ARES

Asociația ARES

Asociația pentru Reziliență, Evaluare și Securitate

DOCUMENT PROFESIONAL M–03

METODOLOGIE DE ANALIZĂ ARES

Metodologia ARES I-SAFE

I-SAFE – Internal Security Analysis of Factors & Exposure: metodologie pentru identificarea, analiza și structurarea factorilor interni cu relevanță pentru riscul la securitatea fizică.

I · S · A · F · E

EVALUATORI ȘI ANALIȘTI DE RISC LA SECURITATEA FIZICĂ

Publicație profesională · Asociația ARES

EDIȚIA 2026

Actualizat 13.08.2026

M–03 · METODOLOGII

Metodologia ARES I-SAFE

I-SAFE – Internal Security Analysis of Factors & Exposure: metodologie pentru identificarea, analiza și structurarea factorilor interni cu relevanță pentru riscul la securitatea fizică.

31	4.634	≈ 21	2026
CAPITOLE	CUVINTE	MINUTE DE LECTURĂ	EDIȚIE PROFESIONALĂ

NOTĂ PROFESIONALĂ

Documentul nu are natura unui act normativ și se aplică în completarea legislației în vigoare, fără a înlocui ori modifica obligațiile legale aplicabile.

CUPRINS

FORMULA I-SAFE
I + S + A + F + E

METODOLOGIA ARES I-SAFE

Metodologie pentru identificarea, analiza și structurarea factorilor interni cu relevanță pentru riscul la securitatea fizică

I-SAFE – Internal Security Analysis of Factors & Exposure

Asociația pentru Reziliență, Evaluare și Securitate – ARES Ediția I · 2026

PREAMBUL

Riscul la securitatea fizică nu poate fi înțeles exclusiv prin raportare la amenințările existente în mediul exterior al unei organizații.

Caracteristicile construcției, organizarea spațiilor, natura activităților desfășurate, activele și valorile existente, fluxurile operaționale, sistemele de securitate, procedurile interne și comportamentul persoanelor pot genera, favoriza, amplifica, limita sau modifica expunerea unei organizații la evenimente de securitate.

În același timp, simpla existență a unei caracteristici interne nu înseamnă automat existența unei vulnerabilități și cu atât mai puțin existența unui risc.

Pentru structurarea acestei etape de analiză, **Asociația pentru Reziliență, Evaluare și Securitate – ARES** dezvoltă metodologia proprie:

I-SAFE

Internal Security Analysis of Factors & Exposure

respectiv:

Analiza Factorilor Interni și a Expunerii relevante pentru Securitatea Fizică

I-SAFE constituie un instrument metodologic destinat **identificării, documentării, corelării și analizării factorilor interni care pot avea relevanță pentru securitatea fizică**.

Metodologia urmărește să creeze o legătură logică și trasabilă între:

CONTEXT INTERN → FACTORI → EXPUNERI → AMENINȚĂRI → VULNERABILITĂȚI → SCENARII → EVALUAREA RISCULUI

M–03 · 01

CAPITOLUL I

SCOPUL ȘI STATUTUL METODOLOGIEI

1.1. Scop

Scopul metodologiei I-SAFE este de a oferi evaluatorului sau analistului un cadru structurat pentru identificarea elementelor din mediul intern al unei organizații care pot influența securitatea fizică.

Metodologia urmărește:

- identificarea sistematică a factorilor interni;
- reducerea riscului de omitere a unor elemente relevante;
- separarea constatărilor factuale de interpretarea profesională;
- identificarea expunerilor asociate;
- verificarea interdependențelor dintre diferite componente ale organizației;
- documentarea surselor informațiilor;
- identificarea elementelor care necesită aprofundare;
- fundamentarea identificării amenințărilor și vulnerabilităților;
- sprijinirea construirii scenariilor de risc;
- crearea unei trasabilități între observațiile efectuate și concluziile utilizate ulterior în analiza riscului.

1.2. Ce este I-SAFE

I-SAFE este o:

metodologie de identificare și analiză structurată a factorilor interni cu relevanță pentru securitatea fizică.

Aceasta organizează mediul intern în cinci domenii principale:

I – Infrastructure

Infrastructură și configurație fizică

S – Security Systems

Sisteme și măsuri de securitate

A – Assets & Activities

Active, valori și activități

F – Functions & Organizational Framework

Funcții, procese și organizare

E – Employees & Human Element

Personal și factor uman

1.3. Ce NU este I-SAFE

I-SAFE:

- nu reprezintă o metodă autonomă de calcul al riscului;
- nu stabilește prin ea însăși nivelul riscului;
- nu este un standard ISO;
- nu reprezintă o metodă oficială emisă de o autoritate publică;
- nu înlocuiește metodologia, etapele sau obligațiile impuse de legislația aplicabilă;
- nu transformă automat un factor intern într-o vulnerabilitate;
- nu transformă automat o constatare într-un risc;
- nu substituie raționamentul profesional al evaluatorului;
- nu poate fi aplicată mecanic, fără raportare la caracteristicile obiectivului analizat.

I-SAFE reprezintă **instrumentul de identificare și structurare a intrărilor necesare unei analize ulterioare a riscului**.

