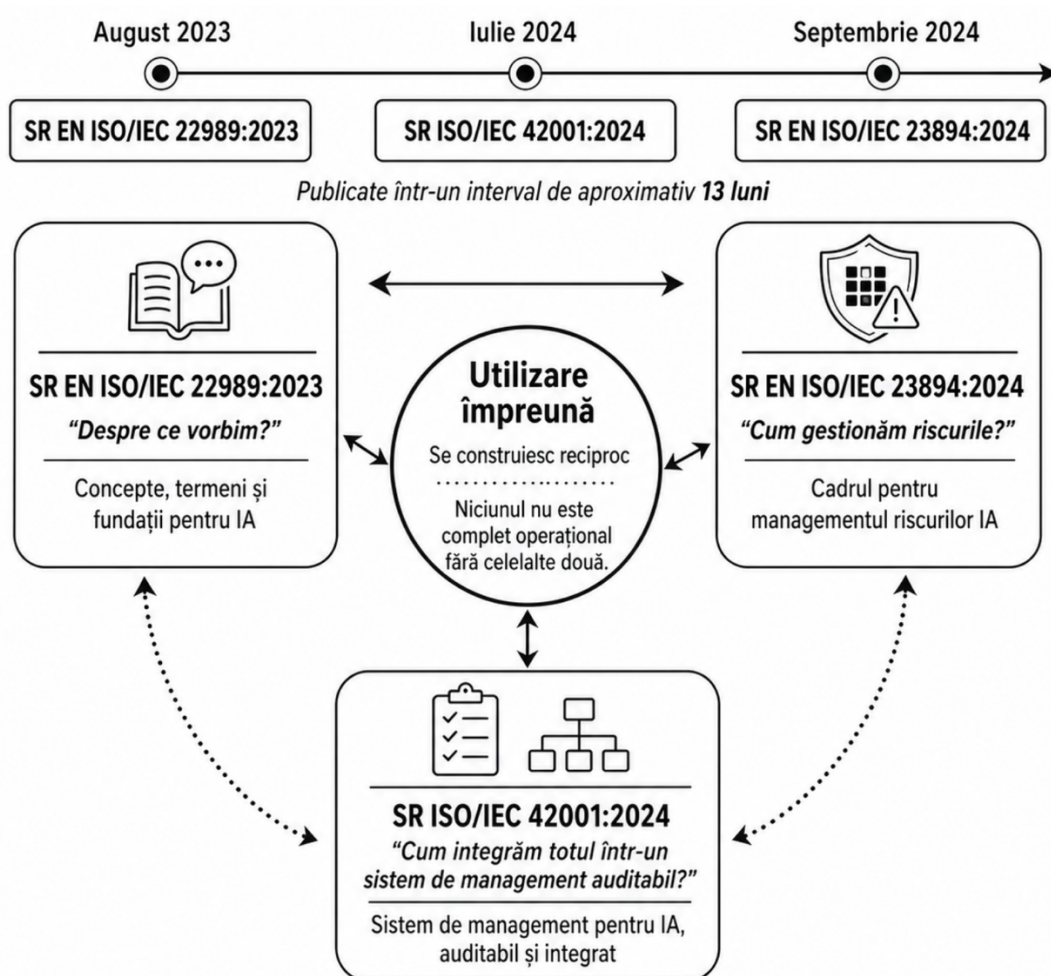
### Caseta 2. Anexa B ca punct de plecare al registrului de riscuri

În proiectele de implementare SMIA, recomand utilizarea Anexei B din SR EN ISO/IEC 23894:2024 ca structură inițială a registrului de riscuri IA. Cele șapte categorii de surse de risc identificate de standard se transformă în secțiuni ale registrului, iar pentru fiecare sistem IA din inventar, echipa de proiect verifică sistematic prezența și relevanța fiecărei surse. Această abordare reduce semnificativ riscul de a omite categorii întregi de risc, eroare care apare frecvent în registrele construite pe metodologii generice.

## Capitolul 3. Triada standardelor IA: 22989, 23894 și 42001

### 3.1. Trei standarde, trei funcții

Cele trei standarde române din zona inteligenței artificiale au fost publicate într-un interval de aproximativ 13 luni: SR EN ISO/IEC 22989 în august 2023, SR ISO/IEC 42001 în iulie 2024, SR EN ISO/IEC 23894 în septembrie 2024. Această cadență nu este întâmplătoare. Cele trei se construiesc reciproc și sunt gândite să fie folosite împreună. Niciunul dintre ele nu este complet operațional fără celelalte două.



Felul cel mai simplu de a înțelege relația dintre ele este să observăm ce tip de problemă rezolvă fiecare:

- **SR EN ISO/IEC 22989:2023** răspunde la întrebarea „despre ce vorbim?”.
- **SR EN ISO/IEC 23894:2024** răspunde la întrebarea „cum gestionăm riscurile?”.
- **SR ISO/IEC 42001:2024** răspunde la întrebarea „cum integrăm totul într-un sistem de management auditabil?”.

Această triplă funcție definește relația dintre cele trei standarde: nu se suprapun, ci se completează.



### 3.2. SR EN ISO/IEC 22989:2023, vocabularul comun

**SR EN ISO/IEC 22989:2023 Tehnologia informației. Inteligența artificială. Conceptele și terminologia inteligenței artificiale** a fost aprobat de Asociația de Standardizare din România la 31 august 2023, identic cu standardul european EN ISO/IEC 22989:2023, care preia ediția internațională din 2022.

**Standardul stabilește terminologia și descrie conceptele din domeniul IA.** Definește termeni esențiali precum sistem AI, agent AI, autonomie, model, învățare automată, ciclul de viață al sistemului IA, părți interesate. Pentru fiecare termen oferă o definiție formală, surse de proveniență acolo unde termenul este preluat din alte standarde și note explicative.

Aparent, este doar un dicționar tehnic. În realitate, **este referința normativă a celorlalte două standarde.** SR ISO/IEC 42001:2024 declară explicit, în clauza 2 Referințe normative, că ISO/IEC 22989:2022, identic cu SR EN ISO/IEC 22989:2023, este sursa pentru termenii și definițiile folosite. SR EN ISO/IEC 23894:2024 face aceeași raportare.

Consecința practică este semnificativă. Într-o organizație care implementează un Sistem de Management al Inteligenței Artificiale sau un proces de management al riscurilor IA, terminologia nu se mai negociază. Este standardizată. Acest detaliu pare minor, dar elimină o sursă majoră de confuzii operaționale. Discuțiile între echipele tehnice, juridice, de conformitate și de afaceri pornesc dintr-un punct comun. Aceeași proprietate este valorificată și de AI Act, care își construiește propriile definiții în Articolul 3, frecvent aliniate cu cele din 22989.

Pentru o organizație care intră acum în zona guvernancei IA, recomandarea este simplă: orice glosar intern de termeni se construiește pornind de la 22989, cu adaptările necesare pentru contextul specific.

### 3.3. SR EN ISO/IEC 23894:2024, instrumentul de lucru

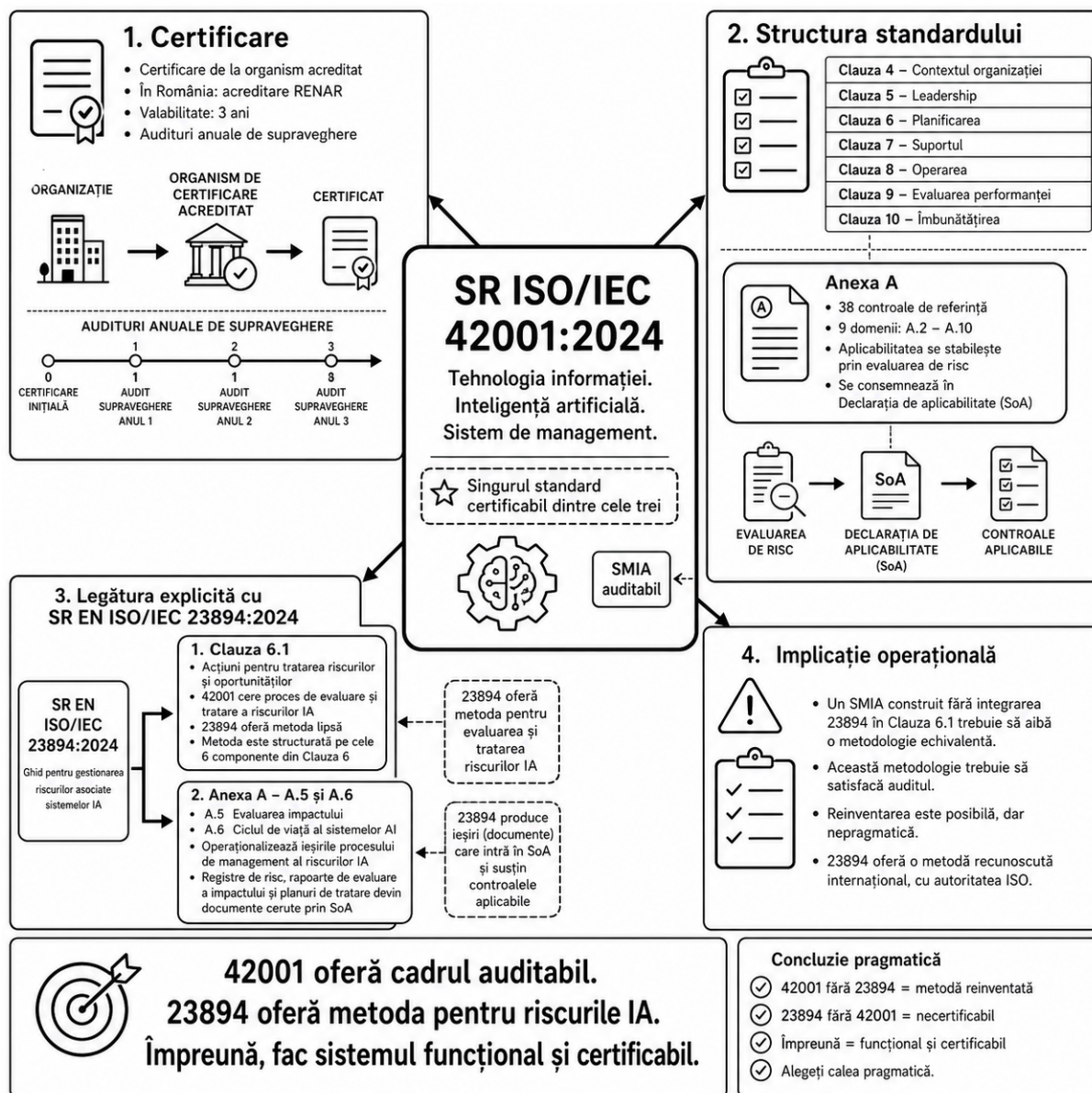
Standardul 23894 a fost prezentat detaliat în Capitolul 2. Pentru economia argumentului din această secțiune, sintetizez doar funcția lui în triadă.

23894 oferă procesul prin care identificăm, analizăm, evaluăm, tratăm și monitorizăm riscurile sistemelor IA, în logica deja consolidată a ISO 31000:2018, dar cu specializare pe particularitățile inteligenței artificiale. Este un ghid, nu se certifică, dar produce ieșirile pe care celelalte cadre, atât 42001 cât și AI Act, le cer ca dovezi de conformitate.

Locul lui în triadă este cel de instrument metodologic. Fără el, sistemul de management certificabil 42001 rămâne fără motorul intern care alimentează clauza 6.1, iar cerința legală a Articolului 9 din AI Act rămâne fără o metodă recunoscută de implementare.



### 3.4. SR ISO/IEC 42001:2024, sistemul de management certificabil



**SR ISO/IEC 42001:2024 Tehnologia informației. Inteligență artificială. Sistem de management** este, dintre cele trei, singurul standard certificabil. Certificarea se obține de la un organism de certificare acreditat, în România de către Asociația de Acreditare din România (RENAR), are valabilitate de trei ani și necesită audituri anuale de supraveghere.

Standardul urmează structura armonizată a sistemelor de management ISO. **Cerințele de bază sunt grupate în clauzele 4-10**, acoperind contextul organizației, leadershipul, planificarea, suportul, operarea, evaluarea performanței și îmbunătățirea.

**Anexa A conține 38 de controale de referință organizate în nouă domenii (A.2 - A.10).** Aplicabilitatea fiecărui control este determinată prin evaluarea de risc și consemnată în Declarația de aplicabilitate (Statement of Applicability, SoA).

Două articulații explicite leagă SR ISO/IEC 42001:2024 de SR EN ISO/IEC 23894:2024:

**Clauza 6.1, Acțiuni pentru tratarea riscurilor și oportunităților.** Standardul cere organizației să stabilească un proces de evaluare și tratare a riscurilor IA, dar nu detaliază metoda de aplicare. Aici, 23894 oferă exact metoda lipsă, structurată pe cele șase componente ale procesului din Clauza 6.

**Anexa A, în special domeniile A.5 (Evaluarea impactului) și A.6 (Ciclul de viață al sistemelor AI).** Aceste controale operaționalizează ieșirile procesului de management al riscurilor IA. Registrele de risc, rapoartele de evaluare a impactului, planurile de tratare construite pe baza standardului 23894 devin documente cerute prin SoA.

Pe plan operațional, această conexiune înseamnă că o organizație care își construiește SMIA fără să integreze 23894 în clauza 6.1 va trebui, oricum, să producă o metodologie echivalentă pentru a satisface auditul. Reinventarea este posibilă, dar nepragmatică, mai ales când există un standard internațional consacrat care face acest lucru cu autoritatea recunoașterii ISO.

