română

FRONTEX

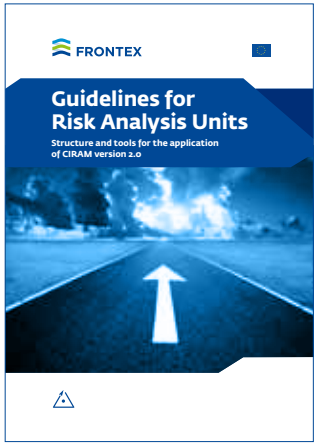
Model comun de analiză de risc integrată

Rezumat

Optimizat pentru vizualizare digitală

Versiunea 2.0

Numărul de referință: 17600 / 2013 ro



CIRAM-ul elaborat de Frontex este descris în două documente. Primul (stânga) descrie modelul general, în timp ce al doilea (dreapta) se axează pe implementarea sa practică, prezentând structura și instrumentele pentru aplicarea modelului. Această broșură este o sinteză a celor două documente.

Conținut

Introducere

Scopul Modelului Comun de Analiză de Risc integrată (CIRAM) este de a stabili o metodologie clară și transparentă pentru analiza de risc în vederea facilitării schimbului de informații și a cooperării eficiente în domeniul securității frontierelor. CIRAM dorește să promoveze un concept comun al analizei de risc și să contribuie la o mai mare coerență în ceea ce privește gestionarea frontierelor externe. În conformitate cu articolul 4 din Regulamentul Frontex dezvoltarea și punerea în aplicare a CIRAM este o obligație legală.

Articolul 4 din Regulamentul Frontex (CE 2007/2004)

Analiză de risc

Agenția elaborează și aplică un model comun de analiză integrată de risc La elaborarea trunchiului comun al planului de învățământ pentru formarea polițiștilor de frontieră Agenția folosește rezultatele modelului comun de analiză integrată de risc.

Ce înseamnă CIRAM?

Deși legiuitorul nu a furnizat definițiile termenilor, în elaborarea versiunii 2.0 s-au utilizat următoarele noțiuni:

„Comun" se referă la o metodologie, elaborată de statele membre și Frontex, care poate fi aplicată atât la nivel național, cât și la nivel UE.

„Integrat" se referă la obiectivul Frontex de a promova managementul integrat al frontierei asigurând un nivel ridicat și uniform al controlului și supravegherii frontierelor externe. O abordare integrată a analizei de risc asigură legătura cu alte organe / autorități cu atribuții de aplicare a legii la frontiere, cum ar fi autoritățile vamale, birourile / servicii de imigrare și poliția națională.

„Analiză de risc" se referă la examinarea sistematică a componentelor riscurilor în scopul informării factorilor de decizie.

„Model" se referă la un cadru analitic, care asigură un vocabular și o structură comună pentru analiza de risc în Statele Membre. Acesta nu este un algoritm care furnizează rezultate absolute.

Prezentarea generală a riscului

Pentru managementul frontierelor externe **riscul** este definit ca magnitudinea și probabilitatea de apariție a unei amenințări la frontierele externe, care ar avea un impact asupra securității interne a UE, asupra securității frontierelor externe, asupra fluxului optim de persoane la frontierele externe sau care ar avea consecințe umanitare, având în vedere măsurile existente la frontiere cât și în interiorul UE.

Astfel, în contextul managementului frontierelor externe, se poate considera că riscul are trei componente: (1) amenințarea care va fi evaluată din perspectiva magnitudinii și probabilității –, (2) vulnerabilitatea în raport cu amenințarea (nivelul și eficiența răspunsului la amenințare) – și (3) impactul – (impactul în cazul în care amenințarea devine reală, asupra securității interne a UE, asupra securității frontierelor externe, precum și impactul în domeniul umanitar și consecința asupra managementului eficace al trecerii de bună credință a frontierei).

