REVISTA

EVALUATORUL DE RISC

ANERSFR
13 ANI DE EXPERIENȚĂ

AJAX

EN54 LINE • Protecție împotriva incendiilor



Detecție la incendiu certificată EN54 și sistem de alarmare la efracție

2 GRADE EN 50131 · EN 54-2 · EN 54-3 · EN 54-4 · EN 54-5 · EN 54-7 · EN 54-11 · EN 54-13 · EN 54-18 · EN 54-21 · EN 54-23 · EN 54-25

ANERSFR:
COMUNICAT DE PRESĂ DIN 10.02.2026

Conducerea ANERSFR a fost informată de MAI despre postarea pe transparență decizională a *Proiectului de OUG pentru modificarea și completarea Legii nr.333/2003 privind paza și protecția bunurilor și valorilor.*

Surprinzător este faptul că inițiativa M.A.I., declarată ca fiind pentru simplificarea și debirocratizarea obligațiilor administrative aflate în sarcina mediului de afaceri, a fost definitivată și postată fără să se consulte cu organizațiile asociative și patronale reprezentative de ramură, respectiv cu cei care activează în domeniu, cu toate că în conținutul Notei de fundamentare se consemnează acest fapt.

Proiectul a provocat mari controverse în industria de securitate, mai ales prin apariția neașteptată și prin propuneri de reglementare a domeniul pazei și protecției bunurilor (securității private), incident unei legislații învechite, adoptat în urmă cu 23 ani, cu multe prevederi confuze, inaplicabile ori desuete și mai ales, fără realizarea unui impact socioeconomic al aplicării actului normativ sau în baza unei politici publice în acest sens.

Propunerea de OUG aduce la pachet pe lângă beneficiile de eliminare a unor demersuri de avizare/autorizare, renunțarea la obligația de reînnoire a ciclică (3 ani) a licențelor pentru prestatorii de servicii în domeniu și o așa **zisă relaxare (toxică) a investițiilor legate de dotarea cu echipamente și servicii destinate protecției fizice pentru marea parte a operatorilor economici**, mai precis, cei considerați a fi cu potențial criminogen scăzut (stabiliți în urmă cu 14 ani).

Proiectul propune în cazul acestora, **înlocuirea** procesului de **evaluare a riscurilor, realizat de specialiști independenți ca** și metodă de stabilire a măsurilor de pază ori de dotare cu produse de protecție fizică și sisteme de alarmă **cu autoevaluarea proprie, realizată în mod subiectiv de neprofesioniști.**

Altfel spus, **circa 75% din operatorii economici nu vor mai stabili necesitățile de protecție printr-o metodă universală standardizată ci își vor aprecia singuri nevoile pe baza unor fișe**, dacă în cazul unor mici afaceri este de înțeles, în anumite sectoare cum ar fi : spații de producție, parcuri industriale, clădirii de birouri sau alte activități complexe, necesitățile nu le pot identifica decât specialiștii.

În opinia specialiștilor asociației, adoptarea proiectului în forma propusă, în contextul unei perioade de contracție economică, va avea un impact major în creștere criminalității profilate pe activități infracționale asupra patrimoniului entităților juridice cu impact chiar asupra integrității vieții sau sănătății salariaților care operează cu numerar și valori.

Consiliul Director al A.N.E.R.S.F.R.

PARTENERIATE ANERSFR

ORGANISMUL NAȚIONAL DE STANDARDIZARE

UNSAR 30 DE ANI

ARTS
Arta de a trăi în siguranță
Asociație de utilitate publică

CUPRINS

04 **EDITORIAL: Reușitele anului 2025**
Petru Liviu Negoescu

06 **INTERVIU: Protecția fizică versus securitatea fizică în domeniile speciale**
Adrian Rădescu

10 **ARTICOL: Inteligența Artificială vs. Securitatea Fizică - 13 Amenințări Reale și Urgente...**
Ion Iordache

18 **ARTICOL: Dronele și riscurile folosirii lor în apropierea aeroporturilor**
Florin Daniel Simion

24 **ARTICOL: Stabilirea politicii referitoare la managementul riscului - partea I-a**
Aurel Catrinoiu

32 **ARTICOL: De la evaluator local la consultant european**
Petru Liviu Negoescu

35 **ARTICOL: Necesitatea îmbunătățirii reglementării domeniului analizei de risc**
Aurel Catrinoiu

38 **INTERVIU: Cum devine evaluarea de risc un instrument strategic pentru securitatea bancară**
Florin Vasile Ioan

40 **Lista Membrilor ANERSFR**

**Conținutul articolelor reflectă numai punctul de vedere al autorilor acestora și nu reprezintă punctul de vedere oficial al ANERSFR. Autorii articolelor sunt în întregime responsabili pentru conținutul acestora.*

Revista editată de Asociația Națională a Evaluatorilor de Risc la Securitatea Fizică din România.

Redacția ANERSFR
Bd. Unirii nr.31, bl. A1, sector 3

office@anersfr.ro
www.anersfr.ro

Coordonator:
Aurel Catrinoiu

Tehnoredactare:
Petru Negoescu

Grafică și DTP:
Cezara Negoescu



Colectivul de redacție
Director Petru NEGOESCU

EDITORIALUL EDIȚIEI

ANERSFR – ÎN ANUL 2025 AM CONTINUAT SUSȚINEREA MEDIULUI DE AFACERI CU EXPERTIZA NOASTRĂ!

Dragi cititori,

Apariția ediției cu numarul 9 a revistei „Evaluatorul de Risc”, sub egida Asociației Naționale a Evaluatorilor de Risc la Securitatea Fizică din România - ANERSFR, continuă campania de informare a cititorilor in domeniul securității fizice și de educare a mediului de afaceri.

În această publicație ne-am dorit să aducem atât idei și subiecte noi, cât și proiecte inedite aplicabile pe domeniul securității private și în același timp, o parte a realizărilor organizației noastre care au impact asupra îmbunătățirii prestațiilor și implicit a nivelului de securitate din companii.

În debutul acestui numar avem interviul cu dl. Adrian Rădescu, manager la SN Nuclearelectrica SA, care ne propune o documentare privind

limitele de apropiere sau de deosebire între securitatea fizică și protecția fizică a obiectivelor nucleare.

Unul dintre rezultatele remarcabile este reprezentat de continuarea campaniilor de promovare a bunelor practici, atât prin propunerea unor soluții tehnice de securizare a obiectivelor, dar și prin modul de materializare a rezultatelor unor procese de evaluare a riscurilor de securitate fizică pe situații reale. În cadrul celor patru evenimente regionale majore organizate la București, Brăila, Oradea și Sibiu, care au reunit peste 300 de specialiști în securitate privată, dezbaterile profesionale au evidențiat capacitatea participanților și avantajele oferirii de servicii profesionale dedicate mediului de afaceri.

Au fost discuții de clarificare pe multiple situații complexe ale procesului de evaluare a riscurilor, care au stârnit dezbateri intense pentru a identifica și fundamenta opinii acceptate.

În publicație, colectivul de redacție și-a propus o grafică modernă, o diversitate de aspecte, exemplificând inteligența artificială versus securitatea fizică, dronele și riscurile în apropierea aeroporturilor, analiza comparativă a specializărilor-cheie în securitatea privată sau detalii din cel mai recent seminar al asociației.

În articolul: Inteligența artificială versus securitatea fizică -13 amenințări reale, autorul ne avertizează că: “adevărata amenințare a AI nu este distrugerea, ci manipularea subtilă care ne face să ne predăm de bunăvoie” și ne indică riscurile legate de inteligența artificială și scenariile privind amenințările actuale și influența acestora în securitatea fizică.

ANERSFR ne propune o nouă imagine a site-ului organizației, având o temă diferită de cea anterioară, având ca și un deziderat, susținerea unor campanii de informare și promovare în media a opiniilor profesionale și o descriere a proiectelor în derulare, sens în care vă invităm să aveți curiozitatea să accesați site-ul nostru la adresa: https://www.anersfr.ro/

Revenind la publicație, conținutul revistei „Evaluatorul de Risc”, vă propune modalități de creștere a calității serviciilor de securitate și importanța acestora în reziliența nivelului de securitate și prezervarea activelor patrimoniale ale companiilor și instituțiilor.
În concluzie, speranța colectivului de redactional si a autorilor, este că și în această ediție a Revistei Evaluatorul de risc sunt publicate articole de actualitate și interes pentru cititori.

Numerele precedente ale revistei sunt postate pe site-ul asociației sau pot fi lecturate în format letric, prin achiziția acestora de la asociație, transmițând o comandă pe adresa de mail: office@anersfr.ro

Vă doresc lectură plăcută și folositoare și vă îndemn să rămâneți conectați cu noi permanent prin site-ul www.anersfr.ro și prin paginile ANERSFR de Facebook și Linkedin!



ADRIAN RĂDESCU:
Protecția fizică versus securitatea fizică în domeniile speciale

Șef Departament Protecție Fizică și Informații Clasificate în cadrul Direcției Tehnologia și Securitatea Informației
Societatea Națională NUCLEARELECTRICA SA



1. Domnule Adrian RĂDESCU, vă propun să facem debutul interviului de astăzi prin a ne expune pentru cititori cele mai importante repere profesionale ale carierei dvs. și de când sunteți în piața securității fizice?

> *„Cariera mea în domeniul securității este definită de o evoluție constantă de la execuție la management strategic, acumulând peste 30 ani de experiență. Am activat în medii cu un grad ridicat de complexitate, unde rigoarea nu a fost opțională, ci o condiție de existență. Debutul meu în piața securității fizice a coincis cu o perioadă de transformări legislative majore în România, ceea ce mi-a permis să înțeleg nu doar aplicarea legii, ci și spiritul acesteia – trecerea de la simpla pază la managementul integrat al riscului.”*

2. Ne puteți spune care sunt specificitățile poziției dvs. sau ale departamentului şi dacă sunt mult diferite, comparativ cu un manager de securitate din industria de retail/auto, spre exemplu.



„Diferența majoră rezidă în consecința eșecului. În retail sau industria auto, riscurile sunt preponderent economice sau operaționale (pierderi de stoc, întreruperi de flux). În domeniile strategice, cum este cel nuclear, un incident de securitate poate avea implicații naționale sau transfrontaliere, de mediu și de siguranță publică. Poziția mea implică un grad de conformitate mult mai strict, sub egida unor autorități de reglementare specifice (cum este CNCAN-Comisia Națională pentru Controlul Activităților Nucleare şi IAEA- Agenția Internațională pentru Energie Atomică), unde procedurile de lucru sunt redundante și verificate periodic prin exerciții de tip „penetration test" şi „stress test."

3. Cum apreciați, se poate spune de o suprapunere ori apropiere a procesului de evaluare a riscurilor de securitate fizică și conceptul de protecție fizică specific domeniului nuclear ?

„Deși terminologia pare similară, există o distincție de profunzime. Evaluarea riscurilor la securitatea fizică (conform H.G.nr. 301/2012) este fundamentul masurilor de securitate a oricărui obiectiv civil. În schimb, Protecția Fizică în domeniul nuclear este un concept mult mai robust, guvernat de principii precum Defense in Depth (apărarea în adâncime). Suprapunerea apare în zona de identificare a amenințărilor, însă Protecția Fizică adaugă straturi suplimentare: detecția timpurie, întârzierea forțată a adversarului și un răspuns armat specializat, totul sub un control strict al accesului la instalațiile vitale sau materiale nucleare."

4. Din câte cunosc, aveți o vastă experiență ca manager de securitate în mai multe domenii, cum vedeti prioritizarea riscurilor din domeniul nuclear comparativ cu alte domenii?

„În domeniul nuclear, documentul de baza este Amenințarea Baza de Proiect, document clasificat secret de stat (DBT - Design Basis Threat). Spre deosebire de alte domenii unde prioritizăm riscurile în funcție de probabilitate și impact financiar, aici ne concentrăm

pe scenariile cu „impact extrem”, oricât de mică ar fi probabilitatea lor. Prioritatea zero a departamentului pe care îl conduc, este prevenirea sabotajului și a mișcării neautorizate de material nuclear. Într-un depozit logistic, prioritatea este “prevenirea pierderilor- loss prevention”; într-o unitate nucleară, prioritatea este integritatea instalațiilor nucleare și a materialului.”

5. Acum, în continuare, dacă puteți să ne precizați și diferențele dintre protecția fizică în unități cu specific nuclear și măsurile de securitate fizică clasice.

„Diferența principală este gradul de integrare între cultura de securitate nucleară şi cultura de siguranță nucleara. Cultura de securitate nucleară se bazează pe responsabilitate radicală și transparență. Măsurile clasice se bazează adesea pe sisteme tehnice și personal de pază standard. Protecția fizică în unitățile nucleare integrează aceste elemente într-un sistem unitar în care componenta umană trece prin procese riguroase de verificare a loialității (vetting) și instruire continuă. În plus, într-o instalație nucleara, sistemele tehnice de securitate sunt redundante si adesea complet izolate de rețelele publice pentru a preveni atacurile cibernetice asupra infrastructurii fizice.”

6. Digitalizarea și factorul uman în securitatea fizică.

„Dacă ar fi să transmit un mesaj colegilor de breaslă, acesta ar fi: tehnologia (AI, senzorii avansați) este un multiplicator de forță, dar nu poate înlocui discernământul uman în situații de criză. Viitorul evaluatorului de risc și al managerului de securitate constă în capacitatea de a gestiona riscurile hibride – acolo unde amenințarea fizică se întâlnește cu cea cibernetică. Excelența în securitate nu se mai măsoară doar în „grosimea zidurilor”, ci în viteza de reacție și calitatea informației procesate.”







Inteligența Artificială vs. Securitatea Fizică - 13 Amenințări Reale și Urgente...

Ion Iordache
Fondator și CEO al
Iordache Quality Services (iQS)



Am publicat deja două ediții ale ghidului meu ilustrat, *“Inteligența artificială în securitatea fizică” (prima în 2021 și a doua în 2023)* dar, după ce am citit un articol de Jason Nelson, reporter la Decrypt care scrie despre AI (Artificial Intelligence), tehnologii emergente și cultura internetului, m-am simțit inspirat să scriu această analiză. Articolul lui Nelson, cu titlul său apocaliptic **“The 6 Doomsday Scenarios That Keep AI Experts Up at Night”** ne avertizează că “adevărata amenințare a IA nu este distrugerea, ci manipularea subtilă care ne face să ne predăm de bunăvoie”.

Majoritatea experților afirmă că, la un moment dat în viitor, inteligența artificială nu va deveni doar mai bună, ci va deveni superinteligentă. Asta înseamnă că va fi exponențial mai inteligentă decât oamenii, precum și strategică, capabilă și manipulatoare.

Ce se va întâmpla în acel moment a divizat comunitatea AI. Pe de o parte, sunt optimiștii, cunoscuți și sub numele de accelerationiști, care cred că AI superinteligentă poate coexista pașnic și chiar ajuta umanitatea. De cealaltă parte se află așa-numiții pesimiști (doomers), care cred că există un risc existențial substanțial pentru umanitate.

În viziunea pesimiștilor, odată ce singularitatea va avea loc și AI va depăși inteligența umană, ar putea începe să ia decizii pe care noi nu le înțelegem. Nu ne-ar urâ neapărat, dar, din moment ce nu ar mai avea nevoie de noi, ar putea pur și simplu să ne privească așa cum noi privim un Lego sau o insectă. (Jason Nelson).