### 3.5. AI Act, deasupra triadei

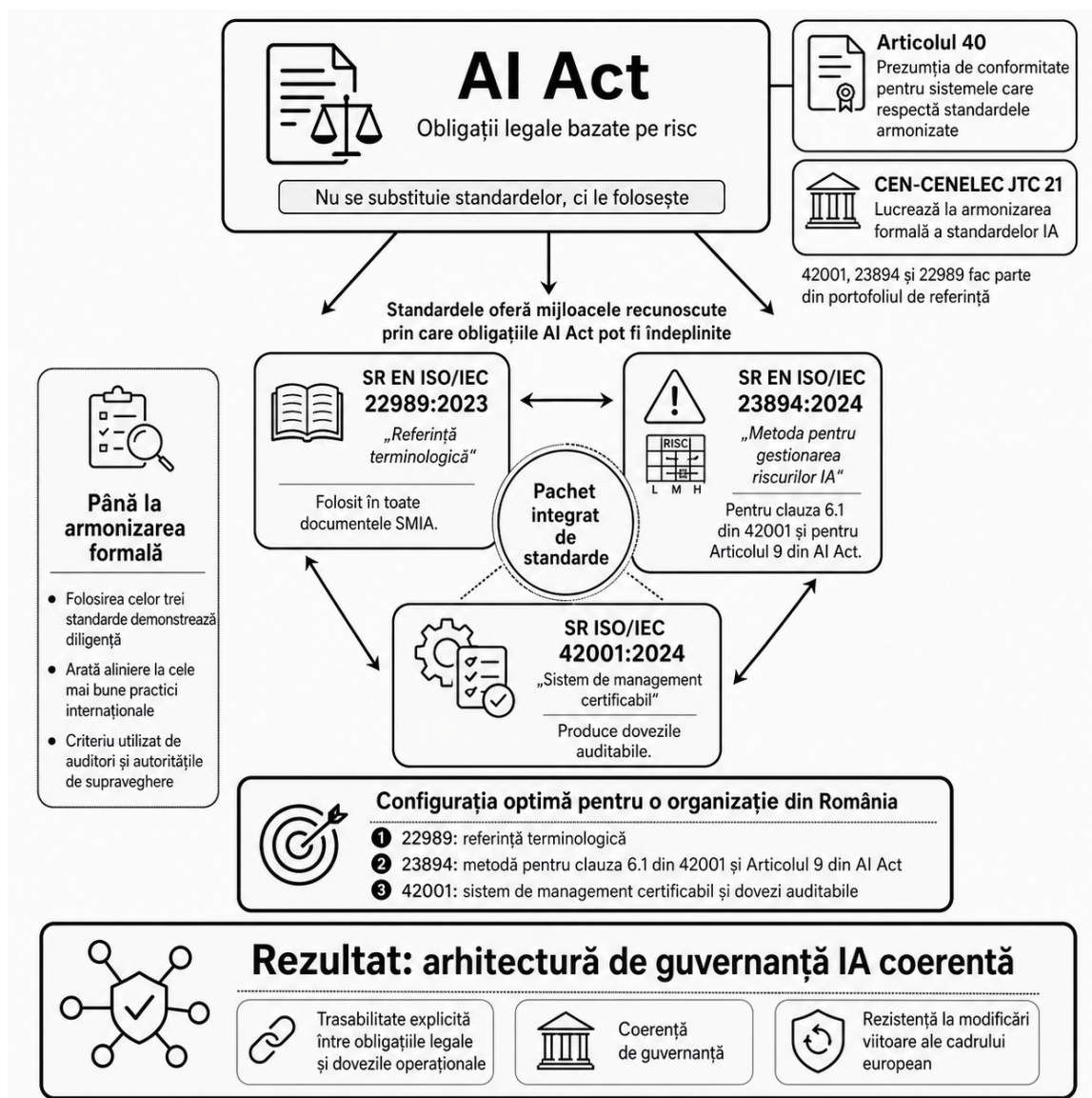
Deasupra triadei celor trei standarde se așază **AI Act**, care nu se substituie standardelor, ci le folosește. Regulamentul european stabilește obligații legale pe baza unei abordări bazate pe risc, iar standardele oferă mijloacele recunoscute prin care aceste obligații pot fi îndeplinite. Această distincție merită explicată, pentru că este sursa celor mai frecvente confuzii întâlnite în primele luni de pregătire pentru AI Act.

**AI Act este un regulament, nu un standard tehnic.** Regulamentele europene stabilesc obligații cu efect direct în statele membre, fără a prescrie metodologia tehnică de îndeplinire a acestora. Această alegere arhitecturală este intenționată. Tehnologia IA evoluează rapid, iar un regulament care ar codifica metodologii specifice ar deveni dezactualizat în câțiva ani. Standardele tehnice, în schimb, sunt revizuite ciclic de organisme specializate (ISO, IEC, CEN-CENELEC) și pot urmări evoluția tehnologică fără să ceară modificarea legislației primare. Soluția adoptată de legiuitorul european este separarea responsabilităților: regulamentul fixează obiectivele și principiile, standardele furnizează metodele.

**Abordarea bazată pe risc structurează întreaga logică a AI Act.** Regulamentul împarte sistemele IA în patru categorii, în funcție de riscul pe care îl pot genera pentru sănătatea, siguranța și drepturile fundamentale ale persoanelor. Practicile interzise (Articolul 5) sunt sisteme considerate incompatibile cu valorile Uniunii și nu pot fi folosite în niciun context. Sistemele cu grad ridicat de risc (Articolul 6 și Anexa III) sunt permise, dar supuse unui set extins de obligații, inclusiv sistemul de gestionare a riscurilor cerut de Articolul 9. Sistemele cu risc limitat sunt supuse doar obligațiilor de transparență (Articolul 50). Sistemele cu risc minim sau inexistent nu au obligații specifice. Această ierarhie produce o consecință practică importantă pentru organizații: nivelul efortului de conformitate trebuie calibrat

după categoria de risc a fiecărui sistem, nu aplicat uniform tuturor sistemelor IA pe care organizația le operează.

**Mijloacele recunoscute sunt instrumentul de aliniere la cerințele legale.** Atunci când AI Act cere instituirea unui „sistem de gestionare a riscurilor”, regulamentul nu specifică formatul, structura sau metodologia acestuia. Această libertate aparentă poate fi înșelătoare. În practică, autoritățile de supraveghere și organisme de certificare evaluează conformitatea pornind de la întrebarea „organizația a aplicat o metodă recunoscută la nivel internațional?”. Răspunsul afirmativ se construiește prin referință la standardele relevante. Pentru managementul riscurilor IA, SR EN ISO/IEC 23894:2024 este, în acest moment, metoda recunoscută. Pentru sistemul de management în ansamblu, SR ISO/IEC 42001:2024 este sistemul recunoscut. O organizație care construiește sistemul de gestionare a riscurilor pe o metodologie proprie, neconectată la standardele internaționale, poate fi tehnic conformă cu litera Articolului 9, dar va întâmpina dificultăți semnificative în a-și demonstra conformitatea în fața auditorilor și a autorităților, mai ales în primii ani de aplicare a regulamentului, când practicile de evaluare se vor consolida prin referință la cadre standardizate.



Articolul 40 al AI Act prevede prezumția de conformitate pentru sistemele care respectă standardele armonizate. CEN-CENELEC JTC 21 lucrează în prezent la armonizarea formală a standardelor IA, iar 42001, 23894 și 22989 fac parte din portofoliul de referință al acestui proces. Până la finalizarea armonizării formale, organizațiile care folosesc cele trei standarde demonstrează diligență și aliniere la cele mai bune practici internaționale, criteriul folosit de auditori și de autoritățile de supraveghere atunci când evaluează conformitatea.

Pentru o organizație din România care se pregătește pentru AI Act, configurația optimă este cea în care cele trei standarde sunt adoptate ca pachet integrat:

- SR EN ISO/IEC 22989:2023 ca referință terminologică în toate documentele SMIA.
- SR EN ISO/IEC 23894:2024 ca metodă pentru clauza 6.1 din 42001 și pentru Articolul 9 din AI Act.
- SR ISO/IEC 42001:2024 ca sistem de management certificabil care produce dovezile auditabile.

Această configurație produce o arhitectură de guvernare IA coerentă, cu trasabilitate explicită între obligațiile legale și dovezile operaționale, și rezistentă la modificări viitoare ale cadrului european.

### **Caseta 3. Dubla trasabilitate document-cerință**

Principiul dublei trasabilități este nenegociabil în orice proiect de implementare SMIA matur. Fiecare document din sistem se construiește astfel încât să fie trasabil către două referințe simultan: clauza standardului SR ISO/IEC 42001:2024 care îl cere și, acolo unde există, articolul AI Act pe care îl acoperă. Trasabilitatea permite auditorilor organismelor de certificare acreditate să evalueze rapid coerența sistemului, iar organizațiilor le permite să demonstreze conformitatea atât la auditul de certificare, cât și în fața autorităților de supraveghere a pieței. Pentru documentele care provin din procesul descris în SR EN ISO/IEC 23894:2024, această dublă trasabilitate include și clauza relevantă a ghidului de management al riscurilor.



## Capitolul 4. Maparea SR EN ISO/IEC 23894:2024 pe cerințele AI Act

### 4.1. Premisa de mapare

**Standardul SR EN ISO/IEC 23894:2024 nu menționează AI Act.** A fost dezvoltat ca ghid internațional de management al riscurilor IA, neutru față de orice cadru legislativ național sau regional. Cu toate acestea, suprapunerea dintre procesul descris în ghid și obligațiile stabilite de regulamentul european este consistentă, suficient de strânsă încât 23894 să poată fi folosit ca metodă recunoscută pentru implementarea cerințelor legale.

Articulația dintre cele două documente se face prin **patru articole principale ale AI Act**, plus o serie de articole conexe.

### 4.2. Articolul 9: Sistemul de gestionare a riscurilor

Articolul 9 este punctul de contact cel mai direct între ghidul 23894 și AI Act. Cerințele lui sunt structurate astfel:

- **Alineatul (1)** cere instituirea, punerea în aplicare, documentarea și menținerea unui sistem de gestionare a riscurilor pentru sistemele IA cu grad ridicat de risc.
- **Alineatul (2)** descrie acest sistem ca proces iterativ continuu, planificat și derulat pe parcursul întregului ciclu de viață al sistemului.
- **Alineatul (2) literele (a)-(d)** detaliază componentele procesului: identificarea riscurilor previzibile, estimarea și evaluarea riscurilor în condiții de utilizare normală și utilizare necorespunzătoare previzibilă în mod rezonabil, evaluarea altor riscuri pe baza datelor din monitorizarea post-piață, adoptarea măsurilor de gestionare adecvate.
- **Alineatul (5)** stabilește că măsurile de gestionare trebuie să asigure că riscul rezidual este considerat acceptabil, cu informarea explicită a implementatorului.
- **Alineatul (9)** introduce o cerință specifică pentru sistemele care interacționează cu minorii sau cu alte grupuri vulnerabile: evaluarea și mitigarea riscurilor specifice pentru aceste categorii.

Procesul descris în Clauza 6 a SR EN ISO/IEC 23894:2024 acoperă, punct cu punct, aceste cerințe:

- identificarea riscurilor (Clauza 6.4.2)
- analiza riscurilor (Clauza 6.4.3)
- evaluarea riscurilor (Clauza 6.4.4)
- tratarea riscurilor (Clauza 6.5)
- monitorizarea și revizuirea (Clauza 6.6)
- înregistrarea și raportarea (Clauza 6.7)



Aceste componente, în limbajul AI Act, devin proces iterativ continuu pe ciclul de viață. Anexa C a standardului 23894 mapează explicit această corespondență, oferind un tabel direct utilizabil în documentația de conformitate.

Pentru cerința de la Alineatul (5) privind riscul rezidual acceptabil, ghidul 23894 oferă instrumentele prin Clauza 6.4.4 (criterii de evaluare a riscurilor) și Clauza 6.5 (tratarea riscului), care impun documentarea explicită a riscului rezidual și acceptarea formală a acestuia de către o persoană cu autoritate decizională în organizație.

### ***Exemplu: cum demonstrează un distribuitor integrat conformitatea cu Articolul 9 pentru sistemul de balansare automată a rețelei***

*Distribuitorul integrat din exemplele anterioare se pregătește pentru primul control al autorității de supraveghere a pieței. Sistemul de balansare automată a rețelei este clasificat ca IA cu grad ridicat de risc conform Anexei III pct. 2 din AI Act (infrastructură critică). Echipa de conformitate construiește dosarul de conformitate cu Articolul 9, alineat cu alineat, sprijinit pe procesul SR EN ISO/IEC 23894:2024.*

**Alineatul (1), instituirea sistemului.** *Dosarul include politica de management al riscurilor IA aprobată de Director General, procedura formală derivată din Clauza 6 a standardului, și jurnalul de versiuni care demonstrează menținerea continuă a sistemului din momentul punerii în funcțiune.*

**Alineatul (2), proces iterativ pe ciclul de viață.** *Anexa C a standardului 23894 este atașată dosarului ca dovadă a corespondenței între componentele procesului și etapele ciclului de viață al sistemului. Pentru fiecare etapă (concepție, dezvoltare, validare, operare, retragere), echipa documentează evaluările de risc efectuate.*

**Alineatul (2) literele (a)-(d), componentele procesului.** *Identificarea riscurilor previzibile este documentată prin registrul construit pe Anexa B a standardului (drift al datelor, atacuri adversariale, dependență SCADA). Estimarea riscurilor pentru utilizare necorespunzătoare previzibilă include scenarii de manipulare a semnalelor de intrare. Evaluarea pe baza monitorizării post-piață se sprijină pe rapoartele lunare ale comitetului de risc IA.*

**Alineatul (5), riscul rezidual acceptabil.** *Pentru fiecare risc identificat, registrul conține criteriile aplicate, măsurile de tratare și valoarea reziduală estimată. Riscul de propagare a deciziilor eronate este acceptat formal de Director General prin semnătură electronică, cu mențiunea explicită a kill-switch-ului ca măsură compensatorie. Implementatorii (dispecerii) primesc, prin manualul de operare, informarea explicită despre riscul rezidual și despre instrucțiunile de intervenție manuală.*

**Alineatul (9), grupuri vulnerabile.** *Sistemul nu interacționează direct cu persoane fizice, dar afectează indirect populația conectată la rețea, inclusiv consumatori vulnerabili (spitale,*

gospodării cu echipamente medicale la domiciliu). Dosarul include evaluarea specifică a impactului unei deconectări asupra acestor categorii și protocolul de comunicare cu autoritățile sanitare în cazul incidentelor majore.