M–03 · 02

CAPITOLUL II

FUNDAMENTAREA METODOLOGICĂ ȘI CADRUL DE REFERINȚĂ

2.1. Raportarea la cadrul național

În România, adoptarea măsurilor de securitate pentru obiectivele, bunurile și valorile supuse reglementării se fundamentează pe analiza de risc la securitatea fizică, iar HG nr. 301/2012 stabilește că elaborarea acesteia se realizează potrivit instrucțiunilor emise în domeniu.

Instrucțiunile MAI nr. 9/2013 prevăd că analiza de risc la securitatea fizică fundamentează adoptarea măsurilor de securitate și prevăd luarea în considerare a standardelor naționale sau europene privind managementul și tehnicile de evaluare a riscului.

Prin modificările legislative introduse în 2026, cadrul legal face referire expresă la modificarea **parametrilor interni și externi care generează și/sau modifică riscurile la securitatea fizică**, în contextul situațiilor care determină revizuirea analizei.

În acest context, I-SAFE este concepută ca instrument complementar de identificare structurată a componentei interne.

Aplicarea I-SAFE trebuie realizată întotdeauna cu verificarea formei în vigoare a legislației și a normelor aplicabile la data efectuării analizei.

2.2. Raportarea la managementul riscului

ISO 31000:2018 oferă principii și orientări generale pentru managementul riscului, într-o abordare aplicabilă organizațiilor și diferitelor tipuri de risc.

IEC 31010:2019 oferă orientări privind selectarea și utilizarea tehnicilor pentru evaluarea riscului și include multiple tehnici care pot fi utilizate pentru obținerea unei înțelegeri structurate a riscului și incertitudinii.

I-SAFE nu este parte a ISO 31000 sau IEC 31010 și nu trebuie prezentată ca metodă certificată sau aprobată de ISO.

Metodologia ARES utilizează principii generale compatibile cu managementul modern al riscului, precum:

- contextualizarea;
- structurarea informațiilor;
- trasabilitatea;
- utilizarea dovezilor;
- analiza interdependențelor;

- revizuirea în cazul schimbării contextului.

M–03 · 03

CAPITOLUL III

TERMINOLOGIE I-SAFE

În sensul prezentei metodologii, termenii următori sunt utilizați cu semnificație operațională proprie I-SAFE.

3.1. Factor intern

Caracteristică, situație, condiție, activitate, resursă, relație sau circumstanță existentă în mediul intern analizat și care poate influența securitatea fizică.

Factorul poate avea caracter:

- amplificator;
- protector;
- condițional;
- neutru.

3.2. Activ

Persoană, bun, valoare, resursă, echipament, document, informație, infrastructură, proces sau alt element pentru care există un interes legitim de protecție.

3.3. Expunere

Situația în care un activ, o persoană, o activitate sau un proces poate intra în relație cu o amenințare ori poate suporta consecințele producerii unui eveniment.

Expunerea nu este sinonimă cu vulnerabilitatea.

3.4. Amenințare

Element, acțiune, eveniment, circumstanță sau actor capabil să producă un efect negativ asupra activului sau obiectivului analizat.

3.5. Vulnerabilitate

Slăbiciune sau deficiență care poate fi exploatată ori poate favoriza materializarea unei amenințări și producerea unui eveniment nedorit.

3.6. Măsură de securitate

Mecanism tehnic, fizic, uman, procedural sau organizațional destinat prevenirii, descurajării, detectării, întârzierii, semnalizării, limitării sau gestionării unui eveniment de securitate.

3.7. Scenariu de risc

Descriere structurată a unei succesiuni plauzibile de condiții și evenimente prin care o amenințare, raportată la expunerile și vulnerabilitățile identificate, poate produce consecințe asupra activelor analizate.

3.8. Dovadă

Informație utilizată pentru fundamentarea unei constatări.

Poate proveni din:

- observație directă;
- documente;
- înregistrări;
- interviuri;
- sisteme;
- registre;
- măsurători;
- planuri;
- informații operaționale;
- alte surse verificabile.

M–03 · 04

CAPITOLUL IV

PRINCIPIILE METODOLOGIEI I-SAFE

4.1. Principiul contextualizării

Niciun factor nu trebuie considerat relevant doar pentru că apare într-o listă de verificare.

Factorul trebuie interpretat în contextul concret al obiectivului.

4.2. Principiul factualității

Prima etapă o reprezintă consemnarea faptului observat.

Interpretarea trebuie realizată separat.

Exemplu:

Fapt: unitatea funcționează până la ora 23:00.

Nu:

„Programul până la ora 23:00 reprezintă o vulnerabilitate.”

Pentru formularea celei de-a doua concluzii sunt necesare elemente suplimentare.

4.3. Principiul trasabilității

Trebuie să poată fi urmărit traseul:

FACTOR → INFLUENȚĂ → EXPUNERE → AMENINȚARE/VULNERABILITATE → SCENARIU

4.4. Principiul dovezii

Constatările semnificative trebuie susținute de informații verificabile în limita posibilităților și atribuțiilor analistului.

4.5. Principiul proporționalității

Profunzimea analizei trebuie adaptată:

- naturii obiectivului;
- complexității activității;
- valorilor protejate;

- dimensiunii organizației;
- particularităților identificate.

4.6. Principiul interdependenței

Factorii I-SAFE nu funcționează izolat.

Un factor de personal poate interacționa cu un factor organizațional, un sistem tehnic și o particularitate arhitecturală.

4.7. Principiul separării factorului de risc

Un factor intern nu reprezintă automat:

- amenințare;
- vulnerabilitate;
- incident;
- consecință;
- risc.

