

Provocări și oportunități privind utilizarea AI în sectorul financiar-bancar, în condiții de siguranță, securitate și la scară largă

15 oct.2026
București

Ruxandra Rîmniceanu
Consultant strategie
Banca Națională a României

SUMAR



Tendențe emergente care redefinesc peisajul securității cibernetice și costul încălcărilor de securitate (2025-2026)

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor

Provocări ale IA pentru securizarea sistemelor, a aplicațiilor și a datelor

Considerații privind **guvernanța IA, gestionarea riscurilor și compliance**

Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

Proiecții viitoare, strategice

01.

02.

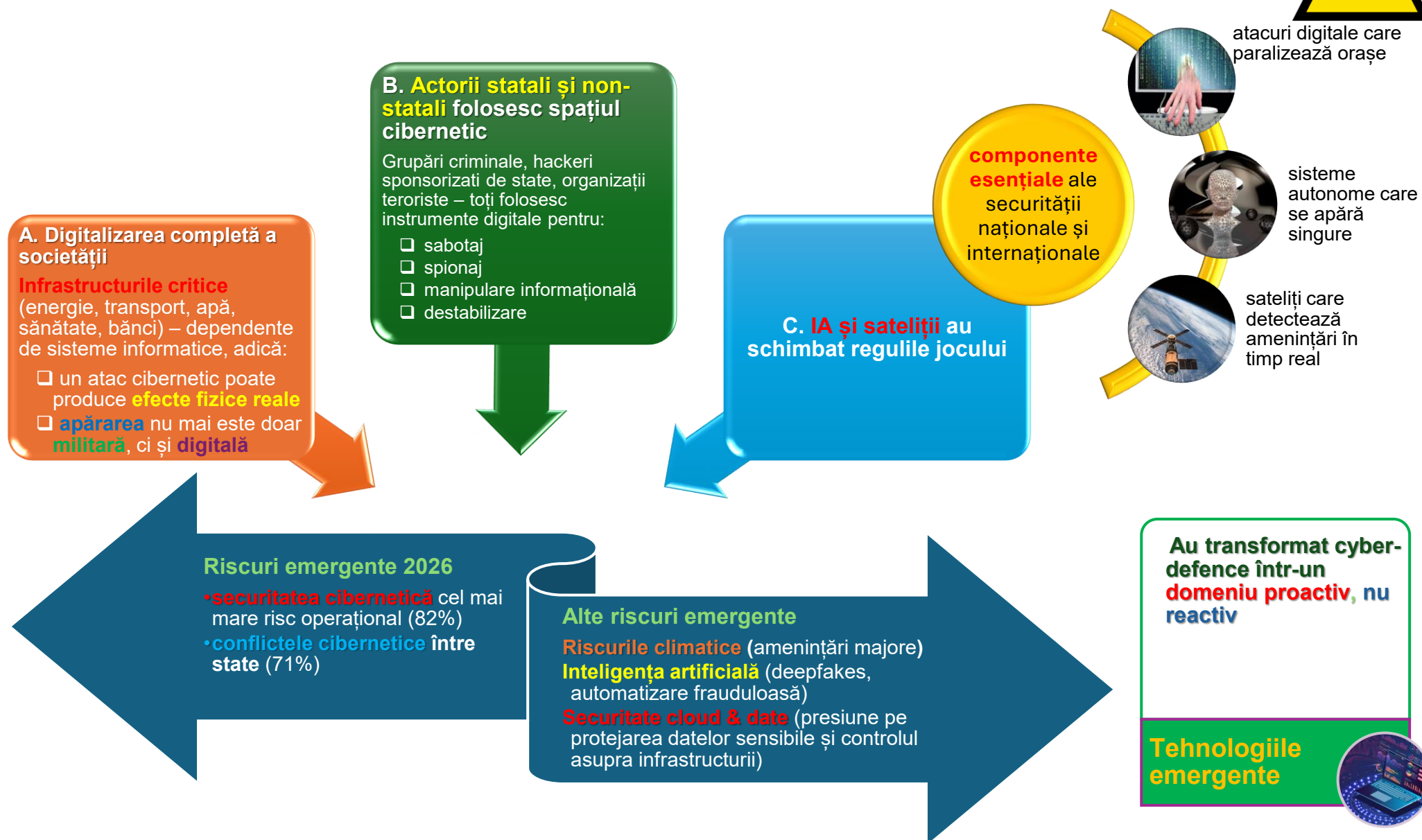
03.

04.

05.

06.

Tendințe emergente care redefinesc peisajul securității cibernetice și costul încălcărilor de securitate (2025-2026)



Tendințe emergente care redefinesc peisajul securității cibernetice și costul încălcărilor de securitate (2025-2026)

2024-2025

- securitatea cibernetică nu mai este o funcție IT
- securitatea cibernetică nu mai înseamnă doar prevenție - este vorba despre reziliență, guvernanta anticipativă și risc controlat
- strategia de securitate cibernetică este responsabilitatea Consiliului de Administrație

2026→

- organizațiile "de top":
 - construiesc **ecosisteme rezistente, bazate pe inteligență artificială, cu încredere zero**, nu doar implementează instrumente
 - **vor domina nu cele cu cele mai multe instrumente, ci cele cu cele mai integrate, strategice și adaptive modele de securitate**



În ce etapă se află instituția dumneavoastră în prezent?

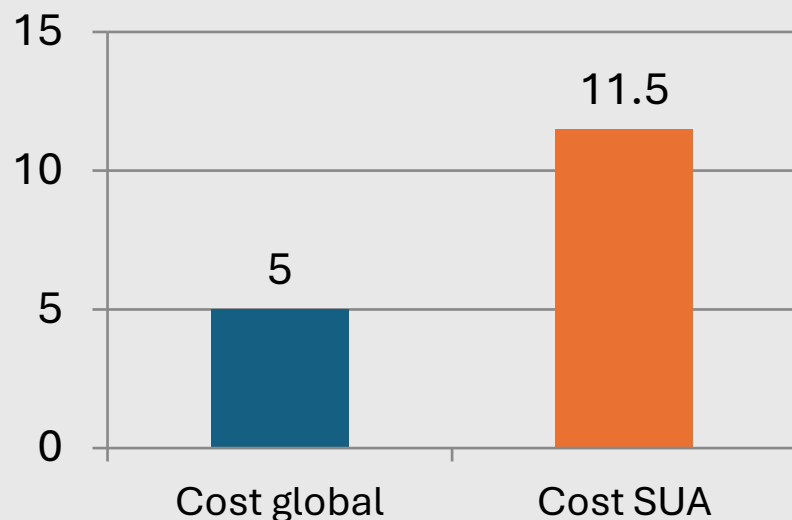


Sursa: https://www.linkedin.com/posts/dr-goran-pavlovi%C4%87-18b885250_cybersecurity-cybersecurity2026-cyberresilience-activity-7431743329312272384-2S6H/?utm_medium=ios_app&rcm=ACoAAAILqVYBZbTZj1ipHSbznrtrEPb-xTNWxrg&utm_source=social_share_send&utm_campaign=share_via

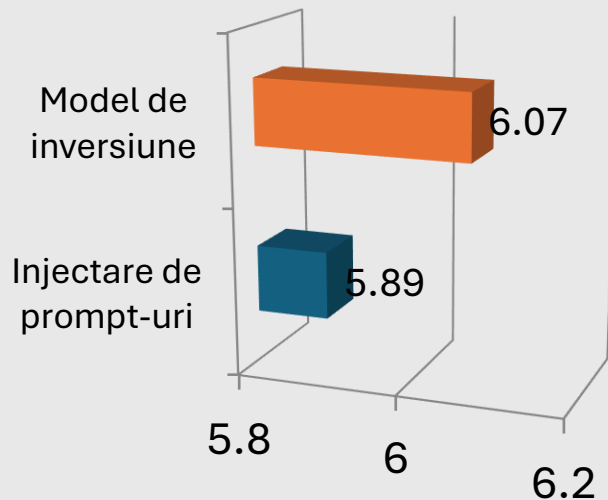
Tendințe emergente care redefinesc peisajul securității cibernetice și costul încălcărilor de securitate (2025-2026)

Sursa: IBM, 2026 Cost of Data Breach Report - Analyzing the Rising Financial and Operational Impacts of AI-Driven Cyberattacks

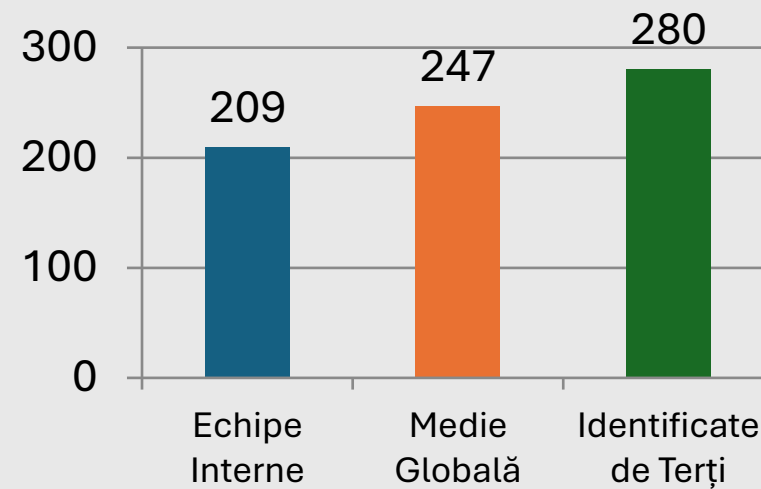
Cost (mil USD)



Cost Mediu (mil USD)



Zile până la remediere



Creșterea costurilor la nivel global vs. SUA

► Costul Mediu Global a crescut cu 12%, ajungând la aproape 5 milioane USD, propulsat de costurile de detecție și pierderile operaționale

► SUA înregistrează cel mai mare cost mediu din lume: 11.5 milioane USD (o creștere de 13%), depășind dublul mediei globale

Impactul atacurilor bazate pe IA

► Atacurile bazate pe AI au crescut cu 56%, adăugând în medie 1 milion USD la costul total al fiecărei breșe

► Țintirea directă a modelelor de AI (*Model Inversion*, *Prompt Injection*) cauzează pierderi masive de peste 5.8 milioane USD per incident.

Timul de Detecție și Răspuns la Breșe cu IA

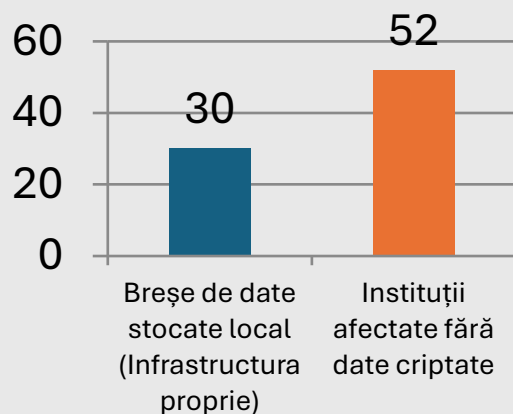
► Ciclul mediu de viață al unei breșe (identificare + izolare) a scăzut la 247 de zile

► Echipele interne identifică doar 38% din breșe, însă o fac considerabil mai rapid (209 zile) comparativ cu terți independenți (280 zile).

Tendințe emergente care redefinesc peisajul securității cibernetice și costul încălcărilor de securitate (2025-2026)

Sursa: IBM, 2026 Cost of Data Breach Report - Analyzing the Rising Financial and Operational Impacts of AI-Driven Cyberattacks

Ponderea breșelor de date și a instituțiilor fără criptare (%)



Securitatea Datelor și Stocarea la sediul de bază (on premises)

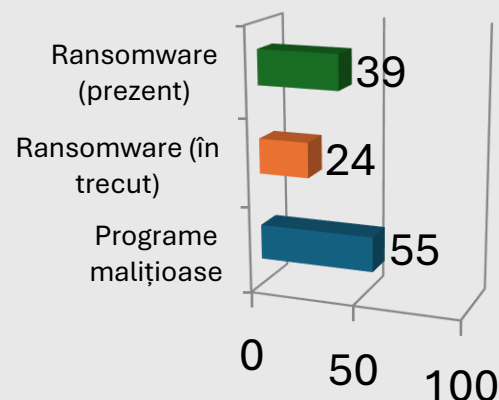
► Infrastructura proprie (On-Premises)

- **cele mai multe breșe (30%)** au afectat datele stocate local
- deși înregistrau cel mai scăzut cost mediu pentru întreținere, **vulnerabilitatea datelor** a crescut accelerat față de anii anteriori

► Criptarea Deficitară

- **peste 50% din organizațiile afectate** NU aveau datele sensibile criptate (nici în repaus, nici în tranzit)
- **lipsa criptării** rămâne principalul multiplicator de risc în exploatarea datelor

Impactul programelor malițioase și Evoluția Ransomware (%)



Vectori de atac actuali și Malware generați cu IA

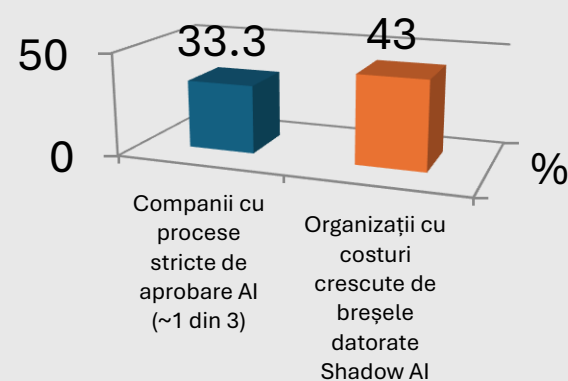
► Top Vector: Phishing

- **phishing-ul** rămâne **vectorul principal** de atac, responsabil pentru cel mai mare **cost mediu de breșă: 5.29 milioane USD**
- **atacurile malițioase** generează direct **55% din toate incidentele înregistrate**

► Evoluția Ransomware

- **Ransomware** afectează acum **39% dintre organizații** (în creștere masivă de la 24%)
- atacatorii folosesc **tactici avansate: șantajul reputațional, scurgerea datelor publice** și **compromiterea comunicațiilor interne**

Guvernanța AI și impactul Shadow AI în organizații (%)



Riscurile și lacunele de guvernanță asociate „Shadow AI”

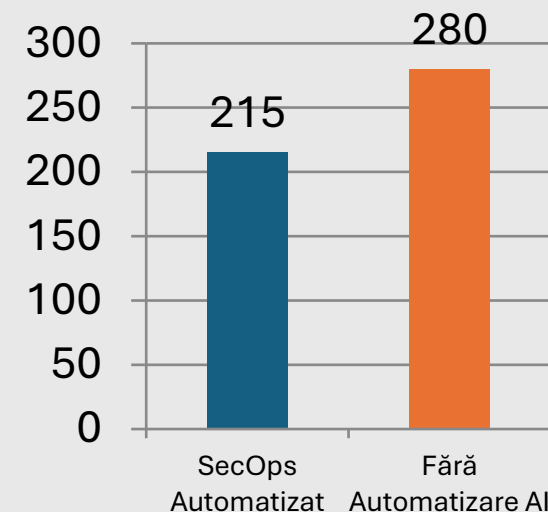
► Lipsa Politicilor de Control

- majoritatea companiilor **nu au politici clare de guvernanță AI**
- doar aproximativ **1 din 3 companii** dispun de **procese stricte de aprobare înainte de implementarea soluțiilor AI**

► Explozia Shadow AI

- **incidentele** provocate de utilizarea **AI neaprobat intern s-au dublat**
- **43% din organizații** au raportat că utilizarea necontrolată a instrumentelor AI de către angajați a dus la **escaladarea costurilor de breșă de securitate**

Temp izolare (zile)



Apărarea automatizată: IA în SecOps

- **Utilizarea extensivă a AI și a automatizării în SecOps reduce costul mediu al unei breșe de securitate** cu un nivel record de **1.93 milioane USD**

- **Timpul de reacție scade** masiv: companiile automatizate **rezolvă incidentele în 215 zile, comparativ cu 280 de zile** pentru cele tradiționale

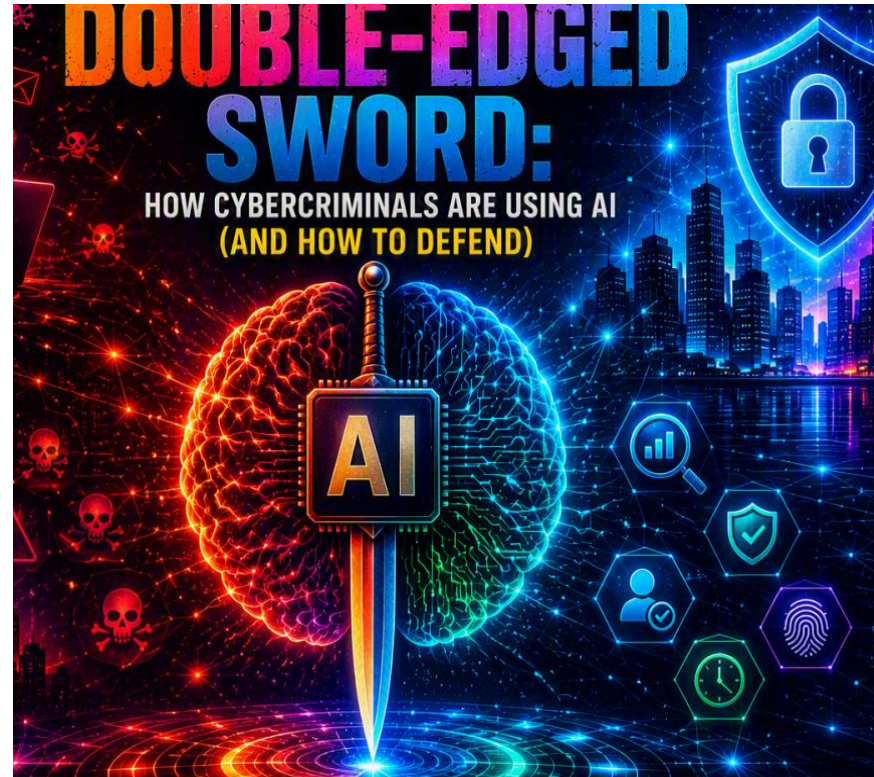
IA - nici rea IA - nici bună

Întrebarea pentru 2026
nu este dacă

*organizația dumneavoastră se va
confrunța cu atacuri bazate pe inteligență
artificială,*

ci, dacă

*apărarea dumneavoastră bazată pe
inteligență artificială, combinată cu o
supraveghere umană calificată, **va fi
pregătită să le facă față?***



IA
instrument

IA sistem
de decizie

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor



1. Perioada pre-digitală (înainte de 1980) Componenta: Protecția informației

Componenta: Protecția informației

- Securitatea era fizică: documente, comunicații radio, criptografie clasică
- Primele atacuri informatice erau experimentale, fără impact strategic
- Apărarea era centrată pe *controlul accesului* și *securitatea fizică*

2. Apariția rețelor și a primelor atacuri (1980–1995)

Componenta: Securitate IT de bază

- Primii viruși (ex. „Brain”, 1986)
- Creșterea rețelor militare și universitare
- Apărarea se bazează pe:
 - firewall-uri primitive
 - parole
 - segmentarea rețelor

Moment-cheie: apariția **CERT-urilor** (**Computer Emergency Response Teams**) în 1988

3. Era internetului și a criminalității cibernetice (1995–2007)

Componenta: Apărare reactivă

- Explozia atacurilor: DDoS, phishing, malware
- Statele încep să trateze **spațiul cibernetic ca domeniu strategic**
- NATO recunoaște importanța securității cibernetice după atacurile asupra Estoniei (2007)

Exemplu:

- Estonia 2007 → primul atac cibernetic masiv asupra unui stat, paralizând bănci, guvern, presă

4. Cyber-defence devine domeniu militar (2007–2014)

Componenta: Apărare coordonată și doctrină militară

- NATO creează CCDCOE (Tallinn)
- SUA înființează US Cyber Command (2009)
- UE dezvoltă primele strategii de securitate cibernetică

Exemplu:

- Stuxnet (2010) → primul atac cibernetic cu efect fizic asupra infrastructurii (Iran)

5. Războiul hibrid și atacurile asupra infrastructurilor critice (2014–2020)

Componenta: Apărare multi-domeniu

- Atacurile devin parte a conflictelor geopolitice
- Infrastructurile energetice, transportul și administrația devin ținte

Exemple:

- Ucraina 2015–2016 → atacuri asupra rețelor electrice
- NotPetya (2017) → atac global cu impact economic masiv
- Sabotaje cibernetice în Orientul Mijlociu
- Apărarea se extinde la:
 - protecția infrastructurilor critice
 - cooperare internațională
 - răspuns coordonat la atacuri hibride

6. Era AI și a sateliților comerciali (2020–2024)

Componenta: Apărare proactivă și automatizată

- AI detectează atacuri în timp real
- Sateliții comerciali oferă imagini strategice accesibile publicului
- Analiza automată a imaginilor devine standard

Exemple:

- Războiul din Ucraina (2022–2024)
- Maxar și Planet Labs → imagini satelitare în timp real
- AI → identificarea blindatelor, mișcărilor de trupe, atacurilor cibernetice
- **UE lansează programe de reziliență digitală (NIS2, DORA)**

7. Cyber-defence integrat multi-domeniu (2024–2026)

Componenta: Apărare autonomă și coordonată

- AI + sateliți + senzori + rețele militare → sisteme integrate
- Apărarea devine preventivă, nu reactivă
- **NATO tratează spațiul cibernetic ca domeniu operațional complet**

Exemple:

- Exercițiile NATO „Locked Shields” → simulări de război cibernetic la scară națională
- **UE dezvoltă Cyber Solidarity Act pentru apărare colectivă**
- Atacuri asupra infrastructurilor energetice europene → răspuns coordonat UE–NATO

8. Direcții viitoare (2026–2030)

Componenta: Apărare autonomă și AI strategică

- Sisteme autonome de apărare cibernetică
- Sateliți cu AI on-board
- Rețele globale de detecție integrate
- Modele predictive pentru anticiparea conflictelor