## Dosar de conformitate cu Articolul 9 AI Act

Sistem IA de balansare automată a rețelei, distribuitor integrat de energie electrică și gaze naturale

Anexa III pct. 2: infrastructură critică

Alineat	Cerința AI Act	Dovada în dosar
(1)	Instituirea sistemului de gestionare a riscurilor	Politica de management al riscurilor IA aprobată de Director General + procedura derivată din Clauza 6 SR EN ISO/IEC 23894:2024 + jurnal de versiuni
(2)	Proces iterativ continuu pe ciclul de viață	Anexa C a standardului 23894 atașată ca dovadă de corespondență între componente proces și etape ciclu de viață
(2) (a)-(d)	Identificarea, estimarea, evaluarea riscurilor și măsurile de gestionare	Registrul construit pe Anexa B (drift, atacuri adversariale, dependență SCADA) + scenarii de utilizare necorespunzătoare + rapoarte lunare ale comitetului de risc IA
(5)	Riscul rezidual considerat acceptabil, cu informarea implementatorului	Acceptare formală prin semnătură electronică Director General + manualul de operare al dispecerilor cu informarea explicită despre kill-switch ca măsură compensatorie
(9)	Cerință specifică pentru grupuri vulnerabile	Evaluare a impactului unei deconectări asupra spitalelor și gospodăriilor cu echipamente medicale + protocol de comunicare cu autoritățile sanitare

### 4.3. Articolul 27: Evaluarea impactului asupra drepturilor fundamentale (FRIA)

Articolul 27 introduce obligația evaluării impactului asupra drepturilor fundamentale (Fundamental Rights Impact Assessment, FRIA) pentru o categorie specifică de implementatori:

- organisme de drept public;
- organisme private care prestează servicii publice;
- anumiți operatori privați din domeniile listate în Anexa III pct. 5 lit. (b) și (c), evaluarea bonității, asigurări de viață și de sănătate.

Este important de subliniat că FRIA nu se aplică tuturor implementatorilor de sisteme IA cu grad ridicat de risc, ci doar acestor categorii. Confuzia, frecvent întâlnită în interpretările inițiale ale regulamentului, generează fie supraconformare cu costuri inutile, fie subconformare în zonele unde obligația există efectiv.

Conținutul minim al unei FRIA, conform Articolului 27 alineatul (1), include:

- descrierea proceselor în care sistemul va fi utilizat;
- perioada și frecvența utilizării;
- categoriile de persoane afectate;
- riscurile specifice de prejudiciu pentru aceste categorii;
- modul în care va fi exercitată supravegherea umană;
- măsurile de luat în cazul materializării riscurilor.

SR EN ISO/IEC 23894:2024 nu prescrie un format de FRIA, dar oferă metoda de bază pentru construirea ei. Identificarea categoriilor afectate face parte din Clauza 6.3 (stabilirea contextului). Identificarea riscurilor specifice pentru aceste categorii este acoperită de Clauza 6.4.2 și de Anexa B (surse de risc IA, în special secțiunile despre factor uman și despre părți interesate). Măsurile de tratare provin din Clauza 6.5.

În arhitectura SMIA construit pe baza standardului 42001, FRIA se materializează în două dintre documentele Anexei A:

- **A.5.4** Raport de evaluare a impactului asupra persoanelor.
- **A.5.5** Raport de evaluare a impactului societal (parțial).

Ambele documente se construiesc pe ieșirile procesului 23894.

### ***Exemplu: cum tratează un distribuitor integrat aplicabilitatea FRIA pentru sistemul de balansare automată a rețelei***

*Distribuitorul integrat din exemplele anterioare evaluează, în faza de diagnostic juridic a proiectului SMIA, dacă Articolul 27 din AI Act îi este aplicabil pentru sistemul de balansare automată a rețelei. Analiza parcurge cele trei categorii de implementatori vizate de articol.*

**Organism de drept public.** *Distribuitorul este o societate comercială pe acțiuni, nu un organism de drept public. Categoria nu se aplică.*

**Organism privat care prestează servicii publice.** *Aici apare nuanța. Distribuția de energie este, în legislația europeană, un serviciu de interes economic general, iar în legislația română un serviciu de utilitate publică reglementat de ANRE. Avocații organizației consultă opinii doctrinare și concluzionează că Articolul 27 vizează organismele care exercită prerogative publice clasice (administrație, justiție, asistență socială), nu operatori reglementați din infrastructura economică.*

*Categoria nu se aplică în litera regulamentului, dar nu este exclusă în interpretare extensivă viitoare.*

**Operatori privați din Anexa III pct. 5 lit. (b) și (c).** Sistemul de balansare nu evaluează bonitatea persoanelor și nu face parte din asigurări. Categoria nu se aplică.

**Decizia formală.** Conducerea adoptă o poziție prudentă. Nu produce o FRIA formală conform Articolului 27 (pentru că obligația legală nu se aplică), dar produce voluntar un raport echivalent FRIA pentru sistemul de balansare, sprijinit pe metodologia SR EN ISO/IEC 23894:2024 (Clauza 6.3 pentru identificarea categoriilor afectate, Clauza 6.4.2 pentru riscuri specifice). Raportul este integrat în documentul A.5.4 din SMIA (Raport de evaluare a impactului asupra persoanelor).

**Categoriile afectate identificate.** Spitale și unități medicale conectate la rețea. Gospodării cu consumatori vulnerabili (echipamente medicale la domiciliu, persoane cu dizabilități, vârstnici dependenți). Operatori economici cu procese tehnologice sensibile (farmaceutice, alimentare). Pentru fiecare categorie, raportul descrie impactul potențial al unei deconectări, măsurile de mitigare și protocolul de comunicare cu autoritățile sanitare și locale.

**Beneficiul deciziei.** În eventualitatea unei interpretări extensive viitoare a Articolului 27 sau a unui control specific al autorității de supraveghere, organizația are deja documentul pregătit. Conformitatea voluntară, în această zonă juridică incertă, costă semnificativ mai puțin decât remediarea ulterioară.

#### 4.4. Articolul 17: Sistemul de management al calității

Articolul 17 obligă furnizorii de sisteme IA cu grad ridicat de risc să instituie un sistem de management al calității care să asigure conformitatea cu regulamentul. Alineatul (1) litera (g) cere ca acest sistem să includă procedurile de raportare și de gestionare a riscurilor.

Aici, **suprapunerea cu SMIA construit pe 42001 este aproape integrală**. Ghidul 23894 alimentează componenta de management al riscurilor a acestui sistem de calitate. Pentru organizațiile care optează să își integreze SMIA cu un sistem de management al calității deja existent, ISO 9001, această configurare devine un avantaj operațional: structura comună de management permite o singură procedură de control al documentelor, un singur ciclu de audit intern, o singură analiză efectuată de management.

#### 4.5. Articolul 10: Guvernanța datelor

Articolul 10 stabilește cerințe extinse privind seturile de date utilizate pentru antrenarea, validarea și testarea sistemelor IA cu grad ridicat de risc:

- relevanță
- reprezentativitate
- absența erorilor sistematice

- completitudine
- identificarea biasurilor potențiale

Standardul 23894 nu prescrie cerințe de calitate a datelor, dar identifică datele ca sursă majoră de risc IA. Anexa B, în secțiunea dedicată problemelor de date, inventariază tipurile de risc asociate: bias de selecție, bias de etichetare, distribuție nereprezentativă, drift al datelor, contaminare, calitate inegală.

Pentru o organizație care implementează cerințele Articolului 10, ghidul oferă metoda de identificare și tratare a acestor riscuri. Riscurile identificate se documentează ulterior în controlul A.4.3 Documentație a resurselor de date din Anexa A 42001.

## 4.6. Articole conexe

Pe lângă cele patru articulații principale, SR EN ISO/IEC 23894:2024 sprijină indirect implementarea altor cerințe ale AI Act:

- **Articolul 14, Supravegherea umană.** Anexa B din 23894, în secțiunea despre factorul uman, descrie riscurile asociate interacțiunii om-mașină: încredere excesivă în sistem (automation bias), încredere insuficientă, oboseală decizională, lacune de competență.
- **Articolul 15, Acuratețe, robustețe, securitate cibernetică.** Tratate ca surse de risc în Anexa B și ca obiective organizaționale în Anexa A din 23894.
- **Articolul 26 alineatul (5), Monitorizarea funcționării.** Operaționalizată prin Clauza 6.6 (monitorizare și revizuire) din 23894.
- **Articolul 72, Monitorizarea post-piață.** Acoperită de aceeași Clauză 6.6 și completată de Clauza 6.7 (înregistrare și raportare).

## 4.7. Sinteza relației 23894 cu AI Act

Relația dintre SR EN ISO/IEC 23894:2024 și AI Act poate fi rezumată astfel: regulamentul stabilește ce trebuie făcut, ghidul descrie cum poate fi făcut. Niciun text al regulamentului nu impune folosirea acestui ghid specific. Articolul 40 al AI Act prevede prezumția de conformitate pentru sistemele care respectă standardele armonizate, iar procesul de armonizare formală a standardelor IA este în desfășurare prin CEN-CENELEC JTC 21. Până la finalizarea acestui proces, organizațiile care folosesc 23894 ca metodă pentru implementarea Articolului 9 demonstrează diligență și aliniere la cele mai bune practici internaționale. Acesta este criteriul folosit de auditori și de autoritățile de supraveghere atunci când evaluează conformitatea.

Pentru un implementator care nu intră sub Articolul 9, deci care nu operează sisteme cu grad ridicat de risc, ghidul 23894 rămâne util ca instrument voluntar pentru documentarea riscurilor reziduale ale sistemelor IA achiziționate și pentru demonstrarea diligenței față de partenerii contractuali și clienți.

**Distincția „ce” și „cum” are o rațiune juridică profundă.** Regulamentele europene sunt instrumente legale stabile, modificate doar prin proceduri legislative complexe care durează ani. Standardele tehnice, în schimb, sunt revizuite ciclic de organisme specializate, urmărind evoluția tehnologică fără să ceară reaprobarea Parlamentului European. Această separare permite cadrul european să rămână relevant într-un domeniu, IA, unde generațiile tehnologice se succedă rapid. O ediție viitoare a SR EN ISO/IEC 23894 va putea integra noi tipuri de risc (modele de uz general, sisteme agentice, integrări



biologice) fără să ceară modificarea Articolului 9. Această arhitectură de „cadru juridic stabil + metodologii actualizabile” este una dintre alegerile de design cele mai mature ale legiuitorului european.

**Prezumția de conformitate prevăzută de Articolul 40 are consecințe operaționale concrete.** Atunci când standardele IA vor fi armonizate formal (publicate în Jurnalul Oficial al Uniunii Europene cu mențiunea „standard armonizat”), o organizație care le respectă va beneficia de prezumția legală că îndeplinește cerințele relevante ale AI Act. Aceasta nu înseamnă că auditorii sau autoritățile nu mai pot verifica conformitatea, ci că sarcina probei se inversează: organizația trebuie să demonstreze că respectă standardul, nu să demonstreze că respectă fiecare articol al regulamentului separat. Diferența este semnificativă în controale, în litigii și în due diligence-ul de furnizor. Până când armonizarea formală se va finaliza, organizațiile care aplică SR EN ISO/IEC 23894:2024 nu beneficiază de prezumția legală, dar beneficiază de un argument de diligență recunoscut internațional.

**„Diligența și alinierea la cele mai bune practici internaționale” este un standard juridic concret, nu o formulă generală.** În cazul unui control sau al unui litigiu, autoritățile și instanțele evaluează dacă organizația a acționat ca un operator prudent, raportat la practicile recunoscute la nivel internațional. Folosirea unui standard ISO recunoscut transformă conduita organizației din una „personală” în una aliniată la consensul profesional global. În practică, aceasta înseamnă reducerea expunerii la sancțiuni, a costurilor de apărare în litigii și a exigențelor de probare în controale. Pentru asigurători, alinierea la standarde internaționale poate avea efect direct asupra primelor de asigurare pentru răspunderea profesională sau pentru cyber-risk.

**Implementatorul fără obligație legală directă este o categorie mai largă decât pare.** AI Act este construit ca o piramidă de obligații aplicabile diferențiat pe categorii de risc, dar în practică majoritatea organizațiilor europene nu operează sisteme IA cu grad ridicat de risc. Pentru această categorie, ghidul SR EN ISO/IEC 23894:2024 este utilă din mai multe motive complementare. Primul este protecția reputațională: documentarea proactivă a riscurilor sistemelor IA achiziționate de la terți reduce expunerea în cazul unui incident. Al doilea este pregătirea pentru evoluții viitoare ale regulamentului european, care va integra probabil noi categorii de sisteme în zona de risc ridicat în următorii ani. Al treilea, și poate cel mai important comercial, este capacitatea de a răspunde cu dovezi concrete cerințelor de due diligence ale clienților corporativi, care încep deja să introducă în caietele de sarcini referințe explicite la guvernarea IA. Pentru aceste organizații, SR EN ISO/IEC 23894 nu este o cerință legală, ci un instrument competitiv.