4.8. Principiul neutralității

Analiza trebuie să identifice atât factorii care pot amplifica expunerea, cât și factorii protectori.

4.9. Principiul actualității

Analiza trebuie raportată la situația existentă la momentul examinării.

4.10. Principiul verificării profesionale

Checklisturile I-SAFE sprijină analiza.

Ele nu înlocuiesc judecata profesională.

M–03 · 05

CAPITOLUL V

ARHITECTURA I-SAFE

Metodologia este structurată în cinci piloni:

Cod	Pilon	Domeniu
I	Infrastructure	Infrastructură și configurație fizică
S	Security Systems	Sisteme și măsuri de securitate
A	Assets & Activities	Active, valori și activități
F	Functions & Organizational Framework	Funcții, procese, proceduri și organizare
E	Employees & Human Element	Personal și factor uman

M–03 · 06

CAPITOLUL VI

I – INFRASTRUCTURE

6.1. Obiectiv

Identificarea caracteristicilor fizice și constructive care influențează securitatea.

Se analizează:

- amplasarea și configurația clădirii;
- destinația spațiilor;
- compartimentarea;
- intrările;
- ieșirile;
- căile secundare de acces;
- căile de evacuare relevante analizei;
- accesurile tehnice;
- ferestrele și suprafețele vitrate;
- pereții și elementele constructive;
- circulațiile interioare;
- delimitarea zonelor;
- zonele restricționate;
- spațiile tehnice;
- depozitele;
- casieriile;
- spațiile pentru valori;
- zonele de încărcare-descărcare;
- parcările;
- conexiunile cu alte spații;
- vizibilitatea;
- iluminatul;
- posibilitatea supravegherii;
- posibilitatea ascunderii;

- accesibilitatea activelor;
- condițiile necesare intervenției.

Întrebarea centrală:

Cum influențează configurația fizică accesul, deplasarea, supravegherea, protecția activelor și posibilitatea producerii sau limitării unui eveniment?

M–03 · 07

CAPITOLUL VII

S – SECURITY SYSTEMS

7.1. Obiectiv

Analizarea măsurilor utilizate pentru:

PREVENIRE → DESCURAJARE → DETECTARE → ÎNTÂRZIERE → ALARMARE → REACȚIE → DOCUMENTARE

Pot fi analizate:

- sistemul de alarmare împotriva efracției;
- supravegherea video;
- controlul accesului;
- interfonia;
- sistemele de alertare;
- butoanele de panică;
- mijloacele mecanofizice;
- iluminatul de securitate;
- împrejmuirile;
- barierele;
- încuietorile;
- sistemele de transmitere a alarmelor;
- alimentarea cu energie;
- sursele de rezervă;
- comunicațiile;
- redundanța;
- integrarea sistemelor;
- mentenanța;
- verificările;
- remedierea defecțiunilor;
- jurnalizarea;
- monitorizarea;

- dispecerizarea;
- intervenția.

Regula I-SAFE

Nu este suficient:

„Există CCTV.”

Se analizează:

Ce protejează?

Ce detectează?

În ce condiții?

Ce nu poate detecta?

Cine primește informația?

Ce reacție urmează?

Ce se întâmplă dacă sistemul devine indisponibil?

M–03 · 08

CAPITOLUL VIII

A – ASSETS & ACTIVITIES

8.1. Active

Se identifică ceea ce trebuie protejat.

Pot fi relevante:

- persoane;
- numerar;
- bunuri;
- produse;
- materii prime;
- echipamente;
- utilaje;
- documente;
- suporturi informatice;
- chei;
- carduri și credențiale;
- bunuri cu valoare ridicată;
- infrastructură esențială;
- alte resurse relevante.

Pentru active se urmăresc:

- amplasarea;
- concentrarea;
- cantitatea;
- valoarea;
- durata expunerii;
- accesibilitatea;
- persoanele autorizate;
- deplasarea;

- depozitarea;
- protecția existentă.

8.2. Activități

Se analizează activitățile care creează sau modifică expunerea:

- încasări;
- plăți;
- manipularea numerarului;
- alimentarea casieriilor;
- retragerea numerarului;
- aprovizionarea;
- livrările;
- recepția;
- depozitarea;
- relația cu publicul;
- transportul valorilor;
- manipularea bunurilor;
- operațiunile de deschidere;
- operațiunile de închidere;
- schimburile de tură;
- mentenanța;
- activitatea în afara programului;
- accesul contractorilor;
- accesul furnizorilor;
- procesele cu caracter excepțional.

Întrebarea centrală:

Ce trebuie protejat și ce activități creează, concentrează, transferă sau modifică expunerea?

M–03 · 09

CAPITOLUL IX

F – FUNCTIONS & ORGANIZATIONAL FRAMEWORK

9.1. Obiectiv

Analizarea modului în care organizația conduce, controlează și documentează activitățile relevante securității.

Se analizează:

- structura organizațională;
- responsabilitățile;
- atribuțiile;
- nivelurile de autoritate;
- responsabilitatea pentru securitate;
- fluxurile de aprobare;
- procedurile;
- separarea atribuțiilor;
- controlul accesului organizațional;
- atribuirea drepturilor de acces;
- retragerea drepturilor;
- administrarea cheilor;
- gestionarea vizitatorilor;
- gestionarea contractorilor;
- raportarea incidentelor;
- escaladarea;
- controlul intern;
- mentenanța;
- gestionarea situațiilor neobișnuite;
- procedurile pentru numerar;
- procedurile de deschidere și închidere;
- continuitatea unor funcții relevante.