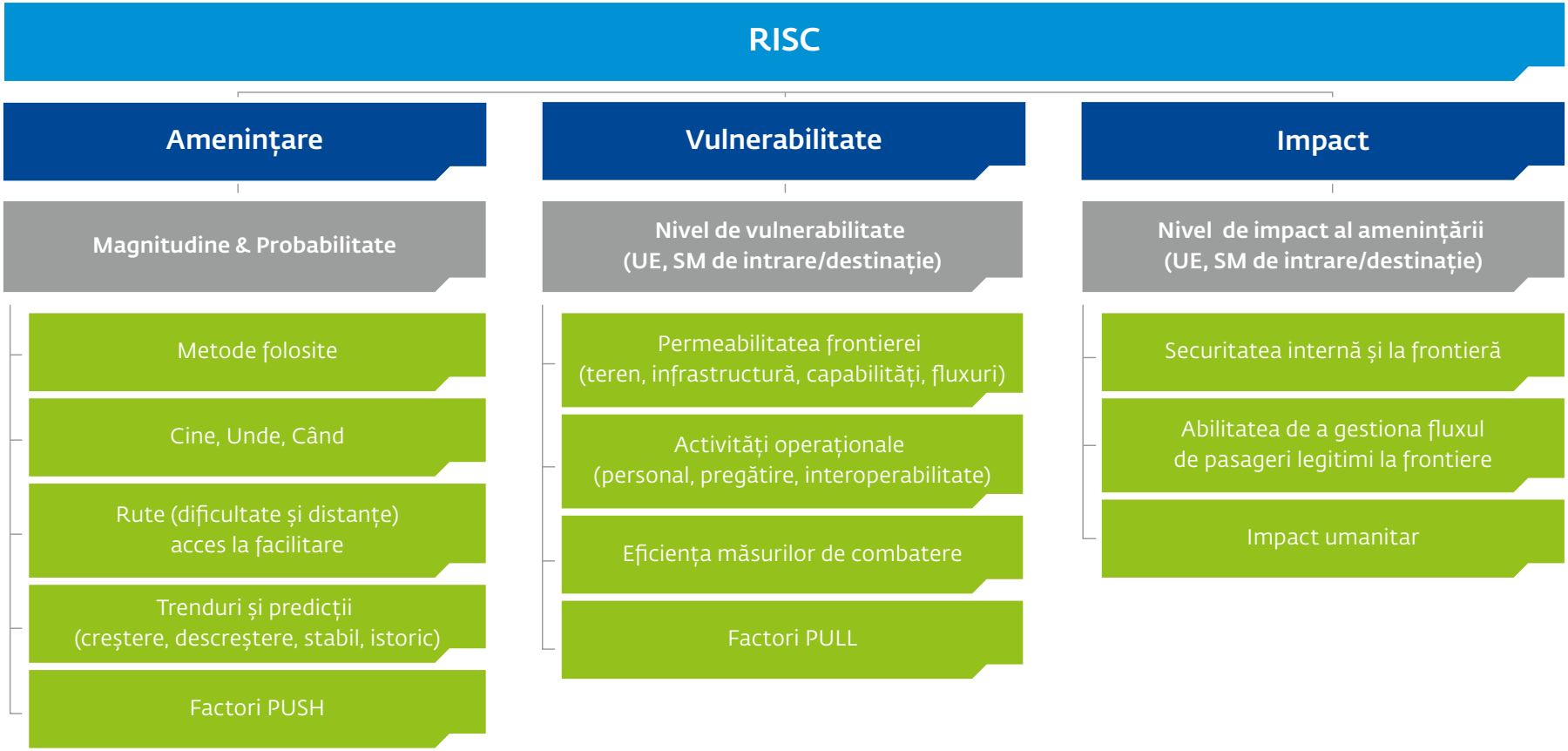
Cele trei componente nu sunt izolate și nu vor fi evaluate într-o ordine fixă, fiecare putând fi privită ca o perspectivă diferită din care poate fi studiat riscul. Evaluarea uneia dintre componente asigură materialul pentru evaluarea celorlalte două.