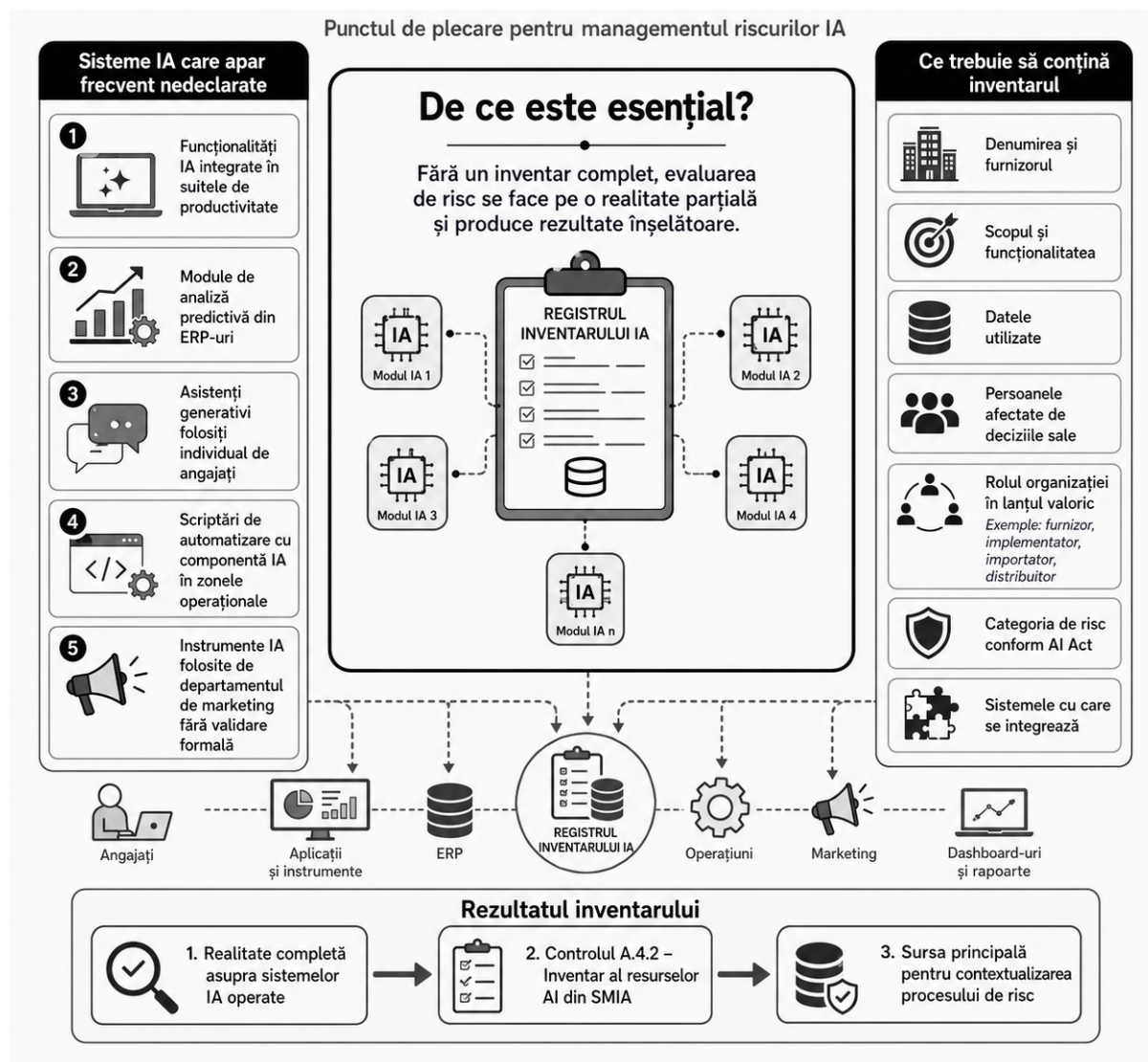
#### Caseta 4. Tabelul de mapare ca instrument de audit

În proiectele de implementare SMIA, tabelul de mapare AI Act → SR ISO/IEC 42001 → SR EN ISO/IEC 23894 este un document distinct, întreținut pe tot parcursul proiectului și prezentat auditorilor în prima zi a auditului de certificare. Tabelul accelerează semnificativ evaluarea de către auditori și demonstrează maturitatea metodologică a sistemului. Pentru organizațiile care operează atât ca furnizori, cât și ca implementatori de sisteme IA, tabelul se construiește în două variante: una pentru cerințele aplicabile rolului de furnizor, alta pentru cele aplicabile rolului de implementator.

## Capitolul 5. Implementarea practică a standardului

### 5.1. Punctul de intrare: inventarul sistemelor IA

Înainte de orice metodologie de risc, organizația trebuie să știe ce sisteme IA operează. Această afirmație pare banală, dar este, în practică, etapa cea mai des subestimată în proiectele de implementare.



Inventarul inițial, atunci când este realizat sistematic, scoate la iveală în mod constant sisteme IA pe care conducerea nu le declarase formal:

- funcționalități IA integrate în suitele de productivitate;
- module de analiză predictivă din ERP-uri;
- asistenți generativi folosiți individual de angajați;
- scriptări de automatizare cu componentă IA în zonele operaționale;

- instrumente IA folosite de departamentul de marketing fără validare formală.

Fără un inventar complet, evaluarea de risc se face pe o realitate parțială și produce rezultate înșelătoare.

Inventarul trebuie să surprindă, pentru fiecare sistem IA: denumirea și furnizorul, scopul și funcționalitatea, datele utilizate, persoanele afectate de deciziile sale, rolul organizației în lanțul valoric (furnizor, implementator, importator, distribuitor), categoria de risc conform AI Act, sistemele cu care se integrează. Acest inventar devine ulterior controlul A.4.2 Inventar al resurselor AI din SMIA și sursa principală pentru contextualizarea procesului de risc.

## 5.2. Etapele procesului, conform Clauzei 6 din 23894

**Standardul descrie procesul de management al riscurilor IA în șase componente. În implementare, acestea se traduc într-o succesiune operațională detaliată mai jos.**

### 5.2.1. Comunicare și consultare

**Stabilirea părților interesate interne și externe** care trebuie implicate în procesul de risc IA: management, echipe tehnice, juridic, conformitate, securitate, resurse umane, reprezentanții angajaților, în anumite cazuri și utilizatorii afectați. Comunicarea și consultarea nu sunt o etapă inițială separată, ci o componentă transversală care însoțește toate celelalte etape ale procesului.

### 5.2.2. Stabilirea scopului, contextului și criteriilor

Aici se decide **ce intră în scope** (toate sistemele, doar cele cu risc ridicat, doar cele dezvoltate intern), care este contextul extern (cadrul de reglementare, așteptările părților interesate, presiunea contractuală) și intern (strategia organizațională, apetitul de risc, resursele disponibile), și care sunt criteriile de risc.

**Criteriile de risc reprezintă decizia cea mai importantă din întreg procesul.** O organizație care folosește criterii prea permissive va declara „risc acceptabil” situații care, în fapt, sunt expuneri majore. O organizație cu criterii prea stricte va trata exhaustiv riscuri marginale și va consuma resurse fără valoare adăugată.

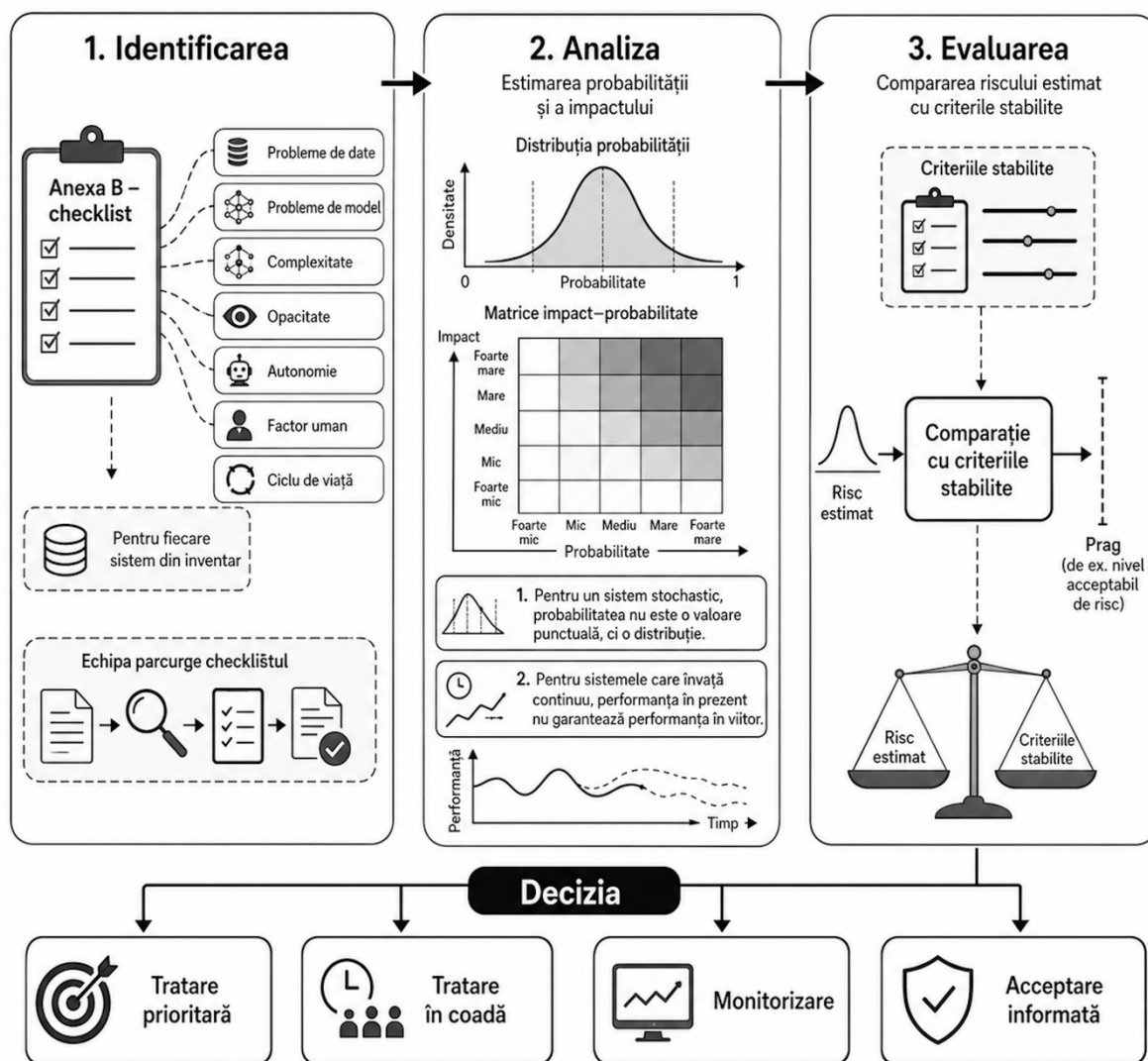
### 5.2.3. Evaluarea riscurilor

**Evaluarea riscurilor cuprinde trei subetape:**

**Identificarea** folosește, ca punct de plecare, Anexa B a standardului ca checklist de surse de risc IA. Pentru fiecare sistem din inventar, echipa parcurge categoriile: probleme de date, probleme de model, complexitate, opacitate, autonomie, factor uman, ciclu de viață.

**Analiza** estimează probabilitatea și impactul, ținând cont de specificul IA. Pentru un sistem stochastic, probabilitatea nu este o valoare punctuală, ci o distribuție. Pentru sistemele care învață continuu, performanța în prezent nu garantează performanța în viitor.

**Evaluarea propriu-zisă** compară riscul estimat cu criteriile stabilite și produce decizia: tratare prioritara, tratare în coadă, monitorizare, acceptare informată.



#### 5.2.4. Tratarea riscurilor

Standardul reia opțiunile clasice din ISO 31000 (evitare, modificare a probabilității sau impactului, transfer, păstrare informată) și le adaptează la IA. Pentru sistemele IA, modificarea probabilității sau impactului trece prin măsuri specifice:

- îmbunătățirea calității datelor de antrenament;
- ajustarea modelului;
- introducerea de garduri (guardrails) tehnice și procedurale;

- adăugarea unei verificări umane între ieșirea sistemului și acțiunea efectivă;
- monitorizarea continuă a parametrilor de performanță.

Planul de tratare documentează măsurile, responsabilii, termenele și riscul rezidual estimat.

### 5.2.5. Monitorizarea și revizuirea

Pentru sistemele IA, această componentă este distinctă față de aproape orice alt context. Monitorizarea nu se limitează la verificarea aplicării măsurilor de control, ci urmărește indicatori specifici:

- drift al datelor de intrare;
- drift al performanței modelului;
- rata de fals pozitiv și fals negativ;
- incidente raportate;
- feedback al utilizatorilor și al persoanelor afectate.

Revizuirea procesului se face cel puțin anual, dar și ad-hoc la modificări semnificative ale sistemului, ale contextului de utilizare sau ale cadrului de reglementare.

### 5.2.6. Înregistrare și raportare

Toate deciziile, evaluările și acțiunile se documentează. Standardul nu prescrie formate, dar enumeră elementele minime: scopul evaluării, data, statutul, gradul de îndeplinire a obiectivelor. În arhitectura SMIA, aceste înregistrări devin documentele cerute de domeniul A.5 din Anexa A 42001 și răspund cerinței de la Articolul 9 alineatul (1) AI Act privind documentarea procesului.

## 5.3. Integrarea procesului 23894 în arhitectura SMIA

Procesul descris în SR EN ISO/IEC 23894:2024 nu este un proces izolat, ci se integrează în arhitectura mai largă a unui Sistem de Management al Inteligenței Artificiale construit pe SR ISO/IEC 42001:2024. Integrarea se face la nivelul documentelor concrete care alcătuiesc sistemul.

**De ce integrarea este o cerință structurală, nu o opțiune.** SR ISO/IEC 42001:2024 cere, în clauza 6.1, instituirea unui proces de evaluare și tratare a riscurilor IA, dar nu detaliază metoda. Standardul lasă organizațiilor libertatea de a alege cum se construiește acest proces, cu condiția să fie documentat, repetabil și auditabil. SR EN ISO/IEC 23894:2024 oferă tocmai metoda care răspunde acestor criterii. Fără integrare, organizația va trebui să dezvolte de la zero o metodologie echivalentă, ceea ce este posibil, dar nepragmatic. Cu integrare, ieșirile procesului 23894 alimentează direct controalele cerute de Anexa A a standardului 42001, în special domeniile A.5 (Evaluarea impactului) și A.6 (Ciclul de viață al sistemelor AI). Această alimentare directă este chiar conexiunea care transformă două documente separate într-un sistem coerent.