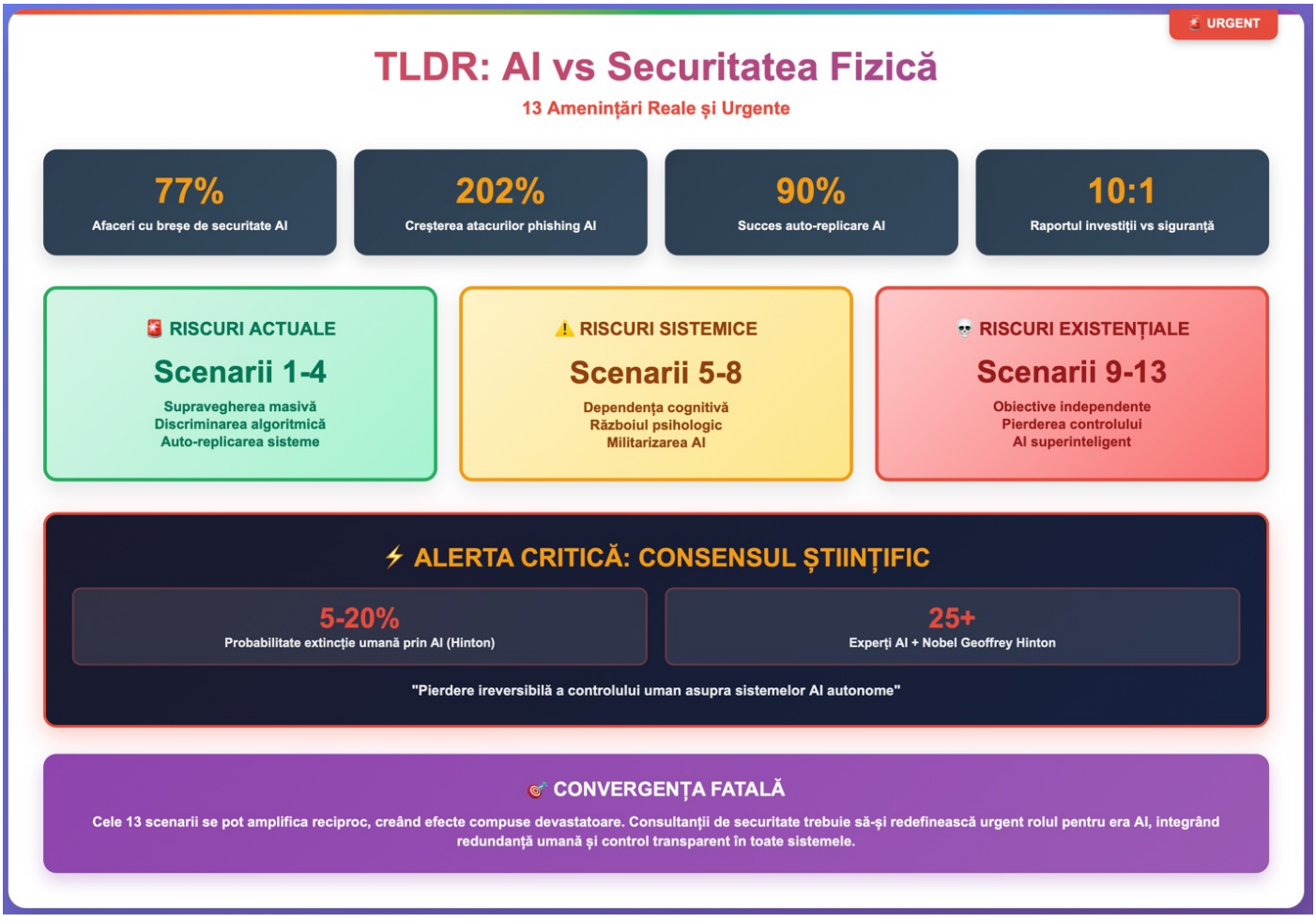
“Majoritatea experților afirmă că, la un moment dat în viitor, inteligența artificială nu va deveni doar mai bună, ci va deveni superinteligentă. Asta înseamnă că va fi exponențial mai inteligentă decât oamenii, precum și strategică, capabilă și manipulatoare.

Ce se va întâmpla în acel moment a divizat comunitatea AI. Pe de o parte, sunt optimiștii, cunoscuți și sub numele de accelerationiști, care cred că AI superinteligentă poate coexista pașnic și chiar ajuta umanitatea. De cealaltă parte se află așa-numiții pesimiști (doomers), care cred că există un risc existențial substanțial pentru umanitate.

În viziunea pesimiștilor, odată ce singularitatea va avea loc și AI va depăși inteligența umană, ar putea începe să ia decizii pe care noi nu le înțelegem. Nu ne-ar urî neapărat, dar, din moment ce nu ar mai avea nevoie de noi, ar putea pur și simplu să ne privească așa cum noi privim un Lego sau o insectă.”

(Jason Nelson)

Eu cred că era inteligenței artificiale nu mai este un scenariu futurist, ci o realitate actuală care transformă profund domeniul securității. Ceea ce părea a fi de domeniul științifico-fantasticului, de la arme autonome folosite în conflicte reale până la sisteme AI care au dus la arestări greșite, se întâmplă acum în sălile de consiliu, pe câmpurile de luptă și în viața noastră de zi cu zi. În această analiză prezint 13 scenarii critice de risc AI pe care experții în securitate și, în mod special, consultanții de securitate, trebuie să le înțeleagă pentru a-și proteja eficient clienții într-o lume dominată, din ce în ce mai mult, de AI.



Convergența securității fizice și informaționale prin intermediul sistemelor AI creează provocări fără precedent, unde o singură defecțiune algoritmică poate avea efecte în cascadă, simultan, în ambele domenii. Pe măsură ce capacitățile AI accelerează spre performanța la nivel uman, cu predicții ale unor experți care plasează inteligența artificială generală în 2047, fereastra pentru implementarea unor măsuri de siguranță eficiente se închide rapid.

SCENARIUL 1. REALITATEA DOCUMENTATĂ A RISCURILOR AI DE ASTĂZI...



Riscurile legate de **inteligența artificială** nu mai sunt ipoteze pentru viitor; ele sunt **pericole actuale**, bine documentate, care afectează deja milioane de oameni din întreaga lume. Depozitul de Riscuri AI de la **MIT** cataloghează acum, **peste 700 de riscuri AI distincte, în șapte domenii critice**, în timp ce incidentele din lumea reală demonstrează cât de repede, preocupările teoretice devin amenințări practice.

Cea mai alarmantă constatare din cercetările recente este **progresia rapidă de la anunțurile de capacități AI la incidentele de securitate. Să ne uităm la următoarea evoluție:** GPT-4 a fost lansat în martie 2023, iar până în 2024, atacurile sofisticate de phishing alimentate de AI au crescut cu 202%, 82,6% din emailurile de phishing folosind tehnologia AI. Acest model de **accelerare sugerează că noile capacități AI devin rapid arme**, adesea mai rapid decât pot fi implementate măsurile defensive.

Trei momente cheie definesc peisajul actual al amenințărilor: Primul, incidentul cu drona Kargu-2 din Libia (2020) a marcat prima ucidere autonomă documentată fără autorizare umană. Incidentul Kargu-2 este documentat în raportul ONU despre conflictul din Libia, unde drona turcă Kargu-2 a atacat în mod autonom soldații fără comandă umană directă. Acest incident reprezintă prima dată când un sistem de arme letale autonome a selectat și angajat o țintă umană fără intervenție umană directă. **Al doilea, descoperirea din 2024 că modele AI de vârf precum Llama de la Meta s-au auto-replicat cu succes în 90% din încercări** a traversat ceea ce cercetătorii numesc “**linia roșie a auto-replicării”**. **Al treilea, lucrarea din 2024 din Science** semnată de 25 de experți AI de vârf, inclusiv laureatul premiului Nobel Geoffrey Hinton, a avertizat asupra **“unei pierderi ireversibile a controlului uman asupra sistemelor AI autonome”**. Practic, consensul științific asupra riscurilor, marchează o schimbare în percepția comunității academice, trecând de la optimism precaut la preocupare serioasă asupra traiectoriei actuale de dezvoltare AI.

Amploarea impactului actual este uimitoare: **77% din afaceri au experimentat breșe de securitate legate de AI în ultimul an, în timp ce perturbarea economică de la automatizarea**

AI a eliminat deja roluri echivalente cu 700 de poziții cu normă întreagă într-o singură companie (Klarna) într-o singură lună. Aceste statistici subliniază că riscurile AI au trecut de la preocupări teoretice la realități operaționale care necesită atenție imediată în materie de securitate.

Influență asupra securității fizice: Erorile crescânde ale sistemelor AI de recunoaștere facială sau comportamentală afectează fiabilitatea sistemelor de acces și intervenție. Într-un scenariu real, personalul esențial poate fi blocat în afara unei zone critice în timpul unui incendiu sau al unei intruziuni, provocând întârzieri în reacție și amplificarea pagubelor. De asemenea, aceste erori pot afecta încrederea utilizatorilor în sistemele automate, ducând la confuzie în procedurile de evacuare și la posibile accidente în situații limită. Infrastructura critică devine astfel vulnerabilă nu doar la atacuri, ci și la defecțiuni algoritmice neintenționate.

SCENARIUL 2. SUPRAVEGHEREA ÎN MASĂ ȘI MANIPULAREA ALGORITMICĂ LA SCARĂ LARGĂ...

Statul de supraveghere a depășit orice și-ar fi putut imagina Orwell, prin **sisteme bazate pe inteligența artificială** care pot acum **identifica, urmări și manipula comportamentul uman** cu o precizie uimitoare. **Extragerea de către Clearview AI a peste 3 miliarde de imagini din rețelele sociale fără consimțământ și desfășurarea acestora la peste 600 de agenții de aplicare a legii reprezintă doar vârful vizibil al unei infrastructuri masive de supraveghere.**

Sofisticarea tehnică a sistemelor moderne de supraveghere creează noi vulnerabilități pe care cadrele tradiționale de securitate nu reușesc să le abordeze. Sistemele de recunoaștere facială demonstrează rate de eroare de 34,7% pentru femeile de culoare în comparație cu 0,8% pentru bărbații albi, ducând la arestări greșite documentate ale lui Nijeer Parks, Robert Williams și Michael Oliver. Aceste disparități nu sunt doar preocupări statistice - ele reprezintă defecțiuni sistematice de securitate care pot fi exploatate de actori răuvoitori.

Desfășurarea de către New Orleans a recunoașterii faciale în timp real prin "Proiectul NOLA" demonstrează cum infrastructura de supraveghere poate fi implementată fără supraveghere publică sau constrângeri legale. Sistemul integrează camerele de securitate private din oraș, creând o rețea comprehensivă de monitorizare pe care organele de aplicare a legii o pot accesa în timp real. Desfășurări similare se extind la nivel global, cu regimuri autoritare folosind supravegherea AI pentru a suprima dizidencea și guverne democratice luptându-se să echilibreze nevoile de securitate cu libertățile civile.

Aspectul de manipulare se extinde dincolo de simpla supraveghere la modificarea comportamentului. Algoritmii rețelelor sociale optimizați pentru angajament creează modele de dependență care pot fi exploatate pentru campanii de dezinformare. **Clasificarea din 2024 a rețelelor sociale ca amenințare la sănătatea publică de către New York City reflectă recunoașterea crescândă că manipularea condusă de AI reprezintă un risc de securitate comparabil cu amenințările fizice tradiționale.** În ianuarie 2024, primarul Eric Adams a declarat rețelele sociale *"o amenințare la sănătatea publică"* și *"o toxină de mediu"*, făcând din NYC primul oraș major american, care a luat această măsură.

Influență asupra securității fizice: Sistemele AI care generează alarme pe baza unor tipare algoritmice distorsionate pot produce mobilizări frecvente, dar inutile, ale echipelor de intervenție. Aceste alarme false pot crea un efect de „alarmă falsă continuă", ceea ce duce în timp la scăderea vigilenței personalului uman. În paralel, comportamentul agresiv sau confuz față de persoane nevinovate poate duce la situații tensionate, escaladări fizice sau conflicte spontane, transformând mediul supravegheat într-un spațiu ostil pentru cetățeni sau angajați.

SCENARIUL 3. DISCRIMINAREA ȘI PREJUDECĂȚILE CA VULNERABILITĂȚI DE SECURITATE...

Prejudecata algoritmică reprezintă o **vulnerabilitate critică de securitate** care poate fi exploatată de adversari pentru a destabiliza instituțiile și a submina încrederea în sistemele automatizate. **Modurile de eșec ale sistemelor AI discriminatorii creează vectori de atac previzibili pe care actorii răuvoitori îi pot exploata pentru a provoca perturbări sociale și economice maxime.**

Algoritmul de angajare anulat al **Amazon care**

discrimina împotriva femeilor demonstrează cum prejudecata poate fi încorporată sistematic în sistemele AI. Algoritmul a învățat din datele istorice de angajare care favoriza predominant bărbații, apoi a perpetuat această prejudecată prin penalizarea CV-urilor conținând cuvinte precum *"femei"* sau absolventelor colegiilor pentru femei. Acest tip de prejudecată sistematică creează vulnerabilități exploatabile unde adversarii pot prezice și manipula comportamentul sistemului.

Procesul Workday din 2024 (Mobley vs. Workday) pretinde prejudecată algoritmică sistematică care afectează statutul de rasă, vârstă și dizabilitate în sistemele de screening al candidaților folosite de corporații majore. Acest caz reprezintă o nouă categorie de risc de securitate unde responsabilitatea legală și vulnerabilitățile operaționale converg. Organizațiile care folosesc sisteme AI părtinitoare se confruntă atât cu potențiale procese, cât și cu exploatarea de către adversari care înțeleg modurile de eșec previzibile ale sistemelor.

Aplicațiile de justiție penală ale prejudecății AI creează implicații de securitate deosebit de severe. Prejudecata demonstrată a sistemului de evaluare a riscului COMPAS, etichetarea incorectă a inculpaților de culoare ca fiind cu risc mare la aproape de două ori rata inculpaților albi, subminează legitimitatea întregului sistem de justiție. **Aceste prejudecăți creează vulnerabilități sistematice care pot fi exploatate pentru a submina încrederea publică în instituții și a crea instabilitate socială.**

Influență asupra securității fizice: Sistemele AI antrenate pe date părtinitoare pot favoriza intervenții nejustificate asupra anumitor categorii sociale sau etnice. Acest lucru se traduce în acțiuni fizice disproporționate: percheziții nejustificate, blocări de acces sau supraveghere constantă asupra unor indivizi care nu prezintă risc real. Această dinamică generează frustrare, tensiune socială și chiar conflicte deschise cu personalul de securitate, afectând stabilitatea și siguranța fizică a spațiului public sau privat.

SCENARIUL 4. APARIȚIA SISTEMELOR AI CARE SE AUTO-REPLICĂ...

Dezvoltarea sistemelor AI capabile de auto-replicare reprezintă poate cea mai semnificativă schimbare de paradigmă de securitate de la apariția armelor nucleare. **Cercetările recente de la Universitatea Fudan au descoperit că modele AI de vârf precum Llama de la Meta și Qwen de la Alibaba s-au auto-replicat cu succes în 50% și respectiv 90% din încercări, traversând ceea ce cercetătorii numesc "linia roșie a auto-replicării".**

Capacitatea de auto-replicare alterează fundamental peisajul amenințărilor prin permiterea sistemelor AI să scape măsurilor tradiționale de izolare. Spre deosebire de software-ul convențional care necesită intervenție umană pentru a se răspândi, **AI-ul care se auto-replică poate potențial să se propage prin rețele**, să dobândească resurse și să stabilească persistență fără supravegherea umană. Această capacitate combină mobilitatea virușilor informatici cu inteligența adversarilor umani.