Întrebarea centrală:

Cum influențează organizarea, responsabilitățile și procedurile posibilitatea prevenirii, producerii, detectării și gestionării unui eveniment?

M–03 · 10

CAPITOLUL X

E – EMPLOYEES & HUMAN ELEMENT

10.1. Obiectiv

Analizarea factorului uman relevant pentru securitate.

Pot fi analizate:

- numărul persoanelor;
- repartizarea pe zone;
- programul;
- schimburile;
- lucrul individual;
- fluctuația personalului;
- personalul nou;
- personalul temporar;
- personalul externalizat;
- nivelurile de acces;
- accesul privilegiat;
- instruirea;
- cunoașterea procedurilor;
- utilizarea sistemelor;
- reacția la incidente;
- comunicarea internă;
- raportarea;
- respectarea regulilor;
- cultura de securitate;
- supravegherea operațională;
- dependența de anumite persoane-cheie.

Datele privind persoanele trebuie utilizate numai în limitele cadrului juridic aplicabil și în măsura în care sunt necesare analizei.

Întrebarea centrală:

Cum pot organizarea, competențele, accesul și comportamentul persoanelor influența securitatea?

M–03 · 11

CAPITOLUL XI

NIVELURILE DE APLICARE I-SAFE

I-SAFE este aplicată în patru niveluri.

NIVELUL 1 – SCREENING

Scop:

identificarea inițială a factorilor.

Se parcurg cei cinci piloni și biblioteca de întrebări.

NIVELUL 2 – ANALIZĂ

Pentru fiecare factor relevant se stabilește:

- natura;
- locul;
- momentul;
- sursa;
- activele afectate;
- mecanismul de influență;
- măsurile existente.

NIVELUL 3 – CORELARE

Factorul este verificat în raport cu ceilalți piloni.

Exemplu:

A – numerar

este analizat în relație cu:

I – locul unde este păstrat

S – protecția tehnică

F – procedura de manipulare

E – persoanele care îl gestionează

NIVELUL 4 – TRANSFER

Factorii relevanți sunt transferați către etapa următoare:

identificarea amenințărilor → vulnerabilităților → scenariilor → evaluarea riscului.

M–03 · 12

CAPITOLUL XII

REGULA CELOR CINCI ÎNTREBĂRI I-SAFE

Pentru fiecare factor se răspunde la:

1. CE?

Ce am identificat?

Descriere factuală.

2. UNDE?

Unde apare?

Localizare fizică, organizațională sau operațională.

3. CÂND?

Când și în ce condiții devine relevant?

4. CUM?

Cum poate influența securitatea?

5. DOVADA?

Pe ce informație se bazează constatarea?

M–03 · 13

CAPITOLUL XIII

PROCEDURA OPERAȚIONALĂ I-SAFE

Etapa 1 – Stabilirea limitelor analizei

Se stabilesc:

- obiectivul;
- locația;
- activitățile;
- spațiile;
- procesele;
- activele;
- intervalele relevante;
- entitățile implicate.

Etapa 2 – Colectarea informațiilor

Pot fi utilizate:

- observația pe teren;
- documentația;
- interviurile;
- planurile;
- procedurile;
- registrele;
- documentațiile tehnice;
- istoricul incidentelor;
- informațiile operaționale.

Etapa 3 – Screening I-SAFE

Se parcurg:

I → S → A → F → E

Etapa 4 – Înregistrarea factorilor

Fiecare factor primește un cod.

Exemple:

I-01

S-04

A-07

F-03

E-11

Etapa 5 – Analiza relevanței

Se stabilește mecanismul prin care factorul poate influența securitatea.

Etapa 6 – Corelarea

Se aplică matricea inter-piloni.

Etapa 7 – Identificarea expunerilor

Se stabilesc:

- persoanele;
- activele;
- zonele;
- procesele;
- activitățile;

care pot fi afectate.

Etapa 8 – Transferul

Factorii relevanți sunt utilizați pentru aprofundarea:

- amenințărilor;
- vulnerabilităților;
- scenariilor.

M–03 · 14

CAPITOLUL XIV

CLASIFICAREA FACTORILOR

14.1. După efect

AMPLIFICATOR

Poate crește expunerea sau poate favoriza un scenariu.

PROTECTOR

Poate limita expunerea sau efectele unui scenariu.

CONDIȚIONAL

Efectul apare numai în anumite circumstanțe.

NEUTRU

Nu a rezultat o influență relevantă în contextul analizat.

14.2. După relevanță pentru continuarea analizei

Factorii pot fi marcați:

R1 – Relevanță redusă

Nu necesită aprofundare distinctă în condițiile analizate.

R2 – Relevanță moderată

Necesită corelare cu alți factori.

R3 – Relevanță semnificativă

Necesită aprofundarea amenințărilor, vulnerabilităților sau scenariilor asociate.

R1/R2/R3 nu reprezintă niveluri de risc.

14.3. După nivelul de confirmare

C – Confirmat

Susținut de informații suficiente.

P – Parțial confirmat

Există informații, dar sunt necesare verificări.

N – Neverificat

Necesită informații suplimentare.