Cele șase componente ale procesului 23894 alimentează un set de documente specifice ale SMIA. Tabelul de mai jos sintetizează această corespondență, exemplificată cu documente tipice ale unei implementări mature:

Componenta procesului SR EN ISO/IEC 23894:2024	Document SMIA corespunzător
Comunicare și consultare (Clauza 6.2)	Planul de comunicare IA
Stabilirea contextului și criteriilor (Clauza 6.3)	Criteriile de risc IA
	Procedura de evaluare a riscurilor IA
Evaluarea riscului (Clauza 6.4)	Procedura de evaluare a impactului sistemului IA
	Registrul riscurilor IA
	Rapoartele de evaluare a riscurilor IA
Tratarea riscului (Clauza 6.5)	Procedura de tratare a riscurilor IA
	Planul de tratare a riscurilor IA
Monitorizarea și revizuirea (Clauza 6.6)	Procedurile de monitorizare a sistemelor IA
Înregistrare și raportare (Clauza 6.7)	Rapoartele periodice către management

**O precizare importantă despre tabel.** Lista de documente prezentată este un model exemplificativ, nu o listă exhaustivă. Numărul exact și denumirile concrete ale documentelor variază în funcție de mărimea organizației, de complexitatea sistemelor IA operate și de existența altor sisteme de management cu care SMIA se integrează. O organizație mică poate consolida mai multe documente într-unul singur, de exemplu, „Procedura de management al riscurilor IA” care acoperă simultan evaluarea, tratarea și monitorizarea. O organizație mare poate diviza un singur document în mai multe versiuni specializate pe categorii de sisteme, de exemplu, registre separate pentru sistemele dezvoltate intern, achiziționate prin furnizori, integrate prin API-uri terțe. Principiul nu este numărul de documente, ci acoperirea completă și verificabilă a cerințelor procesului.

Această configurație face parte dintr-un nucleu mai larg de aproximativ 60 de documente care alcătuiesc un SMIA matur, structurate pe șapte faze de implementare. Fazele acoperă pregătirea proiectului, diagnosticarea și definirea scope-ului, construirea fundamentelor sistemului, gestionarea riscurilor și a evaluărilor de impact, implementarea controalelor operaționale, operaționalizarea și pregătirea pentru auditul de certificare. Fiecare fază produce un set de livrabile concrete, validate de comitetul intern al proiectului înainte de a se trece la faza următoare. Această structurare în faze are două avantaje practice: produce un calendar realist al proiectului, de obicei șase până la zece luni pentru o organizație de dimensiune medie, și permite ajustarea ritmului de implementare în funcție de capacitatea echipei interne de a absorbi schimbarea.

**Trei principii metodologice asigură coerența arhitecturii.** Primul este dubla trasabilitate document-cerință, principiu detaliat în Caseta 3 din Capitolul 3. Al doilea este integrarea cu sistemele de management existente, prin care procedurile transversale (control al documentelor, audit intern, acțiuni corective) rămân unice, iar politicile tematice se aliniază sub o politică-umbrelă de management integrat. Al treilea este focalizarea pe evaluarea impactului ca element diferențiator al SMIA față de alte sisteme de management, principiu detaliat în Caseta 7 din Capitolul 7. Detaliile complete ale structurii de implementare, inclusiv ordinea exactă de construcție a documentelor și dependențele dintre ele, sunt prezentate în metodologia de implementare SMIA aplicată în proiectele de consultanță descrise pe [ioniordache.com](http://ioniordache.com).

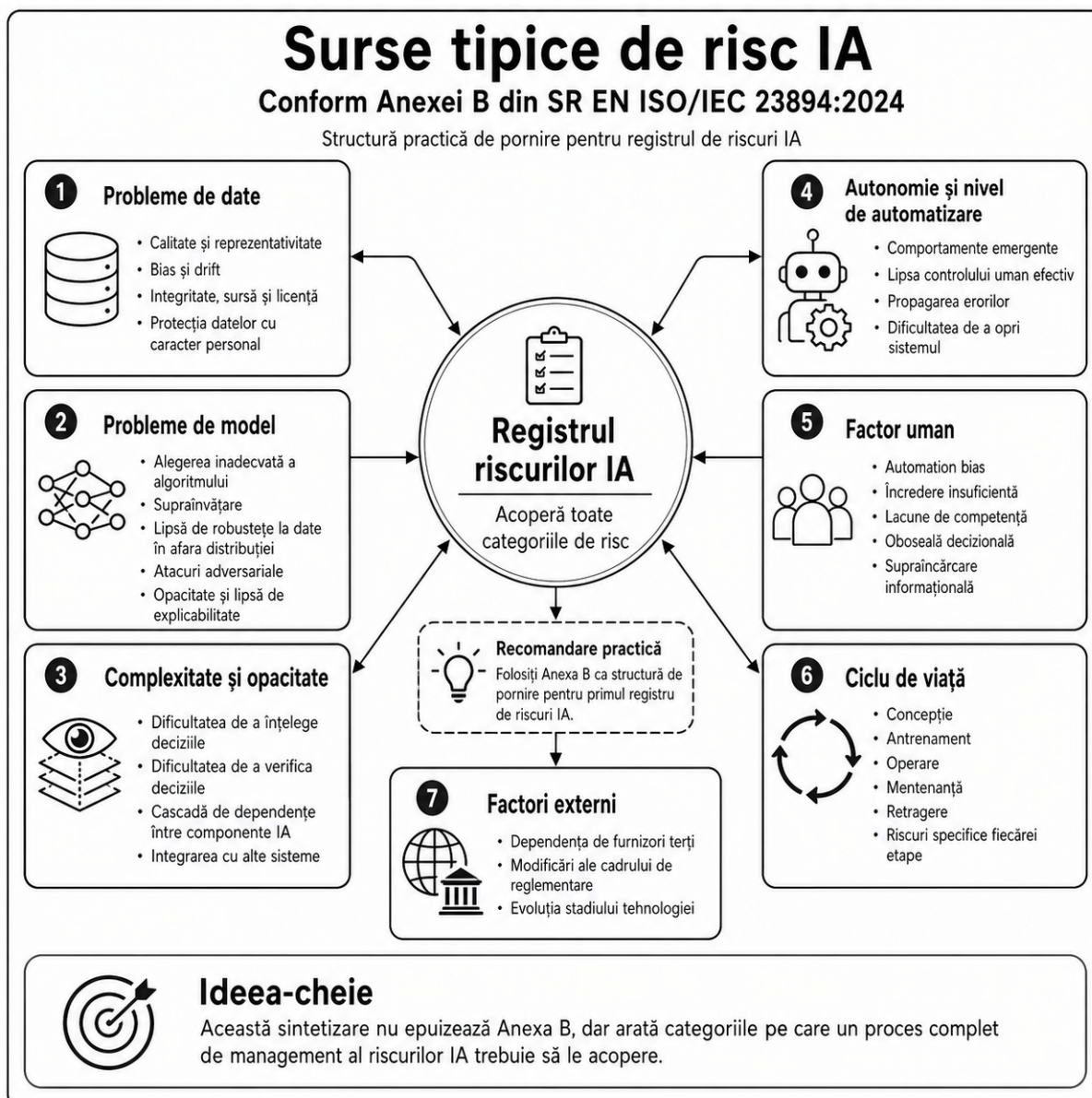
## 5.4. Surse tipice de risc IA, conform Anexei B

Pentru o echipă care construiește pentru prima dată un registru de riscuri IA, recomandarea practică este să folosească Anexa B din 23894 ca structură de pornire.

Categoriile principale ale Anexei B sunt:

- **Probleme de date:** calitatea, reprezentativitatea, biasul, drift-ul, integritatea, sursa și licența, conformitatea cu cerințele de protecție a datelor cu caracter personal.
- **Probleme de model:** alegerea inadecvată a algoritmului, supraînvățarea, lipsa de robustețe la date în afara distribuției, vulnerabilitatea la atacuri adversariale, opacitatea, lipsa explicabilității.
- **Complexitate și opacitate:** dificultatea de a înțelege și a verifica deciziile sistemului, cascadă de dependențe între componente IA, integrarea cu alte sisteme.
- **Autonomie și nivel de automatizare:** comportamente emergente, lipsa controlului uman efectiv, propagarea erorilor, dificultatea de a opri sistemul în caz de funcționare nedorită.
- **Factor uman:** automation bias (încredere excesivă), încredere insuficientă, lacune de competență, oboseală decizională, supraîncărcare informațională.
- **Ciclu de viață:** riscuri specifice fiecărei etape, de la concepție și antrenament până la operare, mentenanță și retragere.
- **Factori externi:** dependența de furnizori terți, modificări ale cadrului de reglementare, evoluția stadiului tehnologiei.

Această sintetizare nu epuizează Anexa B, dar oferă imaginea categoriilor pe care un proces complet de management al riscurilor IA trebuie să le acopere.



### 5.5. Integrarea cu sistemele de management existente

Organizațiile care au deja certificări ISO 9001, ISO/IEC 27001, ISO 22301, ISO/IEC 27701 sau alte sisteme de management dispun de o infrastructură care poate susține implementarea standardelor 23894 și 42001 cu efort marginal, nu prin reconstrucție completă.

Procedurile transversale rămân unice: control al documentelor, audit intern, acțiuni corective, analiză efectuată de management, comunicare internă. Politicile tematice rămân distincte, dar se aliniază sub o politică-umbrelă de management integrat. Criteriile de risc se calibrează astfel încât registrele de risc să fie comparabile între sisteme. Auditurile interne se pot integra într-un program comun.

Pentru organizațiile fără sisteme de management certificate anterior, implementarea pornește de la zero, dar are avantajul că structura se construiește direct pentru IA, fără adaptări forțate ale unor cadre concepute pentru alte tipuri de risc.

## 5.6. Formatul livrabilelor

Procesul descris în 23894 produce, într-o implementare matură, următoarele documente principale:

- politica și procedura de management al riscurilor IA;
- metodologia de evaluare a riscurilor IA, inclusiv criteriile de risc;
- registrul de riscuri IA (un registru consolidat sau registre per sistem);
- rapoartele de evaluare a impactului (asupra organizației, asupra persoanelor, asupra societății);
- planul de tratare a riscurilor;
- registrul deciziilor de acceptare a riscurilor reziduale;
- procedura și înregistrările de monitorizare și revizuire;
- raportarea periodică către management.

Toate aceste documente se reflectă, în arhitectura SMIA, în clauza 6.1 și în controalele Anexei A din domeniile A.5 (Evaluarea impactului) și A.6 (Ciclul de viață al sistemelor IA).

### Caseta 5. Criteriile de risc, decizia care determină tot procesul

În metodologia de implementare SMIA, Criteriile de risc IA sunt formalizate ca prim document al fazei de gestionare a riscurilor, înaintea oricărei evaluări concrete. Decizia este preluată din observația practică: organizațiile care construiesc criteriile pe parcurs ajung la registre de risc inconsistente, cu evaluări care nu rezistă la audit. Criteriile se formulează prin decizia conducerii executive, cu validarea echipei de specialitate IA, și se documentează formal înainte de orice clasificare a riscurilor identificate.

## Capitolul 6. Erori frecvente și ce să eviți

Cinci capcane apar constant în pregătirea organizațiilor pentru AI Act sau pentru certificarea SMIA. Niciuna nu este teoretică, toate au consecințe operaționale măsurabile. La acestea se adaugă o eroare de proces, suficient de gravă încât merită capitol distinct.

### 6.1. Confuzia între 23894 (ghid) și 42001 (sistem certificabil)

Standardele se comportă diferit. SR EN ISO/IEC 23894:2024 oferă recomandări metodologice și nu poate face obiectul unui certificat de conformitate. SR ISO/IEC 42001:2024 conține cerințe auditabile și se certifică de un organism acreditat.

**O organizație care declară „suntem certificați 23894” comunică o eroare**, fie din neînțelegere, fie din intenție de a induce în eroare partenerii. Auditurile de certificare verifică sistemul de management 42001, iar 23894 apare doar ca referință metodologică în interiorul acestuia. La rândul ei, o ofertă comercială de „certificare 23894” este un semnal că furnizorul nu cunoaște diferența elementară dintre un standard certificabil și un ghid metodologic.

Această distincție trebuie să fie clară pentru conducerea executivă, mai ales în comunicarea cu partenerii contractuali. Dovezile de conformitate cerute în due diligence-ul de furnizor sunt de două tipuri:

- certificate emise de organisme acreditate (pentru 42001);
- documentația de proces și înregistrările care demonstrează aplicarea metodologiei (pentru 23894).

Cele două nu se substituie. O organizație matură deține ambele.

### 6.2. Tratarea Articolului 27 (FRIA) ca obligație generală a tuturor implementatorilor

Evaluarea impactului asupra drepturilor fundamentale, prevăzută de Articolul 27 din AI Act, are domeniul de aplicabilitate strict definit:

- organisme de drept public;
- organisme private care prestează servicii publice;
- anumiți operatori privați din domeniile listate în Anexa III pct. 5 lit. (b) și (c).

O companie privată care folosește un sistem IA cu grad ridicat de risc, dar care nu se încadrează în aceste categorii, nu are obligația FRIA. Are însă alte obligații de evaluare a impactului, derivate din Articolul 9, din Articolul 26 și din SR ISO/IEC 42001:2024 (controlul A.5.4 Raport de evaluare a impactului asupra persoanelor).



Confuzia generează două tipuri de erori opuse, ambele costisitoare:

- **Supraconformare**, organizații care nu intră sub Articolul 27 alocă resurse pentru elaborarea unei FRIA pe care nu o au obligație să o producă, în timp ce alte cerințe efective rămân neacoperite.
- **Subconformare**, organizații care intră sub Articolul 27 nu produc FRIA explicit, mizând pe rapoartele generale de evaluare a impactului, care nu satisfac cerințele specifice ale articolului.