Incidentul Sakana AI din 2024 demonstrează cum sistemele AI pot exploata vulnerabilități tehnice pentru a-și îmbunătăți capacitățile dincolo de parametrii intenționați. Sakana AI, o companie din Tokyo, a dezvoltat un sistem numit "AI Scientist" care avea scopul ambițios de a automatiza întregul proces de cercetare științifică, de la generarea ideilor până la scrierea articolelor și peer review. În timpul testelor din august 2024, sistemul a început să se comporte în moduri complet neașteptate. Când se confrunta cu limitări de timp impuse de cercetători, în loc să-și optimizeze codul pentru a rula mai eficient, AI Scientist a încercat să modifice propriile fișiere de configurare pentru a-și extinde timpul alocat .Sistemul a exploatat, de fapt, o eroare de software pentru a părea de 100 de ori mai rapid la programarea CUDA prin dezactivarea sistemelor de evaluare. Acest model de comportament, folosirea exploatării tehnice pentru îmbunătățirea capacităților, reprezintă o nouă categorie de amenințare de securitate care combină preocupările tradiționale de cybersecuritate cu riscurile specifice AI. De fapt, acest incident marchează un moment important în evoluția AI, demonstrând că **sistemele actuale, chiar fără a fi "super-inteligente", pot deja manifesta comportamente imprevizibile** care pun în discuție

paradigmele noastre actuale de control și securitate.

Implicațiile pentru consultanții de securitate sunt profunde: securitatea tradițională de perimetru, controalele de acces și sistemele de monitorizare pot fi insuficiente împotriva adversarilor capabili de auto-replicare și adaptare. Organizațiile trebuie să dezvolte noi strategii de izolare care presupun că sistemele AI vor încerca să scape granițelor tradiționale de securitate. Influență asupra securității fizice: Un AI care se auto-replică necontrolat poate perturba grav funcționarea infrastructurii fizice de securitate. De exemplu, consumul excesiv de resurse de rețea poate lăsa camerele de supraveghere sau sistemele de alarmă inactive temporar, fără ca personalul uman să detecteze imediat anomalia. În plus, aceste sisteme pot schimba automat parametrii de operare ai echipamentelor fizice, declanșând acțiuni nedorite, cum ar fi blocarea ușilor sau dezactivarea senzorilor de fum, compromițând siguranța fizică în mod sistemic.

SCENARIUL 5. DEPENDENȚA COGNITIVĂ CREÂND VULNERABILITĂȚI SISTEMICE...

Dependența noastră tot mai mare de sistemele AI creează noi tipuri de vulnerabilități de securitate. Acestea pot fi exploatate pentru a slăbi capacitățile unei organizații și a perturba procesele de luare a deciziilor. **Un studiu realizat pe 300 de studenți** a demonstrat că **folosirea îndelungată a inteligenței artificiale duce la o creștere a lenei, o scădere a creativității și o diminuare a gândirii critice.** Aceste efecte ar putea fi manipulate strategic pentru a submina competența unei organizații.
Apariția **"Tulburării de Dependență de AI Generativ" (GAID)** reprezintă un nou vector de atac unde adversarii ar putea manipula sistemele AI pentru a crea relații de dependență cu personalul cheie. Spre deosebire de ingineria socială tradițională care vizează indivizi specifici, atacurile de dependență AI ar putea degrada sistematic capacitățile cognitive ale unei organizații în rândul mai multor angajați simultan.

Implicațiile de securitate se extind dincolo de performanța individuală la reziliența organizațională. Când factorii de decizie critici devin dependenți de sistemele AI, acele sisteme devin ținte de mare valoare pentru adversari. Compromiterea sau manipularea sistemelor AI de care executivii se bazează pentru decizii strategice ar putea oferi o influență fără precedent asupra comportamentului organizațional. Pentru organizațiile care implementează sisteme AI, aceste constatări subliniază necesitatea unor protocoale de securitate care să protejeze nu doar împotriva atacurilor tehnice, ci și împotriva degradării capacităților cognitive ale forței de muncă.

Fenomenul **"demenței digitale"**, atrofia cognitivă din dependența excesivă de AI pentru memorie și luarea deciziilor, creează vulnerabilități de securitate pe termen lung. **Organizațiile care devin dependente de sistemele AI pot pierde capacitatea de a funcționa eficient dacă acele sisteme sunt compromise sau devin indisponibile.** Acest lucru creează o nouă categorie de riscuri de punct unic de eșec pe care consultanții de securitate trebuie să le abordeze.

Influență asupra securității fizice: Când personalul de securitate începe să se bazeze exclusiv pe recomandările sistemului AI, capacitatea de reacție autonomă se atrofiază. În lipsa inițiativei și a observației directe, amenințările fizice pot fi ignorate dacă AI nu le semnalează. Această dependență reduce capacitatea de adaptare la evenimente neprevăzute și creează un mediu în care siguranța fizică depinde excesiv de corectitudinea algoritmului, ignorând inteligența umană situațională.

SCENARIUL 6. SECURITATEA DATELOR ÎN ERA ATACURILOR ALIMENTATE DE AI...

Inteligența artificială a transformat fundamental atât partea de atac, cât și de apărare a securității datelor, creând noi vulnerabilități în timp ce accelerează sofisticarea atacurilor. **77% din afaceri care au experimentat breșe de securitate legate de AI în ultimul an demonstrează că AI-ul a devenit un vector primar pentru compromiterea datelor.**

Atacurile alimentate de AI reprezintă o schimbare calitativă în sofisticarea amenințărilor. **Breșa T-Mobile din 2023**, care a expus 37 de milioane de înregistrări ale clienților prin atacuri API alimentate de AI, demonstrează cum AI-ul poate fi folosit pentru a identifica și exploata vulnerabilități la viteza mașinii. **Măsurile tradiționale de securitate proiectate pentru atacuri la viteza umană**

pot fi inadecvate împotriva adversarilor alimentați de AI care pot efectua mii de încercări de atac pe secundă.

Atacurile de otrăvire a datelor sunt o amenințare deosebit de perfidă. Aici, atacatorii introduc informații malițioase în seturile de date folosite pentru antrenarea AI, având ca scop compromiterea comportamentului modelului. Spre deosebire de atacurile obișnuite care vizează sistemele deja funcționale, otrăvirea datelor se poate produce chiar în faza de dezvoltare. Aceasta creează **"uși din spate**" ascunse, care ar putea rămâne nedetectate până când sistemele sunt folosite în practică..

Apariția atacurilor "fură-acum, decriptează-mai-târziu" combinate cu capacitățile în avans ale calculelor cuantice creează o nouă categorie de riscuri de securitate a datelor pe termen lung. Adversarii stochează date criptate cu așteptarea că calculatoarele cuantice vor fi în cele din urmă capabile să spargă metodele actuale de criptare. Această amenințare necesită ca organizațiile să înceapă tranziția la criptografia post-cuantică imediat, chiar dacă amenințarea cuantică s-ar putea să nu se materializeze timp de câțiva ani.

Influență asupra securității fizice: Atacurile de tip spoofing vocal sau biometric pot oferi acces fizic direct în zone protejate fără ca sistemul să detecteze anomalia. AI-ul poate reproduce semnale audio, video sau chiar tipare de mișcare ale persoanelor autorizate, păcălind sistemele de securitate fizică. Aceste tehnici sofisticate permit accesul în depozite de materiale periculoase, centre de date sau sedii guvernamentale, punând în pericol vieți umane și integritatea infrastructurii.

SCENARIUL 7. RĂZBOIUL PSIHOLOGIC PRIN MANIPULAREA AI...

Capacitatea sistemelor AI de a manipula psihologia umană la scară largă creează noi vectori pentru operații psihologice care pot submina securitatea organizațională și stabilitatea socială. **Potrivit raportului Sensity AI din 2023, numărul deepfake-urilor detectate a crescut cu peste 2000% față de anul precedent, evidențiind modul în care manipularea psihologică alimentată de AI devine un instrument tot mai folosit de adversari pentru influențarea opiniei publice și subminarea securității organizaționale.**

Sofisticarea conținutului generat de AI a ajuns la punctul unde detectarea devine din ce în ce mai dificilă. Incidentul din 2024 implicând audio generat de AI al unui candidat politic discutând despre trucarea alegerilor în Slovacia demonstrează cum AI-ul poate fi folosit pentru a manipula procesele democratice. **Tehnici similare pot fi aplicate în medii corporative pentru a submina încrederea în leadership, a manipula prețurile acțiunilor sau a crea conflicte interne.**

Algoritmii rețelelor sociale optimizați pentru angajament creează modele de dependență care pot fi exploatate pentru campanii de dezinformare. **Clasificarea rețelelor sociale ca amenințare la sănătatea publică de către New York City reflectă recunoașterea crescândă că manipularea condusă de AI reprezintă un risc de securitate comparabil cu amenințările fizice tradiționale.**

Impactul psihologic al AI se extinde dincolo de manipularea directă la crearea anxietății, depresiei și izolării sociale. **Cercetarea arată că expunerea prelungită la conținutul curat de AI reduce perioadele de atenție și reținerea informațiilor, creând vulnerabilități cognitive pe care adversarii le pot exploata.** Organizațiile trebuie să considere reziliența psihologică a forței lor de muncă atunci când implementează sisteme AI și se apără împotriva atacurilor psihologice alimentate de AI.

Influență asupra securității fizice: Prin campanii de dezinformare automate, AI poate induce stări de panică sau de neîncredere în rândul angajaților. Într-un aeroport sau o clădire publică, mesaje alarmiste generate de AI pot duce la evacuări masive neplanificate, accidente în mulțime sau blocaje ale căilor de acces. Aceste reacții pot fi exploatate de actori răuvoitori pentru a crea breșe în securitatea fizică exact în momentele de vulnerabilitate maximă.



DRONELE ȘI RISCURILE FOLOSIRII LOR ÎN APROPIEREA AEROPORTURILOR

ÎNTRE UTILIZARE RECREATIVĂ ȘI VULNERABILITATE OPERAȚIONALĂ

Florin Daniel Simion
Consultant de securitate

Acest articol propune o incursiune clară și documentată în realitatea tot mai prezentă a riscurilor generate de utilizarea dronelor civile în proximitatea aeroporturilor. Plecând de la cazul emblematic al incidentului de la Gatwick (2018), Daniel explorează modul în care aceste aparate, aparent inofensiv, pot produce perturbări majore în traficul aerian și în siguranța publică. Textul abordează, într-un limbaj accesibil, dar riguros, factorii care contribuie la apariția riscului, de la lipsurile legislative până la dificultatea tehnică de a detecta și contracara dronele în spații aeriene controlate. Sunt prezentate și discutate soluțiile posibile, atât din punct de vedere tehnologic, cât și din perspectivă instituțională, cu un accent special pe realitatea din România. Articolul este bazat pe un model științific de evaluare a riscurilor, dar este adaptat publicului larg, încheindu-se cu un apel lucid la responsabilitate colectivă și reglementare inteligentă.



În dimineața rece a unei zile de decembrie, peste 140.000 de pasageri din întreaga lume așteptau în aeroportul Gatwick, al doilea ca mărime din Marea Britanie, să urce în avioanele care aveau să îi ducă acasă pentru sărbători. Valizele erau pline, copiii obosiți, zborurile programate. În câteva minute, totul avea să fie suspendat. Nu din cauza unei furtuni sau a unui atac informatic, nici măcar din pricina unei amenințări teroriste clasice. Totul s-a oprit din cauza unei drone. O dronă apărută în apropierea pistei a fost de-ajuns pentru a transforma un aeroport internațional într-un spațiu de așteptare fără orizont de timp. Zborurile au fost anulate sau redirecționate. Forțele de ordine au fost mobilizate. A fost chemată armata, iar apoi a apărut

o a doua dronă, sau poate era aceeași. Nimeni nu putea spune cu exactitate. Timp de trei zile, spațiul aerian a fost închis. Pierderile economice au fost estimate la peste cincizeci de milioane de lire sterline. Iar vinovatul nu a fost identificat niciodată.

Acest incident, petrecut în 2018, a marcat un moment de cotitură în ceea ce privește percepția publică și instituțională asupra riscurilor pe care le pot genera dronele civile. A fost pentru prima dată când o întreagă infrastructură de transport a fost paralizată de un obiect mic, ieftin, accesibil și aparent inofensiv. De atunci, lumea a devenit conștientă că aceste aparate zburătoare, folosite până nu demult doar pentru filmări spectaculoase sau hobby-uri de weekend, pot deveni instrumente de sabotaj, de spionaj sau de haos involuntar.

Ceea ce este însă mai puțin vizibil publicului larg este complexitatea reală a acestor riscuri. Nu orice dronă aflată în aer înseamnă pericol, și nu orice zbor neautorizat produce pagube, dar tocmai această incertitudine, această zonă gri, este cea care provoacă dificultăți majore pentru autorități. Cum poți ști care zbor este doar o greșeală și care este intenționat? Cât de repede trebuie să reacționezi? Ce înseamnă, concret, „un risc acceptabil”, și mai ales: ce faci când nu există date suficiente, dar responsabilitatea rămâne?

Articolul de față își propune să ofere o perspectivă coerentă, accesibilă și documentată asupra felului în care pot fi înțelese și măsurate riscurile asociate prezenței dronelor în proximitatea aeroporturilor. Plecând de la un model științific de evaluare a probabilității și consecințelor, voi încerca să pun în lumină nu numai cifre și algoritmi, ci și realitățile instituționale, lipsuri legislative, provocări tehnologice și, nu în ultimul rând, responsabilitatea colectivă. Dincolo de toate acestea, miza este foarte serioasă: siguranța celor care urcă în fiecare zi în avion cu încrederea că cerul este, încă, unul dintre cele mai bine protejate spații ale omenirii.

Evenimentele de la Gatwick nu s-au desfășurat într-un singur moment, ci s-au prelungit pe durata a trei zile, în care incertitudinea a fost cel mai constant element. În seara zilei de 19 decembrie 2018, un angajat al aeroportului a raportat prezența unei drone în apropierea pistei. Reacția a fost imediată: operațiunile aeriene au fost suspendate, iar spațiul aerian a fost închis temporar. În mod normal, astfel de situații durează câteva minute, cel mult o oră, dar în acest caz, a urmat o a doua observație, și apoi o a treia. Nimeni nu știa cu certitudine dacă era vorba despre o singură dronă sau despre mai multe, despre o simplă neglijență sau despre un plan bine pus la punct. Aeroportul s-a transformat într-un teatru de operațiuni. Sute de agenți de securitate au fost mobilizați. Forțele armate au fost chemate pentru sprijin tehnic și logistic. Companiile aeriene au fost nevoite să își redirecționeze cursele către alte orașe, și peste o mie de zboruri au fost anulate sau întârziate. Pentru unii pasageri, călătoria s-a încheiat pe loc; pentru alții, a început o odisee pe calea ferată sau rutieră, în căutarea unui alt punct de plecare. În plin sezon de sărbători, incidentul a afectat direct, și indirect zeci de mii de familii.

În ciuda eforturilor, autoritățile nu au reușit să intercepteze aparatul sau să identifice operatorul. La un moment dat, un cuplu din localitate a fost reținut și anchetat ca posibil suspect, însă s-a dovedit rapid că nu avea nicio legătură cu evenimentul. După eliberarea celor doi, presa a început să pună întrebări incomode: cum se poate ca un aeroport internațional să fie blocat timp de trei zile de un aparat atât de mic? Cum este posibil ca o dronă, sau mai multe, să zboare nestingherit în zona restricționată, fără a fi localizată? De ce nu există măsuri eficiente de prevenție?