În ceea ce privește informarea factorilor de decizie analiza de risc implică o perioadă de referință – o zi, o săptămână, o lună sau un an. De exemplu, analiza de risc de la nivelul **punctelor de trecere a frontierei** (PTF) va fi elaborată pentru a facilita deciziile pe termen scurt, precum mobilizarea resurselor pentru ziua în curs sau săptămâna următoare, în timp ce analiza de risc care trebuie să vină în sprijinul procesului de luare a deciziilor la nivelul Consiliului de administrație al Frontex este realizată pe o perioadă de un an.

Riscurile sunt identificate și apoi evaluate în fucție de nivelul de amenințare, vulnerabilitate și impact, fiind ulterior comunicate factorilor de decizie. În timp ce analiștii sunt responsabili cu identificarea și evaluarea amenințării, factorii de decizie sunt responsabili, în cadrul competențelor lor de luare a deciziilor, cu gestionarea riscurilor.

Exemple: Analiștii strategici de risc din cadrul Frontex comunică riscurile Consiliului de administrație, astfel încât acesta să poată lua o decizie informată cu privire la alocarea bugetului anual în funcție de o varietate de riscuri. Analiștii de risc de la nivelul PTF comunică riscurile operaționale șefului PTF, astfel încât acesta să poată lua o decizie informată atunci când alocă personalul pentru control și supraveghere.

Definirea exactă a probabilității, prin utilizarea,de exemplu, a metodelor de determinare a acesteia, este adesea imposibilă. Cu toate acestea, este utilă folosirea constantă a aceluiași vocabular pentru a face referire la același nivel de probabilitate.


RISC
Amenințare
Magnitudine & Probabilitate
Metode folosite
Cine, Unde, Când
Rute (dificultate și distanțe)
acces la facilitare
Trenduri și predicții
(creștere, descreștere, stabil, istoric)
Factori PUSH
Vulnerabilitate
Nivel de vulnerabilitate
(UE, SM de intrare/destinație)
Permeabilitatea frontierei
(teren, infrastructură, capabilități, fluxuri)
Activități operaționale
(personal, pregătire, interoperabilitate)
Eficiența măsurilor de combatere
Factori PULL
Impact
Nivel de impact al amenințării
(UE, SM de intrare/destinație)
Securitatea internă și la frontieră
Abilitatea de a gestiona fluxul
de pasageri legitimi la frontiere
Impact umanitar

Amenințarea

Amenințarea este definită ca forța sau presiunea care acționează la frontierele externe. Se caracterizează prin magnitudine și probabilitatea de apariție a acesteia.

Identificarea amenințărilor presupune capacitatea de a centraliza, în cea mai potivită formă pentru factorii de decizie, datele și informațiile care au fost comunicate analiștilor sau colectate de aceștia. Există numeroase tehnici de identificare a amenințărilor iar unele dintre acestea se completează reciproc.

O descriere exhaustivă a tuturor amenințărilor ar fi prea lungă pentru a veni în sprijinul procesului de luare a deciziei. În mod empiric, este preferabil să se comunice factorilor de decizie între cinci și zece amenințări. În unele cazuri, se va avea în vedere o singură amenințare.

Descrierea unei amenințări include de obicei, descrierea modului de operare, obiectivele autorului infracțiunii, motivele și capabilitățile (cine, unde, când, câți), tendințele și predicțiile, factorii de tip „push" care îi influențează magnitudinea și probabilitatea.

Analiștii trebuie să le prezinte factorilor de decizie o anumită valoare a magnitudinii amenințării, astfel încât diferite amenințări să poată fi comparate și astfel să fie stabilite prioritățile. De exemplu, magnitudinea amenințării trecerii ilegale a frontierei de-a lungul frontierei externe diferă mult, de la câteva mii de treceri ilegale pe lună în timpul perioadei de criză în zona mediteraneană, până la mai puțin de 10 pe an de-a lungul anumitor secțiuni ale frontierei externe. În cazul în care măsurătorile exacte nu sunt posibile pot fi utilizate scale sau niveluri relative.