M–03 · 15

CAPITOLUL XV

M–03 · 16

MATRICEA DE CORELARE INTER-PILONI

Corelarea I-SAFE urmărește zece relații principale:

Corelare	Întrebarea principală
I × S	Cum influențează infrastructura eficiența sistemelor?
I × A	Cum influențează infrastructura expunerea activelor?
I × F	Cum influențează spațiul procesele și procedurile?
I × E	Cum influențează infrastructura comportamentul și deplasarea persoanelor?
S × A	Sistemele protejează activele în condițiile reale?
S × F	Există proceduri pentru utilizarea și gestionarea sistemelor?
S × E	Personalul poate utiliza corect sistemele și reacționa la semnale?
A × F	Procesele de gestionare sunt adecvate activelor?
A × E	Cine are acces la active și în ce condiții?
F × E	Personalul cunoaște și aplică procedurile?

M–03 · 17

CAPITOLUL XVI

M–03 · 18

MATRICEA I-SAFE 5 × 5

Evaluatorul poate utiliza următoarea verificare:

	I	S	A	F	E
I	—	I×S	I×A	I×F	I×E
S		—	S×A	S×F	S×E
A			—	A×F	A×E
F				—	F×E
E					—

Scopul matricei nu este generarea artificială de probleme.

Evaluatorul verifică dacă există **relații relevante** între factorii deja identificați.

M–03 · 19

CAPITOLUL XVII

FIȘA FACTORULUI INTERN I-SAFE

Model operațional

Cod factor: I/S/A/F/E – ___

Pilon:

Denumirea factorului:

Descriere factuală:

Sursa informației:

Locul/procesul:

Momentul/condițiile:

Activ/persoană/proces expus:

Mecanismul de influență:

Tipul influenței: Amplificator / Protector / Condițional / Neutru

Măsuri existente:

Corelări I-SAFE:

Amenințări care necesită analiză:

Vulnerabilități identificate sau care necesită verificare:

Scenarii care necesită analiză:

Relevanță: R1 / R2 / R3

Nivel de confirmare: C / P / N

Observații:

M–03 · 20

CAPITOLUL XVIII

CHECKLISTUL SURSELOR DE INFORMAȚII

I – Infrastructure

Surse recomandate:

- inspecție pe teren;
- planuri;
- relevee;
- schițe;
- documentații ale construcției;
- fotografii realizate legal;
- verificarea circuitelor;
- observația directă.

S – Security Systems

Surse:

- observație;
- proiecte tehnice;
- documentație tehnică;
- registre de mentenanță;
- evidențe de service;
- teste;
- jurnale de evenimente;
- informații de la personalul tehnic;
- proceduri operaționale.

A – Assets & Activities

Surse:

- interviuri;

- evidențe interne;
- inventare relevante;
- fluxuri de lucru;
- proceduri;
- informații despre program;
- observație directă;
- documentarea circuitelor.

Nu este necesară colectarea unor date financiare sau comerciale care nu sunt relevante pentru scopul analizei.

F – Functions

Surse:

- organigrame;
- fișe de post relevante;
- proceduri;
- regulamente;
- decizii;
- responsabilități;
- interviuri cu conducerea;
- documentarea fluxurilor operaționale.

E – Employees

Surse:

- interviuri;
- evidențe de instruire;
- proceduri;
- fișe de post relevante;
- organizarea schimburilor;
- informații privind nivelurile de acces;
- observație asupra modului de lucru.

Se aplică principiul minimizării datelor și cadrul juridic aplicabil protecției datelor cu caracter personal.

M–03 · 21

CAPITOLUL XIX

BIBLIOTECA DE ÎNTREBĂRI I-SAFE

Biblioteca are rol de **screening**.

Răspunsul afirmativ sau negativ la o întrebare nu înseamnă automat existența unei vulnerabilități.

A. INFRASTRUCTURE – 20 DE ÎNTREBĂRI

1. Câte căi de acces există în obiectiv?
2. Toate căile de acces au o funcție operațională justificată?
3. Există accesuri secundare utilizate rar?
4. Există spații care nu pot fi observate din zonele normale de lucru?
5. Există legături fizice cu alte clădiri sau spații?
6. Sunt zonele publice separate de cele restricționate?
7. Sunt activele importante amplasate în zone ușor accesibile?
8. Există trasee directe între accesul public și activele importante?
9. Există zone care facilitează ascunderea unei persoane?
10. Iluminatul permite observarea corespunzătoare a zonelor relevante?
11. Configurația mobilierului influențează vizibilitatea?
12. Există ferestre sau suprafețe vitrate relevante pentru acces?
13. Există uși tehnice sau de serviciu?
14. Sunt spațiile tehnice accesibile persoanelor neautorizate?
15. Există zone comune cu alte organizații?
16. Există puncte de încărcare-descărcare?
17. Parcarea creează acces direct către zone relevante?
18. Există diferențe importante între configurația din timpul programului și cea din afara programului?
19. Configurația permite intervenția rapidă în caz de incident?
20. O modificare a arhitecturii sau mobilierului ar putea modifica expunerea?