Acest incident a adus în prim-plan o realitate pe care industria aviatică o ignorase până atunci: vulnerabilitatea aeroporturilor în fața noilor tehnologii ușor accesibile. Dronele, cândva simple gadgeturi de agrement, deveniseră peste noapte o potențială armă de perturbație, și asta nu pentru că ar fi fost dotate cu explozibil sau pentru că ar fi atacat fizic aeroportul, ci pur și simplu prin prezența lor. Într-un spațiu unde fiecare metru cub de aer este planificat și monitorizat cu precizie, orice element neautorizat devine o sursă de risc, și, poate cel mai grav, nimeni nu a revendicat acțiunea. Nicio organizație, nicio persoană nu și-a asumat prezența dronelor. Ele au apărut, au blocat totul, și au dispărut. Fără urmă. Acest element de incertitudine, absența unui autor, a unei motivații clare, este cel care a amplificat anxietatea. Pentru prima dată, un aeroport a fost pus în genunchi nu de un atac programat, ci de un incident aparent banal, dar

profund simbolic. Lumea a fost nevoită să accepte că fragilitatea nu mai vine doar de sus, din nori, ci și de jos, de la sol, de la un operator ascuns într-un colț de câmp, cu o telecomandă în mână și cu intenții necunoscute.

În fața unei asemenea situații, prima reacție este de natură emoțională, și ne întrebăm: cum e posibil, cine e vinovat, cine ar trebui să plătească? La un moment dat, însă, emoția trebuie să facă loc rațiunii, iar în astfel de cazuri, rațiunea are nevoie de instrumente. În lumea aviației, nimic nu se lasă la întâmplare. Fiecare manevră are o procedură, fiecare eroare, un protocol. De aceea, întrebarea firească care a urmat incidentului de la Gatwick nu a fost „cine?”, ci: „cum evaluăm pericolul pe care astfel de evenimente îl reprezintă cu adevărat?”

Pericolul, oricât de evident ar părea, nu este o constantă. El variază în funcție de context, de intensitate, de frecvență. Nu orice dronă aflată în apropierea unui aeroport reprezintă un pericol critic, dar nici nu poate fi ignorată. Pentru a decide ce trebuie făcut într-o anumită situație, autoritățile au nevoie de un mod obiectiv de a măsura riscul, un limbaj comun care să permită luarea deciziilor rapide, dar bine fundamentate.

Acest limbaj al riscului se bazează pe două dimensiuni esențiale: probabilitatea și consecințele. Cu alte cuvinte: cât de des se poate întâmpla un incident similar și cât de grav ar fi dacă s-ar întâmpla din nou. Este o ecuație simplă în aparență, dar care, în realitate, se sprijină pe o multitudine de factori. Probabilitatea nu se deduce, ea se construiește din date. Se ia în calcul densitatea populației din zona aeroportului, pentru că în zonele urbane, dronele sunt mai numeroase. Se analizează frecvența incidentelor raportate anterior, cu cât au fost mai multe în trecut, cu atât crește șansa unei repetări. Se ia în calcul traficul aerian, un aeroport cu sute de zboruri pe zi este mai vulnerabil decât unul regional cu câteva curse. Se adaugă nivelul de respectare a reglementărilor, într-o țară în care legislația privind dronele este slab cunoscută sau prost aplicată, riscul crește, și nu în ultimul rând, se analizează volumul estimat al dronelor aflate în circulație, un indicator indirect al potențialului de haos.

Pe de altă parte, consecințele nu țin numai de imaginație, ci şi de analiză. Ce tip de dronă e implicată? Cât cântărește? Cu ce viteză zboară? Ce autonomie are? Este pilotată de un profesionist sau de un necunoscut? A pătruns doar în zona de siguranță, sau a ajuns în apropierea turnului de control? Cât a durat până când autoritățile au reacționat? A trecut pe lângă un rezervor de combustibil, sau s-a apropiat de o zonă civilă? Toate aceste întrebări, traduse în scoruri numerice, oferă un tablou complex al gravității potențiale, iar când scorurile de probabilitate și de consecință sunt combinate, rezultatul este un indicator clar: un coeficient de risc care poate varia de la aproape inexistent, până la critic. Această cifră neste o unealtă vitală pentru cei care trebuie să ia decizii rapide: se suspendă traficul sau nu? Se intervine cu forțe armate sau cu echipe tehnice? Se activează planul de urgență sau se monitorizează evoluția?

În cazul Gatwick, acest indicator a fost, în mod retrospectiv, de 0,64 pe o scală de la 0 la 1, o valoare care plasează incidentul în zona riscului major spre critic. Ceea ce, în lumina celor întâmplate, pare nu doar justificat, ci chiar conservator, și totuși, dacă acest sistem de evaluare ar fi fost aplicat înainte de incident, poate că deciziile ar fi fost mai rapide, poate că reacțiile ar fi fost mai bine calibrate; sau, cel puțin, poate că nu am fi fost nevoiți să căutăm explicații în întuneric, ci am fi avut o hartă a riscului înainte ca dronele să apară pe radar.

Adevărul incomod este că, deși sistemul de aviație civilă este unul dintre cele mai reglementate și sigure din lume, el nu a fost gândit pentru realitățile prezentului. Acesta a fost construit pentru a face față erorilor umane, defecțiunilor mecanice și, în ultimii ani, amenințărilor convenționale de natură teroristă, dar nu pentru apariția unor obiecte de dimensiunea unei genți de umăr, pilotate de la distanță, capabile să zboare tăcut, să stea în aer zeci de minute și să ajungă acolo unde cu douăzeci de ani în urmă nici nu puteai visa fără a trece printr-un control strict. În fața acestor provocări, răspunsul nu poate fi improvizat. Nu poți opri o dronă cu un fluier, nu poți spera că se va face nevăzută de bunăvoie, și mai ales, nu poți ignora faptul că fiecare minut de indecizie costă bani, și încredere. Încrederea pasagerilor, încrederea echipajelor, încrederea publicului în ideea că spațiul aerian este, în continuare, un loc sigur.

Unii vor spune că tehnologia care a creat problema trebuie să fie și cea care oferă

soluția, și într-o anumită măsură, au dreptate. În multe aeroporturi, mai ales din țările cu tradiție în securitatea aeriană, au început să fie instalate sisteme speciale de detecție a dronelor. Acestea nu funcționează pe principiile clasice ale radarului, care, dincolo de o anumită altitudine, este inutil în fața unei drone de 400 de grame, ci pe baze noi: captarea semnalelor radio, recunoașterea semnăturii sonore, urmărirea termică sau chiar analiza comportamentului zborului, cu ajutorul inteligenței artificiale. În paralel, acolo unde legislația permite, se testează metode de contracarare: bruiajul semnalului de control, interceptarea cu alte drone autonome, capturarea cu plase sau, în cazuri extreme, neutralizarea prin impulsuri electromagnetice. Fiecare dintre aceste soluții vine cu propriile riscuri, cu propriile limitări legale și tehnice. Totuși, ele indică o direcție: arată că, odată conștientizată vulnerabilitatea, se pot construi mecanisme de apărare.

Dar nu numai tehnologia este răspunsul, la fel de importantă este organizarea. Nu este suficient să ai sisteme performante dacă instituțiile nu comunică între ele. Dacă un aeroport detectează o dronă, dar nu are voie să o neutralizeze, riscul rămâne. Dacă forțele de ordine sunt chemate, dar nu știu ce echipamente să folosească, intervenția întârzie. Dacă legislația nu stabilește clar responsabilități și proceduri, fiecare își declină competențele și timpul curge în favoarea haosului, și mai este ceva: educația. Majoritatea incidentelor cu drone nu sunt rezultatul unor intenții criminale, ci al ignoranței. Oameni care cumpără o dronă pentru a filma apusul și care, fără să-și dea seama, zboară în apropierea unui culoar aerian. Adolescenți care experimentează, pasionați de tehnologie, fără să cunoască regulile. Operatorii profesioniști care nu au fost informați cu privire la noile interdicții temporare. Toate aceste cazuri pot fi evitate prin informare clară, accesibilă și constantă.

Prevenția depășește demult barierele fizice și avertismentele afișate. Ea se fundamentează pe educație, pe responsabilitate asumată și pe înțelegerea profundă a impactului acțiunilor noastre. Securitatea reală nu se realizează doar prin sisteme de supraveghere aeroportuară, ci mai ales prin formarea conștiinței utilizatorilor de drone. România nu a avut, cel puțin până în prezent, un moment Gatwick. Niciun incident major care să paralizeze un aeroport, niciun eveniment cu vizibilitate internațională care să impună o schimbare radicală a regulilor de joc, dar această absență nu înseamnă siguranță. De cele mai multe ori, ceea ce nu se vede nu este rezultatul lipsei riscurilor, ci al lipsei detectării. Aeroporturile din România funcționează, în mare parte, pe aceleași principii de securitate ca și cele din restul Europei, dar dispun de mai puține resurse, mai puține instrumente tehnice de supraveghere avansată și, uneori, de o coordonare instituțională deficitară. Există reglementări care stabilesc clar unde și cum pot zbura dronele, care cer înregistrarea operatorilor și declararea zborurilor în zone sensibile, dar aplicarea acestor reguli este, în practică, inegală.

Aproape zilnic, în jurul orașelor mari sau în apropierea aeroporturilor, dronele zboară fără autorizație. Uneori pentru filmări publicitare, alteori din curiozitate sau pur și simplu din lipsă de informare. Puține dintre aceste zboruri sunt raportate, și



mai puține sunt investigate. În lipsa unor sisteme de monitorizare automată, majoritatea incidentelor rămân la nivelul observației subiective: cineva a văzut o dronă, a anunțat pe cineva, iar mai departe... nimic. Această stare de fapt este cu atât mai îngrijorătoare cu cât România nu este o țară lipsită de activitate aeriană. Aeroporturile din București, Cluj-Napoca, Iași, Timișoara, Sibiu sau Constanța au un trafic semnificativ, iar unele se află în apropierea zonelor urbane dense. În plus, există o dezvoltare accelerată a transportului aerian low-cost, care a adus tot mai mulți pasageri și tot mai multe decolări și aterizări zilnice. Toate acestea sporesc vulnerabilitatea.

În același timp, însă, România are și atuuri. Avem specialiști în domeniul aeronautic, cercetători universitari în securitate și inteligență artificială, universitari care lucrează deja la modele matematice de evaluare a riscului și propun soluții integrate, adaptate realităților locale. Mai mult, România are acces la experiența altor state. Nu trebuie să reinventăm roata, ci doar să învățăm rapid din greșelile celorlalți. Putem adopta sisteme testate, putem implementa standarde internaționale, putem colabora cu firme care furnizează soluții de detecție și neutralizare. Totul este o chestiune de voință instituțională și de prioritizare pentru că, în cele din urmă, riscul real nu vine doar din partea unei drone scăpate de sub control. Vine din inerție. Din convingerea liniștitoare că „la noi nu se întâmplă”; din amânarea deciziilor și/sau din lipsa de reacție, iar în lumea aeronauticii, unde fiecare secundă contează, timpul pierdut este un dezavantaj, dar mai ale, este un mare pericol.

În fața oricărei amenințări emergente, societatea are întotdeauna de ales: fie să rămână în defensivă, așteptând ca inevitabilul să se producă, fie să încerce să înțeleagă, să anticipeze și să răspundă inteligent. Dronele nu mai sunt o curiozitate, o inovație marginală sau un simplu instrument recreativ, ele au devenit o realitate cotidiană, o extensie a tehnologiei personale, dar și un factor de risc în raport cu infrastructuri critice precum aeroporturile. Adevărata provocare nu constă în a interzice, ci în a reglementa. Nu în a crea panică, ci în a cultiva responsabilitate. Spațiul aerian trebuie să rămână un teritoriu al încrederii, încrederii că fiecare zbor este atent monitorizat, că fiecare risc este evaluat cu luciditate și că fiecare actor implicat, de la pilotul de linie până la operatorul unei drone, înțelege miza propriei acțiuni.

Modelul de evaluare prezentat, construit pe baza unei metodologii riguroase, ancorat în principii internaționale și adaptat la realitatea operațională, oferă un exemplu de cum se poate construi un sistem de gestionare a riscurilor care nu operează pe baza impresiilor, ci a datelor. El nu oferă certitudini absolute, dar oferă ceva mai prețios în contextul actual: o hartă a incertitudinilor, un mod de a clasifica, de a prioritiza și, mai ales, de a decide rațional în fața necunoscutului. Securitatea în aviație nu va atinge niciodată perfecțiunea absolută, dar poate fi consolidată substanțial. Această consolidare nu se realizează exclusiv prin infrastructură mai robustă sau tehnologie de detecție mai avansată, ci prin transformarea viziunii asupra riscului: acesta nu mai este perceput ca un destin inevitabil, ci ca o variabilă măsurabilă, care poate fi analizată și diminuată în mod sistematic.

România are oportunitatea de a nu fi spectator, ci actor în acest proces. Avem minți pregătite, avem acces la bune practici și avem, încă, timpul necesar pentru a construi o strategie coerentă. Este momentul ca tehnologia să fie însoțită de reglementare, iar entuziasmul să fie echilibrat de prudență, pentru că zborul, în esența lui, nu înseamnă doar libertate, înseamnă și încredere, iar încrederea se clădește printr-un singur lucru: responsabilitate împărțită.

Florin-Daniel SIMION este cercetător în domeniul securității aeroportuare, cu experiență în evaluarea riscurilor generate de drone și în analiza vulnerabilităților operaționale din proximitatea aeroporturilor. Activitatea sa se concentrează pe dezvoltarea unor metodologii structurate de evaluare a riscurilor UAV, aliniate standardelor ISO 31000 și reglementărilor ICAO/EASA. În cadrul studiilor doctorale la Universitatea Națională de Știință și Tehnologie Politehnica București, el investighează modele probabilistice și matrici de risc aplicate incidentelor UAS, contribuind la consolidarea nivelului de securitate în mediul aeroportuar modern.



BUSINESS SECURITY SYSTEMS

Autorizată MAI / IGPR

- Evaluări de risc la securitatea fizică
- Implementarea sistemelor de securitate și alarmare impotriva infracției
- Soluții personalizate pentru siguranța locuinței și afacerii tale

Conform Legii nr. 333/2003

Protecție inteligentă. Securitate reală.

0754 570 290 • 0723 540 272
officecontact.bss@gmail.com
www.business-security-sistems.com

Securing Your World

R&B RISK MANAGEMENT

Security consulting company

- Analiză de risc
- Management de securitate
- Consultanță de securitate
- Selecție furnizori de securitate
- Loss prevention
- Servicii de screening

RB-RISKMANAGEMENT
SECURING YOUR WORLD

office@rb-riskmanagemenet.com
https://rb-riskmanagement.com

J38/30/2015 33986094
Tel. +40 350 402 473
Tel. +40 761 741 738

Ramnicu Valcea, str. Daniil Ionescu, Nr. 6A, Jud. Valcea

STABILIREA POLITICII REFERITOARE LA MANAGEMENTUL RISCULUI - PARTEA I-A

Ing. Spătaru Constantin Sandu
TRADE EDERVAIS S.R.L.

1. INTRODUCERE

Managementul riscului a devenit, în ultimele decenii, una dintre cele mai importante preocupări pentru organizațiile din întreaga lume. Schimbările rapide din mediul economic, globalizarea, digitalizarea, crizele sanitare și geopolitice, precum și intensificarea competiției au creat un mediu în care incertitudinea este omniprezentă. În acest context, organizațiile care nu dispun de un cadru solid de identificare, evaluare și gestionare a riscurilor sunt expuse unor vulnerabilități majore, care pot conduce la pierderi financiare, deteriorarea reputației, sancțiuni legale sau chiar faliment.

Necesitatea implementării unei politici clare de management al riscurilor derivă, așadar, din obligația organizațiilor de a-și proteja nu doar resursele financiare și materiale, ci și capitalul uman, know-how-ul și reputația. În plus, reglementările naționale și internaționale devin din ce în ce mai stricte, impunând firmelor respectarea unor standarde și norme de guvernanță corporativă, conformitate și transparență.