Deoarece scopul analizei este de a furniza informații pentru luarea deciziei, iar deciziile vor avea efecte în viitor, analiza amenințării are prin urmare un caracter anticipativ și trebuie să facă referire la o probabilitate pentru un interval de timp prestabilit. Evaluarea probabilității unei amenințări face parte din fluxul informațional care va sprijini procesul de luare a deciziilor.

De exemplu, analistul trebuie să specifice că amenințarea trecerii ilegale a frontierei între PTF X și PTF Y este foarte probabilă, date fiind dovezile din trecut și datele operative disponibile la momentul actual, în timp ce amenințarea este puțin probabilă între PTF Y și PTF Z. Aceste informații permit factorilor de decizie să aloce resurse în mod prioritar zonei cuprinse între PTF X și PTF Y.

Vocabular care evaluează probabilitatea unei amenințări

Nivelul de probabilitate	Măsurarea probabilității (de cele mai multe ori nu este posibilă)	Fraze care exprimă probabilitatea
Sigur	100% – sigur	Fără urmă de îndoială Fără îndoială
Aproape sigur	93% (plus/minus 6%)	Va fi Aproape sigur Foarte probabil Înalt grad de probabilitate Cu un grad foarte înalt de probabilitate
Probabil	75% (plus/minus 12%)	Posibil Probabil Probabilitate rezonabilă
Șanse aproape egale	50% (plus/minus 10%)	Șanse egale Probabilitate medie
Probabil că nu	30% (plus/minus 10%)	Puțin probabil Probabilitate mică Îndoielnic Foarte scăzut
Aproape sigur nu	7% (plus/minus 5%)	Practic imposibil Aproape imposibil Puține șanse Cu un grad mare de îndoială Foarte puțin probabil Extrem de puțin probabil Foarte puține șanse Improbabil Eventualitate scăzută Probabilitate foarte mică
Imposibil	0% – imposibilitate	Șanse zero Nul Nicio șansă

Vulnerabilitatea

Vulnerabilitatea este determinată de capacitatea unui sistem de a combate o amenințare.

Vulnerabilitatea nu înseamnă vulnerabilitatea grupurilor infracționale, care este o definiție des utilizată în literatura de specialitate, ci o descriere a nivelului capacității sistemelor instituite de a detecta sau preveni o amenințare.

Printre factorii principali care influențează vulnerabilitatea se numără caracteristicile geografice ale zonelor de frontieră, care pot varia de la zone de deșert până la zone urbane dense. De asemenea, este foarte important de știut dacă numărul membrilor personalului disponibili pentru supraveghere de-a lungul unei anumite secțiuni a frontierei, este de ordinul zecilor sau sutelor. Cunoașterea capacității existente îi permite analistului să determine motivele tendinței observate în datele colectate periodic. De exemplu, o creștere a numărului de treceri ilegale ale frontierei detectate se poate datora creșterii numărului de încercări ale migranților sau creșterii numărului de membri ai personalului care au capacitatea de a detecta migranții.

Vulnerabilitatea are legătură cu aspecte care pot fi adesea analizate cu atenție și pentru care se pot face estimări corecte în mod rezonabil, de exemplu pe baza registrelor de personal sau a inventarului echipamentelor la nivelul PTF. În practică, este posibil ca simple indicații cu privire la modificarea în timp să fie suficiente pentru a indica direcția în care se îndreaptă măsurile puse în aplicare.

Analiștii ar trebui să dispună de instrumentele necesare pentru a le indica factorilor de decizie care sunt cele mai vulnerabile secțiuni ale frontierei pentru fiecare amenințare în parte, astfel încât să existe posibilitatea unui răspuns rapid în cazul evenimentelor. În mod similar, factorii de decizie trebuie să înțeleagă terminologia utilizată de analiști pentru a evalua nivelul de vulnerabilitate. Prin urmare, este important ca analistul să definească diferitele niveluri de vulnerabilitate, asemenea exemplului de mai jos.