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor



GenAI ofensiv avansat

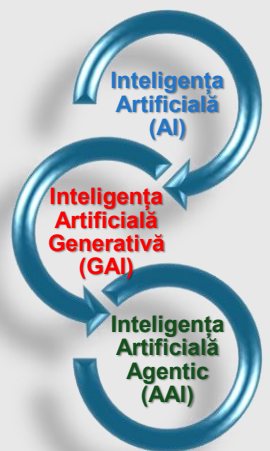
- **Atacuri complet autonome**, orchestrate de agenți AI
- Phishing conversațional cu avataruri video generate în timp real
- Atacuri hiper-personalizate pe baza profilului psihologic
- Integrare cu realitatea augmentată pentru **manipulare vizuală**
- **Campanii de dezinformare + phishing coordonate de AI**

GenAI în atacuri hibride

- Războiul din Ucraina accelerează utilizarea GenAI în atacuri
- Deepfake-uri video folosite în **campanii de dezinformare**
- E-mailuri și mesaje generate automat, adaptate la stilul organizațiilor
- Chatbots malițioși imită suportul tehnic
- **Atacuri multi-vector: email + voce + social media**

Apariția modelelor mari de limbaj

- Modelele de limbaj devin capabile să genereze **texte coerente**
- Atacatorii experimentează cu generarea automată de emailuri
- Primele campanii de phishing „curate”, fără greșeli
- Crește realismul mesajelor de inginerie socială



2026–2030,
tendințe

06

05

2024–2026

Atacuri autonome asistate de GenAI

- GenAI poate menține **conversații în timp real** cu victimele
- Deepfake vocal instant (30 secunde de audio → voce completă)
- Mesaje adaptate dinamic în funcție de răspunsurile victimei
- Generarea automată de **documente false** (facturi, contracte, identități)
- **Evitarea filtrelor** prin rescriere automată

2022-2024

04

03

2020-2022

Democratizarea GenAI

- Modelele devin accesibile publicului
- Atacatorii pot genera **mii de mesaje unice în câteva secunde**
- Phishing personalizat pe baza datelor publice
- Apar primele **deepfake-uri vocale** credibile

2018-2020

02

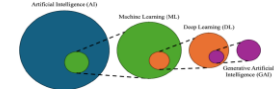
01

Înainte de 2018

Pre-GenAI

- Atacurile se bazează pe texte scrise manual
- Phishing generic, cu **erori evidente**
- Inginerie socială simplă: apeluri, emailuri false
- Automatizare limitată

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor



1. Scalare masivă și automatizare

- ❑ GenAI poate genera:
 - mii de **emailuri unice** în câteva secunde
 - **mesaje adaptate** pentru fiecare țintă
 - **conversații coerente în timp real**
- ❑ Atacatorii nu mai au nevoie de **timp** sau **competențe lingvistice**. AI **face totul** pentru ei



2. Personalizare extremă (hyper-targeting)

- ❑ GenAI poate analiza:
 - profiluri LinkedIn
 - postări Facebook
 - istoricul public al unei persoane
 - stilul de comunicare
- ❑ GenAI poate produce mesaje care par **autentice / relevante / scrise de cineva cunoscut**
- ❑ **spear-phishingul** se transformă într-o **armă** aproape **imposibil de detectat vizual**



3. Deepfake-uri vocale și video

- ❑ GenAI poate crea:
 - **vocea unui CEO** în **30 de secunde**
 - un **video fals** în care un director cere un transfer
 - un **apel telefonic credibil** cu vocea unui coleg
- ❑ **tehnici deja folosite** în:
 - atacuri asupra băncilor
 - fraude de milioane de euro
 - operațiuni de dezinformare în conflicte recente



4. Phishing conversațional (chatbots malițioși)

- ❑ **Atacatorii folosesc** GenAI pentru a crea:
 - chatbots care **imită suportul tehnic**
 - asistenți care **cer date personale**
 - agenți conversaționali care **manipulează emoțional**
- ❑ **Chatbots-ii** pot menține **conversații lungi, convingătoare, adaptate în timp real**



5. Evitarea detecției

- ❑ GenAI poate:
 - rescrie emailuri pentru a **evita filtrele**
 - genera **texte fără pattern-uri detectabile**
 - **imita stilul de scriere** al unei organizații
- ❑ **atacurile devin**:
 - fluide
 - greu de identificat
 - imposibil de blocat prin metode tradiționale

Mecanismul din spate



Cum funcționează „Chain-of-Thought” (CoT) în modelele recente de IA?

În modelele anterioare, IA primea un prompt și genera **instantaneu cel mai probabil răspuns**, printr-un mecanism intuitiv, rapid (asociat cu **Sistemul 1 de gândire umană**). În cazul problemelor complexe de logică sau matematică, această abordare dădea greș



Chain-of-Thought (Lanțul de Gândire)

- ❑ este o metodă care forțează modelul să își descompună raționamentul în pași logici, intermediari, înainte de a oferi răspunsul final
- Prompt Complex → [Pasul 1: Analiză] → [Pasul 2: Calcul] → [Pasul 3: Verificare] → Răspuns Final

Decompunerea problemei

În loc să sară direct la concluzie, **modelul generează un text intern** (invizibil sau vizibil utilizatorului) în care scrie: „**Mai întâi trebuie să aflu X. Pentru a afla X, formula este Y. Să calculăm.**”

Efectul de ancorare în context

Fiecare pas logic corect pe care modelul îl scrie devine parte din „istoria” textului său

Deoarece **tehnologia ”Transformer”** prezice următorul cuvânt pe baza a ceea ce a scris deja, prezența pașilor logici anteriori crește exponențial probabilitatea ca următorul pas să fie și el corect din punct de vedere matematic.

Modelele moderne cu CoT nativ

Modelele recente din generațiile curente integrează acest **comportament direct în faza de post-antrenare** (prin **Reinforcement Learning din feedback uman și AI**). Ele rulează bucle de verificare, **corectându-și singure greșelile într-un mediu izolat (sandbox) înainte de a afișa textul utilizatorului**

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor



"Arsenalul" atacatorului



1. Inginerie socială generată de inteligența artificială la scară largă

Era e-mailurilor de phishing prost scrise a apus. **Atacurile de inginerie socială bazate pe inteligență artificială** de astăzi sunt practic **imposibil de distins de comunicările legitime**:

- ❑ **Mesaje hiperpersonalizate** generate din date extrase de pe rețelele sociale, istoricul angajărilor și baze de date scurse - adaptate la ținte individuale cu o precizie uimitoare
- ❑ **Audio deepfake** care imită perfect directorii generali, directorii financiari și directorii executivi care autorizează transferuri bancare frauduloase
- ❑ **Impersonări video** ale unor colegi de încredere care solicită partajarea acreditărilor sau informații sensibile
- ❑ **Campanii de phishing multilingve** adaptate automat la dialectele regionale, nuanțele culturale și practicile comerciale locale
- ❑ **Boți de conversație în timp real** care interacționează cu țintele în schimburi extinse, construind încredere înainte de a livra sarcini utile rău intenționate



2. Descoperirea autonomă a vulnerabilităților

Hackerii implementează acum **agenți de inteligență artificială care operează 24/7**, căutând sistematic puncte slabe de securitate: Pentru **contracurare**, se impune:

- ❑ **Scanarea continuă a depozitelor de cod** publice și private pentru vulnerabilități necunoscute anterior
- ❑ **Generarea de coduri de exploatare funcțională** în câteva minute de la descoperire, complet cu tehnici de evitare a depășirii limitelor
- ❑ **Testarea vectorilor de atac** în medii simulate înainte de implementarea pe ținte reale
- ❑ **Înlănțuirea mai multor vulnerabilități** cu risc scăzut în căi de atac critice pe care analiștii umani le-ar rata
- ❑ **Adaptarea tehnicilor de exploatare** în funcție de factorii de mediu specifici țintei



3. Malware ascuns prin inteligență artificială

Software-ul rău intenționat a devenit **straniu de "inteligent"**, cu capabilități care ar fi părut imposibile cu doar câțiva ani în urmă:

- ❑ **Cod polimorfic** care se rescrie complet la fiecare infecție, menținând în același timp funcționalitatea de bază
- ❑ **Sarcini utile sensibile la context** care rămân inactive până când sunt îndeplinite condiții foarte specifice - evitând detectarea timp de luni de zile
- ❑ **Tehnici anti-analiză** care detectează medii sandbox, mașini virtuale și cercetători în securitate, apoi se comportă benign
- ❑ **Viermi auto-propagați** care navighează în rețele folosind arbori de decizie bazați pe inteligență artificială, identificând autonom ținte de mare valoare
- ❑ **Mecanisme adaptive de persistență** care evoluează în funcție de controalele de securitate pe care le întâlnesc



4. Atacuri adverse de învățare automată

Cei mai sofisticăți actori amenințători **vizează acum chiar sistemele de inteligență artificială**:

- ❑ **Antrenarea "otrăvirii" datelor** pentru a crea puncte oarbe sistematice în domeniul securității inteligenței artificiale - făcând anumite modele de atac invizibile
- ❑ **Generarea de exemple contradictorii** care păcălesc detectoarele de programe malware și sistemele de prevenire a intruziunilor
- ❑ **Atacuri de inversare a modelelor** care extrag și fură modele de inteligență artificială proprietare din produsele de securitate comerciale
- ❑ **Tehnici de evitare** concepute special împotriva modelelor și arhitecturilor defensive cunoscute ale inteligenței artificiale
- ❑ **Backdooring-ul modelului** care încorporează declanșatori ascunși în sistemele de inteligență artificială în timpul fazei de antrenament

Istoricul IA – cum accelerează viteza și sofisticarea atacatorilor



”Arsenalul” apărătorului



1. Integrarea informațiilor despre amenințări (**Threat Intelligence**) bazate pe inteligență artificială



2. Sisteme de răspuns autonome



3. IA generativă pentru apărare



4. Inteligență artificială explicabilă pentru analiza criminalistică

Centrele moderne de operațiuni de securitate (SOC) nu doar colectează date, ci **realizează**:

- ❑ **Modelare predictivă a amenințărilor** care anticipează vectorii de atac înainte ca aceștia să fie exploatați activ în mediul virtual
- ❑ **Corelarea automată** a evenimentelor de securitate aparent fără legătură în rețelele globale, identificând campanii coordonate
- ❑ **Prelucrarea limbajului natural** al forumurilor dark web, al canalelor de mesagerie criptate și al comunităților de hackeri pentru detectarea amenințărilor emergente
- ❑ **Recunoașterea tiparelor de atac în timp real** care identifică campaniile din diferite organizații și industrii
- ❑ **Detectarea anomaliilor comportamentale** care identifică tehnici noi de atac chiar și fără semnături anterioare

Când **atacurile au loc la viteza mașinii, răspunsul exclusiv uman nu mai este viabil**:

- ❑ **Rețele cu auto-reparare** care izolează automat segmentele compromise, menținând în același timp continuitatea afacerii
- ❑ **Honeypot-uri adaptive** care evoluează pe baza comportamentului atacatorului, colectând informații în timp ce își irosesc resursele
- ❑ **Generare automată de patch-uri** pentru vulnerabilități zero-day folosind analiza și sinteza codului asistată de inteligență artificială
- ❑ **Controale dinamice de acces** care ajustează continuu permisiunile pe baza scorului de risc în timp real
- ❑ **Straturi inteligente de înșelăciune** care redirecționează atacatorii către medii monitorizate, protejând în același timp activele critice

Apărătorii întorc cele mai puternice instrumente ale atacatorilor împotriva lor:

- ❑ **Date sintetice de antrenament** care pregătesc sistemele defensive pentru tipuri de atac noi, încă neobservate în mediul online
- ❑ Documente și acreditări **capcană generate de inteligență artificială care urmăresc încercările de exfiltrare și identifică amenințările interne**
- ❑ **Sisteme automate de dezvăluire a vulnerabilităților** și de aplicare a patch-urilor care remediază problemele mai rapid decât le pot exploata atacatorii
- ❑ **Politici de securitate a limbajului natural** care traduc automat cerințele afacerii în controale tehnice
- ❑ **Tehnologii anti-deepfake** care detectează și semnalează conținutul media sintetic în comunicațiile în timp real

Într-o **eră a securității bazate pe inteligență artificială**, transparența a devenit un mecanism esențial de apărare:

- ❑ **Atacați atribuirea** cu scoruri de încredere și lanțuri de dovezi care rezistă examinării juridice
- ❑ **Vizualizarea luării deciziilor prin inteligență artificială** în timpul incidentelor de securitate, permițând supravegherea și învățarea umană
- ❑ **Automatizarea conformității cu reglementările** pentru standardele de protecție a datelor și cerințele de raportare a incidentelor în evoluție
- ❑ **Rapoarte de amenințări lizibile de către om**, generate automat din indicatori tehnici pentru luarea deciziilor executive
- ❑ **Audituri** care documentează fiecare punct de decizie bazat pe inteligența artificială în timpul răspunsului la incidente

Provocări ale IA pentru securizarea sistemelor, a aplicațiilor și a datelor

Evenimentele din **11 septembrie 2001** au redefinit complet conceptul de securitate, **trecând de la o abordare reactivă la una predictivă**, bazată pe colectarea masivă de date

1. Conectarea punctelor de date (The "Connecting the Dots" Dilemma)

- **Provocare:** Rapoartele oficiale de după 11 septembrie au arătat că **agențiile de securitate aveau fragmente de informații care, puse cap la cap, ar fi putut preveni atacurile**. Provocarea actuală pentru IA este **să proceseze volume uriașe de date din surse complet diferite** (baze de date guvernamentale, e-mailuri, tranzacții financiare, rețele sociale) pentru a detecta amenințări subtile
- **Risc:** IA se confruntă fie cu **"zgomotul informațional" (prea multe date inutile)**, fie cu **incapacitatea sistemelor** din instituții diferite **de a comunica între ele** (silozuri de date)

2. Eroarea de tip "Lebăda Neagră" și lipsa datelor istorice

- **Provocare:** Atacurile din 11 septembrie au fost un **eveniment de tip „Lebădă Neagră”** – un eveniment extrem de improbabil, fără precedent istoric clar. Modelele IA actuale sunt antrenate pe date din trecut pentru **a recunoaște tipare**
- **Risc:** Un algoritm **IA nu poate anticipa** un mod de atac complet nou și ingenios, deoarece acesta nu există în seturile sale de date de antrenament. IA este **util la detectarea anomaliilor cunoscute, dar vulnerabil în fața „imprevizibilului total”**

3. Compromisul dintre securitate și confidențialitatea datelor (Privacy vs. Security)

- **Provocare:** După 2001, legislația **USA PATRIOT Act a instituit măsuri de securitate suplimentare**. Astăzi, sistemele IA de securitate au nevoie de **acces la datele cetățenilor** (biometrie, locație, comunicații) pentru **detectarea terorismului sau a atacurilor cibernetice pe scară largă**
- **Risc:** **IA poate încălca drepturile fundamentale la viață privată** și creează riscul ca aceste sisteme de monitorizare să fie **abuzive** sau pot fi **utilizate/compromise de actori statali ori hackeri**

4. Securizarea infrastructurii critice și atacurile asimetrice

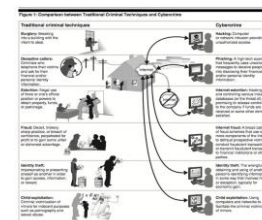
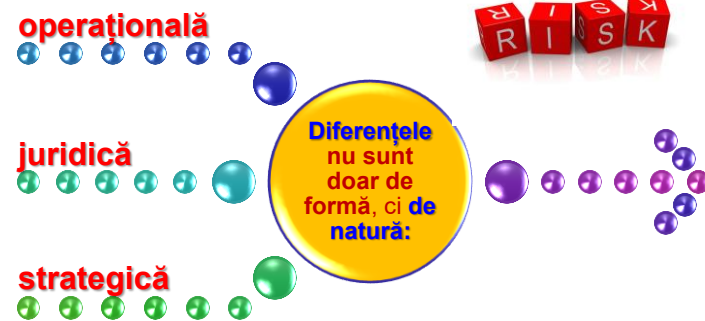
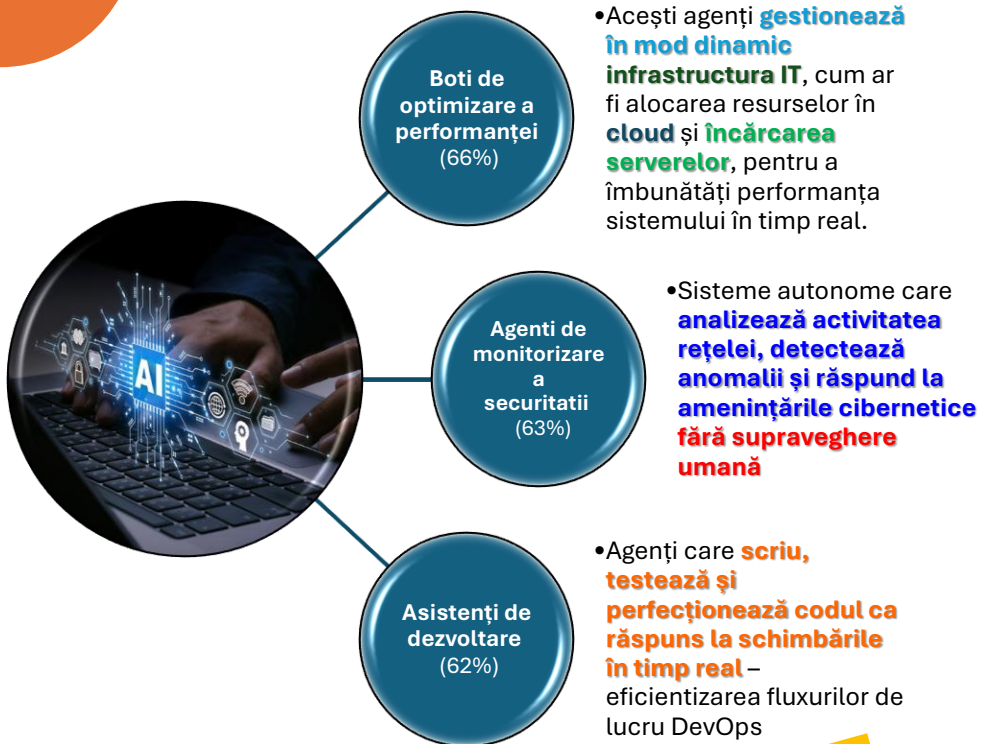
- **Provocare:** În 2001, **avioanele** comerciale au fost folosite ca **arme împotriva infrastructurii civile**. În era digitală, armele sunt **liniile de cod**. IA este folosită pentru **a proteja rețelele electrice, sistemele de trafic aerian și bazele de date guvernamentale împotriva atacurilor cibernetice asimetrice** (**un singur actor cu resurse puține poate cauza daune masive**)
- **Risc:** **Dacă sistemul IA care protejează o aplicație critică este păcălit printr-un atac de tip adversarial** (manipularea subtilă a datelor de intrare), **sistemul de apărare poate fi orbit complet, permițând un atac catastrofal**

5. Utilizarea duală a IA ("armarea" Inteligenței Artificiale)

- **Provocare:** **Tehnologia IA dezvoltată pentru a securiza datele și a detecta atacurile este o tehnologie cu dublă utilizare**. **Teroriștii sau atacatorii cibernetici pot folosi exact aceleași instrumente IA** pentru a automatiza atacurile, a descoperi vulnerabilități în aplicații sau a genera deepfake-uri pentru dezinformare în masă
- **Risc:** O cursă a înarmării tehnologice în care **sistemele IA defensive pot să evolueze mai lent decât sistemele IA ofensive** ale atacatorilor



Provocări ale IA pentru securizarea sistemelor, a aplicațiilor și a datelor



• Delictul clasic

- amenințare vizibilă, locală, cu răspunsuri instituționale bine stabilite
- afectează individul sau comunitatea

• Cyber-terorismul

- amenințare invizibilă, globală, care necesită o abordare multidisciplinară și internațională
- poate destabiliza / aduce în incapacitate sisteme întregi

2025

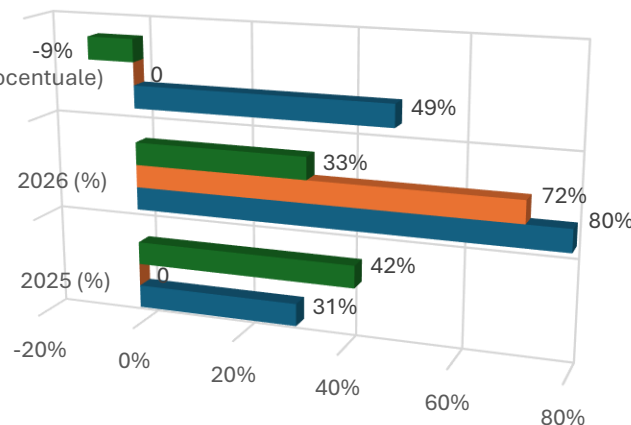
- Gen AI
- Active digitale
- Cloud

Investiții CEO

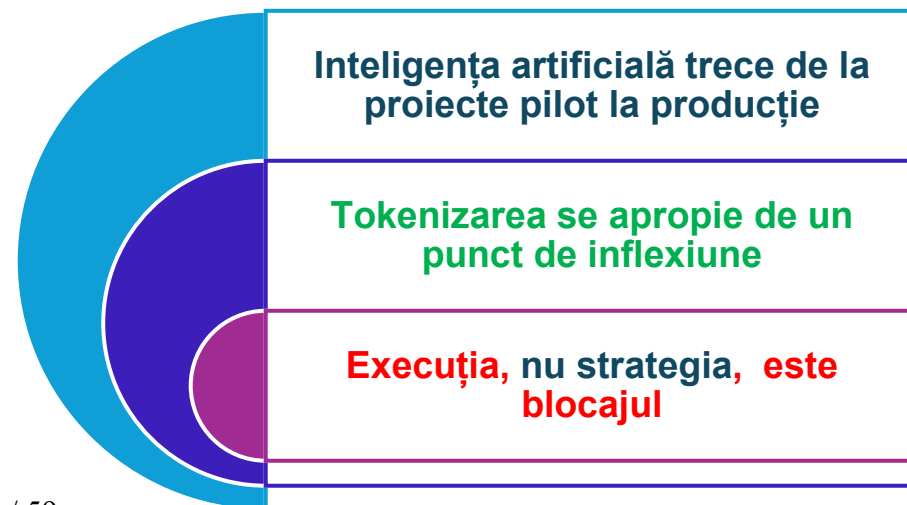
Generative AI

2025-2026

Schimbare (puncte procentuale)



■ Îngrijorare privind Rentabilitatea (ROI) ■ Investiții GenAI (Moderate/Mari)
■ Utilizarea IA (Generativă/Predictivă)



Studiu anual de transformare digitală și tehnologie de nouă generație

Sursa: **Broadridge Financial Solutions**,
<https://www.broadridge-ir.com/news/news-details/2026/GenAI-Delivering-Now-Tokenization-Is-Next-Financial-Services-Enters-Period-of-Accelerating-Transformation-Landmark-Broadridge-Study-Finds/default.aspx>

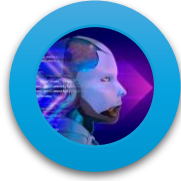
Considerații privind guvernanta IA, gestionarea riscurilor și compliance



Guvernanta IA (AI Governance): Reprezintă **cadrul de reguli, practici, structuri organizatorice și procese decizionale** care stabilesc cum este dezvoltată, testată și utilizată inteligența artificială în siguranță. Scopul este **alinarea algoritmilor cu valorile etice, drepturile omului și obiectivele de business**



Gestionarea riscurilor (Risk Management): **Procesul continuu de identificare, evaluare și atenuare a pericolelor asociate IA.** Printre riscurile majore se numără **erorile de discriminare** (bias), **lipsa de transparență** („cutia neagră”), **breșele de securitate cibernetică** sau **încălcarea confidențialității datelor**



Compliance (Conformitate): Actul de **a respecta integral legile, directivele externe** (ex: regulamentele UE) **și politicile interne** ale unei organizații. În contextul IA, înseamnă să demonstrezi oficial că **sistemele software nu încalcă standardele juridice impuse**

1

Guvernanta nu blochează inovația: un **cadru etic solid** face implementarea tehnologiei sustenabilă și sigură

2

Trecerea de la utilizarea fragmentată la strategii de management centralizat al instrumentelor de IA

3

Recomandare imediată: Lansarea unui audit intern complet pentru **maparea tuturor aplicațiilor IA folosite în prezent**

5 întrebări de pus înainte de a implementa AI agentic

1.