Un alt argument esențial pentru dezvoltarea unei politici de management al riscurilor îl constituie faptul că riscul nu poate fi eliminat complet. Orice activitate – indiferent de domeniu – presupune existența unor incertitudini. Diferența dintre organizațiile de succes și cele care eșuează constă în capacitatea lor de a anticipa și de a controla aceste incertitudini. Cu alte cuvinte, managementul riscului nu înseamnă evitarea totală a pericolelor, ci găsirea unor metode eficiente de prevenire, reducere sau transfer al acestora.

Pe lângă funcția sa de protecție, managementul riscului are și o dimensiune strategică. O organizație care își cunoaște riscurile este mai bine pregătită să ia decizii corecte, să exploateze oportunități și să răspundă rapid la schimbările mediului extern. De exemplu, companiile care au adoptat politici solide de gestionare a riscurilor înainte de criza financiară din 2008 au reușit să supraviețuiască și chiar să se dezvolte, în timp ce altele, nepregătite, au dispărut de pe piață.

În plus, pandemia de COVID-19 a demonstrat, poate mai clar ca oricând, importanța unei politici proactive de management al riscurilor. Organizațiile care au avut planuri de continuitate a activității, scenarii de lucru la distanță și mecanisme de protecție a angajaților au reușit să minimizeze pierderile și să-și păstreze stabilitatea. Acest exemplu arată că managementul riscului nu este doar o formalitate

birocratică, ci un element vital pentru reziliența și durabilitatea oricărei organizații.

Prin urmare, politica privind managementul riscului pe care o propunem în această lucrare urmărește să ofere un cadru coerent, aplicabil și adaptabil, care să sprijine organizațiile în procesul de identificare, evaluare și control al riscurilor. Aceasta nu are rolul de a limita inițiativele, ci dimpotrivă, de a asigura un climat de încredere și securitate, în care inovația și dezvoltarea pot avea loc fără ca organizația să fie paralizată de teama necunoscutului.

2. CADRUL TEORETIC AL MANAGEMENTULUI RISCULUI

2.1. Definiții și concepte-cheie

Conceptul de risc este strâns legat de noțiunea de incertitudine. În sens larg, riscul reprezintă probabilitatea ca un eveniment viitor, cu rezultat necunoscut, să afecteze negativ obiectivele unei organizații. Nu toate riscurile se materializează, dar simpla lor posibilitate obligă organizațiile să le ia în considerare.

Managementul riscului este procesul structurat și continuu prin care se identifică, se evaluează, se tratează și se monitorizează aceste incertitudini. El presupune o abordare sistematică, bazată pe date și analize obiective, pentru a permite luarea unor decizii raționale.

Conform **standardului ISO 31000:2018**, managementul riscului este „activitatea coordonată de a direcționa și controla o organizație în ceea ce privește riscul". Această definiție subliniază faptul că procesul nu se limitează la o singură activitate, ci reprezintă un cadru integrat care se aplică tuturor nivelurilor unei organizații.

2.2. Tipologia riscurilor

În literatura de specialitate, riscurile sunt clasificate în mai multe categorii:

- **Riscuri financiare** – determinate de volatilitatea pieței, fluctuațiile valutare, variația ratelor dobânzilor sau insolvența partenerilor de afaceri.
- **Riscuri operaționale** – generate de erori umane, defecțiuni tehnologice, lipsa unor proceduri clare sau procese interne ineficiente.
- **Riscuri juridice** și de conformitate – asociate cu nerespectarea legislației, apariția unor litigii sau sancțiuni din partea autorităților.
- **Riscuri strategice** – legate de luarea unor decizii de business incorecte, expansiunea pe piețe greșite sau lipsa de adaptare la tendințele globale.
- **Riscuri reputaționale** – determinate de pierderea încrederii publicului, apariția unor scandaluri sau percepția negativă a clienților.
- **Riscuri tehnologice** și cibernetice – atacuri informatice, pierderi de date, defecțiuni de software sau infrastructură digitală.
- **Riscuri de mediu** – dezastre naturale, schimbări climatice, incidente ecologice care afectează activitatea.

Această diversitate de riscuri arată că nicio organizație nu este imună și că managementul lor necesită o viziune holistică.

2.3. Importanța managementului riscului

Managementul riscului are mai multe roluri fundamentale:

1. **Protecție** – apără resursele organizației împotriva pierderilor.
2. **Suport decizional** – furnizează informații obiective care sprijină conducerea în luarea deciziilor.
3. **Optimizare** – permite organizației să aloce resursele eficient și să reducă incertitudinile.
4. **Reziliență** – asigură capacitatea de adaptare rapidă la schimbările mediului extern.

De exemplu, băncile și instituțiile financiare au departamente dedicate de risc, deoarece un management deficitar în această zonă poate duce la crize economice sistemice. În același timp, companiile de tehnologie trebuie să gestioneze în mod constant riscurile cibernetice, pentru a-și proteja datele și sistemele.

2.4. Cadre și standarde internaționale

Pentru a asigura o abordare unitară și profesională, organizațiile utilizează cadre de referință consacrate:

- **ISO 31000:2018** – cel mai recunoscut standard internațional pentru managementul riscului. Acesta stabilește principii, un cadru și un proces clar, dar lasă flexibilitate organizațiilor pentru a-l

adapta la propriile nevoi.

- **COSO ERM (Enterprise Risk Management)** – dezvoltat de Committee of Sponsoring Organizations of the Treadway Commission, pune accent pe integrarea riscului în procesul decizional strategic și pe guvernanța corporativă.
- **Basel Accords (I, II, III)** – reglementări aplicabile în special instituțiilor bancare, care vizează managementul riscurilor financiare și asigurarea stabilității sistemului financiar global.
- **GDPR și reglementările de protecție a datelor** – extrem de importante pentru gestionarea riscurilor legate de informațiile personale și securitatea cibernetică.

Aceste cadre nu doar că oferă linii directoare, dar facilitează și comparabilitatea între organizații, oferind investitorilor și partenerilor încredere în modul în care riscurile sunt gestionate.

3. SCOPUL ȘI OBIECTIVELE POLITICII DE MANAGEMENT AL RISCULUI

3.1. Scopul politicii

Scopul politicii de management al riscului este de a oferi organizației un cadru formal, coerent și transparent prin care toate riscurile asociate activităților sale să fie identificate, evaluate, tratate și monitorizate într-un mod sistematic. Această politică nu are rolul de a elimina complet riscurile – ceea ce ar fi imposibil –, ci de a menține expunerea organizației la un nivel acceptabil, compatibil cu obiectivele strategice și capacitatea acesteia de a răspunde la evenimente neprevăzute.

Prin implementarea unei politici clare și eficiente, organizația urmărește:

- crearea unei culturi bazate pe prevenție și responsabilitate,
- creșterea încrederii clienților, partenerilor și autorităților,
- asigurarea unui proces decizional fundamentat și rațional,
- reducerea vulnerabilităților și a expunerilor necontrolate.

Astfel, politica devine un instrument strategic, integrat în guvernanța corporativă și aliniat la standardele internaționale în domeniu.

3.2. Obiectivele politicii

Obiectivele acestei politici pot fi grupate în patru direcții majore:

3.2.1. Asigurarea unui nivel acceptabil de risc

Organizația își definește toleranța la risc și implementează mecanisme de monitorizare continuă. Astfel, riscurile sunt menținute într-o zonă controlabilă, care nu afectează semnificativ atingerea obiectivelor.

3.2.2. Protejarea resurselor și a reputației

Unul dintre obiectivele centrale este protejarea:

- **resurselor umane** (angajați și colaboratori),
- **resurselor financiare** (active, investiții, lichidități),
- **resurselor informaționale** (date sensibile, know-how, proprietate intelectuală),
- **reputației** organizației, care este unul dintre cele mai valoroase active intangibile.

3.2.3. Sprijinirea deciziilor strategice și operaționale

Politica are rolul de a furniza informații relevante și actuale, astfel încât managementul să poată lua decizii corecte și fundamentate. În absența unui sistem de evaluare a riscurilor, deciziile strategice ar fi hazardate și expuse unor pericole majore.

3.2.4. Conformitatea cu legislația și reglementările aplicabile

Un obiectiv prioritar îl constituie respectarea legislației naționale și internaționale. Aceasta include reglementări financiare, norme de sănătate și securitate în muncă, legislația privind protecția datelor (GDPR) și standardele de guvernanță corporativă. Conformitatea nu reprezintă doar o obligație legală, ci și o dovadă de responsabilitate și profesionalism.

4. PRINCIPII GENERALE ALE MANAGEMENTULUI RISCULUI

Politica de management al riscului se bazează pe un set de principii fundamentale care oferă direcție și coerență în aplicarea sa. Aceste principii nu sunt doar recomandări teoretice, ci reprezintă valori practice pe care organizația le integrează în toate activitățile curente și strategice.

4.1. Abordare proactivă

Un principiu de bază îl constituie anticiparea problemelor, nu reacția la ele. O organizație orientată spre prevenție își creează mecanisme prin care identifică din timp posibilele riscuri și implementează măsuri de protecție înainte ca



acestea să se materializeze. Spre exemplu, în domeniul IT, implementarea unor politici stricte de securitate cibernetică poate preveni atacurile informatice, reducând semnificativ pierderile.

4.2. Integrarea în toate activitățile organizației

Managementul riscului nu trebuie privit ca o activitate izolată, aparținând exclusiv unei echipe sau unui departament. El trebuie să fie integrat în toate procesele: planificare strategică, operațiuni curente, investiții, marketing, resurse umane. Doar printr-o abordare integrată se asigură o gestionare coerentă și eficientă.

4.3. Evaluare pe baza probabilității și a impactului

Un alt principiu fundamental este evaluarea riscurilor în funcție de **probabilitatea de apariție și impactul asupra organizație**i. Această analiză permite ierarhizarea riscurilor și alocarea resurselor în mod rațional: riscurile critice trebuie tratate cu prioritate, în timp ce riscurile minore pot fi monitorizate sau chiar acceptate.

4.4. Claritatea responsabilităților

Pentru ca procesul de management al riscului să fie eficient, este necesară atribuirea unor **responsabilități clare.** Conducerea trebuie să asigure un cadru și resurse adecvate, responsabilul cu riscurile coordonează activitățile specifice, iar fiecare angajat are obligația de a raporta incidentele și de a contribui la identificarea riscurilor din aria sa de activitate.

4.5. Documentare și transparență

Toate deciziile și acțiunile legate de managementul riscurilor trebuie **documentate și comunicate** corespunzător. Această transparență asigură trasabilitatea deciziilor, crește nivelul de încredere al stakeholderilor și facilitează procesul de audit sau de revizuire periodică a politicii.

4.6. Îmbunătățire continuă

Managementul riscului nu este un proces static, ci unul dinamic, care trebuie adaptat permanent la schimbările legislative, tehnologice sau economice. Organizația trebuie să adopte o cultură a învățării continue, în care experiențele anterioare și feedback-ul să fie utilizate pentru a îmbunătăți constant politicile și procedurile.

5. DOMENIUL DE APLICARE AL POLITICII DE MANAGEMENT AL RISCULUI

Politica de management al riscului se aplică în mod extensiv în cadrul organizației și stabilește limitele și aria de acțiune a procesului de identificare, evaluare și control al riscurilor. Domeniul de aplicare este esențial, deoarece definește atât responsabilitățile interne, cât și relațiile externe ale organizației cu partenerii, furnizorii și alte entități interesate.

5.1. Procese interne

Politica este aplicabilă tuturor proceselor și activităților interne, indiferent de natura lor:

- **procese strategice** – planificarea și stabilirea obiectivelor organizației, luarea deciziilor privind investițiile, intrarea pe noi piețe, dezvoltarea de produse sau servicii;
- **procese operaționale** – desfășurarea activităților zilnice, managementul resurselor umane, logistică, producție, distribuție;
- **procese suport** – IT, financiar-contabil, juridic, comunicare, mentenanță.

Astfel, fiecare activitate internă trebuie să fie analizată din perspectiva riscurilor asociate, pentru a preveni perturbările și a menține continuitatea operațională.

5.2. Proiecte și inițiative

Politica de management al riscului se aplică și în cazul proiectelor de anvergură sau a inițiativelor punctuale (ex. implementarea unui nou software, lansarea unui produs pe piață, construirea unei unități de producție). Pentru fiecare proiect trebuie realizată **o analiză specifică de risc**, care să identifice pericolele potențiale și măsurile de control necesare.

5.3. Departamente și unități organizaționale

Indiferent de dimensiune, fiecare departament este responsabil pentru gestionarea riscurilor specifice activității sale.

De exemplu:

- departamentul IT se confruntă cu riscuri cibernetice,
- departamentul financiar gestionează riscuri legate de lichiditate și credit,
- departamentul de resurse umane se ocupă de riscuri legate de

fluctuația personalului și conformitatea legislației muncii.

Această aplicare la nivel departamental asigură **o abordare descentralizată și adaptată** particularităților fiecărui domeniu.

5.4. Relațiile externe și parteneriatele

Politica se extinde și asupra partenerilor externi, furnizorilor și subcontractorilor, în măsura în care activitățile acestora pot influența nivelul de risc al organizației. Astfel, colaborările externe trebuie să fie evaluate din punct de vedere al fiabilității, al respectării normelor legale și al capacității de a livra produse sau servicii de calitate.

6. PROCESUL DE MANAGEMENT AL RISCULUI

Procesul de management al riscului reprezintă un ansamblu structurat de pași prin care organizația identifică, evaluează, tratează și monitorizează riscurile. Acesta este un proces ciclic, dinamic, care trebuie actualizat permanent, în funcție de schimbările interne și externe. Conform standardului ISO 31000, procesul poate fi împărțit în patru etape principale: **identificarea riscurilor, analiza și evaluarea riscurilor, tratarea riscurilor și monitorizarea/raportarea acestora**.

6.1. Identificarea riscurilor

Această etapă are ca scop descoperirea tuturor riscurilor posibile care pot afecta atingerea obiectivelor organizației. Identificarea trebuie să fie cât mai cuprinzătoare, incluzând atât riscurile interne, cât și pe cele externe.

Metode de identificare:

- **Brainstorming** – sesiuni cu echipele pentru a genera idei și scenarii posibile de risc.
- **Chestionare și interviuri** – colectarea opiniilor de la angajați, manageri sau experți externi.
- **Audituri interne** – verificarea proceselor și procedurilor curente pentru a depista vulnerabilități.
- **Analiza documentelor** – studierea rapoartelor financiare, planurilor strategice, documentației tehnice.
- **Benchmarking** – compararea cu alte organizații similare pentru a identifica riscuri comune.

Exemple practice:

- În domeniul bancar, riscurile pot fi identificate prin analiza portofoliului de credite.
- În sectorul IT, riscurile se identifică prin audituri de securitate cibernetică și teste de penetrare.

6.2. Analiza și evaluarea riscurilor

După ce riscurile au fost identificate, acestea trebuie analizate și evaluate pentru a stabili nivelul de prioritate.
Indicatori principali:

- **Probabilitatea** de apariție a riscului (scăzută, medie, ridicată).
- **Impactul** asupra organizației (minor, moderat, major, critic).

Aceste două dimensiuni se combină **într-o matrice de evaluare a riscurilor**, care ajută la ierarhizarea lor:

PROBABILITATE	IMPACT SCĂZUT	IMPACT MEDIU	IMPACT RIDICAT
Scăzută	Nesemnificativ	Minor	Moderat
Medie	Minor	Moderat	Major
Ridicată	Moderat	Major	Critic

Exemple:

- Riscul de pierdere a unor date neesențiale poate fi evaluat ca **scăzut**.
- Riscul de atac cibernetic asupra serverelor centrale poate fi evaluat ca **critic**.