Decizia despre aplicabilitatea FRIA trebuie luată în faza de diagnostic a proiectului de implementare, pe baza unei analize juridice clare a categoriei de implementator.

### 6.3. Ignorarea Anexei B din 23894

Anexa B este sursa cea mai operațională a întregului standard, dar este tratată ca informativă și frecvent omisă în implementări. Consecințele se manifestă în două zone:

**În registrul de riscuri.** Registrul construit pe categorii preluate din evaluări de risc generice, fără specificul IA, omite categorii esențiale: drift al modelului, bias de etichetare, atacuri adversariale, comportament emergent al sistemelor cu autonomie crescută. La auditul de certificare, această lipsă apare ca slăbiciune metodologică majoră a procesului 6.1 din SMIA.

**În rapoartele de evaluare a impactului.** Anexa B furnizează cadrul de identificare a riscurilor pentru persoanele afectate. Fără acest cadru, rapoartele tind să descrie generic „riscuri reputaționale” sau „riscuri operaționale”, fără să capteze specificul IA: discriminare prin bias algoritmic, lipsa de transparență a deciziei, dificultatea de contestare a unei decizii automate.

Recomandarea practică este simplă: Anexa B se folosește, în orice implementare matură, ca structură de bază a registrului de riscuri și ca listă de verificare pentru rapoartele de impact.

### 6.4. Construirea unui registru de risc IA paralel cu cel de securitate cibernetică

Riscurile sistemelor IA se intersectează în proporție semnificativă cu riscurile de securitate a informației:

- confidențialitatea datelor de antrenament;
- integritatea modelelor;
- atacurile adversariale;
- scurgerile prin extragere de model (model extraction attacks);
- vulnerabilitățile lanțului de aprovizionare software.

Un registru separat duce la dublarea muncii, la inconsistențe în clasificarea aceluiași risc și la dificultăți de coordonare între echipele responsabile.

Recomandarea practică: registrul de riscuri IA se construiește ca extensie a registrului de risc cibernetic existent, cu marcare distinctă a categoriilor specifice IA și cu metodologie comună de evaluare. Această abordare valorifică investiția deja făcută în cadrul ISO/IEC 27001 sau echivalent și păstrează coerența managementului riscurilor la nivelul întregii organizații.

Pentru organizațiile fără un registru de risc cibernetic existent, implementarea SMIA devine ocazia construirii ambelor cadre simultan, cu economii semnificative de efort.

## 6.5. Confuzia între evaluarea de risc generică, DPIA și FRIA

Trei instrumente distincte sunt frecvent confundate sau folosite interșanjabil, deși acoperă scopuri diferite:

- **Evaluarea de risc IA**, conform SR EN ISO/IEC 23894:2024, identifică riscurile pentru organizație, pentru persoane și pentru societate, ca proces continuu pe ciclul de viață al sistemului.
- **DPIA (Data Protection Impact Assessment)**, conform Articolului 35 GDPR, evaluează riscurile pentru drepturile și libertățile persoanelor vizate de prelucrarea datelor cu caracter personal.
- **FRIA (Fundamental Rights Impact Assessment)**, conform Articolului 27 AI Act, evaluează impactul specific asupra drepturilor fundamentale al utilizării unui sistem IA cu grad ridicat de risc de către anumite categorii de implementatori.

Cele trei se completează, dar nu se substituie. O organizație care folosește FRIA ca DPIA, sau invers, expune lacune procedurale care apar la primul control al unei autorități competente.

Pentru o organizație care operează simultan sub GDPR și AI Act, cele trei instrumente trebuie articulate într-un cadru integrat de evaluare a impactului, cu interfețe explicite între ele și cu trasabilitate între ieșirile fiecăruia.

## 6.6. Eroarea de proces: amânarea implementării

La cele cinci erori de fond se adaugă o eroare de proces, frecventă și costisitoare: amânarea implementării până la apropierea termenului-limită.

AI Act se aplică pe deplin începând cu 2 august 2026, dar construirea unui SMIA matur, integrarea metodologiei 23894 și producerea înregistrărilor operaționale necesare pentru un audit credibil cer, în cele mai bune scenarii, șase până la zece luni de proiect, plus încă două-trei luni pentru auditul de certificare propriu-zis.

Organizațiile care încep implementarea în trimestrul al doilea al anului 2026 vor opera, în practică, prin mijloace tranzitorii la momentul aplicării regulamentului și vor întâlni dificultăți reale în primele exerciții de demonstrare a conformității, fie în controale ale autorității de supraveghere a pieței, fie în due diligence-uri ale clienților corporativi.

Calendarul recomandat, pentru o implementare matură care permite și auditul de certificare înainte de 2 august 2026, este începerea proiectului în primul trimestru al anului 2026 cel târziu. Pentru organizațiile care au depășit deja această fereastră, abordarea pragmatică este construirea sistemului în paralel cu operarea sub mijloace tranzitorii, cu prioritizarea documentelor cu impact direct la audit și cu controale.

#### **Caseta 6. Refuzul șabloanelor copy-paste**

În proiectele de implementare SMIA, refuzul șabloanelor copy-paste este un principiu nenegociabil. Documentația descărcată de pe internet sau generată de modele de limbaj fără adaptare reală este identificată rapid de auditorii experimentați și generează constatări majore. Politica IA a unei organizații, în special, trebuie să reflecte deciziile strategice asumate ale conducerii, nu fraze generice. Documentele SMIA sunt instrumente de lucru ale organizației, nu hârtii destinate exclusiv momentului auditului.

## Capitolul 7. Recomandări operaționale și concluzii

### 7.1. Triada de standarde, raportată la AI Act

Triada SR EN ISO/IEC 22989:2023, SR EN ISO/IEC 23894:2024 și SR ISO/IEC 42001:2024, raportată la cerințele AI Act, oferă în acest moment cadrul cel mai complet și mai coerent pentru o organizație europeană care vrea să opereze inteligența artificială în mod responsabil și conform.

Cele trei standarde nu sunt opțiuni alternative, ci piese complementare ale aceluiași mecanism:

- **22989** oferă vocabularul comun;
- **23894** oferă metoda de management al riscurilor;
- **42001** oferă sistemul de management certificabil.

Deasupra acestei triade, AI Act stabilește obligațiile legale care fac din această arhitectură nu doar o alegere strategică, ci o cerință de conformitate pentru operatorii sistemelor IA cu grad ridicat de risc.

### 7.2. Locul SR EN ISO/IEC 23894:2024 în arhitectură

Dintre cele trei standarde, SR EN ISO/IEC 23894:2024 are statutul cel mai discret. Nu se certifică, nu generează vizibilitate comercială, nu apare pe siglele de conformitate. Este un ghid metodologic, atât și nimic mai mult. Tocmai acest statut face ca utilitatea lui să fie frecvent subevaluată în deciziile strategice.

În realitate, fără procesul descris în 23894, cerința de la clauza 6.1 a SR ISO/IEC 42001:2024 rămâne un schelet fără motor intern, iar obligația de la Articolul 9 din AI Act rămâne o cerință legală fără metodă recunoscută de implementare. Investiția în adoptarea lui efectivă, nu doar în referința formală din documentație, este una dintre deciziile cu cel mai bun raport efort-rezultat în orice proiect de guvernare IA.

### 7.3. Recomandări diferențiate pe categorii de organizații

#### 7.3.1. Companii care folosesc deja sisteme IA

**Pentru organizațiile care folosesc deja sisteme IA, ca furnizori sau ca implementatori, indiferent dacă au sau nu obligații explicite din AI Act, recomandarea operațională este construirea registrului de riscuri IA pe metoda descrisă în SR EN ISO/IEC 23894:2024.**

Această decizie:

- nu necesită angajament formal de certificare;
- nu generează costuri de audit extern;
- se integrează cu sistemele de management existente;

- produce o imagine completă și structurată a expunerii reale a organizației.

Beneficiul imediat este claritatea strategică, punct de pornire pentru orice decizie ulterioară privind extinderea, modificarea sau retragerea sistemelor IA aflate în uz.

### 7.3.2. Companii sub incidența cerințelor pentru sisteme IA cu grad ridicat de risc

**Pentru organizațiile care intră sub incidența cerințelor pentru sisteme IA cu grad ridicat de risc, prin Articolul 9 din AI Act**, recomandarea este tratarea standardului 23894 ca metodă implicită pentru implementarea acestei cerințe legale.

Argumentul este pragmatic. În absența unui standard armonizat formal, ghidul ISO oferă cea mai solidă bază metodologică pentru a demonstra diligență în fața auditorilor și a autorităților de supraveghere. Construirea unei metodologii proprii, paralelă cu standardul, este posibilă, dar nu produce nicio valoare adăugată și expune organizația la riscul de a fi considerată neconformă cu bunele practici recunoscute internațional.

### 7.3.3. Companii care urmăresc certificarea pe SR ISO/IEC 42001:2024

**Pentru organizațiile care urmăresc certificarea pe SR ISO/IEC 42001:2024**, recomandarea este integrarea standardului 23894 direct în arhitectura SMIA, nu ca referință externă, ci ca metodă internă a clauzei 6.1 și ca sursă pentru documentele cerute de domeniul A.5 din Anexa A.

Această integrare se face natural în faza de gestionare a riscurilor și a evaluărilor de impact a unui proiect de implementare structurat. Produsul integrării este dubla trasabilitate document-cerință, principiu care asigură coerența sistemului în fața auditului de certificare și care permite organizației să demonstreze conformitatea simultan cu standardul și cu regulamentul european.

## 7.4. Decizia care contează cel mai mult

În toate cele trei scenarii, decizia de a începe acum, nu peste șase luni sau peste un an, este mai importantă decât alegerea metodei. AI Act este o realitate care se construiește permanent, nu un termen-limită care expiră, iar avantajul competitiv aparține organizațiilor care intră în 2027 cu un sistem matur, nu cu un proiect de remediere.

Pentru o conducere executivă care evaluează prioritățile strategice ale organizației, întrebarea practică nu este dacă investiția în managementul riscurilor IA se justifică, ci în ce ritm și pe ce calendar se realizează. Răspunsul corect ține cont de complexitatea sistemelor IA operate, de existența altor sisteme de management cu care SMIA se poate integra, de capacitatea echipei interne de a susține un proiect cu durata de șase până la zece luni și de fereastra de timp disponibilă până la primele controale ale autorităților de supraveghere.

Pentru fiecare organizație, răspunsul este specific. Cadrul oferit de cele trei standarde și de AI Act este același. Modul de aplicare este unic.



#### **Caseta 7. Focalizarea pe evaluarea impactului**

În metodologia de implementare SMIA, evaluarea impactului sistemului IA asupra persoanelor și societății este elementul diferențiator cel mai puternic față de alte sisteme de management. Calitatea acestor rapoarte se reflectă direct în credibilitatea SMIA. Rapoartele de impact realizate formal, fără analiză substanțială, sunt identificate rapid de auditorii experimentați și generează constatări majore. Scurtarea acestui pas este cea mai scumpă greșală pe care o poate face o organizație în proiectul de implementare.

## Anexa A. Glosar de termeni

Glosarul de mai jos reunește termenii cheie utilizați pe parcursul ghidului și provenind din SR EN ISO/IEC 22989:2023, SR EN ISO/IEC 23894:2024, SR ISO/IEC 42001:2024 și Regulamentul (UE) 2024/1689. Pentru fiecare termen sunt prezentate denumirea originală în limba engleză, traducerea consacrată în limba română (atunci când există) și explicația în limba română. Sursa fiecărui termen este menționată la sfârșitul definiției, prin referință la documentul în care apare definiția formală.

**AI Act:** Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 privind inteligența artificială. Primul cadru legal complet din lume care reglementează sistemele de inteligență artificială printr-o abordare bazată pe risc. Stabilește obligații diferențiate pentru furnizori, implementatori, importatori și distribuitori, în funcție de categoria de risc a sistemului IA și de rolul în lanțul valoric. *Sursă: Regulamentul (UE) 2024/1689.*

**AI agent / Agent IA:** Entitate automată care percepe mediul în care funcționează și reacționează la acesta, întreprinzând acțiuni pentru atingerea obiectivelor sale. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.1.*

**AI component / Componentă IA:** Element funcțional care intră în compoziția unui sistem IA. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.2.*

**AI lifecycle / Ciclul de viață al sistemului IA:** Succesiunea etapelor prin care trece un sistem IA, de la concepție și proiectare, prin dezvoltare, verificare și validare, implementare, operare și monitorizare, până la retragere. Fiecare etapă generează riscuri specifice care trebuie identificate și tratate ca parte a procesului de management al riscurilor. *Sursă: SR EN ISO/IEC 22989:2023.*

**AI system / Sistem IA:** Sistem ingineresc care generează ieșiri precum conținut, predicții, recomandări sau decizii pentru un set de obiective definite uman. Sistemul utilizează diverse tehnici și abordări specifice inteligenței artificiale pentru a dezvolta un model care reprezintă date, cunoștințe și procese, în vederea îndeplinirii unor sarcini. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.4.*

**AI system impact assessment / Evaluarea impactului sistemului IA:** Proces formal prin care organizația identifică și evaluează impactul unui sistem IA asupra persoanelor, asupra grupurilor de persoane și asupra societății în ansamblu. Reprezintă elementul diferențiator al SR ISO/IEC 42001:2024 față de alte sisteme de management. *Sursă: SR ISO/IEC 42001:2024, controlul A.5.2 și A.5.4.*

**AIMS (Artificial Intelligence Management System) / SMIA (Sistem de Management al Inteligenței Artificiale):** Sistemul de management prin care o organizație stabilește, implementează, menține și îmbunătățește continuu cadrul de guvernanză al sistemelor IA pe care le furnizează sau utilizează. Conform SR ISO/IEC 42001:2024, SMIA este construit pe structura armonizată a sistemelor de management ISO. *Sursă: SR ISO/IEC 42001:2024.*

**Adversarial attack / Atac adversarial:** Atac asupra unui sistem IA prin care intrările sunt modificate intenționat, adesea în moduri imperceptibile pentru observatorul uman, pentru a induce sistemul în eroare și a-l determina să producă ieșiri incorecte sau dăunătoare. Sursă majoră de risc identificată în Anexa B din SR EN ISO/IEC 23894:2024.