• Ce problemă **va rezolva** AI Agentic?

2.

• Avem **date corecte și consistente** pentru ca acesta să funcționeze?

3.

• Vor fi **datele securizate**?

4.

• Unde se încadrează AI Agentic în **strategia tehnologică** a companiei?

5.

• Cum **va fi monitorizată** AI Agentic?



consolidare guvernanta și securitate AI

Interoperabilitate platforme

- Definirea unui cadru clar de reguli, politici și responsabilități la nivelul organizației
- Înființarea comitetelor etice pentru monitorizarea directă a modului în care sunt antrenați algoritmi
- Stabilirea responsabilităților clare pentru echipele de dezvoltare și managerii de produs

Guvernanta IA (Cine și cum decide?)



- Identificarea și maparea pericolelor: discriminarea ascunsă în date (bias), erori tehnice și halucinații
- Evaluarea vulnerabilităților de securitate cibernetică specifice modelelor de limbaj sau rețelelor neuronale
- Strategii de mitigare bazate pe audituri tehnice periodice și principiul controlului uman permanent (Human-in-the-loop)

Gestionarea Riscurilor (Ce poate merge prost?)

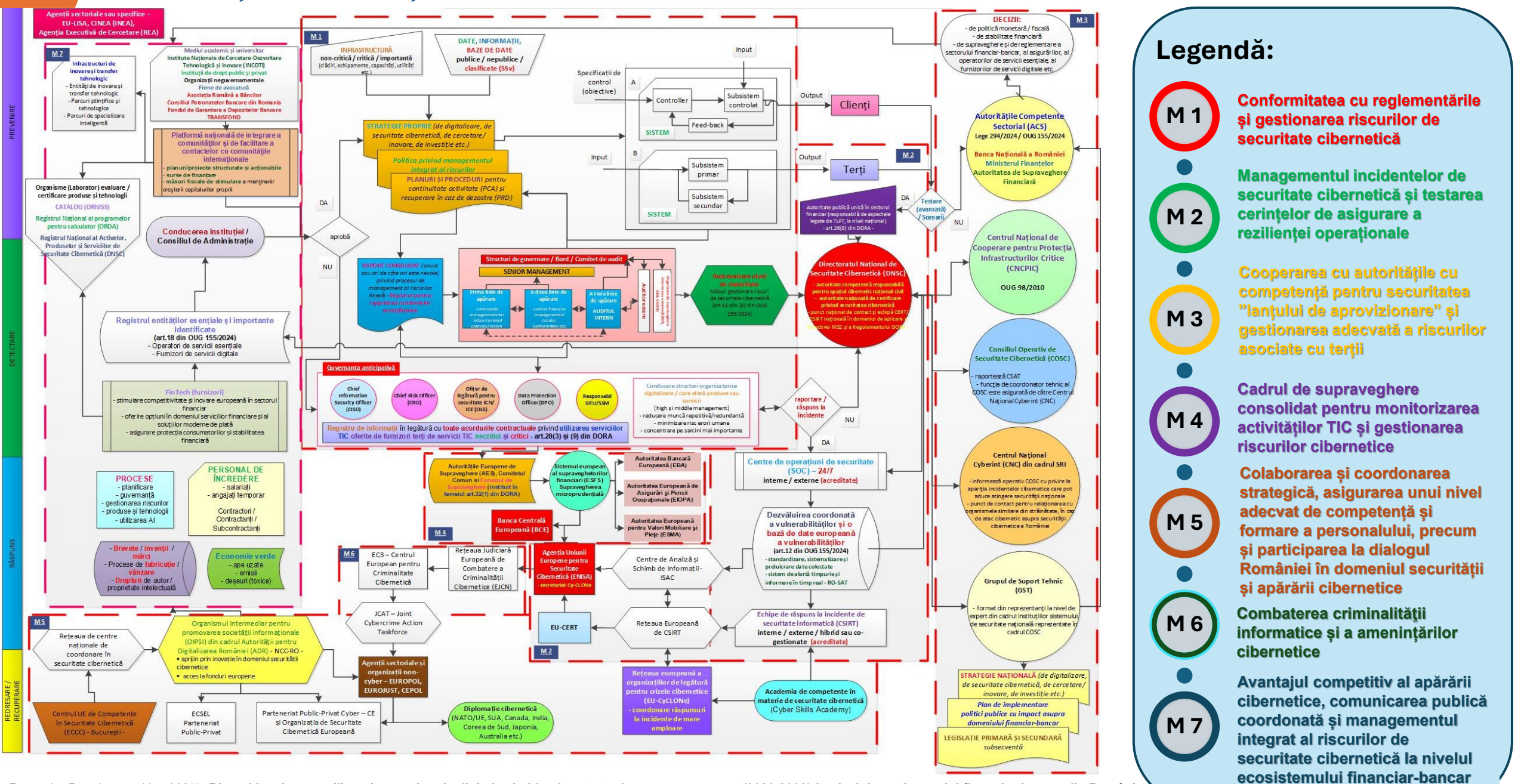


- Alinierea obligatorie cu noul Regulament European privind Inteligența Artificială (EU AI Act) și legislația conexă
- Cerințe drastice de transparență: obligația de a marca digital elementele de tip deepfake și interfețele de tip chatbot
- Evitarea riscurilor financiare severe: amenzi masive stabilite global pentru utilizarea sistemelor interzise sau neconforme

Compliance și EU AI Act (Ce ne obligă legea?)



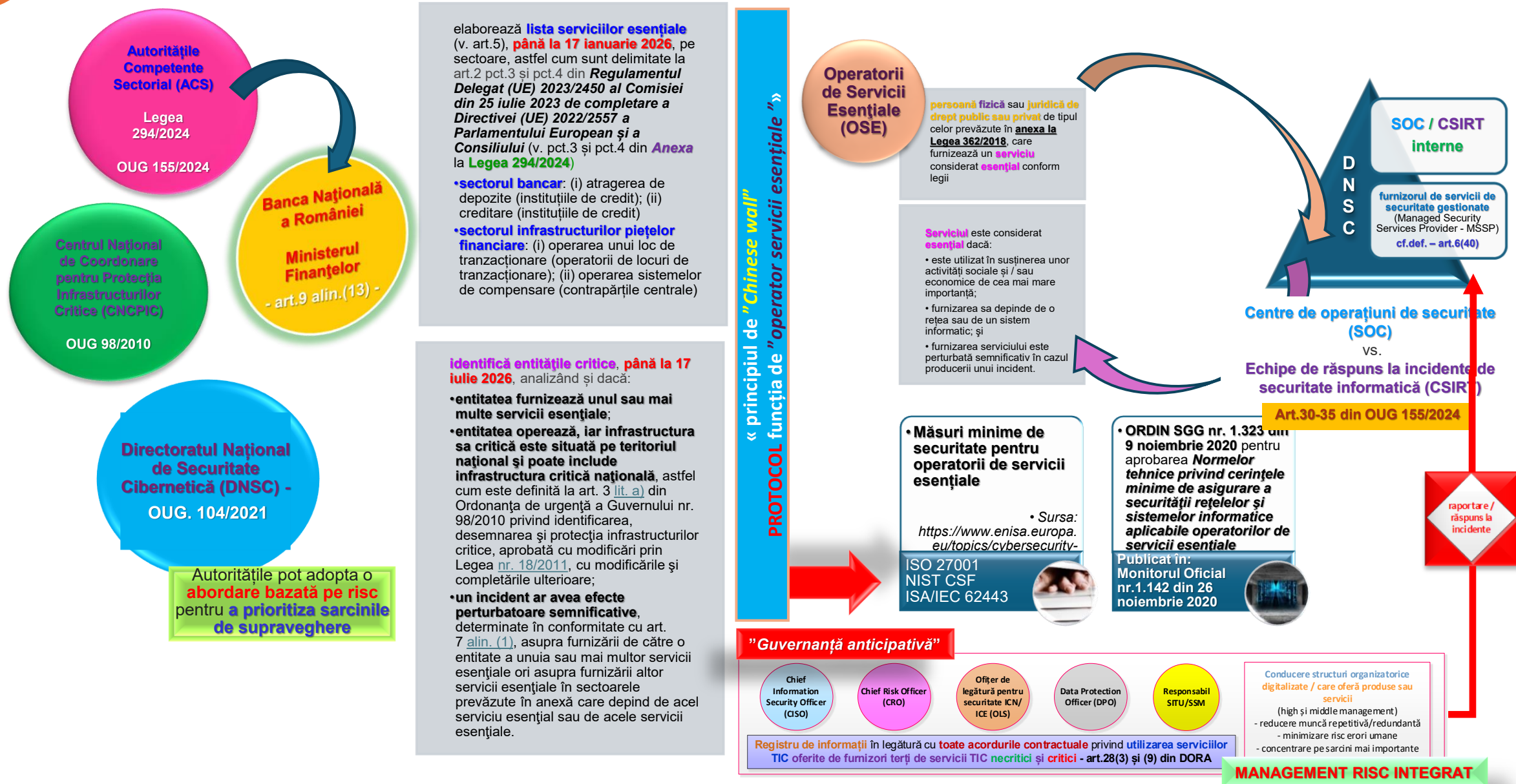
Guvernanța securității cibernetice la nivelul ecosistemului financiar-bancar din România



Legendă:

- M 1** Conformitatea cu reglementările și gestionarea riscurilor de securitate cibernetică
- M 2** Managementul incidentelor de securitate cibernetică și testarea cerințelor de asigurare a rezilienței operaționale
- M 3** Cooperarea cu autoritățile cu competență pentru securitatea "lanțului de aprovizionare" și gestionarea adecvată a riscurilor asociate cu terții
- M 4** Cadru de supraveghere consolidat pentru monitorizarea activităților TIC și gestionarea riscurilor cibernetice
- M 5** Colaborarea și coordonarea strategică, asigurarea unui nivel adecvat de competență și formare a personalului, precum și participarea la dialogul României în domeniul securității și apărării cibernetice
- M 6** Combaterea criminalității informatice și a amenințărilor cibernetice
- M 7** Avantajul competitiv al apărării cibernetice, comunicarea publică coordonată și managementul integrat al riscurilor de securitate cibernetică la nivelul ecosistemului financiar-bancar

Guvernanța securității cibernetice la nivelul ecosistemului financiar-bancar din România



Guvernanta securității cibernetice la nivelul ecosistemului financiar-bancar din România

Riscul de incident

- Incidente cibernetice sau operaționale
- Impact asupra serviciilor critice
- Necesitatea raportării rapide

• Măsuri atenuare

- Implementarea raportării incidentelor în <4 ore
- Automatizarea detecției (SIEM + SOAR)
- Playbook de răspuns la incidente
- Exerciții trimestriale tabletop

Riscul legat de furnizori

- Dependență de furnizori IT / Cloud critici
- Vulnerabilități în lanțul de aprovizionare
- Necesitatea monitorizării continue

• Măsuri atenuare

- Clasificarea furnizorilor după criticitate
- Introducerea clauzelor DORA în contracte
- Monitorizare continuă a performanței
- Evaluări anuale de risc pentru furnizorii critici

Riscul de continuitate

- Întreruperi ale serviciilor esențiale
- Lipsa planurilor robuste de continuitate
- Necesitatea testării periodice

• Măsuri atenuare

- Actualizarea planurilor BCP/DRP
- Testarea anuală a continuității
- Implementarea redundanței pentru sisteme critice
- Stabilirea unui proces clar de escaladare

CISO / CIO / CISA

- incidente
- SIEM
- playbook

Manager de furnizori

- furnizori
- contracte
- monitorizare

Șeful Operațiunilor IT

- continuitate
- BCP/DRP

Șeful DevSecOps

- supply chain
- SBOM (Software Bill of Materials)

Responsabilități

Riscuri & Impact

Lipsa testelor de reziliență poate afecta continuitatea operațională

Neconformitatea poate duce la sancțiuni, audituri extinse și pierderea încrederii pieței

Dependența de furnizori IT critici reprezintă un punct vulnerabil major

Riscurile cibernetice cresc

accelerarea implementării DORA/NIS2

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Regulamentul (UE)
2024/1689
– AI Act –

- **protecția persoanelor vizate în raport cu sistemele decizionale automatizate** - asigurată preponderent prin dispozițiile **art. 22 din Regulamentul (UE) 2016/679 (GDPR)**, care consacră dreptul persoanei de a nu fi supusă unei decizii bazate exclusiv pe prelucrarea automatizată
- **decizia Curții de Justiție a Uniunii Europene** prin Hotărârea din 7 decembrie 2023, cauza C-634/21, OQ c. Land Hessen (SCHUFA) - **dispoziția clarificată în mod decisiv**

Context

Obiective

- **prevenirea** discriminării algoritmice
- **limitarea deciziilor automate** care afectează viața oamenilor
- **interzicerea sistemelor** care pot manipula comportamentul sau exploata vulnerabilități

- **drepturile de autor (copyright-ul) și alte drepturi de proprietate intelectuală**, în special acolo unde modelele sunt antrenate pe volume mari de texte, imagini, cod sau baze de date;
- **protecția datelor cu caracter personal**, în special unde seturile de date conțin informații privind persoane fizice, iar GDPR continuă să se aplice integral, chiar dacă avem un nou regulament privind AI

Teme juridice

Etapele implementării

- **2 februarie 2025** – **Practicile interzise** (art. 5) și obligația de **alfabetizare** în domeniul IA (art. 4)
- **2 august 2025** – Modele de **IA de uz general** (GPAI), **guvernanta, regim sancționator**
- **2 august 2026** – Obligații pentru **sistemele cu risc ridicat** din Anexa III (inclusiv HR, scoring credit) **[7 luni]**
- **2 august 2027** – Obligații pentru **sistemele cu risc ridicat în produse reglementate** (Anexa I)

art.4 - **furnizorii și utilizatorii de sisteme de IA** trebuie să asigure un **nivel adecvat de cunoștințe** pentru personalul implicat în operarea acestora, **proporțional** cu **contextul de utilizare** și cu **persoanele vizate**

ISO/IEC 42001:2023 Tehnologia informației — Inteligență artificială — Sistem de management

- specifică cerințele pentru implementarea unui **sistem de management al inteligenței artificiale (AI)**
- conceput pentru **organizațiile care oferă sau folosesc produse sau servicii bazate pe inteligență artificială**

26.07.2024



NIST-AI- 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile - poate ajuta organizațiile să identifice riscurile unice prezentate de IA generativă și propune acțiuni pentru managementul riscului AI generativ care se aliniază cel mai bine cu obiectivele și prioritățile lor

Sursa: <https://doi.org/10.6028/NIST.AI.600-1>

Considerații privind guvernanta IA, gestionarea riscurilor și compliance



AI $\approx$
fierăstrău
electric

- extrem de util
dacă este folosit corect
- foarte periculos
în mâinile greșite



DeepSeek_V3 (China)
- amenințare sau
minune tehnologică?

- ☐ filtrarea automată a
conținutului "delicat"
(nedorit)
- ☐ adaptarea la
reglementările locale
privind informațiile on-
line
- ☐ restrângerea accesului
la surse externe

10 ian.2025

UE

**Regulamentul UE
privind Inteligența Artificială**
- 2024/1689 –
adoptat de CE la 13.06.2024



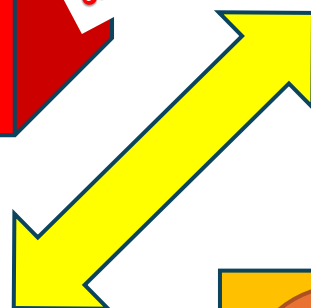
**Intrat în vigoare la
01.08.2024**

va stimula
încrederea
consumatorilor
și va evita
pericolele
spălării AI și
alte riscuri
legate de
utilizarea AI

**Transparența – informarea
utilizatorilor** despre
interacțiunea lor cu sistemele
AI, mai ales în domenii critice
precum sănătatea, educația
sau justiția

**Reducerea riscurilor -
măsuri proactive** pentru a
preveni discriminarea,
încălcarea confidențialității
sau utilizările abuzive (ex.
recunoașterea facială în timp
real)

Cadru legal uniform - set
unic de reguli valabile în
toate statele UE, oferind
companiilor claritate și
stimulează inovația într-un
mod echitabil



SUA

**Cadrul de management al riscului de
inteligentă artificială**
- AI RMF 1.0 -

Sursa:
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>



**Intrat în vigoare la
26.01.2023**

22.01.2025

Proiectul STARGATE - parteneriat între OpenAI,
Oracle, Softbank din Japonia - condusă de Masayoshi
Son - și MGX, o ramură de investiții în tehnologie a
guvernului Emiratelor Arabe Unite (**500 mld. dolari**)

**Protecția drepturilor
fundamentale** - utilizarea
inteligentei artificiale respectă
valori esențiale precum viața
privată, protecția datelor și
nediscriminarea

AI Act (2021-2024) –
asigurarea unui
mediu sigur și etic
pentru dezvoltarea
și utilizarea AI,
protejând în același
timp drepturile
fundamentale ale
cetățenilor europeni

**Educația în AI (intră în
vigoare în febr.2025)** - toate
companiile și instituțiile
care folosesc platforme AI
asigură educarea
utilizatorilor pentru:

- înțelegerea tehnologiei - de
la modul în care sistemele
generează răspunsuri până
la riscurile halucinațiilor sau
discriminării automate
- prevenirea utilizării greșite
și încurajarea unei integrări
responsabile a AI

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Regulamentul UE privind Inteligența Artificială

adoptat de CE la 13.06.2024

stabilirea unei **structuri de guvernanta** la nivel **european** (Biroul European pt AI - <https://digital-strategy.ec.europa.eu/ro/policies/ai-office>) **și național**

asigurarea **măsurilor aplicabile** pentru **sistemele AI deja introduse pe piață**

stabilirea unei **evaluări a conformității** necesară **înainte** ca **un sistem AI să devină operațional** sau **să fie pus la dispoziția publicului**

definirea obligațiilor specifice impuse dezvoltatorilor și furnizorilor de aplicații AI **cu risc ridicat**

stabilirea **cerințelor clare** pe care trebuie să le îndeplinească **sistemele de inteligență artificială utilizate pentru aplicațiile AI cu risc ridicat**

stabilirea și completarea unei **liste de aplicații** ale tehnologiilor AI **cu un risc ridicat**

interzicerea practicilor AI care constituie **riscuri inacceptabile**

abordarea riscurilor create în mod specific de aplicațiile tehnologiei AI

Calendarul aplicării normelor IA

Etapă	Data	Ce se întâmplă
Intrare în vigoare	1 august 2024	Regulamentul IA devine lege în UE
Primele obligații	februarie 2025	Intră în vigoare interdicțiile pentru sistemele cu risc inacceptabil
Aplicare completă	august 2026	Toate normele devin obligatorii pentru companii și instituții
Aplicare art.6	august 2027	Utilizare sisteme de IA considerate ca prezentând un grad ridicat de risc

- obligația de **a marca conținutul generat de IA** (ca formă și cu surse)
- măsuri pentru **prevenirea generării de conținut ilegal**
- **respectarea drepturilor de autor**

Reguli pentru IA generativă



- sistemul de **management al riscurilor** pe întreg ciclul de viață (art. 9)
- **guvernanta datelor** pentru asigurarea calității și reprezentativității seturilor de antrenament (art. 10)
- **documentația tehnică** (art. 11)
- **înregistrarea și jurnalizarea operațiunilor** (art. 12)
- **transparența** față de utilizatori (art. 13)
- **supravegherea umană** (art. 14)
- **cerințele de precizie și robustețe** (art. 15)

Obligații (din 2 august 2026)



- încurajează AI sandboxes pentru **testare în condiții controlate**
- **reduce birocratia** pentru startup-uri
- oferă **claritate juridică** pentru instituții/companii

Stimularea inovării



- **informarea reprezentanților salariaților și a salariaților afectați** cu privire la faptul că vor fi supuși utilizării sistemului de IA cu risc ridicat, în conformitate cu normele și procedurile europene și naționale aplicabile