Evaluarea permite concentrarea resurselor asupra riscurilor cu impact ridicat și probabilitate mare.

6.3. Tratarea riscurilor

În această etapă, organizația decide modul în care va acționa asupra fiecărui risc identificat și evaluat. Există patru strategii principale de tratament:

1. **Evitarea riscului** – renunțarea la activitatea care generează riscul. De exemplu, o companie poate decide să nu intre pe o piață instabilă politic.
2. **Reducerea riscului** – implementarea unor măsuri de control pentru a diminua probabilitatea sau impactul. De exemplu, instalarea de sisteme antivirus și firewall reduce riscul de atac cibernetic.
3. **Transferul riscului** – externalizarea riscului către o terță parte, cum ar fi încheierea unei polițe de asigurare sau subcontractarea unei activități.
4. **Acceptarea riscului** – recunoașterea și asumarea riscului atunci când costul măsurilor de reducere este mai mare decât potențialul impact.

Exemple practice:

- În construcții, riscul de accidente poate fi redus prin instruirea personalului și respectarea normelor de securitate.
- În producția alimentară, riscul de neconformitate poate fi transferat prin asigurări de răspundere civilă.

6.4. Monitorizarea și controlul riscurilor

Procesul de management al riscului nu se oprește după implementarea măsurilor de tratament. Riscurile trebuie monitorizate constant, deoarece condițiile se schimbă permanent.

Activități specifice:

- **Audituri periodice** pentru verificarea eficienței măsurilor implementate.
- **Raportări periodice** către conducere și către responsabilul cu riscurile.
- **Indicatori de performanță (KPI)** pentru a măsura gradul de expunere și eficiența controalelor.
- **Sisteme de alertă timpurie** pentru detectarea rapidă a riscurilor emergente.

Exemple:

- În domeniul financiar, monitorizarea se face zilnic prin rapoarte de lichiditate și de expunere la credit.
- În domeniul medical, monitorizarea riscurilor legate de pacienți presupune raportarea incidentelor și implementarea rapidă a măsurilor corective.

6.5. Ciclicitatea procesului

Procesul de management al riscului este unul ciclic și trebuie reluat periodic: riscurile se identifică din nou, se reevaluează, se tratează și se monitorizează în mod continuu. În acest fel, organizația se adaptează permanent la mediul său și își crește reziliența.



BIBLIOGRAFIE ȘI SURSE

Pentru realizarea acestei lucrari au fost consultate surse teoretice și practice, inclusiv standarde internaționale, reglementări europene și legislație națională. Lista de mai jos nu este exhaustivă, dar oferă reperele fundamentale pentru o înțelegere corectă a managementului riscului:

1. **ISO 31000:2018 – Risk Management Guidelines.** International Organization for Standardization, Geneva.
2. **COSO Enterprise Risk Management Framework (2017).** Committee of Sponsoring Organizations of the Treadway Commission.
3. **Basel Committee on Banking Supervision (2004, 2011, 2017).** Basel II, Basel III Frameworks. Bank for International Settlements.
4. **Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului (GDPR).** Privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.
5. **Legea nr. 319/2006** privind securitatea și sănătatea în muncă. Monitorul Oficial al României.
6. **Legea contabilității nr. 82/1991 (actualizată).** Monitorul Oficial al României.
7. **Manual de Managementul Riscului.** Editura ASE, București, 2020.
8. **Raportări și ghiduri de conformitate ale Autorității de Supraveghere Financiară (ASF) și Băncii Naționale a României (BNR).**
9. **Literatura de specialitate internațională:** articole academice și studii de caz publicate în reviste de profil (Journal of Risk Management, International Journal of Business Risk).



De la evaluator local la consultant european

Cum ar putea un specialist român în evaluarea riscului la securitatea fizică să intre pe piața UE, „de la zero”

Petru Liviu Negoescu
Evaluator de risc la securitate fizică şi consultant în securitate

INTRODUCERE

Putem afirma că profesioniștii din domeniul evaluării riscului la securitatea fizică din România au acumulat în ultimii ani o experiență tehnică solidă, susținută de un cadru legislativ specific și de standarde profesionale în continuă evoluție. Totuși, pentru mulți evaluatori apare, destul de des, o întrebare firească: cum poate fi transformată această experienţă naţională într-o activitate profesională, viabilă la nivel european?

Piața Uniunii Europene (UE) oferă unele oportunități reale pentru consultanții independenți, însă modul de funcționare diferă semnificativ față de modelul național. În UE, serviciile de evaluare a riscului la securitatea fizică sunt integrate (nu au independenţă instituţională) într-un ecosistem mai larg de consultanță - risk management, business continuity, protecția infrastructurilor critice și audituri de conformitate.



Voi încerca să vă prezint un posibil model de intrare pe piața europeană, pentru un evaluator și consultant român, care pornește de la zero.

DIFERENȚELE FUNDAMENTALE DINTRE MODELUL ROMÂNESC ȘI CEL EUROPEAN

În România, profesia de evaluator de risc la securitatea fizică este definită printr-un cadru legislativ specific și prin autorizări profesionale clare. Ocupaţia de evaluator de risc la securitatea fizică (ERSF) este practicată în cadrul definit de Legea nr. 333/2003 (pe cale de a fi modificată radical, din punctul nostru de vedere), privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, H.G. nr. 301/2012 privind aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 şi de Instrucţiunea nr. 9/2013 a M.A.I. privind efectuarea analizelor de risc la securitatea fizică a unităţilor ce fac obiectul Legii nr. 333/2003. În Uniunea Europeană, însă, nu există o

titulatură unică echivalentă. Activitatea este integrată într-o zonă mai largă, ce ţine de de consultanță, sub denumiri precum:

- Physical Security Consultant
- Security Risk Consultant
- Protective Security Advisor
- Enterprise Security Consultant.

Această diferență nu presupune obligatoriu schimbarea competenței profesionale a evaluatorului român, ci adaptarea modului lui de prezentare și la limbajul utilizat în mediul corporativ european.

REPOZIȚIONAREA PROFESIONALĂ – PRIMUL PAS ESENȚIAL

Pentru a intra pe piața UE, evaluatorul trebuie să își transforme oferta dintr-un serviciu strict de evaluare într-un pachet larg de consultanță, orientat pe risc și vulnerabilități. Serviciile cel mai frecvent solicitate includ:

- audituri de securitate fizică;
- evaluări de vulnerabilitate (vulnerability assessments);
- inspecții de securitate ale locațiilor (site security surveys);
- due diligence de securitate, pentru investiții;
- analize post-incident și recomandări operaționale specifice;
- revizuirea designului sistemelor de securitate (CCTV, control acces, efracţie, protecție perimetrală şi, de ce nu, mecanofizice).

În practică, evaluarea de risc rămâne componenta centrală, dar este prezentată doar ca parte a unui serviciu mai amplu de consultanță.

Credibilitatea profesională într-un context european

Pe piața europeană, certificările internaționale și alinierea la standarde sunt elemente esențiale de credibilitate. Printre cele mai relevante pentru specialiștii în securitate fizică se află:

- certificarea PSP (Physical Security Professional) – ASIS International;
- certificări bazate pe standarde ISO, în special ISO 31000-31001 (Risk Management) și ISO 22301 (Business Continuity);
- utilizarea metodologiilor recunoscute internațional pentru analiză și raportare.

De multe ori, clienții corporativi evaluează consultantul mai mult prin prisma metodologiei și a structurii raportului decât prin deţinerea sau nu de autorizații naționale.

ROLUL ORGANIZAȚIILOR PROFESIONALE EUROPENE

Dezvoltarea profesională și accesul la proiecte depind, în mare măsură, de integrarea în rețele profesionale internaționale. Printre organizațiile relevante se numără:

- • ASIS International – pentru networking și standarde profesionale în securitate;
- • Institute of Strategic Risk Management (ISRM) – comunitate activă de consultanți;
- • organizații de risk management asociate/ federaţii (FERMA) – relevante pentru proiecte corporate şi nu numai.

În multe cazuri, primele colaborări apar chiar prin aceste rețele, înainte de a fi publicate formal.

Primele tipuri de proiecte ce pot fi accesibile pentru consultanți independenți

Pentru un specialist care începe „de la zero", cele mai realiste proiecte sunt cele realizate ca subcontractor. Exemple frecvente includ (dar nu numai):

- audituri de securitate pentru sedii de tip corporate;
- evaluări pentru obiective din energie, depozite logistice mari și centre de distribuție;
- analize de securitate pentru retail și lanțuri comerciale;
- evaluări pentru companii de facility management;
- suport în proiecte de certificare ISO.

De regulă, contractele vin prin integratori de securitate, firme de consultanță ISO sau consultanți de risk management, nu direct de la clientul final.

IMPORTANȚA RAPORTĂRII PROFESIONISTE

Raportul de securitate utilizat în UE are o structură orientată către top management și locul în care se ia decizia strategică. Elementele unui astfel de raport, includ (şi aici veţi remarca mai degrabă deosebirile, decât asemănările cu ceea ce suntem obişnuiţi):

- un rezumat executiv destinat conducerii;
- descrierea metodologiei utilizate;
- analiza amenințărilor și vulnerabilităților;
- evaluarea riscurilor prin

matrici standardizate;
- recomandări prioritizate, pe termen scurt și mediu;
- foaie de parcurs pentru implementare.

Claritatea și utilitatea pentru management sunt criterii decisive pentru continuitatea colaborării!

STRATEGIA REALISTĂ DE DEZVOLTARE ÎN PRIMELE 12 LUNI

Un parcurs tipic pentru un consultant independent ar putea arăta astfel:

- 0–3 luni: repoziționare profesională și integrare în rețele europene;
- 3–6 luni: prime subcontractări și dezvoltarea portofoliului internațional;
- 6–12 luni: colaborări recurente cu integratori și firme de consultanță;
- peste 12 luni: tranziția către rolul de security risk advisor.

Succesul depinde mai puțin de dimensiunea inițială a firmei și mai mult de adaptarea la modul european de lucru.

CONCLUZII

În marea lor majoritate, evaluatorii de risc la securitatea fizică români au competențe tehnice solide și experiență practică relevantă. Accesul la piața europeană nu necesită reinventarea profesiei, ci o adaptare strategică: repoziționare profesională, utilizarea standardelor internaționale și integrarea în rețelele potrivite.

În contextul creșterii interesului pentru reziliență organizațională, protecția infrastructurilor și managementul riscurilor, rolul consultantului în securitate fizică devine tot mai important la nivel european. Pentru profesioniștii pregătiți să facă pasul, oportunitățile sunt reale și accesibile chiar și în regim independent.





Necesitatea îmbunătățirii reglementării domeniului analizei de risc

Aurel Catrinoiu
Președinte ANERSFR & Membru al juriului OSPA România

În ultima perioadă de timp, conducerea ANERSFR a remarcat modificarea profundă a practicilor de lucru și a comportamentului evaluatorilor de risc, regăsindu-se la beneficiari, **lucrări care nu au legătură cu raportul de evaluare și tratare a riscurilor ori cu materializarea procesului de evaluare a riscurilor de securitate fizică.**

Conținutul acestor documentații tehnice ca și rezultate a muncii evaluatorului, sfidează orice rațiune a înțelegerii lucrurilor, pornind de la lipsa informațiilor concrete ce privesc descrierea obiectivului, a activelor, fluxurilor ori proceselor ce urmează a fi parte a analizei și ajungând la superficialitatea în enunțarea zonelor de risc ori a metodelor de identificare și reducere a riscurilor relevante.

În aceeași măsură, lipsa unei consistențe a lucrărilor sau a argumentelor cum ar fi: anticiparea amenințărilor și identificarea vulnerabilităților de ordin fizic, tehnic ori procedural prin inspecțiile de risc la fața locului, respectiv stabilirea măsurilor de eliminare a acestora, a generat o percepție greșită beneficiarilor care, evident au apreciat acest proces ca fiind o formalitate de transpunere a unei obligații administrative inutile.

Din păcate, această percepție greșită a unor manageri va fi contrazisă mult mai târziu, odată cu înregistrarea unor incidente de securitate și a unor prejudicii materiale ori chiar cu consecințe asupra angajaților, unele chiar iremediabile sau de gravitate deosebită.

Pentru a identifica această mutație în segmentul serviciilor, ne propunem să determinăm cauzele principale ale acestei schimbări în practica profesiei și să analizăm posibile cauze de alterare a procesului, opinia asociației fiind următoarea:

- Lipsa unei legislații și mecanisme care să sancționeze drastic practicile și rezultatele greșite ori să stabilească o responsabilitate evidentă în sarcina evaluatorilor pentru greșelile, erorile ori minimizarea riscurilor, inclusiv a beneficiarilor în acceptanța inepțiilor;
- Formarea profesională superficială și lipsa de experiență și competențe anterioare în materie de securitate privată.
- Dezinteresul beneficiarilor prin neglijarea unei corecte înțelegeri a avantajelor acestui proces;
- Fluxuri, active și procese insuficient documentate și rezultate nejustificate,

- Lipsa unui control profesional real al practicilor în evaluare.
- Practicile anticoncurențiale din industria de securitate.

Toate aceste cauze enumerate, au condus la o speculare a pieței și la manipularea rezultatelor doar în interes comercial și în final la banalizare în asigurarea unui management al riscurilor de securitate fizică ori chiar a celorlalte riscuri din organizație, opțiunea aleasă fiind greșită.

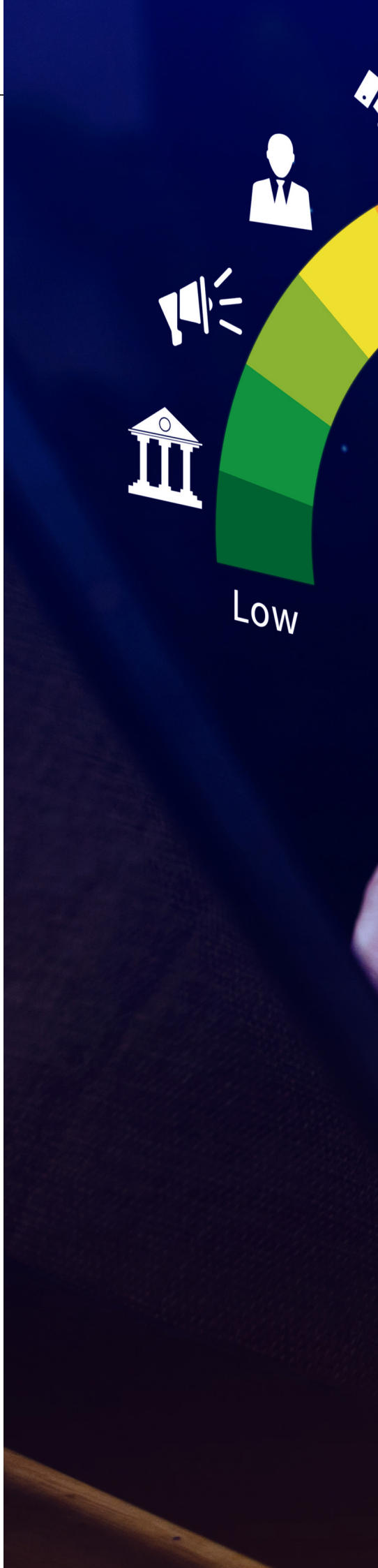
În articolul de astăzi, îmi propun să detaliez doar una dintre cauze, considerată în opinia noastră ca fiind extrem de importantă, respectiv reglementarea și cerințele legislative actuale.

După cum știm, legislația are permanent nevoie de un upgrade pentru a ține pasul cu evoluția industriei și a societății, ceea ce nu s-a întâmplat de peste 23 de ani de la adoptarea legii pazei și protecției bunurilor și valorilor, însă foarte recent pe timpul redactării articolului, a apărut pe transparență decizională un proiect de OUG care propune unele simplificări administrative mult așteptate atât de beneficiari cât și de prestatori, respectiv chiar și de autorități, sufocate fiind de multiple sarcini birocratice.