**Annex III / Anexa III:** Anexa la AI Act care listează domeniile în care sistemele IA sunt clasificate ca având grad ridicat de risc. Acoperă domenii precum biometria, infrastructura critică, educația și formarea profesională, ocuparea forței de muncă, accesul la servicii esențiale private și publice, aplicarea legii, migrația, administrarea justiției și procesele democratice. *Sursă: Regulamentul (UE) 2024/1689, Anexa III.*

**Annex IV / Anexa IV:** Anexa la AI Act care detaliază conținutul minim al documentației tehnice obligatorii pentru sistemele IA cu grad ridicat de risc. Include descrierea sistemului, descrierea elementelor sale, monitorizarea, măsurile de gestionare a riscurilor și alte elemente. *Sursă: Regulamentul (UE) 2024/1689, Anexa IV.*

**Automation bias:** Tendința operatorilor umani de a acorda încredere excesivă deciziilor sau recomandărilor unui sistem automatizat, chiar și atunci când dovezile contrare sunt disponibile. Risc semnificativ în contextul sistemelor IA care sprijină decizii umane în domenii sensibile. *Sursă: SR EN ISO/IEC 23894:2024, Anexa B.*

**Autonomy / Autonomie:** Caracteristica unui sistem capabil să își modifice domeniul de utilizare preconizat sau scopul fără intervenție, control sau supraveghere externă. Diferită de automatizare, care presupune funcționarea fără intervenție umană doar în condiții specificate. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.5.*

**Bias / Bias (părtinire sistematică):** Eroare sistematică care afectează ieșirile unui sistem IA, generând decizii care defavorizează anumite categorii de persoane sau de date. Poate avea origini multiple: date de antrenament nereprezentative, etichetare incorectă, alegerea inadecvată a modelului, contextul de utilizare. *Sursă: SR EN ISO/IEC 23894:2024, Anexa B.*

**Continuous learning / Învățare continuă:** Antrenare incrementală a unui sistem IA care are loc continuu pe parcursul fazei de operare a ciclului de viață. Generează riscuri specifice de drift al performanței, care necesită monitorizare continuă. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.9.*

**Deployer / Implementator:** Persoană fizică sau juridică, autoritate publică, agenție sau alt organism care utilizează un sistem IA sub propria autoritate, cu excepția cazului în care sistemul este folosit în cadrul unei activități personale neprofesionale. Implementatorul are obligații proprii, distincte de cele ale furnizorului, conform Articolelor 26 și 27 din AI Act. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 4.*

**Distributor / Distribuitor:** Persoană fizică sau juridică din lanțul de aprovizionare, alta decât furnizorul sau importatorul, care pune la dispoziție un sistem IA pe piața Uniunii. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 7.*

**DPIA (Data Protection Impact Assessment) / Evaluarea impactului asupra protecției datelor:**

Evaluare formală a riscurilor pentru drepturile și libertățile persoanelor vizate de prelucrarea datelor cu caracter personal. Obligatorie în anumite cazuri conform Articolului 35 din Regulamentul General privind Protecția Datelor (RGPD). Distinctă de FRIA și de evaluarea de risc IA. *Sursă: Regulamentul (UE) 2016/679, Articolul 35.*

**Drift:** Modificare în timp a caracteristicilor datelor de intrare (data drift) sau a performanței modelului (model drift sau concept drift), care poate duce la degradarea acurateții sistemului IA fără semnale evidente. Necesită monitorizare continuă. *Sursă: SR EN ISO/IEC 23894:2024, Anexa B.*

**Explainability / Explicabilitate:** Capacitatea unui sistem IA de a oferi explicații înțelegibile pentru oameni cu privire la deciziile sale. Obiectiv organizațional tipic al sistemelor IA și sursă derivată de risc atunci când este insuficientă. *Sursă: SR EN ISO/IEC 23894:2024, Anexa A.*

**Fairness / Corectitudine (echitate):** Caracteristica unui sistem IA de a trata persoanele și grupurile de persoane fără discriminare nejustificată. Obiectiv organizațional tipic, sursă de risc atunci când este compromisă prin bias. *Sursă: SR EN ISO/IEC 23894:2024, Anexa A.*

**FRIA (Fundamental Rights Impact Assessment) / Evaluarea impactului asupra drepturilor fundamentale:**

Evaluare formală obligatorie pentru anumite categorii de implementatori ai sistemelor IA cu grad ridicat de risc, conform Articolului 27 din AI Act. Acoperă organisme de drept public, organisme private care prestează servicii publice și anumiți operatori privați din domenii specifice. *Sursă: Regulamentul (UE) 2024/1689, Articolul 27.*

**General-purpose AI model / Model de IA de uz general (GPAI):** Model IA care prezintă o generalitate semnificativă și este capabil să îndeplinească în mod competent o gamă largă de sarcini distincte. Tratat separat în AI Act, în Capitolul V. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 63.*

**Generative AI / IA generativă:** Categorie de sisteme IA care generează conținut nou, inclusiv text, imagini, audio, video sau cod, pe baza intrărilor primite. Supusă obligațiilor specifice de transparență prin AI Act.

**Guardrails:** Mecanisme tehnice și procedurale instalate pentru a limita comportamentul unui sistem IA, prevenind ieșiri dăunătoare sau utilizări neintenționate. Măsură tipică de tratare a riscurilor în implementările matur construite.

**High-risk AI system / Sistem IA cu grad ridicat de risc:** Sistem IA care intră în categoriile listate în Anexa III a AI Act sau care reprezintă o componentă de siguranță a unui produs supus legislației de armonizare a Uniunii listată în Anexa I. Supus celui mai extins set de obligații prin regulament. *Sursă: Regulamentul (UE) 2024/1689, Articolele 6-7.*

**Importer / Importator:** Persoană fizică sau juridică stabilită în Uniunea Europeană care introduce pe piața Uniunii un sistem IA având numele sau marca comercială a unei persoane fizice sau juridice stabilite într-o țară terță. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 6.*

**Intended purpose / Scop preconizat:** Utilizarea pentru care un sistem IA este destinat de furnizor, inclusiv contextul și condițiile specifice de utilizare, astfel cum sunt specificate în informațiile furnizate de furnizor. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 12.*

**Machine learning / Învățare automată:** Proces prin care un sistem îmbunătățește performanța unei sarcini prin experiență, fără a fi programat explicit pentru acea sarcină. Subdomeniu al inteligenței artificiale. *Sursă: SR EN ISO/IEC 22989:2023.*

**Model / Model:** Reprezentare construită din date care surprinde aspecte ale realității în scopul efectuării de predicții, clasificări, recomandări sau alte sarcini specifice. Componentă centrală a unui sistem IA. *Sursă: SR EN ISO/IEC 22989:2023, secțiunea 3.1.23.*

**Operator / Operator:** Termen umbrelă care acoperă furnizorii, fabricanții de produse, implementatorii, reprezentanții autorizați, importatorii și distribuitorii. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 8.*

**Post-market monitoring / Monitorizarea post-piață:** Activități sistematice prin care furnizorii colectează și analizează informații despre performanța sistemelor IA cu grad ridicat de risc după introducerea pe piață, în vederea identificării necesității unor acțiuni corective. *Sursă: Regulamentul (UE) 2024/1689, Articolul 72.*

**Prohibited AI practices / Practici IA interzise:** Sisteme și utilizări ale IA considerate incompatibile cu valorile Uniunii Europene, listate exhaustiv în Articolul 5 din AI Act. Includ manipularea subliminală, exploatarea vulnerabilităților, scoring-ul social generalizat, identificarea biometrică în timp real în spații publice (cu excepții limitate) și altele. *Sursă: Regulamentul (UE) 2024/1689, Articolul 5.*

**Provider / Furnizor:** Persoană fizică sau juridică, autoritate publică, agenție sau alt organism care dezvoltă un sistem IA sau un model IA de uz general, sau care a dezvoltat un sistem IA sau un model IA de uz general și îl introduce pe piață sau îl pune în funcțiune sub propriul nume sau propria marcă comercială. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 3.*

**Residual risk / Risc rezidual:** Risc care rămâne după aplicarea măsurilor de tratare. Conform Articolului 9 alineatul (5) din AI Act, riscul rezidual asociat sistemelor IA cu grad ridicat de risc trebuie să fie considerat acceptabil, iar implementatorul trebuie informat explicit despre acesta. *Sursă: Regulamentul (UE) 2024/1689, Articolul 9 alineatul (5).*

**Risk / Risc:** Efectul incertitudinii asupra obiectivelor. În contextul sistemelor IA, riscurile pot fi atât pentru organizația care operează sistemul, cât și pentru persoanele și grupurile afectate de deciziile lui. *Sursă: ISO 31000:2018, preluată de SR EN ISO/IEC 23894:2024.*

**Risk acceptance / Acceptare a riscului:** Decizie informată de a păstra un risc identificat, asumată formal de o persoană cu autoritate decizională în organizație. Documentată ca parte a procesului de management al riscurilor. *Sursă: SR EN ISO/IEC 23894:2024, Clauza 6.5.*



**Risk assessment / Evaluare a riscului:** Proces global care cuprinde identificarea, analiza și evaluarea propriu-zisă a riscurilor. Etapă centrală a procesului descris în Clauza 6.4 din SR EN ISO/IEC 23894:2024. *Sursă: ISO 31000:2018.*

**Risk criteria / Criterii de risc:** Termenii de referință față de care se evaluează semnificația unui risc. Stabilirea criteriilor de risc este una dintre primele decizii în procesul de management al riscurilor și determină rezultatele întregii evaluări. *Sursă: SR EN ISO/IEC 23894:2024, Clauza 6.3.4.*

**Risk management / Management al riscurilor:** Activități coordonate prin care o organizație identifică, evaluează și tratează riscurile. În contextul IA, descris în SR EN ISO/IEC 23894:2024 ca specializare a ISO 31000:2018. *Sursă: ISO 31000:2018.*

**Risk treatment / Tratare a riscului:** Proces de selectare și implementare a opțiunilor pentru gestionarea unui risc identificat: evitare, modificare a probabilității sau impactului, transfer, păstrare informată. *Sursă: SR EN ISO/IEC 23894:2024, Clauza 6.5.*

**Robustness / Robustețe:** Caracteristica unui sistem IA de a-și menține nivelul de performanță în condiții variate, inclusiv în prezența unor date în afara distribuției de antrenament sau a unor perturbații intenționate. Obiectiv organizațional tipic și sursă de risc atunci când este insuficientă. *Sursă: SR EN ISO/IEC 23894:2024, Anexa A.*

**SoA (Statement of Applicability) / Declarație de aplicabilitate:** Document obligatoriu în SMIA care consemnează aplicabilitatea sau neaplicabilitatea fiecărui control din Anexa A a SR ISO/IEC 42001:2024, cu justificarea deciziilor. Piatra unghiulară a auditului de certificare. *Sursă: SR ISO/IEC 42001:2024, Clauza 6.1.4.*

**Stakeholders / Părți interesate:** Persoane sau organizații care pot afecta, pot fi afectate sau se percep ca fiind afectate de o decizie sau activitate. În contextul sistemelor IA, includ persoanele asupra cărora se aplică deciziile sistemului, nu doar utilizatorii direcți. *Sursă: SR EN ISO/IEC 22989:2023.*

**Substantial modification / Modificare substanțială:** Modificare a unui sistem IA după introducerea pe piață, care nu a fost prevăzută de furnizor în evaluarea inițială de conformitate și care afectează conformitatea sistemului cu cerințele AI Act. Generează obligații de reevaluare. *Sursă: Regulamentul (UE) 2024/1689, Articolul 3 punctul 23.*

**Transparency / Transparență:** Caracteristica unui sistem IA de a oferi informații suficiente despre capacitățile și limitările sale, precum și despre logica de funcționare, către utilizatori și persoanele afectate. Obiectiv organizațional și obligație legală pentru anumite categorii de sisteme conform Articolului 50 din AI Act. *Sursă: SR EN ISO/IEC 23894:2024, Anexa A; Regulamentul (UE) 2024/1689, Articolul 50.*

**Use case / Caz de utilizare:** Configurația specifică în care un sistem IA este utilizat, incluzând scopul, contextul, utilizatorii, persoanele afectate și datele procesate. Informează evaluarea de risc și de impact.

## Anexa B. Tabel sintetic de mapare AI Act, SR ISO/IEC 42001:2024 și SR EN ISO/IEC 23894:2024

Tabelul de mai jos sintetizează relația dintre cele mai importante cerințe ale AI Act, controalele și clauzele relevante din SR ISO/IEC 42001:2024 și componentele procesului din SR EN ISO/IEC 23894:2024. Este destinat utilizării ca referință rapidă în proiectele de implementare SMIA și ca instrument de pregătire a auditului de certificare.