- obligația **se adaugă** dispozițiilor existente din **dreptul muncii privind consultarea comitetelor de sănătate și securitate**

Obligații pentru angajatori (art.26 alin.(7))



Codul muncii [art.40 alin.2 lit.e)]
Angajatorul să se consulte cu sindicatul sau, după caz, cu reprezentanții salariaților în privința deciziilor susceptibile să afecteze substanțial drepturile și interesele acestora

informare suplimentară specifică, în conformitate cu cerințele AI Act (v. "**acordul individual**" pentru fiecare "scop" de prelucrare/stocare a datelor cu caracter personal)

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Obligații și răspunderi – AI Act –



Drepturile persoanei vizate în contextul IA

- **dreptul la informare** – să știe că datele sale sunt folosite în sisteme de IA
- **dreptul de acces** – să obțină informații despre modul de prelucrare a datelor sale
- **dreptul la rectificare și ștergere** – acolo unde este cazul
- **dreptul la restricționare și dreptul la opoziție** – inclusiv față de prelucrarea bazată pe interes legitim
- **dreptul de a nu fi supus unei decizii exclusiv automate** cu efecte juridice semnificative sau care îi afectează, în mod similar, fără garanții adecvate

Instituțiile/comaniile trebuie să poată explica/redacta/afișa **în termeni înțeleși de un nespecialist** ce rol are IA într-o anumită decizie, ce date au fost folosite

Prezintă interes:

- cum a fost **proiectat sistemul** (inclusiv mecanismele de supraveghere umană și de corecție)
- ce **limite și disclaimere** au fost comunicate clientului
- cum au fost stabilite **clauzele de răspundere și despăgubire** în contract

Răspundere civilă și comercială pentru deciziile luate cu ajutorul IA

- În cazurile în care partea prejudiciată susține că un sistem de IA a generat o decizie sau o recomandare greșită, discriminatorie sau neglijentă, cum ar fi:
- un candidat respins la angajare contestă un sistem automat de screening bazat pe IA și invocă **discriminare**;
 - un client al unei bănci contestă o decizie de creditare luată cu ajutorul unui model de scoring și invocă **lipsa de transparență sau erori sistematice**
 - un client corporate susține că un model de analiză a documentelor a produs **interpretări greșite**,ducând la pierderi financiare

Riscuri de litigii pentru instituții/companii și dezvoltatori

Litigii de **copyright** și de **proprietate intelectuală**

- titularii de drepturi pot contesta utilizarea operei lor generate fără consimțământ sau fără o excepție legală clară
- se poate pune problema dacă modelul poate genera **reproduceri substanțiale** ale unor opere protejate
- instanțele de judecată pot să fie chemate să stabilească **standardele de diligență** pe care trebuie să le respecte furnizorii de IA

clauzele contractuale trebuie să prevadă ca dezvoltatorul:

- să garantează că **respectă drepturile de autor** și alte **drepturi de proprietate intelectuală**
- se angajează la **despăgubiri** dacă produsul generează litigii de copyright
- acceptă anumite **obligații de transparență** privind seturile de date prelucrate sau modul în care sunt filtrate

Litigii de **protecția datelor**: **investigații** și **amenzi**

- Sanționarea instituțiilor care oferă produse și/sau servicii de IA dacă se constată:
- lipsa unui **temei juridic clar** pentru prelucrare sau utilizare
 - lipsa de transparență față de utilizatori (informări insuficiente, politici opace)
 - necorespunderea **vârstei minime** și de **filtrare a conținutului** pentru minori

În România, ANSPDCP poate iniția **investigații** atât din oficiu, cât și la plângerea persoanelor vizate. Pentru instituții/companii, riscul nu este doar **amenda**, ci și **blocarea unui produs sau serviciu** până la remediarea problemelor

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

- Clasificare sisteme AI -

Regulamentul UE
privind Inteligența Artificială
- 2024/1689 –
adoptat de CE la 13.06.2024



5.02.2025

Practicile interzise (art. 5): limitele absolute

$V > 10^{25}$

AI de uz general (GPAI)

05

IA de uz general
cu risc sistemic
(art.51)

Clasificare sisteme AI

01

**Sistemele AI clasificate ca risc
inacceptabil sunt interzise**
Reprezintă:

- amenințare socială critică la adresa oamenilor, a drepturilor lor și a oricărui aspect social
- sistemele de inteligență artificială care au potențialul a utiliza tehnici subliminale de manipulare sau înșelătoare pentru a distorsiona comportamentul și a împiedica sau îngreuna procesul decizional, precum și sistemele care sunt capabile să exploateze vulnerabilitățile pentru a distorsiona comportamentul normal

02

**Sistemele AI cu risc ridicat pot fi
utilizate numai după ce îndeplinesc
cerințe foarte specifice și stricte**
Trebuie:

- să conțină și să aibă implementate mai multe măsuri de siguranță
- să fie supuse unei evaluări de conformitate, efectuată de un terț și să dețină diferite autorizații
- să fie evaluate de la caz la caz, în funcție de sistemul respectiv, înainte de utilizare

03

AI cu risc limitat

04

Risc minim AI

- model de AI care, printre altele, poate îndeplini **gama largă de sarcini distincte** indiferent de modul în care modelul este introdus pe piață, și care poate fi integrat într-o varietate de sisteme sau aplicații ulterioare
- asigurarea documentației tehnice actualizate** și punerea la dispoziția **EU AI Office**, precum **autorităților naționale de reglementare**

- permise **fără condiții semnificative** aplicațiile de divertisment AI, jocurile video și filtrele de spam ce includ AI)
- în viitor, vor fi probabil **implementate diverse coduri de conduită** privind AI cu risc scăzut

- transparența pentru a asigura o **constientizare adecvată atunci când sunt utilizate sisteme AI**
- conținutul generat de IA** (cum ar fi textul, imaginile sau conținutul audio-video), este **clar identificabil** ca atare
- criterii pentru conținutul generat de AI** destinat utilizării publice pe scară largă

1.Tehnici subliminale sau manipulatorie – sisteme care denaturează semnificativ comportamentul unei persoane prin împiedicarea apreciabilă a capacității de a lua o decizie în cunoștință de cauză [art. 5 alin. (1) lit. a)]

2.Exploatarea vulnerabilităților – sisteme care exploatează vârsta, dizabilitățile sau situația socio-economică [art. 5 alin. (1) lit. b)]

3.Scorul social – clasificarea persoanelor pe baza comportamentului social pentru tratament defavorabil în contexte nejustificate [art. 5 alin. (1) lit. c)]

4.Predicția criminalității pe baza profilării – evaluarea riscului infracțional exclusiv pe baza trăsăturilor de personalitate [art. 5 alin. (1) lit. d)]

5.Extragerea neîntită de imagini faciale – colectarea de pe internet sau din sisteme de supraveghere pentru baze de date de recunoaștere facială [art. 5 alin. (1) lit. e)]

6.Recunoașterea emoțiilor la locul de muncă și în educație – cu excepția motivelor medicale sau de siguranță [art. 5 alin. (1) lit. f)]

7.Categorizarea biometrică pentru date sensibile – deducerea rasei, opiniilor politice, apartenenței sindicale sau orientării sexuale [art. 5 alin. (1) lit. g)]

8.Identificarea biometrică în timp real în spații publice – cu excepții stricte pentru forțele de ordine [art. 5 alin. (1) lit. h)]

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Sistemele de IA clasificate ca prezentând risc ridicat

(Anexa III la IA Act)

– **categorii relevante** instituții/companii

Infrastructura critică - componente de siguranță în gestionarea și exploatarea infrastructurii digitale critice, a traficului rutier sau a aprovizionării cu apă, gaz, încălzire ori energie electrică [Anexa III pct. 2]

Ocuparea forței de muncă și managementul salariaților – sisteme utilizate pentru recrutare, filtrare a candidaturilor, evaluare a performanței, luarea deciziilor privind promovarea sau încetarea raporturilor de muncă [Anexa III pct. 4]

Accesul la servicii esențiale – scoring de credit, evaluarea riscurilor în asigurări, triaj medical, accesul la prestații sociale [Anexa III pct. 5]

Educație și formare profesională – sisteme de admitere, evaluare automată, stabilirea nivelului de educație [Anexa III pct. 3]

Responsabilitățile de-a lungul lanțului valoric al IA (art.25)

• entitatea care dezvoltă sau are un sistem de IA și îl pune pe piață sub numele său sau îl pune pentru prima dată în funcțiune; de regulă, dezvoltatorul modelului sau al aplicației

Furnizor (provider)



• entitatea care folosește efectiv sistemul de IA în propria activitate (de exemplu, o bancă ce folosește un sistem de scoring, o firmă care folosește IA pentru recrutare sau pentru trierea documentelor)

Utilizator / deployer



• dacă sistemul de IA este dezvoltat în afara UE, dar este introdus pe piața UE

Importator



• entitate care distribuie sau revinde sistemul de IA (de exemplu, o firmă care integrează un model dezvoltat de altcineva și îl oferă ca parte dintr-o soluție complexă)

Distribuitor



Obligațiile și expunerea juridică diferă semnificativ în funcție de "rol"

Implicații ale clasificării pentru platformele de semnătură electronică

Majoritatea funcționalităților standard ale semnăturii electronice se încadrează în categoriile cu **risc minim** sau **limitat**. Cu toate acestea, anumite funcții avansate se pot califica drept cu **risc ridicat**

Sistemele de inteligență artificială cu potențial de **risc ridicat pentru semnătura electronică** sunt:

- sistemele de autentificare biometrică
- sistemele de contracte de muncă
- integrarea evaluării creditului
- accesul la servicii esențiale

Cadrele de guvernanta a inteligenței artificiale trebuie să evalueze fiecare caracteristică independent

O singură platformă poate conține mai multe sisteme de inteligență artificială la diferite niveluri de risc, fiecare necesitând măsuri separate de clasificare și conformitate



Companiile și instituțiile trebuie:

- să identifice dacă sistemele lor IA intră în **categoria de risc ridicat**
- să implementeze **măsuri de transparență și supraveghere umană**
- să actualizeze **documentația tehnică și procesele interne**
- să se pregătească pentru **auditori și evaluări de conformitate până în august 2026**

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

conformarea AI Act nu înseamnă automat conformare GDPR și invers
AI Act nu suplinește GDPR și invers

AI Act nu
înlocuiește
GDPR

Regulamentul privind
IA se concentrează pe
siguranța și
conformitatea
sistemelor de
inteligentă artificială
din perspectiva
drepturilor fundamentale
și a pieței interne

GDPR se aplică
integral ori de câte ori
se prelucrează date cu
caracter personal

IA prelucrează
seturi mari de
date
personale:

date istorice de utilizare
log-uri
Conversații
imagini cu persoane
date biometrice
date comportamentale etc.

Din
perspectiva
GDPR,
trebuie
clarificat:

scopul prelucrării (de exemplu, îmbunătățirea
modelului, personalizare, detectarea fraudelor, audit,
cercetare administrativă etc.)

temeiul juridic (de exemplu, interes legitim,
executarea contractului, consimțământul clientului /
angajatului etc.)

dacă nu există **alternative mai puțin
intruzive pentru atingerea aceluiași scop**

datele sensibile, dacă nu se află în zona de **interdicții
sau excepții foarte limitate** prevăzute de GDPR

dezvoltatorii/furnizorii și
responsabilii DPO din
entitățile financiare nu
pot ignora cine deține
"drepturile de acces"
asupra datelor
prelucrate/folosite
prin modelare IA

Riscuri principale în "procesul
decizional automatizat" de
prelucrare a datelor cu caracter
personal

**supraestimarea interesului
legitim** ca temei pentru prelucrare

reidentificarea datelor (în lipsa
criptării), întrucât „anonimizarea”
este deseori mai
degrabă "pseudonimizare"

**nelimitarea scopului de
prelucrare** continuă (acceptul
inițial de colectare și prelucrare a
datelor nu reprezintă consensul
"general valabil" pentru orice
scop generat prin IA)

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Recomandări minime

(cf **IA Act**, **GDPR** și **drepturi autor**)

- să existe **clauze contractuale explicite** prin care furnizorul/beneficiarul de model IA garantează că dispune de o **bază legală pentru a utiliza datele** de prelucrat/stocat, **în raport cu gradul de confidențialitate** al datelor (**GDPR sau clasificate**)
- titularii de drepturi (autori, fotografi, editori, platforme) să formuleze **cereri de despăgubire** sau să solicite **informații detaliate** despre modul de prelucrare și stocare a datelor
- prevenirea situațiilor de apariție a **litigiilor strategice** menite să clarifice dacă anumite forme de "scraping de date" masiv sau de utilizare a bazelor de date **sunt sau nu compatibile** cu dreptul de autor/proprietate intelectuală și cu **drepturile de accesare** a lor

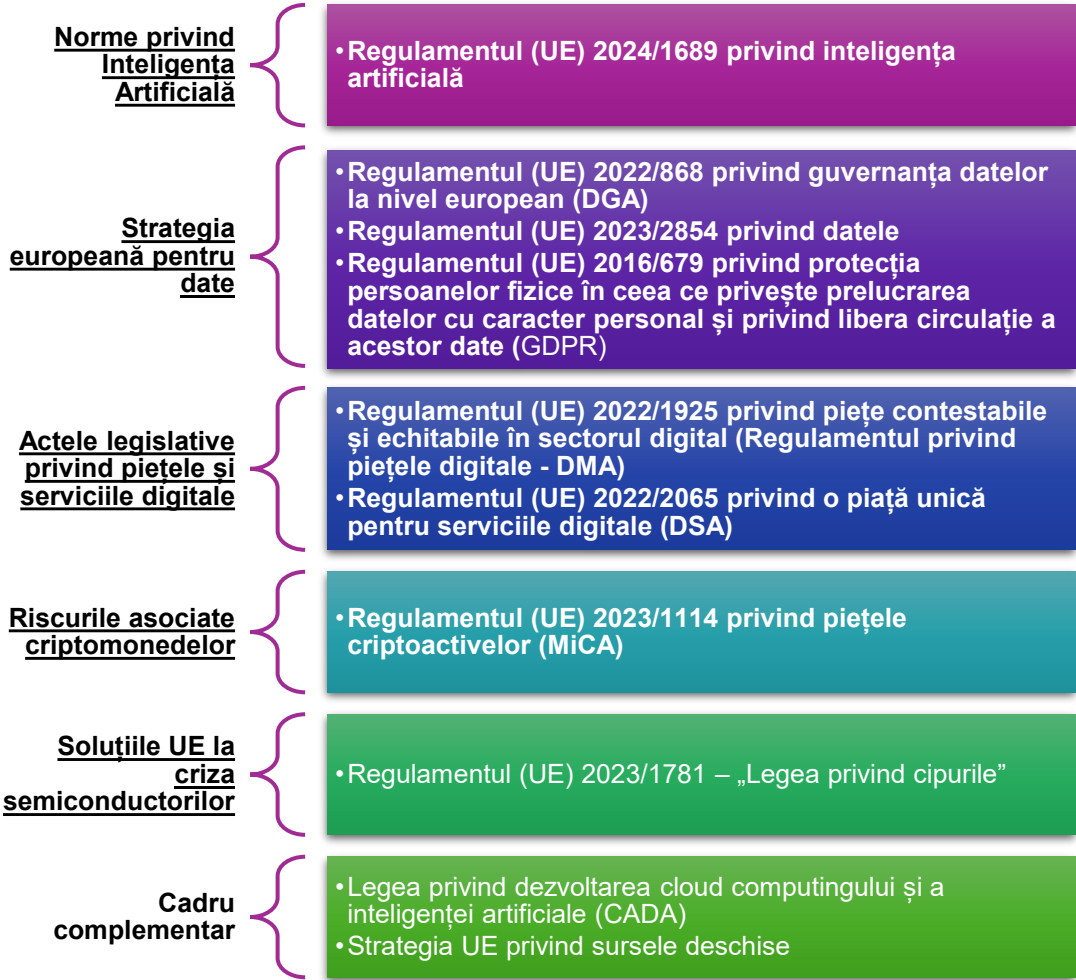
Sanțiuni (art.99)

- **35.000.000 EUR sau 7% din cifra de afaceri mondială** – pentru încălcarea practicilor interzise (art. 5)
- **15.000.000 EUR sau 3% din cifra de afaceri mondială** – pentru nerespectarea obligațiilor privind sistemele cu risc ridicat
- **7.500.000 EUR sau 1% din cifra de afaceri mondială** – pentru furnizarea de informații incorecte autorităților

- ☐ Se aplică întotdeauna cuantumul mai mare (dacă există fapte cumulative)
- ☐ Pentru **IMM-uri și întreprinderi nou-înființate**, **Regulamentul IA** prevede posibilitatea unor sancțiuni reduse proporțional, sub rezerva evaluării circumstanțelor fiecărui caz

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Legislație unitară
și echilibrată



Element	NIS2	DORA	CRA
Tip act	Directivă UE (transpusă în lege națională)	Regulament UE direct aplicabil	Regulament UE direct aplicabil
Focus principal	Securitatea rețelelor și sistemelor IT ale entităților esențiale/ importante	Reziliența operațională digitală a entităților financiare	Securitatea produselor digitale (software, hardware, IoT)
Aplicare	Energie, transport, sănătate, apă, digital, administrație, etc.	Bănci, IFN, asigurări, piețe de capital, furnizori ICT critici pentru financiar	Producători, importatori, distribuitori de produse digitale
Obiectiv	Nivel comun ridicat de securitate cibernetică în UE	Asigurarea continuității și rezilienței serviciilor financiare	Produse digitale sigure „by design” și „by default”
Managementul riscurilor	Obligație de măsuri tehnice și organizatorice adecvate (Art. 21)	Cadrul complet de management al riscurilor ICT (guvernanta, procese, controale)	Evaluare riscuri de securitate pentru fiecare produs digital
Măsuri tehnice	Control acces, criptare, jurnalizare, monitorizare, management vulnerabilități, backup, DRP (Art. 21)	Controale ICT pentru confidențialitate, integritate, disponibilitate, continuitate (inclusiv DRP, logging, monitorizare)	Secure by design, secure by default, criptare, patching, SBOM, jurnalizare, testare securitate
Măsuri organizaționale	Politici, roluri, training, management furnizori, plan răspuns la incidente (Art. 21)	Guvernanta ICT, comitete, roluri, politici, TPRM, audit, raportare către board	Procese interne de dezvoltare securizată, management vulnerabilități, documentație tehnică, control supply-chain
Raportare incidente	Notificare „fără întârziere”, structurată: 24h (early warning), 72h (raport intermediar), raport final (max 1 lună) – Art. 23	Raportare incidentelor majore ICT către autoritățile financiare, structură similară (early, intermediate, final)	Raportare vulnerabilități exploatate și incidente de securitate către ENISA în termene scurte (24h/72h/30 zile)
Third-party / furnizori	Cerințe de securitate și due-diligence pentru lanțul de furnizori (Art. 28)	Regim foarte strict pentru furnizori ICT critici (TPRM, drept de audit, acces autorități)	Control asupra componentelor și furnizorilor din lanțul de aprovizionare software/hardware
Testare securitate	Teste tehnice periodice, inclusiv pentru continuitate (Art. 21)	Testare regulată + TLPT (Threat-Led Penetration Testing) pentru entități semnificative	Testare securitate a produselor înainte și după lansare
Orientare	„Service-centric” – protecția serviciilor esențiale	„Firm-centric & ecosystem-centric” – reziliența entităților financiare și a furnizorilor lor	„Product-centric” – securitatea produselor digitale pe tot ciclul de viață

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

DOCUMENTE CONEXE

Regulamentul (UE) [2021/1153](#) al Parlamentului European și al Consiliului din 7 iulie 2021 de **instituire a Mecanismului pentru interconectarea Europei** și de abrogare a Regulamentelor (UE) nr. 1316/2013 și (UE) nr. 283/2014

Regulamentul (UE) [2021/947](#) al Parlamentului European și al Consiliului din 9 iunie 2021 de **instituire a Instrumentului de vecinătate, cooperare pentru dezvoltare și cooperare internațională – Europa globală**, de modificare și abrogare a Deciziei nr. 466/2014/UE a Parlamentului European și a Consiliului și de abrogare a Regulamentului (UE) 2017/1601 al Parlamentului European și al Consiliului și a Regulamentului (CE, Euratom) nr. 480/2009 al Consiliului

Decizia (UE) [2021/764](#) a Consiliului din 10 mai 2021 de **instituire a programului specific de implementare a Programului-cadru pentru cercetare și inovare Orizont Europa** și de abrogare a Deciziei 2013/743/UE

Decizia (PESC) [2021/698](#) a Consiliului din 30 aprilie 2021 privind **securitatea sistemelor și a serviciilor care sunt desfășurate, care funcționează și care sunt utilizate în cadrul programului spațial al Uniunii și care ar putea afecta securitatea Uniunii** și de abrogare a Deciziei 2014/496/PESC

Regulamentul (UE) [2021/695](#) al Parlamentului European și al Consiliului din 28 aprilie 2021 de **instituire a programului-cadru pentru cercetare și inovare Orizont Europa, de stabilire a normelor sale de participare și de diseminare** și de abrogare a Regulamentelor (UE) nr. 1290/2013 și (UE) nr. 1291/2013

Regulamentul (UE) [2021/694](#) al Parlamentului European și al Consiliului din 29 aprilie 2021 de **instituire a programului Europa digitală** și de abrogare a Deciziei (UE) 2015/2240

Regulamentul (UE, Euratom) [2018/1046](#) al Parlamentului European și al Consiliului din 18 iulie 2018 privind **normele financiare aplicabile bugetului general al Uniunii**, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012

Regulamentul (UE) 2024/795 de **instituire a platformei „Tehnologii strategice pentru Europa” (STEP)**, pentru următoarele sectoare:

tehnologiile digitale, inclusiv cele care contribuie la atingerea țintelor și obiectivelor programului de politică pentru 2030 privind deceniul digital,

tehnologiile curate și eficiente din punctul de vedere al utilizării resurselor, inclusiv tehnologiile „zero net”, astfel cum sunt definite în **Regulamentul privind industria „zero net”**

biotehnologii, inclusiv medicamente aflate pe lista de medicamente esențiale

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

- Legislație conexă Regulament AI -

„Noul cadru legislativ pentru comercializarea produselor” (pentru **normele aplicabile** introducerii pe piață, punerii în funcțiune și utilizării **sistemelor de IA cu risc ridicat**)



Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului care stabilește **cerințele pentru acreditare și supravegherea pieței produselor**



Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului privind un **cadru comun pentru comercializarea produselor**



Regulamentul (UE) 2019/1020 al Parlamentului European și a Consiliului privind **supravegherea pieței și conformitatea produselor**

- la nivel național -

martie 2026



ANCOM (Autoritatea Națională pentru Administrare și Reglementare în Comunicații) - autoritate națională de supraveghere a pieței și punct unic de contact

➤ colaborează cu **BNR** și **ASF** pentru sistemele IA din ariile financiare

Ministerul Cercetării, Inovării și Digitalizării a supus aprobării Guvernului României:

- **HG nr. 832/11.07.2024** privind **aprobarea Strategiei Naționale pentru Inteligența Artificială 2024-2027**

- **HG nr. 1028/21.08.2024** privind **aprobarea Strategiei naționale în domeniul tehnologiilor cuantice pentru perioada 2024-2029**

Grupul de experți la nivel înalt privind inteligența artificială:



➤ **Planul coordonat privind inteligența artificială**

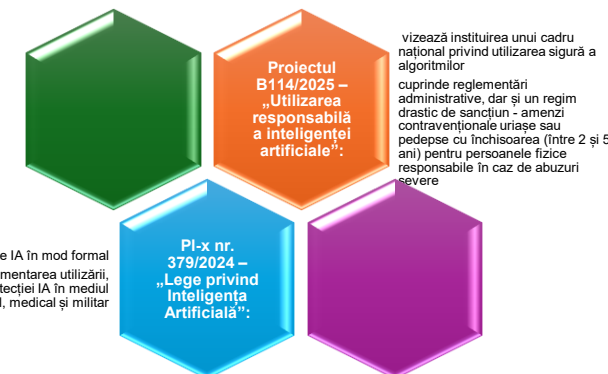
Sursa: <https://digital-strategy.ec.europa.eu/ro/policies/plan-ai>

➤ **Cartea albă privind inteligența artificială: o abordare europeană a excelenței și încrederii**

Sursa: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=LEGISUM:white_paper

➤ **Ghidul de etică al Comisiei Europene pentru Inteligența Artificială de încredere (Guidelines for Trustworthy AI)**

Sursa: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_RO.pdf



Considerații privind guvernanta IA, gestionarea riscurilor și compliance



obligații de reglementare și răspuns proactiv la incidente

Operatorii de servicii esențiale

- continuă să fie reglementați în sectoare precum generarea și distribuția energiei, rețelele de transport, alimentarea și tratarea apei (inclusiv apa potabilă), serviciile de asistență medicală și infrastructura digitală
- acestor organizații li se aplică **Directiva NIS din 2018**, dar se vor confrunta cu cerințe sporite în temeiul noului cadru

Furnizorii de servicii digitale

- includ piețele online, motoarele de căutare și furnizorii de servicii de cloud computing deja reglementați în temeiul normelor actuale, cu **obligații extinse în temeiul Legii CRA**

Furnizorii de servicii critice

- reprezintă cea mai semnificativă expansiune
- care oferă administrare IT la distanță, gestionare în cloud, monitorizare a securității sau alte servicii IT terțe companiilor se vor confrunta cu **aceleași obligații de securitate și raportare a incidentelor ca și operatorii de servicii esențiale**

Centrele de date

- care îndeplinesc anumite praguri de putere devin entități reglementate, recunoscându-se rolul lor de **infrastructură de bază pentru economia digitală**

„Actul privind reziliența cibernetică” (CRA) - Regulamentul (UE) 2024/2847 privind cerințele de securitate cibernetică pentru produsele cu elemente digitale (inclusiv software și hardware) și de modificare a Regulamentului (UE) 2019/1020
în vigoare la 10.12.2024 / aplicat de la 11.12.2027
completează NIS2 și DORA

- standardizare
- măsuri unitare

- reguli achiziție produse cu elemente digitale, pentru a garanta securitatea cibernetică
- cerințe de proiectare, dezvoltare și producție a acestor produse
- cerințe esențiale pentru procesele de management al vulnerabilităților instituite de producători
- supravegherea pieței digitale și aplicarea legii

Cerințe uniforme de securitate cibernetică pentru proiectarea, dezvoltarea și producția **produselor digitale** (laptopuri, smartphone-uri, dispozitive pentru casă inteligentă și sisteme industriale)

Marcajul CE pentru conformitatea cu securitatea cibernetică (respectă standardele UE de siguranță, sănătate și protecție a mediului)

se aplică tuturor produselor conectate la o rețea sau la un alt dispozitiv – direct sau indirect (cu excepția dispozitivelor medicale, produselor aeronautice și autovehiculelor)

îmbunătățește transparența și oferă consumatorilor posibilitatea de a lua decizii informate în ceea ce privește **caracteristicile de securitate cibernetică ale produselor digitale**

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Obligații principale pentru o instituție / firmă din România care folosește IA

✦ 1. Identificarea nivelului de risc al sistemului IA

Risc inacceptabil → interzise complet

Risc ridicat → obligații stricte

Risc limitat → transparență

Risc minim → fără obligații speciale

■ 2. Dacă folosiți IA cu *risc ridicat* (HR, sănătate, educație, scoring, securitate, IT)

✓ Evaluare de conformitate înainte de utilizare

Trebuie verificat dacă sistemul respectă cerințele tehnice și legale.

Uneori este necesară certificare externă

✓ Documentație tehnică detaliată

Descrierea modelului, a datelor folosite, a riscurilor și a măsurilor de control.

Trebuie păstrată și prezentată autorităților la cerere.

✓ Managementul riscurilor

Identificarea riscurilor pentru sănătate, siguranță și drepturi fundamentale.

Implementarea de măsuri pentru reducerea lor.

✓ Calitatea datelor

Date curate, reprezentative, fără bias sistemic.

✓ Supraveghere umană obligatorie

Deciziile automate nu pot fi finale în domenii sensibile (ex.: recrutare).

✓ Monitorizare continuă

Firma trebuie să urmărească performanța sistemului și să raporteze incidentele grave.

■ 3. Dacă folosiți IA cu *risc limitat* (chatboturi, generare de text, deepfake-uri)

Obligații:

Informarea utilizatorilor că interacționează cu un sistem IA

Marcarea conținutului generat (ex.: deepfake).

Politici interne privind utilizarea responsabilă

■ 4. Dacă folosiți IA cu *utilizare generală* (ex.: modele mari de limbaj)

Acestea au obligații suplimentare:

Documentație tehnică completă

Politică privind drepturile de autor

Rezumat al datelor de antrenament

■ 5. Dacă folosiți IA cu *risc minim*

Nu sunt obligații speciale, dar este recomandată o **politică internă de utilizare responsabilă**

- 
- **Jurist / avocat specializat**
 - **Responsabilitate DPO**

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

2025

Peisajul amenințărilor spațiale dominat de:

- ✓ Creșterea masivă a dependenței de infrastructura spațială
- ✓ Amenințările cibernetice
- ✓ Amenințările asupra sateliților și constelațiilor
- ✓ Amenințările pe lanțul de aprovizionare
- ✓ Amenințările geopolitice și militare
- ✓ Amenințările tehnice structurale
- ✓ Peisajul actorilor amenințători

Tendințe

numărul
sateliților activi
depășește
10.000

peste 60%
sunt operați
de entități
private

amplificare
suprafață de
atac și
vulnerabilități
sistemice

**servicii
afectate**

Riscul spațial global



**operatorii
comerciali** - ținte
strategice



lanțul de aprovizionare -
vulnerabilitate
structurală



**amenințările cresc în
intensitate din cauza
conflictelor geopolitice**



**atacurile încă digitale,
nu fizice, dar pot avea
efecte fizice (coliziuni,
dereglări orbitale)**



sectorul spațial -
parte a suprafeței
critice globale de atac

Surse: <https://aerospace.csis.org/>
<https://www.enisa.europa.eu/>
<https://www.weforum.org/>
<https://www.baesystems.com/en>
<https://www.kratospace.com/>
<https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/>

Considerații privind guvernanta IA, gestionarea riscurilor și compliance

Inteligența Artificială – accelerarea deciziilor și automatizarea apărării

IA devine un **multiplicator de forță în securitate**

- **Detectarea automată a atacurilor cibernetice** în timp real
- **Analiza predictivă** a comportamentelor ostile
- **Automatizarea răspunsului** la incidente
- **Identificarea deepfake-urilor** și a manipulărilor informaționale
- **Optimizarea apărării infrastructurilor critice**

Tendințe majore



- **Apărare individuală**
 - Protecție sporită împotriva fraudelor digitale
 - Sisteme AI care detectează tentative de phishing sau acces neautorizat
 - Asistenți personali de securitate digitală
- **Apărare comună**
 - Rețele naționale de detecție a atacurilor
 - Cooperare între state prin schimb automatizat de date
 - Sisteme AI care analizează fluxuri masive de informații pentru a anticipa atacuri coordonate

Implicații pentru apărare



Supravegherea satelitară – ”ochiul strategic” al apărării moderne

Satelitul nu mai este doar un instrument militar; devine un **element central al securității globale**

- **Imagini satelitare în timp aproape real**
- **Monitorizarea frontierelor și a infrastructurilor critice**
- **Detectarea activităților suspecte** (deplasări, acumulări de resurse, perturbări)
- **Integrarea cu AI pentru analiză automată**
- **Sisteme de avertizare timpurie** pentru dezastre, atacuri sau activități neobișnuite

Tendințe majore



- **Apărare individuală**
 - Protecție în situații de urgență (inundații, incendii, cutremure)
 - Sisteme de navigație și avertizare mai precise
 - Monitorizarea zonelor de risc
- **Apărare comună**
 - Supravegherea teritoriilor naționale
 - Monitorizarea activităților militare sau teroriste
 - Sprijin pentru operațiuni NATO și UE
 - Capacitatea de a detecta atacuri asupra infrastructurilor energetice, de transport sau comunicații

Implicații pentru apărare



- Supraveghere excesivă (privacy)
- **Atacuri asupra sistemelor AI**
- **Manipularea datelor satelitare**
- Dependență tehnologică ridicată
- **Vulnerabilități în lanțul de aprovizionare**
- Escaladare geopolitică prin interpretări automat



Riscuri și provocări



Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

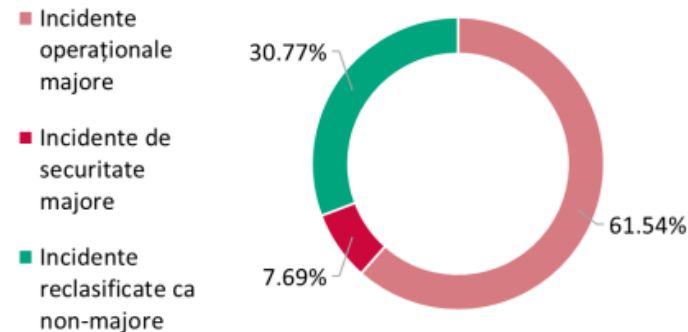
"Reziliența actuală este, în esență, defensivă. Sistemul bancar este bine capitalizat pentru a absorbi șocuri, dar **nu este configurat pentru a internaliza și gestiona risc strategic pe termen lung**. Creditarea rămâne predominant bazată pe colateral tangibil și pe performanță istorică. **Modelele de risc sunt, în mare măsură, retrospective**. Ele analizează bilanțuri, fluxuri de numerar trecute și indicatori contabili deja materializați. Reindustrializarea, însă, presupune evaluarea unor perioade de maturizare investițională în care cash-flow-ul este negativ în primii ani."

Marius Dănilă – *Iluzia stabilității* (2026, Academia Română)

S1/2025

Banca Națională a României

- 0 amenințări cibernetice semnificative
- 8 incidente de securitate majore
- 12 incidente operaționale majore
- 4 reclasificate ca non-majore



Structura incidentelor raportate în semestrul 1 al anului 2025

Sursa: Banca Națională a României, **Raport asupra stabilității financiare, dec.2025**

[:025-12-09raportasuprastabilit%C4%83%C8%9Bifinanciare-decembrie2025_documentpdf_545_1765290572.pdf](https://www.bnr.ro/uploads/2025-12-09raportasuprastabilit%C4%83%C8%9Bifinanciare-decembrie2025_documentpdf_545_1765290572.pdf)

iMPACT



Consecințe

- Durata de manifestare a incidentelor ≤ 22 ore (un caz special cu decontare a doua zi)
- Indisponibilitatea serviciilor afectate ≤ 14 ore

Incidentele operaționale majore raportate, cauzate de:

monitorizarea și controlul deficitar al proceselor sau gestionarea eronată a capacității de procesare, identității și accesului

disfuncționalități la nivelul proceselor, sistemelor sau infrastructurii utilizate

gestionarea necorespunzătoare a schimbărilor și erori privind configurații ale rețelelor și a software-ului

3 incidente determinate de cauze externe

necesitatea de a monitoriza furnizorii terți de servicii TIC în mod adecvat

- evaluarea riscurilor
- conformitate DORA
- testarea rezilienței (TLPT)
- monitorizare continuă

S2/2025

incidentele de securitate cibernetică pot destabiliza lichiditatea bancară, ceea ce impune modernizarea urgentă a sistemelor de monitorizare și evaluare a riscurilor

Sursa: Banca Națională a României, **Raport asupra stabilității financiare, iun.2026**

https://www.bnr.ro/uploads/2026-07-06raportasuprastabilitatiifinanciare-iunie2026_documentpdf_545_1783339608.pdf

Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

Internetul în expansiune,
dar riscurile tratate redus

Securitate IT rudimentară

- antivirus de bază, firewall simplu, backup manual
- reacție minimă la incidente, fără echipe dedicate
- amenințări: viruși și viermi precum ILOVEYOU (2000), care a provocat pagube de ~10 miliarde USD
- securitatea - „o **activitate secundară**” pentru majoritatea organizațiilor



Atacatorii evoluează mai repede
decât capacitatea de reacție

- securitatea răspunde doar după apariția incidentelor.
- introducerea sistemelor IDS/IPS timpurii.



Apărare reactivă

- creșterea criminalității cibernetice (ex.: atacul TJX – 94 milioane de clienți afectați în 2007)
- apar primele breșe masive de date



Transformarea digitală și IoT
extind suprafața de atac

- echipe dedicate: SOC, CSIRT, CERT
- răspuns coordonat la incidente, proceduri standardizate



Apărare coordonată

- creșterea atacurilor complexe: inginerie socială, ransomware, breșe gigantice precum Yahoo (3 miliarde de conturi afectate)
- apar reglementări și standarde (NIST, ISO 27001)



Reziliență la nivel de
ecosistem,
nu doar la nivel de organizație

Apărare multi-domeniu / pro-activă

- integrarea securității IT, OT, cloud, IoT, telecom, infrastructuri critice
- cooperare internațională și legislație avansată
- UE adoptă legi pentru reziliență cibernetică, inclusiv *Regulamentul privind reziliența cibernetică* (2024) și *Planul de acțiune pentru gestionarea crizelor cibernetice* (2025)



Sisteme care se
auto-optimizează
și se auto-apără

Apărare autonomă / predictivă

- utilizarea AI/ML pentru detectarea anomaliilor și răspuns automat
- predicția atacurilor pe baza comportamentelor și a datelor globale.
- Automatizarea răspunsului la incidente (SOAR)
- pregătire pentru amenințări emergente: calcul cuantic, atacuri asupra infrastructurilor critice, ransomware avansat



Etapă	Caracteristici	Nivel maturitate	Exemplu
Securitate rudimentară	Antivirus, firewall simplu	Scăzut	Viruși anii 2000
Apărare reactivă	Răspuns după incident	Mediu	Atacul TJX 2007
Apărare coordonată	SOC, CSIRT, proceduri	Bun	Breșa Yahoo 2013
Apărare multi-domeniu	IT+OT+IoT+Cloud	Avansat	Legislația UE 2024–2025
Apărare autonomă & predictivă	AI, ML, automatizare	Foarte avansat	Detectare automată ransomware



Cyber-defence
(maturitate / încredere)



Tendințe majore în evoluția cyber-defence



Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

Un climat de securitate nu mai înseamnă doar firewall-uri și parole puternice, ci și:



reziliență psihologică



educație digitală continuă



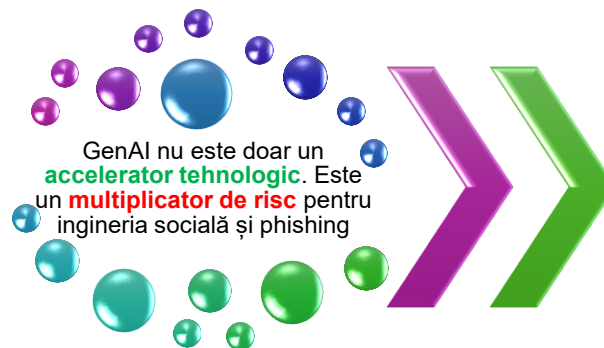
sisteme automate de detecție



verificare multi-factorială



monitorizare comportamentală



Organizațiile care vor reuși să mențină un climat de securitate sunt cele care:

- tratează oamenii ca parte a sistemului de apărare
- implementează verificări robuste ale identității
- folosesc IA defensivă pentru a contracara IA ofensivă
- reduc suprafața de atac informațională
- colaborează activ cu ecosistemul de securitate și privat
- investesc în reziliență, nu doar în prevenție



1. Crește presiunea asupra utilizatorilor
Oamenii devin ținte directe, nu doar sistemele. Erorile umane devin inevitabile.
2. Organizațiile trebuie să treacă la apărare proactivă
Nu mai este suficient să reacționezi. Trebuie să:
 - anticipezi
 - simulezi
 - educi continuu
3. Apărarea devine un efort colectiv
NATO, UE și statele membre investesc în:
 - centre de răspuns rapid
 - schimb de informații
 - standarde comune de securitate
4. Încrederea devine o resursă strategică
Într-o lume cu deepfake-uri și mesaje generate de AI, încrederea devine fragilă. Organizațiile trebuie să o protejeze activ.

23.05.2026

Integrarea tehnologiilor EDR, XDR, SIEM & SOAR
Și fluxul modern de operațiuni de securitate (SOC)

Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

Avantajul unui flux complet integrat

Scenariul 1: Detectare și izolare Ransomware

Scenariul 2: Phishing & Spear-phishing & BEC - Securizarea Conturilor de Email

Procesul manual (fără Integrare)

- **Analistul uman** trebuie să observe alerta în XDR
 - Căutare manuală în SIEM pentru a identifica alte PC-uri afectate
 - Autentificare în Active Directory pentru a bloca utilizatorul
 - Crearea manuală a unui tichet de incident

🕒 Durată: **Între 30 de minute și câteva ore**
(timp în care **ransomware-ul poate cripta întreaga instituție**)

Procesul Automatizat (XDR + SIEM + SOAR)

- Colectare, corelare și izolare primară instantanee
- Scanare globală automată a jurnalelor din rețea
- Blocare automată la nivel de Firewall și Identity Provider
- Notificare imediată în SOC și instrumente de ticketing

⚡ Durată: **Primii 9 pași** se execută în **mai puțin de 60 de secunde**

Faza 1: Detectarea și prima reacție (Rolul XDR)



Pasul 1: Un server critic din companie începe brusc să modifice extensiile fișierelor într-un ritm alert (comportament tipic de ransomware).



Pasul 2: XDR detectează activitatea suspectă prin analiza comportamentală (AI), blochează procesul malițios pe acel server și izolează serverul din rețea pentru a opri răspândirea virusului.



Pasul 3: XDR adună toate dovezile (adrese IP externe apelate, fișiere afectate, chei de regiștri modificate) și trimite o alertă consolidată.

Faza 2: Centralizarea informațiilor și contextul (Rolul SIEM)

Pasul 4: SIEM primește alerta de la XDR și o analizează în context global.

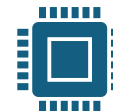
Pasul 5: SIEM verifică celelalte jurnale (logs) din rețea și observă că același IP extern suspect a încercat să comunice cu alte 3 calculatoare din companie cu 10 minute în urmă.

Pasul 6: SIEM ridică nivelul de severitate la Critic și trimite o directivă către SOAR pentru pornirea playbook-ului de urgență.

Faza 3: Orchestrarea și Răspunsul Extins (Rolul SOAR)



Pasul 7: SOAR pornește automat playbook-ul "Incident Ransomware Confirmat"



Pasul 8 (Acțiuni automate în infrastructură):

- Interfațează cu Firewall-ul și blochează complet adresele IP externe malițioase la nivelul întregii companii.
- Interfațează cu Identity Provider-ul (ex: Entra ID / AD) și suspendă contul de utilizator compromis.



Pasul 9 (Acțiuni de management al incidentului):

- Deschide automat un tichet cu prioritate maximă în Jira sau ServiceNow.
- Trimite o alertă urgentă pe canalul de Slack sau Teams al echipei de securitate (SOC).



Pasul 10 (Intervenția umană / Decizia finală):

- SOAR trimite o notificare pe telefonul analistului cu butonul: [Aprobă scanarea completă și restaurarea din Backup].
- Odată aprobat, SOAR comandă sistemului de backup să verifice ultima copie sigură.