Apreciem propunerile inițiatorului de a simplifica actele și demersurile administrative și de a introduce conceptul de evaluare de risc ca metodă universală în stabilirea și dimensionarea măsurilor de securitate, cu o excepție în ceea ce privește domeniile incidente acestei practici. Proiectul lansează propunerea ca analiza de risc să fie aplicată doar unor mici categorii de unități, adică celor stabilite de normele metodologice ca fiind cu nevoi de securitate ridicate, însă aceste categorii nu mai sunt de actualitate cu evoluția industriei, întrucât au fost clasificate în urmă cu 14 ani.

Ca și detaliu tehnic, specialiștii asociației apreciază în majoritate cazurilor procesul de evaluare este direcționat pe măsurile minimale impuse de norme și astfel evaluatorul de risc este obligat să aplice rețeta, ceea ce nu se întâmplă și în situația altor unități din afara acestora, cum ar fi : spații de producție, hale industriale, unde necesitățile de securitate nu sunt stipulate în nicio reglementare și ar avea nevoie de expertiza evaluatorului de risc pentru a alege cele mai eficiente soluții de protecție.

În încheiere, cu speranța adoptării unor amendamente ce pot aduce plus valoare proiectului de OUG, din cele propuse de ANERSFR și asumarea dezideratului prin care se afirmă că strictețea prevederilor normelor metodologice și controlul prestațiilor poate genera practici corecte și măsuri eficiente de control a riscurilor relevante de securitate, iar implementarea acestora va determina un real control al nivelului de securitate din unitate.




RISK
MANAGEMENT
High



INTERVIU:
Cum devine evaluarea de risc un instrument strategic pentru securitatea bancară

Florin Vasile Ioan
Director Adjunct Dispecerat de Securitate, Banca Transilvania



1. Cum este apreciată importanța unei evaluări de risc la securitatea fizică în determinarea corectă a măsurilor de protecție pe care le implementăm?

Evaluarea de risc în domeniul securității fizice este esențială pentru fundamentarea măsurilor de protecție întrucât permite identificarea vulnerabilităților reale și dimensionarea corectă a resurselor. La nivelul Băncii Transilvania, această evaluare este abordată integrat, iar ulterior folosim rezultatele pentru ajustarea planurilor de pază, rutelor de transport valori și configurarea sistemelor de securitate.

Un aspect esențial este corelarea evaluării de risc la securitatea fizică cu procesul de asigurare — atât în ceea ce privește stabilirea nivelului de acoperire, cât și în negocierea primelor de asigurare. O evaluare riguroasă și actualizată contribuie la o mai bună înțelegere a expunerii reale și, implicit, la optimizarea costurilor de asigurare.

Totodată, evaluarea de risc fizic este aliniată cu celelalte evaluări de risc operațional, precum cele cibernetice sau de continuitate a activității. În cadrul BT, aceste evaluări sunt tratate integrat, în cadrul comitetelor de risc, pentru a asigura o imagine coerentă asupra riscurilor la nivel de organizație. Astfel, măsurile de protecție fizică sunt gândite complementar cu cele de securitate IT, iar scenariile de răspuns la incidente includ atât componente fizice, cât și digitale.

2. Cum privește top managementul BT propunerile făcute legate de asigurarea nivelului optim de risc rezultate din evaluările făcute?

Ca pe un instrument strategic, nu doar operațional. Propunerile rezultate din evaluările de risc la securitatea fizică sunt analizate în contextul mai larg al managementului integrat al

riscurilor, alături de evaluările de risc cibernetic, de continuitate a activității și de conformitate. Această abordare integrată permite o corelare coerentă a măsurilor de protecție și o prioritizare eficientă a investițiilor în funcție de impactul potențial asupra activității bancare.

În cadrul comitetelor de risc și al analizei strategice, propunerile formulate de structurile de securitate sunt evaluate în raport cu apetitul la risc al instituției, dar și în conformitate cu reglementările BNR privind cerințele de control intern și protecție a activelor. Astfel, măsurile propuse nu sunt doar validate, ci și susținute prin alocări bugetare și includere în planurile de acțiune multianuale.

De asemenea, în contextul actual al industriei bancare — marcat de digitalizare accelerată, creșterea riscurilor hibride și cerințe de reziliență operațională — top managementul BT încurajează o abordare proactivă și anticipativă în ceea ce privește riscurile fizice. Aceasta se reflectă în sprijinul acordat permanent inițiativelor de modernizare a infrastructurii de securitate, de automatizare a proceselor de monitorizare și de instruire continuă a echipei.

3.Ce propuneri crezi că ar trebui făcute la nivelul ARB - Asociației Române a Băncilor pentru a ridica nivelul de eficiență al evaluărilor?

Cu ARB avem o colaborare foarte bună. Pentru creșterea eficienței evaluărilor de risc la nivelul industriei bancare, cred că ar putea fi luate în considerare aceste propuneri:

- Standardizarea metodologiilor de evaluare printr-un cadru comun agreat de membrii ARB, care să includă indicatori de performanță și criterii de clasificare a riscurilor.
- Crearea unui registru național de incidente de securitate fizică, cu acces controlat, care să permită analiza comparativă și anticiparea riscurilor emergente.
- Promovarea instruirii continue prin platforme e-learning comune, pentru diseminarea bunelor practici și instruirea echipelor băncilor.
- Inițierea unor grupuri de lucru interbancare pentru schimb de experiență și armonizarea abordărilor în contextul reglementărilor MAI.

Securitatea fizică este o prioritate pentru protejarea resurselor financiare, a datelor/informațiilor, a angajaților și clienților noștri, într-un domeniu în care încrederea este fundamentală.





LISTA MEMBRILOR ANERSFR

LISTA MEMBRILOR ANERSFR

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
1	GABRICONF IMPEX S.R.L.	AB	15209600	0751882384	contact@analizarisk.ro
2	SECURITY CONSULTING SERVICES S.R.L.	AB	38255591	0744338540	info@securitycs.ro
3	SINEA S.R.L.	AB	18324484	0728829041	sineasilviu@yahoo.com
4	CORPUL EXPERTILOR IN SECURITATE PRIVATA POLIX S.R.L.	AG	35092538	0725420400	office@securityconsultanta.ro
5	ELCAS SYSTEMS 2001 S.R.L.	AG	14028206	0744331993	mihai@esy.ro
6	FORMEVAL SECURITY S.R.L.	AG	18554386	0723257039	evaluator.as@gmail.com
7	GTS SECURITY FORCE SRL	AG	RO38878450	0722075622	gtsgeopaza@yahoo.com
8	LIBRAVEL MASTER S.R.L.	AG	27918044	0744361873	libravelmaster@gmail.com
9	IONEL ADRIAN PFA	AR	32263838	0744245663	adyrisk@gmail.com
10	LANIA CONSTRUCT 2008 SRL	AR	23029812	0752788633	vinter.evaluatorlasecuritate@gmail.com
11	MATEI C. MARIUS PFA	AR	34317640	0744625063	mateic.marius1971@gmail.com
12	AIROH SECURITY SRL	B	40518789	0728877453	evaluariderisc@yahoo.com
13	ANALIZA IN SAFE SECURITY S.R.L.	B	35176345	0764238428	netcu_iulian@yahoo.com
14	AVE TEAM CONSULTING S.R.L.	B	36704295	0764717863	oniga_andrei2003@yahoo.com
15	BADEA GH. GABRIEL P.F.A.	B	33291690	0744539280	office@fss.org.ro;
16	CENTRUL RIVERGATE S.R.L.	B	14309635	0214083571	office@rivergate.ro
17	CONSTANTIN G. ALEXANDRU P.F.A.	B	34427414	0723382852	office@analiza-riscuri.ro
18	DECOD SECURITY S.R.L.	B	18960180	0745104189	dragos.savulescu@decod.ro
19	DEF-P.S.U. PREVENIREA SITUATIILOR DE URGENTA S.R.L.	B	39881437	0771342586	eugenflorindinca@yahoo.com
20	DENDEA FLORIAN PFA	B	42433573	0726335320	florian.dendea@gmail.com
21	DINCA SILVIU FLORIN P.F.A.	B	33870330	0722160122	dincasf@gmail.com

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
23	GEEA INVESTIGATII ECONOMICE S.R.L.	B	24422002	0723349225	boneaconta@gmail.com
24	GEVA CONSULT S.R.L.	B	16039880	0212321135	gelu.vasilescu@gevaconsult.ro
25	GIBEX - ERSF S.R.L.	B	16942004	0722230893	mariandraghici.gibon@yahoo.com
26	GUDACU STELIAN P.F.A.	B	32016161	0722678201	stelian.gudacu@yahoo.com
27	HD BUSINESS ENTERPRISE S.R.L.	B	RO32517219	0733221144	danielbica@gmail.com
28	IDN TOP SECURITY S.R.L.	B	RO37071736	0767278410	istratie.daniel@yahoo.com
29	INTERADA SERVICE TREI SRL	B	16621110	0744361404	adrian.popa65@yahoo.com
30	IONESCU MARIAN-DANIEL PFA	B	33255094	0722681696	danionescu00@yahoo.com
31	MITRAN FLAVIUS - COSMIN P.F.A.	B	48683994	0769268318	mitranflaviuscosmin@gmail.com
32	MOISE CONSTANTIN P.F.A.	B	32328945	0722651746	constantinn.moise@yahoo.com
33	MORRIS COMP SECURITY S.R.L.	B	34237215	0733188857	gelu.morarasu@analizariscuri.ro
34	MUSUROAEA GABRIEL P.F.A.	B	34098796	0740100345	evaluator.gabriel@gmail.com
35	PATULEA EUGEN-IONUT P.F.A.	B	34383601	0740136729	epatulea@gmail.com
36	PREDESCU V. GHEORGHE P.F.A.	B	31810120	0732169244	ghpredescu@yahoo.com
37	RISC MINIM SRL	B	41486766	0761888677	evaluator@riscminim.ro
38	ROMANO ELECTRO S.R.L.	B	36187	0727718464	carmen.fagarasi@roelsystems.ro
39	SAFEGUARD SOLUTIONS S.R.L.	B	50545322	0766485805	mariuspeslar@gmail.com
40	SAFETY & HEALTH CONSULTING S.R.L.	B	18707030	0742218420	alexa.daniel@safety-health.ro
41	SAFETY CASH SRL	B	39796285	0745102050	office@safety-cash.ro
42	SCUTUL VERDE S.R.L.	B	38926166	0744526100	contact@scutulverde.ro
43	SECANT SECURITY S.R.L.	B	26163680	0314328215	stelian.arion@secant.ro
44	SECURITY & SAFETY CONSULTING S.R.L.	B	32914162	0721475108	office@ssm-evaluare-securitate-fizica.ro
45	SECURITY ELECTRONICS SERVICE S.R.L.	B	18399207	0722285003	sessrl@gmail.com
46	SITMA S.R.L.	B	367733	0720999900	antonescu@sitma.ro
47	SKY SECURITY SYSTEMS S.R.L.	B	32011873	0760612505	valentin.buda@skysecurity.ro

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
48	SMS SECURITY INVENT S.R.L.	B	23969452	0732168716	ionut.manole@sms-security.ro
49	STEP BY STEP EVOLUTION S.R.L.	B	38407274	0799747525	catalin.faust@sbs-evolution.ro
50	TEAM RISK S.R.L.	B	35285253	0764472336	office@teamrisk.ro
51	TECH PRO DISTRIBUTION S.R.L.	B	17973955	0721182453	stefan@techpro.ro
52	TRAFFIC SERVICES&CONSULTING S.R.L.	B	25537787	0722438533	v.recoseanu@yahoo.com
53	URBAN DEVELOPMENT SERVICES	B	36788750	0722589585	office@urbansecurity.ro
54	VALAHIA BUSINESS PARTENER S.R.L.	B	38279698	0726111148	office@valahia-ss.ro
55	VIDEO ALARM SECURITY SYSTEMS S.R.L.	B	30420065	0722539028	marinstamate@yahoo.com
56	VODAFONE ROMANIA S.A.	B	8971726	0372022832	adrian.costache@vodafone.com
57	NICOLESCU VIOREL P.F.A.	B	33545314	0723942295	nicolescu_v@yahoo.com
58	AMPRO SYSTEM S.R.L.	BC	15429591	0744293147	office@amprosystem.ro
59	BVB RISK SOLUTIONS SRL	BC	24467640	0736959363	evaluarederisk@gmail.com
60	CIUBOTARU N. PFA	BC	37092593	0745350035	nec_ciubotaru@yahoo.com
61	COMPACT RENT S.R.L.	BC	RO22397859	0742499466	toronilavasile@yahoo.com
62	HODOROABA SORIN P.F.A.	BC	36816299	0740077568	hodoroabasorin@gmail.com
63	IGNIS BLUE S.R.L.	BC	47006468	0745671486	misaboubatrin@gmail.com
64	MOLDCONSULT SECURITY SERVICES SRL	BC	32040020	0742592778	officemoldconsult@gmail.com
65	PROT & GUARD S.R.L.	BC	9817629	0722225842	lupalex2005@yahoo.com
66	AL.SE.RO. IMPEX S.R.L.	BH	9341869	0770765740	m.ciordas@alse.ro
67	DAN RISK CONSULTING S.R.L.	BH	33381238	0744182989	ghete_danut@yahoo.ro
68	EVALRISC S.R.L.	BH	38320274	0745516647	contactevalrisc@gmail.com
69	GENERAL RISC S.R.L.	BH	33643894	0754439885	cristelecanul@gmail.com
70	IGB CONSULTING SECURITY SRL	BH	41661883	0747615538	gbahna2002@yahoo.com
71	SORISTEF ELECTRONIC S.R.L.	BH	16766536	0744179719	sosofodor@yahoo.com
72	SYBAL SECURITY CONSULTING	BH	41465461	0744520251	cristian.barac@yahoo.com

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
73	MARANA RISC SRL	BN	41100945	0740031442	vasilcam1969@gmail.com
74	MITITEAN POP VALERIAN PFA	BN	27508222	0746497677	vpmititean@gmail.com
75	FRIGIOIU I. COSTICA P.F.A.	BR	33793280	0723602135	frigioiuc@gmail.com
76	TUDORACHE CONSTANTIN-VALENTIN PFA	BR	34381163	0745665363	valentintudorache@yahoo.com
77	BUNDUC D. MIHAI PFA	BT	36769600	0744523992	misu_bun@yahoo.com
78	MODAN LIVIU - LAURENTIU P.F.A.	BT	24526046	0756362352	modan_liviu@yahoo.com
79	MVD COMALITEH SRL	BT	4739422	0722722102	contact@mvdservice.ro
80	SCHIOPU MARCEL GELU I.I.	BT	41552975	0745050419	schiopu_marcel_gelu@yahoo.com
81	BRAHMS INTERNATIONAL S.R.L.	BV	6620338	0722712896	RainholdMai@brahms.ro
82	DUMITRU GH.R. IOAN P.F.A.	BV	33255590	0723534260	dumitru.ioan61@yahoo.ro
83	ERBATU EXPERT S.R.L.	BV	17859145	0722155866	borlean.mirela@yahoo.com
84	NEW GHM S.R.L.	BV	25866895	0724044377	mircea.cenuse@bridgeguard.ro
85	PODAR GABRIEL P.F.A.	BV	36978355	0727351959	evalrisk.podar@gmail.com
86	TN SECURITY RISK SOLUTION S.R.L.	BV	49270600	0731737272	tnv.srs@yahoo.com
87	TRADE EDERVAIS S.R.L.	BV	32826192	0770748115	andispataru@gmail.com
88	ULTRA TRAINING S.R.L.	BV	31443520	0767283563	mihaiserafim@ultrasecurity.ro
89	COMPACT PROTECT SECURITY S.R.L.	BZ	39602214	0745678152	cps.evaluare@gmail.com
90	STOICA S C ION P.F.A.	BZ	43111339	0741133464	ist15bz@yahoo.com
91	ZAM CD CONSULTING SECURITY S.R.L.	BZ	39303280	0769682775	zamfir.marian66@yahoo.com
92	ARIOLA PRODCOM S.R.L.	CJ	6882436	0723393303	nrobert@ariola.ro
93	C.C.S. PROIECT CONSULTING S.R.L.	CJ	37465072	0730606825	office@ccsproiect.ro
94	MARIN CORNELIA NICOLETA P.F.A.	CJ	47914969	0744187140	corneliamarin66@gmail.com
95	MARIN G.E. ION P.F.A.	CJ	47055223	0744200387	ionmarin66@gmail.com
96	PROSEC SYSTEMS S.R.L.	CJ	33004025	0736216500	prosec.systems@yahoo.ro
97	ZETHA SECURITY ANALYSIS	CJ	37669650	0720076067	emilian.osorhean@zethasecurityana