Exemplu de estimări calitative ale nivelului de vulnerabilitate pentru diferite aspecte de vulnerabilitate

Nivel	Permeabilitatea frontierei	Capacități operaționale și răspunsuri legale	Factori de tip „pull”: comunități extinse în statele membre, ușurința percepută a accesului fraudulos la protecția internațională și prestațiile sociale
Vulnerabilitate foarte mare	Terenul sau condițiile naturale ale frontierelor externe sunt exploatate de amenințare	Nu sunt disponibile competențe sau răspunsuri legale pentru abordarea acestei amenințări	Toți acești factori sunt prezenți
Vulnerabilitate mare	Terenul sau condițiile naturale ale frontierelor externe sunt favorabile pentru această amenințare	Un număr foarte limitat de competențe sau răspunsuri legale este disponibil pentru abordarea acestei amenințări	Mai mulți dintre acești factori sunt prezenți
Vulnerabilitate medie	Terenul sau condițiile naturale nu condiționează dezvoltarea acestei amenințări	Un număr moderat de competențe sau răspunsuri legale este disponibil pentru abordarea acestei amenințări	Unul din acești factori este prezent
Vulnerabilitate scăzută	Terenul sau condițiile naturale împiedică dezvoltarea acestei amenințări	Un număr suficient de competențe sau răspunsuri legale este disponibil pentru abordarea acestei amenințări	Niciunul din acești factori nu este prezent

Impactul

Impactul este definit de efectele unei amenințări asupra securității interne și a securității la frontierele externe. De asemeanea, impacturile pot fi analizate din perspectiva efectelor asupra fluxului optim de persoane la frontieră precum și în funcție de consecințele umanitare.

Menținerea securității frontierei și a securității interne a UE, constituie rațiunea principală a activității Frontex și a autorităților cu atribuții în ceea ce privește frontiera din statele membre. Riscurile sunt ulterior evaluate, în funcție de impactul lor asupra frontierei și securității interne.

O parte din evaluare include o analiză a impactului asupra capacității de a gestiona fluxul de persoane, pentru a asigura niveluri optime ale acestuia conform prevederilor Codului Frontierelor Schengen.

De asemenea, polițiștii de frontieră sunt adesea primele autorități care iau contact cu persoanele care necesită asistență internațională. Drepturile fundamentale stau la baza activităților operaționale și de analiză ale Frontex și, astfel, impactul umanitar al riscurilor identificate de Unitatea de Analiză de Risc, este analizat cu atenție.

În cazul în care nu sunt disponibile evaluări cantitative sau calitative, impactul poate fi măsurat pe baza descrierii rezultatelor analizei inductive („estimare avizată") sau ale analizei scenariilor. Ca în cazul unui alt tip de evaluări, este util să se definească în mod clar nivelul diferit de impact utilizat în evaluare.

Exemple de estimări calitative ale nivelului de impact aferente migrației ilegale:

Impact	Critic	Foarte Important	Important	Scăzut
Pierdere de vieți omenești	Viețile omenești sunt expuse riscurilor de un număr foarte mare de evenimente (de exemplu, >75%)	Viețile omenești sunt expuse riscurilor de un număr mare de evenimente (de exemplu, 20%<x<75%)	Viețile omenești sunt expuse riscurilor de un număr moderat de evenimente (<20%)	Viețile omenești nu sunt afectate

Evaluarea riscului

Este posibil ca exprimarea numerică a nivelului de risc, de exemplu în procente, să transmită factorilor de decizie un fals sentiment de exactitate. Estimările cantitative ale nivelurilor de risc se aplică doar în cazuri particulare, în care este disponibilă o cantitate mare de date și rezultatele pot fi validate de-a lungul timpului. În ceea ce privește managementul frontierelor, acesta nu face, cel mai probabil, obiectul acestor estimări, iar analiștii trebuie să se bazeze în primul rând pe descrieri calitative ale riscurilor.