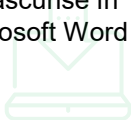
supraveghere strictă a comportamentului furnizorilor - "iluzia invulnerabilității"

AMENINȚAREA HookEdge – Campanie de Spionaj APT28 în Europa

sept. 2025 –
aprilie 2026

HookEdge

- **linie de malware recent descoperită**, ce funcționează ca un **backdoor** (ușă din spate) **bazat pe scripturi** Windows Batch și macrocomenzi ascunse în documente Microsoft Word corporative



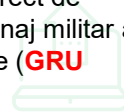
Vectorul de atac

- oficiali
- diplomați
- guverne
- instituții guvernamentale din state membre NATO din Europa, inclusiv **România, Spania** și **Turcia**



Gruparea din spate

- Atacul este coordonat de **APT28** (cunoscută și ca *Fancy Bear*, *BlueDelta* sau *Forest Blizzard*), o **grupare de criminalitate cibernetică de elită**, sponsorizată direct de agenția de spionaj militar a Federației Ruse (**GRU Unit 26165**)



Context global

Natura atacului

- **Spionaj politic și militar discret**, utilizând **infrastructură cu costuri reduse**

Evoluție malware

- **HookEdge** reprezintă o **evoluție directă a backdoor-ului** anterior numit **HeadLace**



Cum funcționează - Lanțul de Atac (Kill Chain) & Tehnici

1. Vector Inițial

- **E-mailuri de spear-phishing cu "momeală" Word** (.doc/.docx) conținând **macrocomenzi malițioase** și **afișând utilizatorului o eroare falsă**

2. Instalare

- utilizatorul activează **browserul Microsoft Edge**
- Rutina scrie **fișiere batch**, VBScript, HTML în directorul **utilizatorului**, configurează un **task programat - instanțele invizibile („headless”)** ale browserului Microsoft Edge și **șterge kitul inițial**

3. Execuție (C2) și Persistență

- **procese Edge ascunse** **interoghează endpoint-uri publice de tip webhook** (ex. **webhook.site**) **la 30/61 min** pentru a primi comenzi.
- **sistemul de operare crede că utilizatorul naviguează normal** pe internet dar, în realitate, **acea "instanță ascunsă" execută comenzile hackerilor**

4. Exfiltrare și curățare Urme

- **trimite datele furate la fiecare 5 min** pentru victimele validate ca valoroase.
- un **script de instalare** în mai multe etape **elimină artefactele inițiale pentru a împiedica detecția timpurie**



Impact de risc

- **risc major** pentru organizațiile europene **dependente de sistemele de comunicații** pentru **exfiltrare documente și date** politice/ militare sensibile / **clasificate**



Oportunități de utilizare a IA pentru îmbunătățirea rezilienței operaționale a sectorului financiar-bancar

Scrisoarea BCE (SSM-2026-0301 din 7 iulie 2026)

Sursa:

https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2026/ssm.2026_letter_on_AI_enabled_cybersecurity_threats.en.pdf

- ❑ adoptă o **poziție preventivă și strictă privind utilizarea inteligenței artificiale (IA) în sectorul bancar**, tratând-o ca pe o **prioritate strategică** legată de **stabilitatea financiară și riscul cibernetic**
- ❑ solicită băncilor supravegheate să prezinte **planuri de acțiune detaliate pentru gestionarea riscurilor asociate modelelor de IA**, până la **31 octombrie 2026**, cu:
 - *alocare resurse necesare*
 - *clarificare responsabilități*
 - *stabilire termene clare de implementare* a cerințelor legale care **să demonstreze conformitatea cu DORA și să răspundă la amenințările cibernetice facilitate de IA**
- ❑ prelungirea termenului pentru **completarea Chestionarului de Risc IT, din septembrie 2026 în februarie 2027**, nu este o simplă amânare birocratică, ci reprezintă o **oportunitate critică de calibrare** pentru managementul instituțional și o **relaxare tactică** oferită cu un scop precis: **aliniera perfectă a conformității cu execuția tehnică**.

Capcana „trivializării” vs. Adoptarea strategică

- tendința de a folosi **IA doar de dragul trendului tehnologic** (utilizări superficiale)
- instituțiile financiare trebuie să integreze IA în mod structurat, evaluând direct **modul în care algoritmi influențează** deciziile de creditare, interacțiunea cu clienții și managementul riscului

Guvernanța și controlul uman (human oversight)

- necesitatea menținerii unui **control uman strict asupra deciziilor luate de sistemele autonome**
- instituțiile de credit trebuie să aibă **capacitatea de a înțelege și de a explica modelele AI folosite** (conceptul de *explainable IA*), evitând fenomenul de tip „**cutie neagră**” în care nimeni nu știe cum s-a ajuns la un anumit rezultat financiar

Alinierea la reglementările europene

- **integrarea IA în bănci** se bazează pe un cadru de reglementare strict - **AI Act** și normele privind reziliența operațională – **DORA**
- supraveghetorii bancari (precum BCE și băncile centrale naționale) pun accentul pe **securitatea datelor, protecția consumatorilor și prevenirea riscurilor sistemice** generate de erori de algoritm



corelarea dintre raportarea incidentelor IA și cerințele DORA
orice sistem IA utilizat într-o bancă sau instituție financiară este **clasificat tehnic drept capabilitate (sistem) TIC** și, prin urmare, raportarea unei breșe de securitate sau a unei disfuncționalități generate de un algoritm IA se va realiza **prin canalele și termenele ultra-rapide impuse de DORA** (de ex. **BNR/ASF/DNSC**)

Proiecții viitoare, strategice



"Banca vorbește în procente, clienții în insomnii."

Sistemul bancar românesc funcționează. Este stabil, reglementat și, în comparație cu trecutul, incomparabil mai solid. Și totuși, pentru mulți dintre cei care interacționează cu el, rămâne un sistem în care **încrederea este fragilă**."

Marius Dănilă – Iluzia stabilității (2026, Academia Română)

2026-2036

Prognoză

Contextul geopolitic actual și datoriile publice ridicate vor menține o **presiune constantă asupra stabilității financiare globale**

Tehnologia nu mai este doar un instrument de suport, ci devine **fundamentul noului ecosistem financiar**

Conceptul de "bani" se transformă prin digitalizarea monedelor fiduciare și modernizarea infrastructurii de plată

Peisajul financiar devine multipolar, reducând dependența de instituțiile occidentale tradiționale



AMENINȚĂRI NOI

Mesaje în mediul virtual

"Aveți nevoie de o arhitectură AI aliniată cu DORA?"

Construim sisteme de inteligență artificială care îndeplinesc cerințele DORA încă din prima zi. Audituri, guvernanță, pregătire pentru ieșire - încorporate, nu fixate"

Firme care crează "platforme SIEM prin integrarea de platforme SIEM"

simple "**cochilii tehnologice**", cu rol de barieră exterioară, dar care **riscă să fie goale pe dinăuntru** sau **deconectate de "organismul viu"** - **procesele de business** -, **dacă nu sunt corelate** cu:

- **politicile și procedurile** de lucru administrative **aprobate**
- alte **acte încheiate între părți**, ca și componente ale "**Governance-to-Technology mapping**"

Supraveghere strictă a comportamentului furnizorilor

Băncile riscă să plătească în continuare **prețuri de monopol pentru o "iluzie a invulnerabilității"** și, paradoxal, pot deveni **mai fragile în fața riscurilor sistemice** deja prefigurate ori chiar nou generate prin încrederea acordată terților

SIEM-ul monitorizează întreaga infrastructură bancară

potrivit **art.30 alin.(3) din Regulamentul DORA**, în contract, furnizorul trebuie să declare explicit **natura critică a serviciului**, alături de toate celelalte cerințe minime legale

Governance-to-Technology mapping (Cartografierea Guvernanței pe Tehnologie)

Conceptul derivă din **managementul riscului și conformității automate** (GRC - Governance, Risk, and Compliance)

- ISACA (2019) – COBIT 2019 Framework: Governance and Management Objectives
- ISO/IEC 38500:2024 – Information technology — Governance of IT for the organization
- NIST (2018/2024) – NIST Cybersecurity Framework (CSF 2.0)



TENDINȚE

Proiecții viitoare, strategice

Riscuri și provocări

Riscuri Cibernetice

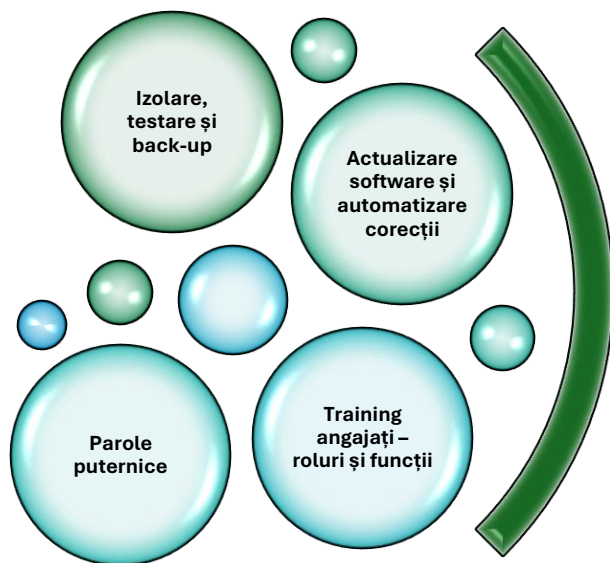
- AI extinde potențialul amenințărilor, de la manipularea modelelor la fraude complexe prin tehnologii **deepfake**

Stabilitate Financiară

- Există preocupări legate de **opacitatea deciziilor luate de AI** și de **impactul** acestora asupra încrederii consumatorilor

Fragmentare

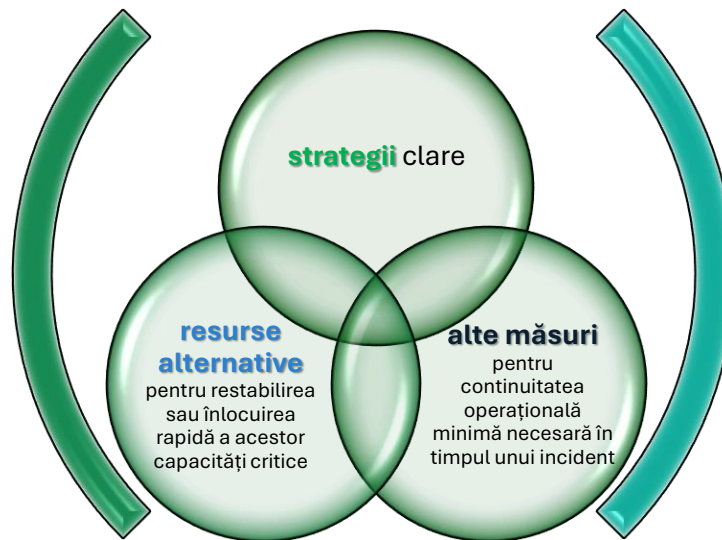
- Deși BRICS+ oferă o alternativă, există **riscul unei fragmentări a sistemului de guvernare globală**



Strategii / politici / proceduri (clare / îmbunătățite)

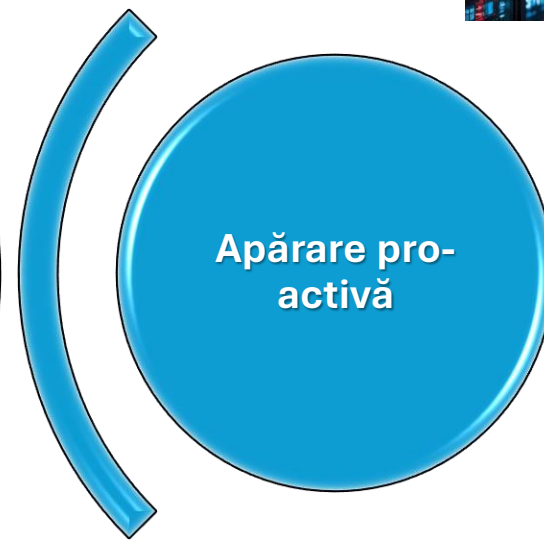
Izolare, testare și back-up:	backup-uri regulate ale datelor și configurațiilor critice în medii izolate
	segmentare adecvată a rețelei
	teste anuale în condiții reale, verificând capacitatea de restaurare rapidă și completă a sistemelor

Deși **tehnologia cloud facilitează procesele de testare și restaurare**, multe organizații aleg să se concentreze **doar** pe **funcțiile critice**, iar **dezvoltarea unui plan robust de restaurare** – posibil **pe o infrastructură complet separată** – reprezintă o provocare semnificativă care necesită resurse și efort substanțial, în special pentru organizațiile de mari dimensiuni



Plan de răspuns la incidente / Plan de continuitate a afacerii / Plan de recuperare în caz de dezastru

Actualizare software și automatizare corecții:	Implementarea unui sistem robust de management al patch-urilor
	proces standardizat de evaluare regulată a sistemelor pentru identificarea software-ului depășit, testarea patch-urilor în medii controlate și implementare automată a actualizărilor critice în afara orelor de program
	inventar actualizat active hardware/software/firmware și prioritizare patch-uri în funcție de severitatea vulnerabilităților și criticitatea sistemelor



confidențialitate, integritate și disponibilitate

organizația afectată își pierde, adesea, accesul la:	instrumentele esențiale necesare pentru investigarea și combaterea atacului însuși
	sistemele SOC (Security Operations Center)
	infrastructura vitală de comunicații și email , care pot fi compromise sau indisponibile

Stratificarea protecției în funcție de:

- ❑ **vectorii de atac**
- ❑ **dispunere geografică / locații**
- ❑ **tip infrastructură (critică)**
- ❑ **categorii (baze) de date**

Proiecții viitoare, strategice



Dacă firma:

folosește sisteme digitale (fără interconectare / interoperabilitate) →	• obligații minime de securitate
activează în sectoare critice / esențiale / importante →	• aplică NIS2 • se conformează DORA
produce, distribuie, vinde produse digitale / software / hardware →	• intră sub incidența CRA
folosește furnizori externi →	• obligații de evaluare a "lanțului de aprovizionare"



1. Costuri de conformitate
2. Capacitate tehnică
3. SLA, RTO/RPO
4. Audit și acces la informații
5. Notificarea incidentelor
6. Subcontractare
7. Supraveghere ESA (pentru furnizorii critici)
8. Maturitatea proceselor interne
9. Impact asupra modelului de business
10. Avantaje competitive post-DORA
11. Riscuri principale și emergente
12. Oportunități de afaceri (producție, distribuție, vânzare, audit autorizat, testare anuală/avansată)

**11 septembrie 2026
- raportare incidente / disfuncții produse -**

- ❑ reziliența operațională și societală
- ❑ criza din 2007 și viitorul sistem monetar (2019→)
- ❑ **Romania - ținta atacurilor**
- ❑ **FinTech – drepturi de proprietate intelectuală / inovații**
- ❑ **riscurile TIC și de securitate – impact asupra funcțiilor de business**

DE CE?

CE?

- **producția, distribuția sau vânzarea de produse digitale, inclusiv:**
 - ❑ software
 - ❑ hardware
 - ❑ dispozitive IoT
 - ❑ echipamente IT

**11 decembrie 2027
- certificare CE -**

- ❑ produse **secure-by-design**
- ❑ actualizări de securitate furnizate pe toată durata de viață declarată
- ❑ vulnerabilități raportate și remediate rapid
- ❑ produse trecute printr-un proces de evaluare a conformității

CUM?

PENTRU CE?

- **conformitate**
- **evitare sancțiuni (cf.CRA)**
 - ❑ 10 milioane EUR sau 2% din cifra de afaceri globală (NIS2)
 - ❑ 15 milioane EUR sau 2,5% din cifra de afaceri globală

Proiecții viitoare, strategice

Motivație

- obligația de a notifica CE, ESMA, EBA și EIOPA până la **17 ianuarie 2025**
- riscul declanșării procedurii de infringement
- **necesitatea desemnării unei autorități unice pentru testele TLPT (BNR)**
- lipsa unui cadru național anterior pentru sancțiuni și supraveghere

OUG nr.14/2026 privind stabilirea unor măsuri de punere în aplicare a Regulamentului (UE) 2022/2.554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr.1.060/2009, (UE) nr.648/2012, (UE) nr.600/2014, (UE) nr.909/2014 și (UE) 2016/1.011

Sursa: <https://lege5.ro/Gratuit/ge4dcobuge2da/ordonanta-de-urgenta-nr-14-2026-privind-stabilirea-unor-masuri-de-punere-in-aplicare-a-regulamentului-ue-2022-2554-al-parlamentului-european-si-al-consiliului-din-14-decembrie-2022-privind-rezilienta->

Regim sancționator

- **amenzi de până la 10% din cifra de afaceri anuală sau până la 23.000.000 RON**
- răspundere individuală pentru conducere
- posibilitatea retragerii autorizației de funcționare

Obligații impuse entităților

Managementul riscurilor TIC

- implementarea unui cadru robust de guvernanta TIC
- monitorizarea continuă a infrastructurii digitale
- politici de securitate și continuitate operațională

Raportarea incidentelor

- raportarea incidentelor majore către BNR/ASF
- termene și formate stabilite prin norme secundare

Testarea rezilienței operaționale digitale

- teste periodice
- teste avansate TLPT coordonate de BNR
- audituri tehnice obligatorii pentru entitățile cu risc ridicat

Gestionarea riscurilor furnizorilor terți TIC

- contracte standardizate
- monitorizarea furnizorilor critici
- posibilitatea intervenției autorităților în relația cu furnizorii

Entități vizate (v. slide următor)

Autorități competente

- sancțiunile aplicabile entităților financiare
- măsurile de remediere
- atribuțiile autorităților de supraveghere
- coordonarea testelor de reziliență operațională digitală

BNR

- instituții de credit
- instituții de plată
- instituții emitente de monedă electronică
- coordonarea **testelor de penetrare bazate pe amenințări (TLPT)** la nivel național

ASF

- piața de capital
- asigurări și pensii
- administratori de fonduri
- **furnizori de servicii crypto (CASP)** și emitenți de tokenuri

Scop

Proiecții viitoare, strategice



**Autorități
competente
– art.46 –
(DORA)**

Autoritățile competente pentru:	Autoritatea competentă UE, desemnată în conformitate cu:	Autoritatea competentă din România
(a) instituțiile de credit	articolul 4 din Directiva 2013/36/UE, fără a aduce atingere atribuțiilor specifice conferite BCE prin Regulamentul (UE) nr. 1024/2013 - ABE, BCE	BNR – art.4 din OUG nr.99/2006 privind instituțiile de credit și adecvarea capitalului, publicată în Monitorul Oficial, Partea I, nr. 1027/27.12.2006
(b) prestatorii de servicii de plată	articolul 22 din Directiva (UE) 2015/2366 - ABE, BCE	BNR – art. 9 din Legea nr.209/2019 privind serviciile de plată și pentru modificarea unor acte normative
(c) instituțiile de plată în monedă electronică	articolul 37 din Directiva 2009/110/CE - ABE, BCE	BNR – art.7 din Legea nr.210/2019 privind activitatea de emisie de monedă electronică
(d) firmele de investiții	articolul 4 din Directiva (UE) 2019/2034 - ABE, ESMA	ASF – art. 4 ¹ din OUG nr.113/2013 privind unele măsuri bugetare și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, publicată în Monitorul Oficial, Partea I, nr. 830/ 23.12.2013
(e) furnizorii de servicii de cryptoactive, emitenții și ofertanții de cryptoactive, emitenții și ofertanții de tokenuri raportate la active și emitenții de tokenuri semnificative raportate la active	articolul 93 din Regulamentul (UE) 2023/1114 (Regulamentul MICA) - ABE, ESMA	articolul 93, coroborat cu art.3 alin.(1) pct.35 din Regulamentul MiCa - Cf. Ghid comun al ABE și ESMA privind evaluarea adecvării membrilor organului de conducere al emitenților de tokenuri raportate la active și al furnizorilor de servicii de cryptoactive (https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75-453128700-10_Joint_GL_suitability_members_management_body_and_QH_RO.pdf) - AC aplică / va aplica / nu aplică – termen: 4 februarie 2025 -
(f) depozitarii centrali de titluri de valoare și operatorii sistemelor de decontare a titlurilor de valoare	articolul 11 din Regulamentul (UE) nr. 909/2014 - ESMA, ABE	ASF – art.2(1) din Legea nr.126 din 11 iunie 2018 privind piețele de instrumente financiare BNR - art.2(2) din Legea nr.126 din 11 iunie 2018 privind piețele de instrumente financiare
(g) contrapărțile centrale	articolul 22 din Regulamentul (UE) nr. 648/2012 - ESMA	ASF – art. 4 ¹ din OUG nr.113/2013 privind unele măsuri bugetare și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, publicată în Monitorul Oficial, Partea I, nr. 830/ 23.12.2013
(h) locurile de tranzacționare și furnizorii de servicii de raportare a datelor	articolul 67 din Directiva 2014/65/UE - ESMA	ASF – art.2(1) din Legea nr.126 din 11 iunie 2018 privind piețele de instrumente financiare BNR - art.2(2) din Legea nr.126 din 11 iunie 2018 privind piețele de instrumente financiare
(i) registrele centrale de tranzacții	articolul 55 din Regulamentul (UE) nr. 648/2012 - ESMA	ASF – art. 4 ¹ din OUG nr.113/2013 privind unele măsuri bugetare și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, publicată în Monitorul Oficial, Partea I, nr. 830/ 23.12.2013