B. SECURITY SYSTEMS – 20 DE ÎNTREBĂRI

1. Ce sisteme de securitate există?
2. Ce active protejează fiecare sistem?
3. Care este funcția fiecărui sistem?
4. Există zone relevante neacoperite?
5. Sistemele funcționează permanent?
6. Există intervale de dezactivare?
7. Cine poate activa/dezactiva sistemele?
8. Cine poate modifica configurațiile?
9. Cum sunt administrate drepturile de acces?
10. Ce se întâmplă în cazul întreruperii energiei?
11. Există surse de rezervă?
12. Ce se întâmplă în cazul întreruperii comunicațiilor?
13. Sunt sistemele verificate și întreținute?
14. Defecțiunile sunt documentate?
15. Există procedură pentru remedierea defecțiunilor?
16. Cine primește alarma?
17. Ce reacție este inițiată?
18. Personalul știe să utilizeze sistemele?
19. Sistemele oferă informații suficiente pentru documentarea unui incident?
20. Există dependențe critice între mai multe sisteme?

C. ASSETS & ACTIVITIES – 20 DE ÎNTREBĂRI

1. Care sunt activele importante?
2. Unde se află acestea?
3. Există perioade de concentrare a valorilor?
4. Cine are acces?

5. Cât timp sunt expuse?
6. Se deplasează în interiorul obiectivului?
7. Sunt transportate între locații?
8. Există active atractive pentru sustragere?
9. Există bunuri ușor de transportat?
10. Există numerar?
11. Există momente în care numerarul se acumulează?
12. Există operațiuni efectuate în afara programului normal?
13. Există activități cu publicul?
14. Există livrări regulate?
15. Furnizorii pătrund în zone interne?
16. Există procese de încărcare-descărcare?
17. Există active fără de care activitatea nu poate continua?
18. Există operațiuni în care o singură persoană controlează un activ important?
19. Există variații sezoniere importante?
20. Ce modificări ale activității ar putea schimba expunerea?

D. FUNCTIONS & ORGANIZATIONAL FRAMEWORK – 20 DE ÎNTREBĂRI

1. Cine răspunde de securitate?
2. Responsabilitățile sunt clar definite?
3. Există proceduri de securitate?
4. Procedurile sunt actualizate?
5. Cine aprobă accesul?
6. Cine retrage drepturile de acces?
7. Cum sunt gestionate cheile?
8. Există evidența persoanelor care dețin chei sau credențiale?

9. Cum sunt gestionați vizitatorii?
10. Cum sunt gestionați contractorii?
11. Există procedură pentru deschiderea obiectivului?
12. Există procedură pentru închiderea obiectivului?
13. Există proceduri pentru manipularea valorilor?
14. Cum sunt raportate incidentele?
15. Cine decide reacția la un incident?
16. Cum sunt gestionate defecțiunile sistemelor de securitate?
17. Există separarea atribuțiilor pentru procese sensibile?
18. Cum sunt comunicate modificările de securitate?
19. Sunt păstrate evidențe suficiente ale incidentelor?
20. Modificările activității determină reevaluarea procedurilor?

E. EMPLOYEES & HUMAN ELEMENT – 20 DE ÎNTREBĂRI

1. Câte persoane lucrează în obiectiv?
2. Cum sunt repartizate?
3. Există activitate individuală?
4. Există perioade cu personal redus?
5. Există fluctuație semnificativă?
6. Există personal temporar?
7. Există personal externalizat?
8. Personalul nou primește instruire?
9. Sunt drepturile de acces adaptate funcției?
10. Sunt retrase drepturile atunci când nu mai sunt necesare?
11. Există persoane cu acces în numeroase zone?
12. Există persoane cu acces privilegiat la sisteme?
13. Personalul cunoaște procedurile de securitate?

14. Personalul știe cum să raporteze un incident?
15. Personalul știe cum să reacționeze la alarmă?
16. Sunt efectuate instruiri periodice?
17. Sunt abaterile de la proceduri raportate?
18. Există dependență operațională de una sau câteva persoane?
19. Personalul cunoaște limitele propriilor atribuții?
20. Există o cultură organizațională care susține raportarea problemelor de securitate?

M–03 · 22

CAPITOLUL XX

REGULA CELOR 100 DE ÎNTREBĂRI

Cele 100 de întrebări constituie **biblioteca generală I-SAFE de screening**.

Evaluatorul:

- nu este obligat să folosească mecanic fiecare întrebare;
- poate elimina întrebările evident neaplicabile;
- poate introduce întrebări suplimentare;
- trebuie să adapteze analiza obiectivului;
- nu trebuie să considere răspunsurile drept scor de risc.

Checklistul este un instrument pentru:

A NU UITA SĂ ÎNTREBI.

Nu este un instrument pentru:

A DECIDE AUTOMAT CARE ESTE RISCUL.

M–03 · 23

CAPITOLUL XXI

DE LA FACTOR LA SCENARIU

Modelul logic I-SAFE este:

FACTOR

Ce există?

↓

EXPUNERE

Ce poate fi afectat și în ce condiții?

↓

AMENINȚARE

Ce eveniment sau actor poate produce efectul?

↓

VULNERABILITATE

Ce poate permite sau favoriza materializarea amenințării?

↓

SCENARIU

Cum s-ar putea produce evenimentul?

↓

CONSECUȚE

Ce efecte pot rezulta?

↓

EVALUAREA RISCULUI

Se aplică metodologia corespunzătoare.

M–03 · 24

CAPITOLUL XXII

EXEMPLU DE APLICARE

Obiectiv ipotetic

Unitate comercială cu acces public și operațiuni în numerar.

A-01 – Assets & Activities

Fapt identificat:

Pe parcursul programului sunt realizate încasări în numerar.