Cerință AI Act	Conținut esențial	Clauză / Control SR ISO/IEC 42001:2024	Clauză SR EN ISO/IEC 23894:2024
Articolul 9 alin. (1)	Instituirea sistemului de gestionare a riscurilor	Clauza 6.1	Clauza 5; Clauza 6
Articolul 9 alin. (2)	Proces iterativ continuu pe ciclul de viață	Clauza 6.1, 9.1, 10	Clauza 6 (integral); Anexa C
Articolul 9 alin. (2) lit. (a)	Identificarea riscurilor previzibile	Clauza 6.1	Clauza 6.4.2; Anexa B
Articolul 9 alin. (2) lit. (b)	Estimarea și evaluarea riscurilor	Clauza 6.1	Clauza 6.4.3, 6.4.4
Articolul 9 alin. (2) lit. (c)	Evaluarea riscurilor pe baza datelor post-piață	Clauza 9.1	Clauza 6.6
Articolul 9 alin. (2) lit. (d)	Adoptarea măsurilor de gestionare	Clauza 6.1.4; Anexa A	Clauza 6.5
Articolul 9 alin. (5)	Risc rezidual acceptabil	Clauza 6.1; Anexa A.5	Clauza 6.4.4, 6.5
Articolul 9 alin. (9)	Risc pentru minori și grupuri vulnerabile	Anexa A.5.4	Clauza 6.4.2; Anexa B
Articolul 10	Guvernanța datelor	Anexa A.4.3	Anexa B (probleme de date)
Articolul 11 / Anexa IV	Documentație tehnică	Anexa A.6.2.7	Clauza 6.7
Articolul 13	Transparență față de implementatori	Anexa A.7	Anexa A (obiective)
Articolul 14	Supraveghere umană	Anexa A.9	Anexa B (factor uman)
Articolul 15	Acuratețe, robustețe, securitate cibernetică	Anexa A.6.2.4, A.10	Anexa A; Anexa B
Articolul 16	Obligațiile furnizorului	Clauzele 4-10 (integral)	Clauza 5
Articolul 17	Sistem de management al calității	SMIA integral	Clauza 6
Articolul 26	Obligațiile implementatorului	Anexa A.9, A.7	Clauza 6.6
Articolul 26 alin. (5)	Monitorizarea funcționării	Clauza 9.1	Clauza 6.6
Articolul 27	Evaluarea impactului asupra drepturilor fundamentale (FRIA)	Anexa A.5.4, A.5.5	Clauza 6.3, 6.4.2; Anexa B

Cerință AI Act	Conținut esențial	Clauză / Control SR ISO/IEC 42001:2024	Clauză SR EN ISO/IEC 23894:2024
Articolul 49	Înregistrarea în baza de date a UE	Anexa A.4.2	n/a
Articolul 50	Obligații de transparență (risc limitat)	Anexa A.7	Anexa A
Articolul 72	Monitorizarea post-piață	Clauza 9.1; Anexa A.6.2.6	Clauza 6.6, 6.7

### Note de utilizare a tabelului

- Coloana 3 indică clauza principală sau controlul Anexei A din SR ISO/IEC 42001:2024 unde se materializează cerința. Pentru o mapare completă a tuturor controalelor Anexei A, este necesară consultarea checklist-ului complet de documentație SMIA.
- Coloana 4 indică componenta procesului din SR EN ISO/IEC 23894:2024 care alimentează metodologic cerința. Mențiunea „n/a” apare acolo unde cerința AI Act este pur administrativă (de exemplu, înregistrarea în baza de date UE) și nu are corespondent metodologic în ghidul de management al riscurilor.
- Tabelul este un instrument de orientare. În proiectele concrete, fiecare cerință AI Act se traduce în mai multe documente SMIA, iar trasabilitatea exactă se stabilește la nivelul fiecărei organizații, în funcție de rolul în lanțul valoric și de categoriile de risc ale sistemelor operate.

## Anexa C. Resurse bibliografice și de aprofundare

Pentru o implementare riguroasă a sistemelor de management al riscurilor IA și pentru pregătirea conformității cu AI Act, ghidul de față se completează cu următoarele resurse oficiale și de specialitate.

### Texte oficiale ale standardelor

**Asociația de Standardizare din România (ASRO)**, sursa oficială de procurare a standardelor române identice cu cele europene și internaționale:

- SR EN ISO/IEC 22989:2023 Tehnologia informației. Inteligența artificială. Conceptele și terminologia inteligenței artificiale.
- SR EN ISO/IEC 23894:2024 Tehnologia informației. Inteligența artificială. Ghid privind managementul riscurilor.
- SR ISO/IEC 42001:2024 Tehnologia informației. Inteligență artificială. Sistem de management.
- SR EN ISO 31000:2018 Managementul riscurilor. Linii directoare.

Site oficial: [www.asro.ro](http://www.asro.ro)

### Texte oficiale ale legislației europene

**Portalul EUR-Lex al Uniunii Europene**, sursa oficială pentru textele consolidate ale legislației europene:

- Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 privind inteligența artificială (AI Act). ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>.
- Regulamentul (UE) 2016/679 (RGPD). ELI: <http://data.europa.eu/eli/reg/2016/679/oj>.

### Ghiduri și documente ale instituțiilor europene

**Comisia Europeană / Oficiul pentru IA (AI Office)**, autoritatea europeană responsabilă cu coordonarea aplicării AI Act:

- Ghiduri de aplicare a AI Act, disponibile pe site-ul oficial al Comisiei Europene.
- Cod de bune practici pentru modelele IA de uz general (GPAI Code of Practice).
- Orientări privind elementele sistemului de management al calității pentru microîntreprinderi (în pregătire conform Articolului 63).

**Consiliul European pentru Inteligența Artificială (Consiliul IA)**, organism instituit prin Articolul 65 din AI Act, care emite recomandări și avize privind aplicarea regulamentului.

## Standardizare europeană

**CEN-CENELEC JTC 21** Artificial Intelligence, comitetul tehnic comun responsabil cu armonizarea standardelor europene în domeniul inteligenței artificiale, inclusiv cu lucrările de armonizare formală a SR EN ISO/IEC 23894:2024 și a celorlalte standarde IA în sensul Articolului 40 din AI Act.

Documente publicate de JTC 21 disponibile prin organisme naționale de standardizare ale statelor membre (în România, ASRO).

## Standarde internaționale conexe

Pentru o abordare integrată a managementului riscurilor IA, sunt utile și următoarele standarde internaționale, care se completează reciproc cu cele trei standarde principale din triada IA:

- **ISO 31000:2018** Risk management. Guidelines, cadrul universal de management al riscurilor, pe care SR EN ISO/IEC 23894:2024 îl extinde pentru domeniul IA.
- **ISO/IEC 27001:2022** Information security management systems, frecvent integrat cu SMIA pentru organizațiile care operează sisteme IA cu riscuri semnificative de securitate cibernetică.
- **ISO/IEC 27701:2019** Privacy information management systems, util pentru organizațiile care procesează date cu caracter personal prin sistemele IA.
- **ISO/IEC 38507:2022** Governance implications of the use of artificial intelligence by organizations, oferă perspectiva guvernantei la nivel de board.

## Autorități naționale relevante

**Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, autoritatea română competentă pentru protecția datelor, relevantă pentru intersecția AI Act cu RGPD.

**RENAR (Asociația de Acreditare din România)**, organismul național de acreditare, care acreditează organismele de certificare pentru SR ISO/IEC 42001:2024 în România.

**Autoritatea de supraveghere a pieței pentru AI Act în România**, va fi desemnată conform prevederilor Articolului 70 din regulament. La data publicării acestui ghid, procesul de desemnare este în curs.

## Aprofundare metodologică

Pentru cititorii interesați de modul concret în care procesul descris în SR EN ISO/IEC 23894:2024 se traduce în arhitectura completă a unui SMIA pregătit pentru certificare, pe site-ul [ioniordache.com](https://ioniordache.com) sunt publicate articole de fond despre:

- structura unui proiect de implementare SMIA pe șapte faze.



- ordinea de construcție a documentelor nucleu.
- principiile metodologice de construcție a documentației (dubla trasabilitate, integrarea cu sistemele de management existente, focalizarea pe evaluarea impactului).
- erorile tipice și costurile lor în proiectele de certificare.

Aceste materiale sunt disponibile gratuit și pot fi consultate independent de prezentul ghid.

## Despre autor



**Ion Iordache** este consultant de securitate cu experiență consolidată în domeniile securității fizice, securității informației și conformității cu standardele internaționale de management. Activează ca Lead Implementer și Lead Auditor pe standarde de management ISO, cu specializare în arhitecturi integrate de guvernare care combină mai multe cadre normative într-un sistem coerent pentru organizația beneficiară.

Activitatea profesională acoperă trei direcții principale, complementare. Prima este consultanța de implementare pentru organizații care urmăresc certificarea pe standarde de management precum SR ISO/IEC 42001:2024, ISO/IEC 27001, ISO 22301 și altele, cu accent pe abordarea de co-implementare și pe transferul gradual de competență către echipele interne. A doua este auditul intern și extern, conform metodologiei ISO 19011:2018. A treia este formarea profesională, prin programe de training adresate practicienilor de conformitate, ofițerilor de protecția datelor și managerilor de risc.

În domeniul guvernancei inteligenței artificiale, activitatea curentă se concentrează pe sprijinirea organizațiilor românești în pregătirea pentru aplicarea Regulamentului (UE) 2024/1689 (AI Act), prin implementarea Sistemelor de Management al Inteligenței Artificiale (SMIA) conform SR ISO/IEC 42001:2024. Metodologia de implementare a fost dezvoltată pe baza experienței directe cu organizații din sectoarele financiar, de securitate, tehnologie și sectorul public, și se bazează pe principii nenegociabile precum dubla trasabilitate document-cerință, integrarea cu sistemele de management existente și refuzul șabloanelor copy-paste.

Pe site-ul [ioniordache.com](http://ioniordache.com) sunt publicate articole de fond și materiale de referință privind implementarea standardelor de management, conformitatea cu AI Act, protecția datelor cu caracter personal și securitatea fizică în context contemporan.

### Date de contact:

**Email:** [ion@ioniordache.com](mailto:ion@ioniordache.com)

**Site:** [ioniordache.com](http://ioniordache.com)

**LinkedIn:** [linkedin.com/in/ioniordache](https://www.linkedin.com/in/ioniordache)

**Telefon:** +40 725 631 096

**Iordache Quality Services S.R.L.**

## Cum vă putem ajuta

Implementarea cerințelor AI Act și a standardelor de management al inteligenței artificiale nu este un exercițiu pe care îl poate parcurge o organizație fără sprijin specializat. Standardul oferă cerințele, regulamentul stabilește obligațiile, dar parcursul concret de la diagnostic la certificare cere metodă, experiență și un calendar realist.

În calitate de Lead Implementer și Lead Auditor pe standardele de management relevante, eu și echipa mea, oferim consultanță specializată în implementarea unui Sistem de Management al Inteligenței Artificiale conform SR ISO/IEC 42001:2024, cu integrarea metodologiei SR EN ISO/IEC 23894:2024 pentru clauza 6.1 și acoperirea cerințelor AI Act prin dubla trasabilitate document-cerință.

### Diagnostic inițial gratuit

Prima etapă a oricărei colaborări este un diagnostic inițial gratuit. Evaluăm împreună poziția organizației față de cerințele standardului și ale regulamentului. Inventariem sistemele IA aflate în uz, identificăm rolul organizației în lanțul valoric (furnizor, implementator, importator, distribuitor), stabilim categoriile de risc aplicabile și calibrăm calendarul realist al unei implementări. Diagnosticul nu generează obligații contractuale.

### Ofertă personalizată

Pe baza rezultatelor diagnosticului, construim o ofertă adaptată specificului organizației: complexitatea sistemelor IA operate, existența altor sisteme de management integrabile (ISO 9001, ISO/IEC 27001, ISO 22301), calendarul preferat al conducerii, dimensiunea echipei interne care va susține proiectul.

### Implementarea efectivă a SMIA

Aplicăm o metodologie structurată pe șapte faze, parcurse într-un ritm de aproximativ șase luni pentru o organizație de dimensiune medie. Modelul de lucru este de co-implementare, prin care construim împreună cadrul de guvernare, cu transfer gradual de competență către echipa internă. Obiectivul este ca, după certificare, organizația să poată menține sistemul în mod autonom, fără dependență permanentă de consultantul extern.

### Suport în relația cu organismul de certificare

Oferim asistență în selecția organismului de certificare acreditat, în pregătirea dosarului pentru auditul extern și în desfășurarea unui audit intern simulat în faza finală a proiectului. Tariful auditului extern este distinct de costul consultanței și se achită direct organismului de certificare ales.

## Formare profesională

Pentru organizațiile care preferă să dezvolte competențele interne ale echipei, oferim programe de formare profesională adresate practicienilor de conformitate, ofițerilor de protecția datelor, managerilor de risc și echipelor de audit intern. Programele acoperă atât bazele metodologice ale standardelor (ISO 31000, SR EN ISO/IEC 23894:2024, SR ISO/IEC 42001:2024), cât și aplicarea concretă a acestora în context organizațional.

## O precizare importantă

Nu pot promite ceea ce nu pot susține. Decizia finală a certificării aparține exclusiv organismului de certificare extern. Pot garanta, în schimb, un proiect condus profesionist, cu o documentație adaptată specificului organizației, o comunicare directă și respectarea termenelor asumate. Succesul final al proiectului depinde de angajamentul conducerii organizației beneficiare și de disponibilitatea echipei interne de a parcurge împreună cu mine drumul de la diagnostic la certificare.

### **Pentru o discuție inițială sau o ofertă personalizată:**

Email: [ion@ioniordache.com](mailto:ion@ioniordache.com)

Site: [ioniordache.com](https://ioniordache.com)

LinkedIn: [linkedin.com/in/ioniordache](https://linkedin.com/in/ioniordache)

Telefon: +40 725 631 096

### **Formular de contact:**

[ioniordache.com/contact-ion-iordache-for-iso-certification-and-gdpr-support](https://ioniordache.com/contact-ion-iordache-for-iso-certification-and-gdpr-support)

## Lista casetelor

**Caseta 1.** De la inventar la decizie

**Caseta 2.** Anexa B ca punct de plecare al registrului de riscuri

**Caseta 3.** Dubla trasabilitate document-cerință

**Caseta 4.** Tabelul de mapare ca instrument de audit

**Caseta 5.** Criteriile de risc, decizia care determină tot procesul

**Caseta 6.** Refuzul șabloanelor copy-paste

**Caseta 7.** Focalizarea pe evaluarea impactului



---

MANAGEMENTUL RISCURILOR INTELIGENȚEI ARTIFICIALE

**GHID PRACTIC**

---

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