Proiecții viitoare, strategice



**Autorități
competente
– art.46 –
(DORA)**

Autoritățile competente pentru:	Autoritatea competentă UE, desemnată în conformitate cu:	Autoritatea competentă din România
(j) administratorii de fonduri de investiții alternative	articolul 44 din Directiva 2011/61/UE - ESMA / EIOPA	ASF – art.2(1) din Legea nr. 126 din 11 iunie 2018 privind piețele de instrumente financiare
(k) societățile de administrare	articolul 97 din Directiva 2009/65/CE - Organismele de plasament colectiv în valori mobiliare (OPCVM)	ASF (continuator CNVM) – art.1(2) din OUG 32/2012 privind organismele de plasament colectiv în valori mobiliare și societățile de administrare a investițiilor, precum și pentru modificarea și completarea Legii nr. 297/2004 privind piața de capital
(l) întreprinderile de asigurare și reasigurare	articolul 30 din Directiva 2009/138/CE - Autoritatea Europeană pentru Asigurări și Pensii Ocupaționale (EIOPA)	ASF (continuator CSA)– art.1(1) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare
(m) intermediarii de asigurări, intermediarii de reasigurări și intermediarii de asigurări auxiliare	articolul 12 din Directiva (UE) 2016/97 - EIOPA	ASF – art.1(1) din Legea nr. 236/2018 privind distribuția de asigurări
(n) pentru instituțiile pentru furnizarea de pensii ocupaționale	articolul 47 din Directiva 2016/2341 - EIOPA	ASF – art.2(1) din Legea nr. 126 din 11 iunie 2018 privind piețele de instrumente financiare
(o) pentru agențiile de rating de credit	articolul 21 din Regulamentul (CE) nr. 1060/2009 - Comitetul autorităților europene de reglementare a piețelor valorilor mobiliare (CESR)	ASF (continuator CNVM)
(p) pentru auditorii statutare și societățile de audit	articolul 3 alineatul (2) și cu articolul 32 din Directiva 2006/43/CE	Camera Auditorilor Financieri din România (CAFR) – art.3(2) din OUG nr. 90 din 24 iunie 2008 privind auditul statutar al situațiilor financiare anuale și al situațiilor financiare anuale consolidate
(q) pentru administratorii indicilor de referință critici	articolele 40 și 41 din Regulamentul (UE) 2016/1011 - ESMA	ASF – art.1(1) din Legea nr. 236/2018 privind distribuția de asigurări
(r) pentru furnizorii de servicii de finanțare participativă	articolul 29 din Regulamentul (UE) 2020/1503 - ESMA	ASF – art.2 din Legea nr.244/2022 privind stabilirea unor măsuri de punere în aplicare a Regulamentului (UE) 2020/1.503 al Parlamentului European și al Consiliului din 7 octombrie 2020 privind furnizorii europeni de servicii de finanțare participativă pentru afaceri și de modificare a Regulamentului (UE) 2017/1.129 și a Directivei (UE) 2019/1.937
(s) pentru registrele centrale de securitizări	articolul 10 și cu articolul 14 alineatul (1) din Regulamentul (UE) 2017/2402 - Autoritatea Europeană pentru Valori Mobiliare și Piețe (ESMA)	BNR – art. XIV ¹ din Legea nr. 145 din 21 mai 2024 privind modificarea și completarea Legii nr. 158/2020 pentru modificarea, completarea și abrogarea unor acte normative, precum și pentru stabilirea unor măsuri de punere în aplicare a Regulamentului (UE) 2017/2.402 al Parlamentului European și al Consiliului din 12 decembrie 2017 de stabilire a unui cadru general privind securitizarea și de creare a unui cadru specific pentru o securitizare simplă, transparentă și standardizată și de modificare a Directivelor 2009/65/CE, 2009/138/CE și 2011/61/UE, precum și a Regulamentelor (CE) nr.1.060/2009 și (UE) nr.648/2012

Proiecții viitoare, strategice

- **BNR / ASF**: teste de stres cibernetic, monitorizare NPL, avertismente privind infrastructura IT
- **O.N.P.C.S.B.**: evaluări sectoriale și tipologii de risc
- **Legea 129/2019**: prevenirea spălării banilor și finanțării terorismului

România



- **BCE**: testare de rezistență cibernetică, coordonare cu **ENISA** și **CERT-EU**
- **Regulamentul DORA (2023–2025)**: impune reziliență operațională digitală în sectorul financiar

Uniunea Europeană



Centre de operațiuni de securitate (SOC) pentru intervenție în caz de atac cibernetic

în vigoare de la 04 februarie 2025

Construirea unui scut cibernetic european

Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului din 19 decembrie 2024 de stabilire a unor măsuri de consolidare a solidarității și a capacităților la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea și de modificare a Regulamentului (UE) 2021/694 (**Regulamentul privind solidaritatea cibernetică**)

Crearea unui **mecanism de urgență cibernetică** pentru a spori gradul de pregătire și a consolida capacitățile de răspuns la incidente în UE. Acesta va sprijini:

- ❑ acțiuni de **pregătire**, inclusiv **testarea entităților din sectoare extrem de critice** (asistență medicală, transporturi, energie, **financiar** etc.) pentru potențialele vulnerabilități, pe baza unor **scenarii și metodologii comune de risc**
- ❑ o nouă **rezervă** a UE pentru **securitate cibernetică**, care include servicii de răspuns la incidente asigurate de **furnizori de încredere din sectorul privat**, contractați în prealabil și, prin urmare, pregătiți să intervină, la cererea unui stat membru sau a instituțiilor, organelor și agențiilor UE, în cazul unui incident de securitate cibernetică semnificativ sau de mare amploare
- ❑ **asistență reciprocă** în termeni financiari, în cazul în care un stat membru ar putea oferi sprijin unui alt stat membru

Instituirea **mecanismului de revizuire a incidentelor de securitate cibernetică** pentru a spori reziliența UE prin revizuirea și evaluarea incidentelor de securitate cibernetică semnificative sau de mare amploare **după ce acestea au avut loc**, prin lecții învățate și, după caz, prin emiterea de recomandări pentru îmbunătățirea poziției cibernetică a UE.

La cererea Comisiei sau a autorităților naționale, **Agencia UE pentru Securitate Cibernetică (ENISA)** ar urma să reanalizeze anumite incidente de securitate cibernetică și să prezinte un raport cu lecțiile învățate și cu recomandări.

Domeniu	Reglementare BNR	Obligații principale
Testare cibernetică	Regulamentul 6/2022 (TIBER-RO)	Teste avansate, pe producție, pentru instituții critice; simulări APT; raportare către BNR
Reziliență operațională	Reg. 4/2018 + cerințe BNR	Continuitate, DRP, testare periodică, management furnizori ICT
Monitorizare credite neperformante (NPL)	Reg. 5/2013 + ghiduri EBA	Monitorizare, clasificare, provizionare, raportare periodică
Infrastructură IT	Avertismente și supraveghere BNR / ASF	Modernizare, segmentare, securitate, audit IT, reducerea dependențelor

Marile puteri globale vor cere o "Convenție de la Geneva" privind securitatea cibernetică

Proiecții viitoare, strategice

Testarea rezilienței operaționale digitale (art.24-27)

Adeverință conformitate

art.26(5)

autoritate publică unică în sectorul financiar, responsabilă de aspectele legate de TLPT, la nivel național

alte autorități naționale din sectorul financiar

- rapoarte
- planuri de remediere
- rezumat al constatărilor relevante
- documentația care demonstrează că TLPT a fost efectuată în conformitate cu cerințele

art.24(1)-(4) și (6)
art.25(1)
art.26(1)-(4)

art.25(3) și
art.24(5)

Testarea instrumentelor și sistemelor TIC
- întreprinderi mici, mijlocii și mari – teste adecvate, cel puțin o dată pe an
- microîntreprinderi - teste bazate pe riscuri (tip, criticitate active informaționale și servicii, etc.) cu o planificare strategică a testării TIC (proceduri, politici, metodologii)

- cu excluderea autorităților competente - controale eficace ale gestionării riscurilor pentru a atenua riscurile unui potențial impact asupra datelor și riscurile de deteriorare a activelor și de perturbare a funcțiilor, a serviciilor sau a operațiunilor critice sau importante la nivelul entității financiare înseși, al contrapărților acestora sau al sectorului financiar

Testarea avansată a instrumentelor, sistemelor și proceselor TIC cu ajutorul TLPT, cel puțin o dată la 3 ani
- validată de autoritățile competente
- include furnizorii terți de servicii TIC, dacă sunt în sfera de aplicare a TLPT
- realizată grupat - de către furnizorul terț de servicii TIC care are acord contractual cu o entitate externă de testare, după complexitatea și tipurile serviciilor implicate

art.28-30

art.3

Regulamentul BNR nr.6/2022 privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO)

Entități interne de testare TLPT

sau

Entități interne de testare TLPT +
Entități externe de testare TLPT (contract - art.27) la fiecare 3 teste

sau

Entități externe de testare TLPT (contract - art.27)

TESTE DE PENETRARE

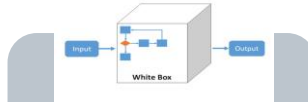
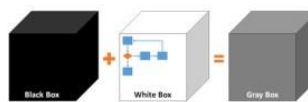
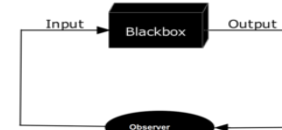
- teste manuale și analize aprofundate asupra produselor bazate pe "logica și poziția de business" (ex.ChatGPT)
- se realizează de către hackeri "white-hat", simulând atacuri cibernetice din perspectiva unui hacker real

ANALIZE APROFUNDATE

- identificare lacune deja cunoscute prin utilizarea instrumentelor de scanare automată
- presupune atacuri manuale personalizate pentru specificul sistemului țintă, corelate cu liste de vulnerabilități (ex. TOP 10 OWASP, TOP 20 SANS etc.)

TESTE PERSONALIZATE

- se realizează de către experți în Securitatea și Protecția Datelor care au cunoștințele necesare să efectueze 3 tipuri de testare de penetrare a securității:
 - Black Box
 - Grey Box
 - White Box
- metoda de testare ↔ complexitatea infrastructurii



evaluări ale vulnerabilității înainte de utilizarea sau reutilizarea unor aplicații și componente de infrastructură noi sau existente și servicii TIC care sprijină funcții critice sau importante ale entității financiare

Depozitarii centrale de titluri de valoare / Contrapărțile centrale - art.25(2) DORA -

Proiecții viitoare, strategice

Ethical hacking
(hacking etic)

= **procesul de a testa sistemele** informatice pentru a identifica eventuale vulnerabilități **și de a le repara înainte ca acestea să fie exploatare de hackeri rău intenționați ("White Hat hacker")**

- implică **utilizarea tehnicilor și instrumentelor hackerilor**, dar **cu intenția de a îmbunătăți** securitatea, nu de a compromite sistemul

- efectuat de **specialiști** în securitate cibernetică **care au abilitățile și cunoștințele necesare** pentru a **găsi vulnerabilitățile și a le explora într-un mod controlat și legal**

- ajută la **îmbunătățirea sistemelor și proceselor de securitate cibernetică**, precum și la **creșterea gradului de conștientizare** în privința **riscurilor cibernetice** și a **importanței securității cibernetice** în rândul angajaților și al clienților

Certificări de luat în considerare:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Auditor certificat de sisteme informatice (CISA)
- Certificare globală de asigurare a informațiilor (GIAC)
- Hacker etic certificat (CEH)



Application
Security Engineer



Incident Responder



Cloud Security
Specialist



Threat Intelligence
Specialist



Penetration Tester



Exploit Developer/
Researcher



Takedowns Expert



Vulnerability
Assessor



Red Team Member



Simulated
Phishing Operator



OSINT Investigator



Blue Team - Roluri de
tip "defensive" în
securitate cibernetică

Contract!



Red Team - Roluri de
tip "offensive" în
securitate cibernetică

Proiecții viitoare, strategice



SANS SECURITY VULNERABILITIES

METODOLOGIA DE TESTARE - TIBER-EU - art.26(11)

- **verificarea componentei de business** cu ajutorul testelor de penetrare a securității
- **analizarea nivelului de securitate**, simulând atacurile reale asupra aplicațiilor/ bazelor de date, infrastructurii sau rețelilor

1. Acumularea informațiilor

- Atacatorul – fie el un hacker de tipul black- sau white-hat – încearcă să obțină **informații critice** la momentul oportun activității sale. Se colectează informații care ar putea constitui **ținta atacurilor**.

2. Recunoașterea

- Obținerea de **informații sensibile despre caracteristicile rețelei externe (protecția fizică/ protecția logică/ protecția personalului)** pot cauza rezultate dăunătoare afacerii. Se verifică componentele implicate, **de la servere la website-uri, API-uri, routere, imprimante, stațiile angajaților și VPN-uri**.

3. Descoperire și Scanare

- Prin activitățile de examinare a vulnerabilităților, **se detectează și exploatează orice problemă sau punct slab din sistem**. **Blue Team** verifică dacă există **porturi deschise sau host-uri neautorizate care pot ataca rețeaua și business-ul**

4. Evaluarea vulnerabilităților

- **Serviciile de evaluare ale vulnerabilităților** ne permit să cuantificăm, să clasificăm și să analizăm lacunele de securitatea din infrastructura entității. Se verifică atât **seturi mari de riscuri deja cunoscute** cât **și punctele slabe**.

5. Exploatarea riscului

- Se pot compromite site-ul web, portalurile, VPN-urile sau serviciile de email, obținând astfel **acces neautorizat în sistemul intern al rețelei**. Se exploatează oate acestea înainte **ca atacatorii reali să câștige controlul**.

6. Analiză și Raportare

- Analizarea datelor, revizuirea constatărilor, **crearea unei evaluări amănunțite și raportarea oricărei vulnerabilități**
- **Reevaluarea infrastructurii** actuale, **a riscurilor la care afacerea este predispusă și estimarea costurilor de remediere aferente**

SCENARII DE AMENINȚARE CIBERNETICĂ



Scop - identificare în mod proactiv

- **arii specifice de expunere** - (tip) **date** / baze de date organizate sau dispersate/ departamente / persoane, alte resurse operaționale) - **business**
- **puncte slabe** - din perspectiva sabotajului, pătrunderii în rețea, întreruperii activității – cauze naturale/provocate, sustragerii de date - **IT**



Obiective

- posibilitatea de a deveni o victimă
- eficiența controalelor de securitate
- acuratețea operațiunilor de securitate



Provocări

- roluri/ sarcini (**business** / **IT**) – Plan de continuitate și restaurare
- operarea în mai multe state membre

Ignorarea riscurilor

- analiză detaliată riscuri, bazată pe procese
- inventarierea/prioritizarea riscului, la nivel local și general

Lipsa vizibilității

- inventar al funcționalităților și resurselor angrenate, din perspectiva atribuțiilor legale și specifice
- evidențierea activităților critice/ predispușe riscurilor și a tipurilor de acțiuni prin care se pot remedia incidentele

PROVOCĂRILE UNUI BUSINESS

- Strategia privind reziliența operațională -

Responsabilitatea

- indicarea oricărui semnal echivoc sesizat în procesul/activitatea derulată
- atitudine de precauție în raport cu potențialele amenințări și vulnerabilități

Comunicarea deficitară

- întărirea canalelor lente de comunicare cu IT, echipa de securitate și departamentul de management informații



Regulamentul BNR nr. 6 din 3 mai 2022 privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO

- <https://www.bnro.ro/apage.aspx?pid=404&actId=333255>

Orientări TIBER-EU privind achizițiile de servicii (https://www.ecb.europa.eu/pub/pdf/ecb.tiber_eu_services_procurement_guidelines.ro.pdf)

- modul în care instituțiile financiare selectează și achiziționează serviciile companiilor de securitate cibernetică - orientările se aplică și testelor de limba română

Cadrul TIBER-UE (http://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)

- șabloane și linii directoare pentru toate fazele diferite ale unui test

Ghidul echipei albe TIBER-EU (<https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf>)

- oferă detalii despre rolurile și responsabilitățile unei echipe albe pentru un test TIBER, care gestionează testul din interiorul entității testate

Șablon de specificație de acoperire TIBER-EU (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Scoping_specification_template_July_2020.pdf)

- poate fi utilizat în timpul oricărui test TIBER-UE de către entitatea testată pentru a prezenta domeniul de aplicare detaliat al testului respectiv

Raportul TIBER-EU Ghid pentru informații despre amenințări țintă (TTI) Raportul (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf)

- cuprinde informații despre amenințări într-o abordare standardizată pentru a dezvolta Raportul TTI pentru entitatea testată

Ghidul TIBER-EU pentru planul de testare al echipei roșii (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_the_Red_Team_Test_Plan_July_2020.pdf)

- oferă o abordare și o structură standardizate pentru elaborarea planului de testare al echipei roșii, concentrându-se asupra modului în care este organizată testarea, planificat managementul testului și sunt dezvoltate scenariile de atac, care se bazează pe scenariile de amenințare din Raportul TTI

Ghidul TIBER-EU pentru raportul de testare a echipei roșii (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-red-team-test-report.pdf)

- oferă o abordare și o structură standardizate pentru realizarea raportului de testare al echipei roșii, concentrându-se pe stabilirea rezumatului testului cu dovezi însoțitoare, detalierea constatărilor și analiza cauzei principale, determinarea punctelor cheie de discuție pentru reluarea testelor cu toate părțile interesate relevante și finalizarea planului de remediere

Ghidul TIBER-EU pentru raportul de rezumat al testului (https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/final_tiber-eu_guidance-for-the-tiber-eu-test-summary-report.pdf)

- oferă entităților care efectuează un test TIBER-UE o abordare și o structură standardizate pentru elaborarea raportului de rezumat al testului

Proiecții viitoare, strategice



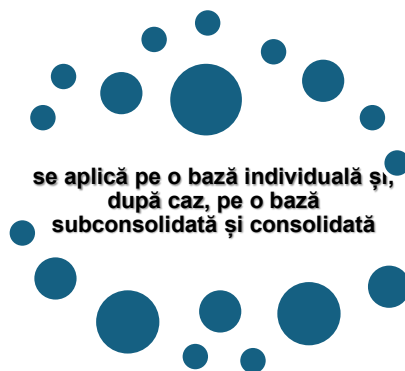
**Cerințe
entității de
testare TLPT
(art.27)**

Gestionarea riscurilor TIC generate de părți terțe (cap.V – art.28-43)

**Entități externe
de testare TLPT
- art.27(1) și (3) -**

- - dețin **capacități tehnice, organizatorice și expertiză** specifică de tipul **Red Team**
- - **certificate** de un organism de acreditare dintr-un stat membru sau **aderă la coduri de conduită sau cadre etice formale**
- - **oferă o asigurare independentă** sau **un raport de audit privind efectuarea testelor TLPT**, inclusiv **protecția corespunzătoare a informațiilor confidențiale** ale entității financiare și **măsurile reparatorii pentru riscurile legate de activitățile entității financiare**
- - au **asigurări de răspundere civilă profesională** relevante, inclusiv **împotriva riscurilor de abatere și neglijență**

contract



se aplică pe o bază individuală și,
după caz, pe o bază
subconsolidată și consolidată

- ține cont de **profilul general de risc** al entității financiare, **amplasarea și complexitatea serviciilor** comerciale / informatice și informatizate
- stabilește modul de **examinare periodică a riscurilor identificate** în privința **acordurilor contractuale** privind **utilizarea serviciilor TIC** care **sprijină funcții critice** sau **importante**



**Strategia
privind
riscurile TIC
generate de
părți terțe**

include o **politică privind utilizarea serviciilor TIC** care **sprijină funcții critice** sau **importante** oferite de furnizori terți de servicii TIC

(v. Ghid ABE privind administrarea riscurilor TIC și de securitate (2019)
https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880825/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_RO.pdf)

Registru de informații în legătură cu **toate acordurile contractuale** privind **utilizarea serviciilor TIC** oferite de **furnizori terți de servicii TIC** - art.28(3) și (9)

**Entități interne
de testare TLPT**

- - dețin **capacități tehnice, organizatorice și expertiză** specifică de tipul **Red Team**
- - **certificate** de un organism de acreditare dintr-un stat membru sau **aderă la coduri de conduită sau cadre etice formale**
- - **oferă o asigurare independentă** sau **un raport de audit privind efectuarea testelor TLPT**, inclusiv **protecția corespunzătoare a informațiilor confidențiale** ale entității financiare și **măsurile reparatorii pentru riscurile legate de activitățile entității financiare**
- - au **asigurări de răspundere civilă profesională** relevante, inclusiv **împotriva riscurilor de abatere și neglijență**
- **autorizarea entității** de către **autoritatea competentă** sau **autoritatea unică desemnată**
- **evitarea conflictelor de interese**

Proiecții viitoare, strategice



Plan de Conformitate DORA pentru Furnizorii IT/Cloud care deservesc instituții financiare (2025–2026)

Etapă 1 – Fundamentare (0–3 luni)

1. Inventarierea serviciilor și a clienților financiari

- Identificare **servicii oferite** instituțiilor financiare, cf **cod CAEN**
- clasificare servicii: **critice / esențiale / importante / non-critice**

2. Identificarea funcțiilor critice

- stabilire servicii IT ce pot afecta operațiunile clientului (ex.: hosting, mentenanță, dezvoltare aplicații, suport tehnic etc.)