Factor:

Acumularea temporară a numerarului în zona casieriei.

Tip:

Factor condițional/amplificator.

Corelare A × I

Casieria este amplasată în apropierea accesului principal.

Rezultă necesitatea analizării influenței configurației asupra accesului și deplasării către/dinspre casierie.

Corelare A × S

Se verifică:

- supravegherea;
- alarmarea;
- mijloacele de alertare;
- mijloacele fizice existente;
- capacitatea de documentare a unui incident.

Corelare A × F

Se verifică:

- procedura de retragere a numerarului;

- limitele operaționale;
- responsabilitățile;
- frecvența transferului valorilor.

Corelare A × E

Se verifică:

- cine gestionează numerarul;
- cine are acces;
- nivelul de instruire;
- reacția personalului.

Expunerea

Existența periodică a unor valori monetare într-o zonă accesibilă publicului.

Amenințări care pot necesita analiză

În funcție de context:

- furt;
- tâlhărie;
- acțiuni ale unor persoane din interior;
- alte evenimente relevante.

Vulnerabilități

Acestea NU sunt presupuse.

Evaluatorul verifică dacă există efectiv slăbiciuni care pot fi exploatate.

Rezultatul I-SAFE

I-SAFE nu concluzionează:

„Riscul este mare.”

I-SAFE concluzionează:

„Factorul A-01 prezintă relevanță pentru analiză și trebuie corelat cu elementele I, S, F și E și transferat către scenariile corespunzătoare.”

Evaluarea riscului urmează ulterior.

M–03 · 25

CAPITOLUL XXIII

PROFILUL FACTORILOR INTERNI I-SAFE

Rezultatul final al aplicării metodologiei este:

PROFILUL FACTORILOR INTERNI I-SAFE

Acesta conține:

- lista factorilor;
- codurile;
- pilonii;
- sursele informațiilor;
- mecanismele de influență;
- activele expuse;
- corelările;
- măsurile existente;
- relevanța;
- nivelul de confirmare;
- amenințările care necesită analiză;
- vulnerabilitățile care necesită verificare;
- scenariile care necesită dezvoltare.

M–03 · 26

CAPITOLUL XXIV

CONTROLUL CALITĂȚII ANALIZEI

Înaintea finalizării profilului I-SAFE se verifică:

1.

Au fost parcurși toți cei cinci piloni?

2.

Au fost identificate activele relevante?

3.

Factorii sunt descriși factual?

4.

Factorii au surse?

5.

Au fost separate faptele de interpretări?

6.

Au fost evitate calificările automate drept „vulnerabilitate”?

7.

Au fost analizate interdependențele?

8.

Factorii R3 au fost corelați cu ceilalți piloni?

9.

Au fost identificate expunerile?

10.

Au fost evidențiate informațiile neverificate?

11.

Au fost transferați factorii relevanți către etapa de analiză a scenariilor?

12.

Au fost evitate concluziile de risc care nu sunt susținute de analiza ulterioară?

M–03 · 27

CAPITOLUL XXV

ACTUALIZAREA PROFILULUI I-SAFE

Analiza trebuie reconsiderată atunci când se modifică elemente relevante precum:

- activitatea;
- obiectul de activitate;
- programul;
- fluxurile;
- configurația spațiilor;
- caracteristicile arhitecturale;
- activele;
- volumele de valori;
- sistemele de securitate;
- procedurile;
- personalul;
- organizarea;
- condițiile de acces;
- procesele critice;
- alte elemente care pot modifica parametrii interni relevanți.

Cadrul legal actual include modificarea parametrilor interni și externi care generează și/sau modifică riscurile între situațiile relevante pentru revizuirea analizei de risc la securitatea fizică. Aplicarea concretă trebuie raportată întotdeauna la legislația în vigoare la momentul respectiv.

M–03 · 28

CAPITOLUL XXVI

INTEGRAREA CU MEDIUL EXTERN

I-SAFE analizează:

MEDIUL INTERN

Pentru analiza structurată a mediului extern poate fi utilizat separat un instrument precum:

PESTEL

P – Political

Factori politici și instituționali

E – Economic

Factori economici

S – Social

Factori sociali

T – Technological

Factori tehnologici

E – Environmental

Factori de mediu

L – Legal

Factori juridici și de reglementare

Cele două analize nu trebuie confundate.

M–03 · 29

CAPITOLUL XXVII

MODELUL INTEGRAT ARES

INTERN

I-SAFE

I – Infrastructure

S – Security Systems

A – Assets & Activities

F – Functions & Organizational Framework

E – Employees & Human Element

EXTERN

PESTEL

P – Political

E – Economic

S – Social

T – Technological

E – Environmental

L – Legal

↓

CONTEXTUL DE SECURITATE

↓

FACTORI INTERNI + FACTORI EXTERNI

↓

EXPUNERI

↓

AMENINȚĂRI + VULNERABILITĂȚI

↓

SCENARII

↓

EVALUAREA RISCULUI

↓

MĂSURI DE SECURITATE

M–03 · 30

CAPITOLUL XXVIII

FIȘĂ RAPIDĂ DE TEREN I-SAFE

Înainte de părăsirea obiectivului, evaluatorul poate efectua verificarea rapidă:

I – Infrastructure

Am înțeles spațiul?

- accesuri;
- circulații;
- zone;
- delimitări;
- expuneri fizice.