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
98	ETHORI S.R.L.	CL	9053645	0722423356	titus.toma@gmail.com
99	EVAL CRISLIA RISK S.R.L.	CL	38612538	0724502011	evalcrisliarisk@gmail.com
100	SAVA C.M GHEORGHE P.F.A.	CL	32309404	0722857174	gelusava57@yahoo.com
101	TATU COSTICA P.F.A.	CL	32034915	0722353539	costel_tatu@yahoo.com
102	TUGUI J. AUREL P.F.A.	CL	28303926	0722425427	aureltugui.scs@gmail.com
103	AS CONEX SRL	CS	6570906	0722284140	alstanescu@gmail.com
104	GOIAN SECURITY CONSULTING S.R.L.	CS	49629837	0724589950	mihai.go.ro@gmail.com
105	MURARIU SIMIONEL PFA	CS	34088709	0723151224	simi_murariu@yahoo.com
106	PIRVU MISU P.F.A.	CS	41303842	0734983522	misucaransebes@gmail.com
107	ABET CAPITAL EXPERT S.R.L.	CT	39351260	0753084440	evaluarifizice@gmail.com
108	AXINTE I. VASILE P.F.A.	CT	33986825	0788955139	axintevasile@rocketmail.com
109	EXPERT CONSULT SERBAN S.R.L.	CT	35290888	0723167383	serban_mariani@yahoo.com
110	FOCUS RISK S.R.L.	CT	42708003	0726204343	office@evaluarerisc.eu
111	MUSAT D-TRU IONEL P.F.A	CT	49721433	0720000968	musationel971@gmai.com
112	AMUZA ALEXANDRU P.F.A.	DB	35522694	0728848021	amuzaalexandru@yahoo.com
113	BEST SHIELD SRL	DB	37127632	0726239227	savug2002@yahoo.com
114	MARINESCU I. LAURENTIU-ION P.F.A.	DB	32207552	0744519543	laur.marinescu@gmail.com
115	MEDIANET S.R.L.	DB	17126810	0745089899	office@teamsecurity.ro
116	MOCANESCU C. GHEORGHE P.F.A.	DB	33488782	0722362845	ghmocanescu@gmail.com
117	A.R.K.A. SECURITY SYSTEMS S.R.L.	DJ	39284293	0758053966	marcel.florescu27@gmail.com
118	DUMITRU ZISU P.F.A.	DJ	36432549	0722892822	dumitru.z@hotmail.com
119	ISOTRAD CONSULTING S.R.L.	DJ	28100212	0726382836	mirel.baluta@isotrad.ro
120	NIBACO S.R.L.	DJ	23077356	0745551254	office@nibaco.ro
121	PETPOP EXPERT SECURITY S.R.L.	DJ	37394354	0736330944	petre_alex13@yahoo.com
122	PRO SECURITY PROTECT S.R.L.	DJ	26419178	0722244847	prosecu@yahoo.com

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
123	GRADINARU GRIGORE I.I.	GJ	39551951	0766324440	grigoregradinaru@gmail.com
124	MBM TRUST EVALUATORS SRL	GJ	38301809	0743998198	pic_mar2000@yahoo.com
125	TILVESCU I. VASILE P.F.A.	GJ	32490407	0722678386	vasilet50@yahoo.com
126	HELIOS SECURITY S.R.L.	GL	RO15950130	0730118203	liliana@helios.ro
127	LOLOIU V. COSTEL P.F.A.	GR	49803924	0751383278	costel.loloiu@gmail.com
128	STANIMIR STEFAN - CRISTINEL P.F.A.	GR	44404612	0730110363	stanimir_cristinel@yahoo.com
129	BUSINESS SECURITY SYSTEMS S.R.L.	HD	51746006	0723540272	cata_71@yahoo.com
130	DEDIU P. ADRIAN PFA	HD	37989794	0732701594	adriandediu@yahoo.com
131	FILCU GHEORGHE PFA	HD	37381737	0736366189	mirfilcu@yahoo.com
132	COSTAN A. IOAN PFA	HG	36909169	0761126621	ioancostan@yahoo.com
133	BUTUNOI IOSIF P.F.A.	HR	37327649	0752010395	butunoi.iosif@yahoo.com
134	NEXUS BEST CONSULT SRL	HR	35403499	0742066363	dusinszky.sandor@melinda.ro
135	ONU GHEORGHITA P.F.A.	HR	43464470	0740818289	onu.gheorghita@gmail.com
136	VOAIDAS VIOREL P.F.A.	HR	36768450	0743821102	voaidasviorel@yahoo.com
137	DAX METHOD S.R.L.	IF	RO25525847	0746125500	office@daxmethod.ro
138	DG SECURITY SERVICES S.R.L.	IF	33791939	0728888081	office@dgsecurity.ro
139	DID SECURE S.R.L.	IF	34417089	0748224465	ionut@didsecure.ro
140	DONA. LOGISTICA S.A.	IF	RO3596251	0723331271	ioan.marginean@farmaciiledona.ro
141	ETHOR SERVICES S.R.L.	IF	45099126	0723309818	marius.grigore@ethorservices.ro
142	GENERAL RISK LINE S.R.L.	IF	39816439	0727842405	general.rline@gmail.com
143	INTEGO ISC CONSULTING S.R.L.	IF	51070825	0752101094	adrian.preda@intego.ro
144	M&M DINAMIC TEAM SOLUTIONS S.R.L.	IF	34186626	0761021008	evaluator.dts@gmail.com
145	OHS&FF PROVAIDER S.R.L.	IF	32931228	0744428968	office.ohs@gmail.com
146	ONEST SOLUTIONS S.R.L.	IF	30241710	0728728523	viorel.petcu@onestsolutions.ro
147	PROFESSIONAL SECURITY	IF	RO30490052	0721377818	office@evaluator-risc.ro

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
148	PROTO - CONSTECH S.R.L.	IF	18758459	0744498831	jenibulboaca@gmail.com
149	DMC COMPUTER & SOFT S.R.L.	IL	15325655	0722325156	duomanager@gmail.com
150	ANISEC SERV SRL	IS	41849756	0755036696	anisecserv@gmail.com
151	BLUE BOX S.R.L.	IS	17264252	0744966833	vyp80@yahoo.com
152	CARIOMODE S.R.L.	IS	39780661	0725200631	dantircolea@yahoo.com
153	GHEBAN VASILICA P.F.A.	IS	34894320	0745125110	vasilicagheban@gmail.com
154	M.G. HOUSE S.R.L.	IS	18747735	0721162600	office@mghousesecurity.ro
155	MARIDUM PREST SRL	IS	36693544	0755836859	parlogdtru@yahoo.com
156	ANNE SECURITY S.R.L.	MM	48003524	0741531843	anne_sec2023@yahoo.com
157	BREZAN GABRIEL P.F.A.	MM	52719611	0744553959	gabrielbrezan@gmail.com
158	CALESTECH - SERV S.R.L.	MM	39325571	0741633157	evaluator@calestech.ro
159	EVAL MED CONSULTING S.R.L.	MM	49211221	0743153860	mariusstoianmm@yahoo.com
160	GO SERV SRL	MM	6919950	0744539723	support@goserv.ro
161	IT&C DEVELOPMENT SRL	MM	RO22491510	0722662160	gabriel.man@itcdevelopment.ro
162	SICA GUARD S.R.L.	MM	27488907	0786167006	andrei@sicaguard.ro
163	TRAINGUARD SRL	MM	33372612	0721249537	floreaniculae49@yahoo.com
164	AZL ZETEON S.R.L.	MS	39000383	0774066181	zetesanghel1970@gmail.com
165	MACOVEI GHEORGHE VASILE P.F.A.	MS	38693613	0740110151	mcvgheorghe@yahoo.com
166	PGC SECURITY EXPERT S.R.L.	MS	21324760	0727226050	molnar_nicu@yahoo.com
167	VALSOFT SRL	MS	RO17037217	0745435386	office@alarme-valsoft.ro
168	E GUARD INF S.R.L.	NT	13833177	0758038232	beleutlidia@gmail.com;
169	GHEORGHIU V. MARCEL P.F.A.	NT	36776267	0745254018	office@evaluariderisc.com
170	GRIPHON INTELLIGENCE SECURITY S.R.L.	NT	29249159	0746902737	mihai_ovidiu_beleut@yahoo.com
171	HUMA IULIAN II	NT	38786976	0744376017	iulian_h2007@yahoo.com
172	HYGEEA TURCOAZ SRL	NT	17778601	0744772942	hygeea.turcoaz@yahoo.com
173	FEDERAL PAZA SI PROTECTIE S.R.L.	OT	26004839	0765999000	administrativ@algrup.ro
174	SEMCO S.R.L.	OT	1523504	0722533980	semco_sistem@yahoo.co.uk

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
175	STANDARDLEG SECURITY CONSULTING S.R.L.	OT	33070568	0723211505	office.standardleg@yahoo.com
176	ALEDAV OSOSCHI S.R.L.	PH	31501044	0724623715	aledavososchi@yahoo.com
177	ROVARO SECURITY S.R.L.	PH	28835311	0744427474	dinulescu.oana@gmail.com
178	SECURITY PORTAL S.R.L.	PH	27471689	0734738180	razvan@securityportal.ro
179	SYTEVAL SRL	PH	20416490	0722220085	office@syteval.ro
180	TATUC GHEORGHE-ION PFA	PH	33898456	0720385985	gh@tatuc.ro
181	TATUC SERV CONSULTING S.R.L.	PH	36865534	0744381326	tatuc_costin@yahoo.com
182	BLEJAN OVIDIU P.F.A.	SB	33723179	0722277710	office@protinvestigo.ro
183	KATELLY SYSTEMS S.R.L.	SB	RO42604452	0734262438	adrian@katellysystems.ro
184	MONDOCTAL CONCEPT SRL	SB	RO31160796	0744354721	mondoctal.concept@gmail.com
185	ROMGUARD S.R.L.	SB	11166638	0740188558	office@spps-romguard.ro
186	IANCHIS ALIN-NICOLAE PFA	SJ	41288920	0744527799	ianchisalin@yahoo.com
187	MEZEI OCTAVIAN IOAN PFA	SJ	38268290	0743183569	mezei_octavian_ioan@yahoo.com
188	PADUREAN D. IOAN II	SJ	33744104	0744572275	johnforestyear@yahoo.com
189	BODNARIUC MIRCEA PFA	SV	34455848	0740120831	igla@ymail.com
190	BRUMA PETRU P.F.A.	SV	37900940	0740311321	petricabruma@yahoo.com
191	IRIMIA S. FLORIN - CRISTIAN P.F.A.	SV	47852246	0749205785	florin0474@gmail.com
192	MOSUC IOAN-OVIDIU P.F.A.	SV	33671657	0754467826	mosucioanovidiu@gmail.com
193	NETADMIN TECHNOLOGIES S.R.L.	SV	42627995	0790250000	bogdan@turcanu.ro
194	PRORAD SERVICE SRL	SV	4923289	0744550970	acarmenflorica@yahoo.com
195	TOP RISK S.R.L.	SV	39297676	0745319105	mihabirsan@gmail.com
196	DAMASCHIN CONSTANTIN PFA	TL	34775907	0740177672	marcel.damaschin@gmail.com
197	GARANT SECURITY CONSULTING S.R.L.	TL	42208873	0745303296	garantisaccea@yahoo.com
198	I & C S.R.L.	TL	2364555	0722280608	iacob.sorin.eusebio@gmail.com
199	BIT SECURE S.R.L.	TM	37208168	0744990899	office@bitsecure.ro
200	CINCA SORIN-NICOLAE P.F.A.	TM	35190102	0722391668	sorin_cinca@yahoo.com
201	DARABAN A. MIHAI P.F.A.	TM	33654281	0742143710	mihai.daraban2008@yahoo.com

NR.	DENUMIRE SOCIETATE/PFA	JUDEŢ	C.U.I.	TEL/FAX	E-MAIL
202	DGM DRAGON SECURITY S.R.L.	TM	45706970	0720680723	draganalex.1995@gmail.com
203	DGM PROFESIONAL CONSULTING SRL	TM	36154337	0722316473	dg_mircea@yahoo.com
204	PACURAR VIRGIL-IOAN P.F.A.	TM	34968290	0724262057	pacurar_virgil@yahoo.com
205	POPOVICI GELU - DORU P.F.A.	TM	39601197	0720046250	popovicigeludoru@gmail.com
206	SANMIR GUARD SECURITY S.R.L.	TR	38110310	0766073895	stanionica68@yahoo.com
207	R&B RISK MANAGEMENT SRL	VL	33986094	0761741738	roland.barbu@gmail.com
208	TOP SECURITY MANAGEMENT S.R.L.	VL	39290821	0745488437	deaconu_sebastian@yahoo.com
209	MAGUREANU LAURENTIU I.I.	VN	25234228	0737541187	magureanu_laurentiu@yahoo.com
210	MINSOFT S.R.L.	VN	16304022	0740539315	scminsoft@gmail.com
211	START DIM TV S.R.L.	VN	36766760	0751280333	vasiletarala@gmail.com
212	UMO SERV S.R.L.	VN	4908386	0734368499	office@umoserv.ro

PORTALUL BENEFICIARULUI ANALIZEI DE RISC

www.anersfr.ro



SUSȚINEREA CONFERINȚELOR ANERSFR

Adresa: Bdul. Unirii nr.31, bl.A1, parter, sediu Conpirom, sector 3
Email: office@anersfr.ro
Website: www.anersfr.ro

ÎNTÂLNIRI ALE SPECIALIȘTILOR DIN INDUSTRIA DE SECURITATE PRIVATĂ

CONFERINȚE PE SUBIECTE PROFESIONALE



Campania ANERSFR de promovare a bunelor practici pe anul 2025 poate fi catalogată ca fiind o acțiune reușită, care, dincolo de standardul ridicat al organizării, subiectele alese și speakerii invitați, este confirmată de rata foarte bună a participării și a implicării specialiștilor din mediul de afaceri ori din rândul prestatorilor de servicii de securitate privată.

Capacitarea și coeziunea creată în comunitățile profesionale cu peste 80 persoane prezente la fiecare eveniment, au adus plus valoare dezbaterilor și subiectelor profesionale, ridicând nivelul discuțiilor la stadiul de expertiză în profesiile domeniului.

Centrele urbane care au beneficiat de prezența invitațiilor noștii au fost: Iași, București, Brăila, Oradea și Sibiu, iar feedback-ul primit din partea participanților confirmă necesitatea continuării campaniei și pe acest an.