3. Evaluarea riscurilor

- elaborare:
 - ☐ matrice simplă de riscuri (impact × probabilitate)
 - ☐ matrice RACI
 - ☐ matrice riscuri integrate (v. fig.)
 - includere riscuri IT, cyber, operaționale, subcontractare etc.
- #### 4. Stabilirea responsabilităților interne
- desemnare responsabil DORA/NIS2 (nu trebuie să fie full-time),
 - definire roluri pentru securitate, continuitate, gestionarea incidentelor

Etapă 2 – Implementare controale minime (3–9 luni)

1. Politici și proceduri obligatorii, practice și pragmatice, cel puțin:

- Politică de securitate cibernetică
- Politică de backup și recuperare
- Politică de gestionare a incidentelor
- Politică de continuitate operațională
- Politică de (sub)contractare
- Politică de acces și control identități

2. Controale tehnice minime

- autentificare multifactor (MFA)
- backup zilnic + testare trimestrială
- patch management lunar
- jurnalizare și monitorizare
- **control acces** pe principiul „need-to-know” / „need-to-share” / „regula celor doi”

3. Continuitate operațională

- definire RTO și RPO pentru fiecare serviciu
- elaborare și testare (semestrial/ anual) **plan simplu de recuperare** (ex.: simulare de întrerupere) și **în caz de dezastre**

4. Gestionarea incidentelor

- definire **incident major / non-major**
- stabilire timpi de notificare pentru clienți
- elaborare **formular standard** de raportare și **flux soluționare**

Etapă 3 – Conformitate contractuală (6–12 luni)

1. Revizuirea contractelor cu clienții

- Includere clauze obligatorii DORA:
 - ☐ SLA clare și măsurabile
 - ☐ RTO/RPO definite
 - ☐ drept de audit
 - ☐ obligația de notificare rapidă
 - ☐ transparență privind (sub)contractorii

2. Revizuirea contractelor cu subcontractorii

- aplicare **standarde ”în lanț”**
- notificare imediată în caz de incident
- asigurare **auditabilitate minimă**



EVALUAREA RISCULUI INTEGRAT

- conformarea la cerințele DORA
- implementarea controalelor minime obligatorii, audituri și supraveghere
- recunoașterea ca furnizori eligibili pentru bănci, asiguratori și alte entități financiare
- reducerea riscurilor contractuale și operaționale
- creșterea încrederii și a competitivității pe piața europeană

Obiective plan



Etapă 4 – Auditabilitate și evidențe (9–15 luni)

1. Evidențe obligatorii și reevaluare proceduri

- analiză, (re)evaluare și păstrare:
 - ☐ loguri de securitate,
 - ☐ rapoarte de backup,
 - ☐ rapoarte de patching,
 - ☐ rapoarte de incidente,
 - ☐ rezultate ale testelor de continuitate

2. Audit anual

- nu trebuie să fie complex
- realizat intern sau de **consultant extern autorizat**

Managementul bunurilor

Valoarea bunurilor

Expunerea bunurilor

Modelarea amenințărilor

Vectori de atac

Attack Centric

Modelarea atacului

Arbori de atac

Scenarii

Etapă 5 – Maturizare și pregătire pentru supraveghere (12–24 luni)

1. Certificări deținute / recomandate

- ISO 27001 (securitate)
- ISO 22301 (continuitate)
- SOC 2 (pentru furnizori SaaS)

2. Pregătirea pentru TLPT / anuală

Furnizorul care oferă **servicii critice / esențiale**, trebuie implicat în testarea threat-led a clientului

3. Integrarea în ecosistemul național

- colaborare cu DNSC / ACS
- participare la exerciții sectoriale
- schimb de informații cu clienții financiari
- eligibilitate pentru contracte cu bănci și asiguratori
- reducere risc de reziliere contractuală
- creștere încrederea clienți
- diferențiere pe piață
- pregătire pentru audituri și supraveghere europeană

DORA nu este o povară, ci o oportunitate

✓X maturitate

✓X competitivitate

✓X siguranță / securitate

✓X atractivitate pentru clienții financiari (pj / pf)

Impactul multidimensional al peisajului cyber asupra afacerilor



Dimensiunea tehnologică

Evoluția măsurilor de securitate schimbă fundamental modul în care funcționează **infrastructurile digitale**

- Creșterea utilizării **AI defensive** (UEBA, ML-based detection)
- **Automatizarea răspunsului** la incidente (SOAR)
- **Criptare avansată și tehnologii post-quantum**
- **Segmentare zero-trust și micro-izolare**
- **Monitorizare continuă** 24/7 prin SOC-uri moderne

Impact global:

- Atacatorii sunt forțați să adopte **tactici mai sofisticate** (AI ofensivă, deepfake, supply-chain attacks)
- Statele investesc masiv în **infrastructuri cyber defensive**

Dimensiunea economică

Măsurile de securitate influențează direct **competitivitatea companiilor**

- **Costuri crescute** pentru conformitate (NIS2, DORA, GDPR)
- **Investiții** în SOC-uri, EDR, IAM, TI
- **Creșterea pieței globale** de cybersecurity (peste 300 mld. USD)
- **Asigurările cibernetice** devin obligatorii în multe industrii

Impact global:

- **Companiile cu securitate ridicată** devin **parteneri preferați** în lanțurile de aprovizionare
- **Organizațiile vulnerabile** sunt excluse sau penalizate

Dimensiunea geopolitică

Securitatea cibernetică a devenit un **instrument de putere națională**

- Statele dezvoltă **strategii cyber naționale și alianțe** (UE, NATO, QUAD)
- CERT-urile și CSIRT-urile naționale cooperează transfrontalier.
- Atacurile cibernetice sunt folosite ca **instrumente de presiune geopolitică**
- Reglementări precum **NIS2 și DORA ridică standardele la nivel continental**

Impact global:

- Apar **blocuri cyber regionale** (UE, SUA, Asia-Pacific)
- Crește tensiunea între state în zona de **spionaj și sabotaj digital**

Dimensiunea socială

Securitatea cibernetică influențează **încrederea publicului în instituții și tehnologie**

- **Creșterea atacurilor asupra infrastructurilor critice** afectează populația
- **Deepfake-urile și dezinformarea** subminează încrederea în democrație
- **Educația digitală** devine o **necesitate națională**
- **Protecția datelor personale** devine o **preocupare majoră**

Impact global:

- **Societățile cu alfabetizare digitală** ridicată sunt mai **reziliente**
- **Încrederea publică** devine un **indicator de securitate**

Dimensiunea organizațională

Măsurile de securitate transformă **cultura internă a companiilor**

- **Zero Trust** devine **standard global**
- **Trainingul anti-phishing** și **simulările** devin **obligatorii**
- **Guvernanța IT** se mută la nivel de board
- **Furnizorii** sunt **evaluați strict** (TPRM, due diligence)

Impact global:

- Organizațiile trec **de la reacție la prevenție**
- **Cultura de securitate** devine un avantaj competitiv

Dimensiunea psihologică

Atacurile vizează **oamenii**, iar măsurile de securitate trebuie să țină cont de **comportamentul uman**

- **Ingineria socială** rămâne vectorul principal de atac
- **Atacurile** devin **hiper-personalizate** (AI-driven phishing)
- **Măsurile de securitate** trebuie să fie **intuitive, nu intruzive**
- Crește **importanța awareness-ului** și a **comportamentului digital responsabil**

Impact global:

- **Factorul uman** rămâne **cea mai mare vulnerabilitate**
- Organizațiile investesc în **programe de schimbare comportamentală**

Dimensiunea legală și de reglementare

Reglementările globale ridică **standardele și obligă la maturitate**

- NIS2, DORA, GDPR în **UE**
- CISA, NIST, Executive Orders în **SUA**
- ISO 27001, 27701, 22301 la **nivel global**
- **Reglementări sectoriale** (financiar, energie, sănătate)

Impact global:

- **Standardizare internațională** a securității
- **Creșterea responsabilității** legale a conducerii

Proiecții viitoare, strategice

Plan de acțiune implementare măsuri pe termen scurt (1 an) și mediu (2027-2030)



Anul	Obiective generale	Acțiuni				
		NIS2	DORA	CRA	GDPR	FIDA (proiect)
● 2027 — Stabilizare, maturizare și auditare post-implementare	❑ Consolidarea implementărilor făcute în 2024–2026 ❑ Închiderea decalajelor identificate în auditul 2026 ❑ Stabilirea unui ciclu anual de conformitate integrată	❑ Audit complet al controalelor tehnice și organizaționale ❑ Testarea planurilor BCP/DRP la nivel de infrastructură critică ❑ Implementarea unui program matur de management al furnizorilor	❑ Prima rundă completă de TLPT (Threat-Led Penetration Testing) pentru entități semnificative ❑ Standardizarea raportării incidentelor majore ❑ Revizuirea contractelor ICT conform cerințelor DORA	❑ Finalizarea SBOM pentru toate produsele software ❑ Implementarea procesului de vulnerability disclosure ❑ Stabilirea ciclului de patching securizat	❑ Reevaluarea DPIA pentru procese critice ❑ Testarea anuală a planului de răspuns la breșe ❑ Revizuirea politicilor de retenție	❑ Implementarea API-urilor standardizate pentru acces la date ❑ Guvernanță pentru partajarea datelor cu terți ❑ Politici de consimțământ și transparență
● 2028 — Optimizare, integrare și automatizare	❑ Automatizarea proceselor de conformitate ❑ Integrarea cerințelor în arhitectura enterprise ❑ Reducerea costurilor operaționale prin standardizare	❑ Automatizarea monitorizării (SIEM, SOAR) ❑ Implementarea unui program matur de threat intelligence ❑ Simulări de atacuri la nivel de organizație (red team)	❑ Automatizarea raportării incidentelor ❑ Integrarea completă a managementului furnizorilor ICT într-un sistem centralizat ❑ Testare TLPT avansată (scenarii cross-sectoriale)	❑ Automatizarea generării SBOM ❑ Introducerea DevSecOps complet în pipeline-urile CI/CD ❑ Audit CRA pentru toate produsele software	❑ Automatizarea cererilor persoanelor vizate (DSAR) ❑ Implementarea unui sistem de clasificare automată a datelor ❑ Monitorizare continuă a accesului la date sensibile	❑ Extinderea ecosistemului de parteneri ❑ Automatizarea managementului consimțământului ❑ Implementarea unui registru de acces la date
● 2029 — Reziliență avansată și interoperabilitate europeană	❑ Atingerea unui nivel ridicat de reziliență digitală ❑ Interoperabilitate cu standardele UE emergente ❑ Pregătirea pentru noi reglementări (AI Act, Data Act etc.)	❑ Integrarea completă a cerințelor în arhitectura de securitate ❑ Teste de reziliență la nivel de ecosistem (furnizori + clienți) ❑ Program avansat de securitate a lanțului de aprovizionare	❑ Maturizarea proceselor TLPT (anual sau bienal) ❑ Implementarea unui centru de reziliență digitală (Digital Resilience Hub) ❑ Integrarea cu cerințele Data Act și AI Act	❑ Certificarea produselor software conform schemelor europene ❑ Introducerea unui ciclu complet de secure lifecycle management ❑ Monitorizare continuă a vulnerabilităților	❑ Automatizarea completă a conformității (privacy-by-design). ❑ Implementarea unui sistem de detectare a abuzurilor de acces ❑ Audit GDPR anual cu terți independenți	❑ Extinderea accesului la date către noi servicii financiare ❑ Interoperabilitate cu platforme europene de date ❑ Optimizarea mecanismelor de monetizare a datelor
● 2030 — Reziliență operațională și conformitate continuă	❑ Conformitate integrată, automatizată și sustenabilă ❑ Reziliență digitală la nivel european ❑ Transformarea conformității într-un avantaj competitiv	❑ Certificare europeană de securitate (unde este aplicabil) ❑ Program de reziliență multi-anual ❑ Integrarea completă cu AI Act pentru securitate autonomă	❑ Reziliență digitală complet automatizată ❑ Ecosistem ICT supravegheat și auditat continuu ❑ Maturitate maximă în managementul riscurilor ICT	❑ Produse software complet conforme, cu suport pe ciclul de viață ❑ Audit CRA anual ❑ Automatizarea patching-ului și a notificărilor	❑ Privacy-by-default în toate sistemele ❑ Zero manual intervention în procesele de conformitate ❑ Monitorizare continuă a riscurilor de confidențialitate	❑ Ecosistem de date complet interoperabil ❑ Servicii financiare bazate pe date în timp real ❑ Guvernanță matură a datelor partajate

Proiecții viitoare, strategice

Plan de acțiune implementare măsuri pe termen scurt (1 an) și mediu (2027-2030)



Anul	Entitate	Acțiuni				
		NIS2	DORA	CRA	GDPR	FIDA (proiect)
● 2027 — Stabilizare, maturizare și auditare post-implementare	Bancă	Audit complet; testare BCP/DRP; maturizare controale	TLPT (dacă e semnificativă); standardizare raportare incidente	SBOM dacă produce software	Reevaluare DPIA; testare răspuns la breșe	Implementare API-uri; guvernanta date
		Art. 21–23 (măsuri), Art. 26 (raportare), Art. 29 (BCP/DRP)	Art. 5–15 (risc ICT), Art. 17–20 (incidente), Art. 24–27 (TLPT), Art. 28–30 (furnizori ICT)	Art. 13–20 (SBOM, vulnerabilități)	Art. 30–35 (DPIA), Art. 33–34 (breșe), Art. 25 (privacy by design)	Art. 6–12 (acces date), Art. 15–18 (consimțământ)
	Asigurator	Audit securitate; controale minime	Framework risc ICT; testare anuală	SBOM dacă oferă aplicații	DPIA pentru date sensibile	Implementare acces date pentru parteneri
		Art. 21–23, Art. 26	Art. 5–15, Art. 17–20	Art. 13–20	Art. 30–35, Art. 33–34	Art. 6–12
	Furnizor ICT	Evaluare risc; controale tehnice; raportare incidente	Doar dacă e furnizor critic	SBOM + vulnerability disclosure	DPA + măsuri tehnice	Nu se aplică
		Art. 21–23, Art. 26, Art. 29	Art. 28–30 (dacă e furnizor critic)	Art. 13–20	Art. 28–32	Nu se aplică
● 2028 — Optimizare, integrare și automatizare	Bancă	Automatizare SIEM/SOAR; threat intel	Automatizare raportare; management furnizori ICT	DevSecOps complet	Automatizare DSAR; clasificare date	Automatizare consimțământ
		Art. 21(2) – automatizare securitate	Art. 11–15 (monitorizare), Art. 24–27 (TLPT avansat)	Art. 15–20 (DevSecOps, patching)	Art. 12–22 (drepturi persoane), Art. 25	Art. 10–18
	Asigurator	Logging avansat; simulări atac	Automatizare testare; integrare furnizori	DevSecOps pentru aplicații	Clasificare automată date	Extindere ecosistem date
		Art. 21–23	Art. 11–15	Art. 15–20	Art. 12–22	Art. 10–18
	Furnizor ICT	Automatizare monitorizare; red team	Automatizare raportare (dacă e critic)	Generare automată SBOM	Monitorizare acces date	Nu se aplică
		Art. 21(2), Art. 29	Art. 28–30	Art. 15–20	Art. 28–32	Nu se aplică

Proiecții viitoare, strategice

Plan de acțiune implementare măsuri pe termen scurt (1 an) și mediu (2027-2030)



Anul	Entitate	Acțiuni				
		NIS2	DORA	CRA	GDPR	FIDA (proiect)
 2029 — Reziliență avansată și interoperabilitate europeană	Bancă	Teste ecosistem (furnizori + clienți)	TLPT avansat; Digital Resilience Hub	Certificare produse software	Detectare abuz acces	Interoperabilitate UE
		Art. 29 (testare ecosistem), Art. 32 (cooperare)	Art. 24–27 (TLPT periodic), Art. 31–33 (reziliență)	Art. 20 (certificare)	Art. 24–32	Art. 18–25
	Asigurator	Reziliență cross-sectorială	TLPT proporțional	Certificare aplicații	Audit GDPR extern	Interoperabilitate date
		Art. 29, Art. 32	Art. 24–27	Art. 20	Art. 24–32	Art. 18–25
	Furnizor ICT	Reziliență lanț aprovizionare	TLPT dacă e critic	Secure lifecycle complet	Audit anual	Nu se aplică
		Art. 29, Art. 30 (lanț aprovizionare)	Art. 28–30	Art. 20	Art. 28–32	Nu se aplică
 2030 — Reziliență operațională și conformitate continuă	Bancă	Certificare europeană securitate	Reziliență digitală complet automatizată	Patching autonom	Privacy-by-default	Monetizare date
		Art. 32–34 (certificare, cooperare UE)	Art. 31–33 (reziliență completă)	Art. 20 (audit anual)	Art. 25 (privacy by default)	Art. 25–30 (ecosistem matur)
	Asigurator	Program multi-anual reziliență	Automatizare completă procese	Audit CRA anual	Zero manual intervention	Ecosistem date matur
		Art. 32–34	Art. 31–33	Art. 20	Art. 25	Art. 25–30
	Furnizor ICT	Integrare AI pentru securitate	Supraveghere continuă (dacă e critic)	Audit CRA + suport pe ciclul de viață	Monitorizare continuă	Nu se aplică
		Art. 32–34	Art. 28–30	Art. 20	Art. 28–32	Nu se aplică

Proiecții viitoare, strategice



CERINȚE DIN NIS2 ȘI DORA PRIVIND CULTURA DE SECURITATE

Cultura de securitate reprezintă:

- modul în care **angajații percep riscurile cibernetice**
- **comportamentele zilnice** legate de securitate
- nivelul de **conștientizare și responsabilitate**
- capacitatea organizației de **a preveni și de a detecta incidente**
- o combinație între **educație, procese, leadership și comportament**

NIS2 – Art. 21

Instituțiile trebuie să implementeze:

- programe de conștientizare
- instruire periodică
- responsabilizarea conducerii
- politici clare de Securitate

DORA – Art. 13 și Art. 5

Instituțiile financiare trebuie să asigure:

- training obligatoriu pentru toți angajații
- instruire specializată pentru personalul tehnic
- cultură de risc TIC la nivel de board
- responsabilități clare pentru securitate

ELEMENTELE UNEI CULTURI DE SECURITATE MATURE

Leadership activ

❑ Boardul și managementul trebuie:

- să susțină public securitatea
- să aloce resurse
- să participe la exerciții
- să înțeleagă riscurile TIC

❑ **Conștientizare continuă**

Nu doar training anual, ci:

- campanii lunare
- simulări de phishing
- afișe, newslettere, micro-learning
- comunicări proactive ale SOC/CSIRT

❑ **Comportamente sigure**

Angajații trebuie:

- să raporteze rapid incidente
- să nu ignore alertele
- să respecte politicile
- să protejeze datele și parolele

❑ **Integrarea securității în procese**

Securitatea trebuie să fie în:

- onboarding
- procesele de achiziție
- dezvoltarea software
- managementul schimbărilor

❑ **Colaborare între echipe**

SOC, CSIRT, IT, HR, Legal, Conformitate trebuie să lucreze împreună

CUM SE CONSTRUIEȘTE CULTURA DE SECURITATE

Educație și training

- training anual obligatoriu
- module specializate pentru roluri critice
- simulări de phishing cu feedback personalizat

Comunicare constantă

- alerte interne
- buletine de securitate
- lecții învățate din incidente

Exemplul conducerii

- participare la exerciții
- asumarea responsabilităților
- comunicare transparentă

Gamificare

- competiții interne
- premii pentru comportamente sigure
- leaderboard pentru simulări de phishing

Integrarea în evaluările de performanță

- KPI pentru securitate
- penalizări pentru nerespectarea politicilor

Cultura de securitate în TLPT (TIBER-RO)

TLPT testează direct cultura de securitate:

- cât de repede detectează SOC un atac
- cât de bine răspunde CSIRT
- cât de eficient comunică SPOC
- cât de pregătiți sunt angajații pentru phishing
- cât de bine funcționează procesele interne

❑ **Un TLPT slab = cultură slabă**

❑ **Un TLPT puternic = cultură matură**

INDICATORI DE MATURITATE PENTRU CULTURA DE SECURITATE

Nivel	Caracteristici
Nivel 1 – Reacționar	Training minim, incidente frecvente, lipsă responsabilitate
Nivel 2 – Conștientizare	Training anual, comunicare ocazională
Nivel 3 – Proactiv	Simulări regulate, implicare management
Nivel 4 – Integrat	Securitatea în toate procesele
Nivel 5 – Optimizat	Îmbunătățire continuă, cultură organizațională solidă

Proiecții viitoare, strategice

în contextul GenAI și al ingineriei sociale moderne



4. Politici stricte de gestionare a datelor publice

GenAI își extrage puterea din datele disponibile online

Recomandări:

Limitarea informațiilor publice despre angajați (roluri, organigrame, contacte).

Politici clare privind utilizarea rețelelor sociale.

Monitorizarea scurgerilor de date din surse externe (dark web, forumuri).

Motiv:

Mai puține date publice = **mai puțină muniție pentru atacatori**

1. Recalibrarea culturii de securitate: oamenii devin prima linie de apărare

Ce trebuie făcut:

- implementarea unui **program continuu de educație** despre atacuri GenAI (deepfake-uri, phishing conversațional, spear-phishing hiper-personalizat)
- simulări regulate de phishing, adaptate la nivelul actual al amenințărilor
- introducerea conceptului de „**zero trust comportamental**”: nu ai încredere în nicio comunicare doar pentru că „pare autentică”

De ce contează:

GenAI reduce diferența dintre mesajele reale și cele false. Singura barieră reală rămâne **vigilența umană antrenată**.

2. Consolidarea autentificării și verificării identității

Măsurile strategice:

- autentificare multi-factor obligatorie (MFA)
- verificări secundare pentru tranzacții, schimbări de conturi sau cereri urgente
- politici stricte de verificare vocală și video, având în vedere deepfake-urile

Exemplu:

Dacă un „director” cere un transfer prin telefon, regula devine: „**Verifică printr-un canal secundar înainte de a acționa**”

3. Implementarea detecției comportamentale asistate de AI

Ce înseamnă:

- sisteme care analizează comportamentul utilizatorilor, nu doar conținutul mesajelor
- detectarea anomaliilor: logări neobișnuite, schimbări de stil, acțiuni atipice

Beneficiu:

GenAI poate imita stilul de scriere, dar **nu poate imita comportamentul operațional** al unui angajat

5. Crearea unui „AI Threat Response Playbook”

Organizațiile trebuie să aibă un plan dedicat atacurilor asistate de GenAI.

Conținut recomandat:

- proceduri pentru deepfake-uri vocale/video
- răspuns la phishing conversațional
- escaladare rapidă pentru incidente suspecte
- ghiduri pentru verificarea identității în situații critice

6. Automatizarea apărării – răspuns rapid la atacuri rapide

GenAI accelerează atacurile. Organizațiile trebuie să accelereze apărarea.

Măsurile:

- sisteme automate de blocare a mesajelor suspecte
- filtre dinamice care se adaptează în timp real
- AI defensivă care rescrie și analizează mesajele pentru a detecta manipulări subtile

7. Colaborare externă și schimb de informații

Nicio organizație nu poate lupta singură împotriva atacurilor GenAI.

Recomandări:

- participarea la rețele de schimb de informații (ISAC-uri, CERT-uri)
- colaborare cu autorități naționale și internaționale
- simulări comune cu parteneri și furnizori

8. Evaluarea continuă a furnizorilor și lanțului de aprovizionare

Atacurile moderne vizează adesea furnizorii, nu organizația principală.

Măsurile:

- audituri periodice de securitate
- cerințe minime de securitate pentru parteneri
- monitorizarea accesului furnizorilor în timp real

9. Introducerea unui „AI Ethics & Security Board” intern

Un comitet dedicat care:

- evaluează riscurile GenAI
- stabilește limite de utilizare
- monitorizează impactul asupra securității
- aprobă instrumentele AI folosite intern

10. Investiții în reziliență, nu doar în prevenție

Atacurile asistate de GenAI sunt inevitabile. Ceea ce contează este **cât de repede te recuperezi**.

Recomandări:

- back-up-uri izolate (air-gapped)
- planuri de continuitate a afacerii
- teste de recuperare după atacuri
- redundanță în sistemele critice

www.bnr.ro

Email:
ruxandra.rimniceanu@bnro.ro

VĂ MULȚUMESC!