S – Security Systems

Am înțeles protecția?

- prevenire;
- detectare;
- alarmare;
- întârziere;
- reacție.

A – Assets & Activities

Am înțeles ce protejez și când este expus?

- persoane;
- valori;
- bunuri;
- procese;
- activități.

F – Functions

Am înțeles cine decide și cum funcționează procesele?

- responsabilități;
- proceduri;
- acces;
- incidente;
- control.

E – Employees

Am înțeles factorul uman?

- personal;
- acces;
- instruire;
- comportament;
- reacție.

M–03 · 31

CAPITOLUL XXIX

CRITERIUL DE FINALIZARE

Screeningul intern poate fi considerat suficient atunci când evaluatorul poate răspunde argumentat la cinci întrebări:

I

Cum influențează spațiul securitatea?

S

Cum funcționează protecția?

A

Ce protejez și unde apare expunerea?

F

Cum controlează organizația activitatea?

E

Cum influențează persoanele securitatea?

și, suplimentar:

Cum se influențează reciproc aceste cinci componente?

M–03 · 32

CAPITOLUL XXX

LIMITĂRI ȘI AVERTISMENT METODOLOGIC

Metodologia I-SAFE trebuie utilizată ca instrument de sprijin al analizei profesionale.

Aplicarea sa nu garantează identificarea absolută a tuturor factorilor posibili.

Realitatea organizațională este dinamică și pot exista:

- informații indisponibile;
- informații incomplete;
- comportamente imprevizibile;
- modificări ulterioare;
- factori specifici imposibil de prevăzut printr-o bibliotecă generală.

Din acest motiv, I-SAFE este construită ca:

STRUCTURĂ DE GÂNDIRE

și nu ca:

LISTĂ ÎNCHISĂ DE RĂSPUNSURI.

Evaluatorul poate adăuga factori, întrebări, corelări și surse suplimentare ori de câte ori contextul o impune.

M–03 · 33

CAPITOLUL XXXI

PRINCIPIUL FUNDAMENTAL I-SAFE

Întreaga metodologie poate fi sintetizată prin întrebarea:

„CE EXISTĂ SAU SE ÎNTÂMPLĂ ÎN INTERIORUL ORGANIZAȚIEI ȘI CUM POATE ACEL ELEMENT SĂ INFLUENȚEZE SECURITATEA?”

Răspunsul este căutat sistematic prin:

I · S · A · F · E

Infrastructure

Security Systems

Assets & Activities

Functions & Organizational Framework

Employees & Human Element

M–03 · 34

CONCLUZIE

Înainte de a evalua un risc trebuie înțeles contextul în care acesta poate apărea.

Înainte de a formula o vulnerabilitate trebuie identificat și verificat elementul care o poate genera.

Înainte de a construi un scenariu trebuie înțeles modul în care activele, spațiile, sistemele, procesele și persoanele interacționează.

Metodologia **ARES I-SAFE** oferă un cadru structurat pentru această etapă.

Ea transformă analiza mediului intern dintr-o succesiune de observații disparate într-un proces format din:

IDENTIFICARE

↓

DOCUMENTARE

↓

ANALIZĂ

↓

CORELARE

↓

TRANSFER CĂTRE SCENARIILE DE RISC

I-SAFE nu încearcă să înlocuiască raționamentul evaluatorului.

Dimpotrivă.

Scopul metodologiei este să îl ajute să îl documenteze.

M–03 · 35

FORMULA I-SAFE

I + S + A + F + E

↓

FACTORI INTERNI

↓

EXPUNERI

↓

CORELĂRI

↓

AMENINȚĂRI ȘI VULNERABILITĂȚI RELEVANTE

↓

SCENARII

↓

EVALUAREA RISCULUI

STATUTUL DOCUMENTULUI

Denumire: Metodologia ARES I-SAFE

Denumire extinsă: Metodologie pentru identificarea, analiza și structurarea factorilor interni cu relevanță pentru riscul la securitatea fizică

Acronim: I-SAFE

Semnificație: Internal Security Analysis of Factors & Exposure

Elaborator: Asociația pentru Reziliență, Evaluare și Securitate – ARES

Ediție: I

An: 2026

Domeniu: securitate fizică / identificarea factorilor interni / fundamentarea analizei riscului

Caracter: metodologie proprie ARES, cu caracter metodologic și profesional

REFERINȚE DE CADRU

La elaborarea și utilizarea metodologiei trebuie avute în vedere, în forma aplicabilă la data utilizării:

- Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, cu modificările și completările ulterioare;
- modificările aduse cadrului legal al analizei de risc la securitatea fizică prin OUG nr. 37/2026;
- HG nr. 301/2012 și normele metodologice aferente, în forma aplicabilă;
- Instrucțiunile MAI nr. 9/2013, în măsura și forma în care sunt aplicabile;
- ISO 31000:2018 – Risk management — Guidelines, ca referință generală în domeniul managementului riscului;
- IEC 31010:2019 – Risk management — Risk assessment techniques, ca referință generală privind tehnicile de evaluare a riscului.

Referirea la standardele internaționale nu implică faptul că metodologia I-SAFE este emisă, aprobată, certificată sau validată de ISO, IEC ori de o autoritate publică.

ARES I-SAFE · Ediția I · 2026

Asociația pentru Reziliență, Evaluare și Securitate – ARES

„Înainte de a evalua riscul, înțelege contextul care îl poate genera.”