În majoritatea cazurilor, se recomandă să se recurgă la evaluări calitative și clasificarea riscurilor în categorii de importanță. Analistul are responsabilitatea de a alege numărul de niveluri de risc și de a-și documenta opiniile cu privire la risc.

Nivelurile de risc pot fi descrise utilizând o terminologie variată, dar exemplele de mai jos furnizează câteva recomandări. Descrierile nivelurilor de risc sunt un rezultat important al procesului de analiză și sunt esențiale pentru sprijinirea procesului de luare a deciziei. Analiștii trebuie să țină cont de faptul că activitatea lor influențează deciziile și trebuie să facă tot posibilul pentru ca descrierile și explicațiile să fie cât mai clare.

Exemple de trei niveluri de risc

Nivelul de risc	Descriere
Scăzut	Risc acceptabil. Impactul poate fi gestionat, iar vulnerabilitatea este acceptabilă, dar amenințările trebuie monitorizate pentru a descoperi schimbările ce ar putea duce la creșterea nivelului de risc.
Mediu	Risc tolerabil, dar impactul nu este ușor de gestionat având în vedere capacitățile actuale. O mică creștere a magnitudinii amenințării ar putea pune în pericol eficiența răspunsului. Dezvoltarea amenințării trebuie monitorizată continuu, analizând dacă este necesar să se aplice și alte măsuri.
Ridicat	Risc neacceptabil. Impacturile nu pot fi gestionate adecvat având în vedere capacitățile existente și înainte ca tratamentul de reducere a riscului să fie implementat.

Colectarea datelor și a informațiilor

Eficacitatea analizei de risc depinde de accesul la un volum suficient de date și informații. Colectarea datelor / informațiilor reprezintă un efort de cooperare între unitățile analitice și alte entități care colectează date. Datele / informațiile pot fi primite din surse variate și pot fi date clasificate sau date disponibile publicului.

Datele (metrice) sunt cel mai adesea utilizate pentru a descrie tiparul și tendința într-o evaluare a amenințării, precum și magnitudinea amenințării, dar pot fi, de asemenea, incluse în evaluarea vulnerabilității sau a unui impact.

La nivel național, sursele potențiale de date rapid accesibile sunt:

- baze de date specializate, precum VIS, SIS, Eurodac;
- baze de date în care se înregistrează fluxul de persoane;
- evidența numărului de polițiști de frontieră.

La nivelul Frontex, începând din anul 2008, Rețeaua Frontex a Unităților de Analiză de Risc a colectat lunar date cu privire la: detecții de treceri ilegale a frontierei între PTF-uri, detecții de intrare clandestină prin PTF-uri, detecții de persoane suspecte de a fi facilitatori, detecții de ședere ilegală, refuzuri ale intrării, cereri de azil, detecții de documente false, decizii de returnare emise, returnări efective.

Informațiile (date non-metrice) sunt esențiale pentru identificarea și caracterizarea riscurilor, amenințărilor, vulnerabilității și impacturilor.

La nivel național, sursele potențiale de informații rapid accesibile sunt:

- baze de date naționale în care se înregistrează informațiile cu privire la persoane (țara de origine, motivul vizitei, informațiile de călătorie, tipul de vehicul cu care trece frontiera etc.)
- baze de date din domeniul aplicării legii, inclusiv baze de date care înregistrează persoanele căutate, cazierul judiciar, declarațiile date de persoanele reținute, informații prelucrate, documente furate etc.
- rapoarte care furnizează analize sau tablouri situaționale și surse deschise.

La nivelul Frontex, începând din 2008, Rețeaua Frontex a Unităților de Analiză de Risc a colectat de două ori pe lună rapoarte analitice care furnizează statelor membre rezumate cu privire la patru subiecte: țările terțe, situația la frontieră, șederea ilegală pe teritoriul UE, modificările instituționale la nivel național.

Sistemul de clasificare a evaluării informațiilor

Se utilizează multe sisteme de evaluare a informațiilor, dar cel mai frecvent este sistemul de evaluare a informațiilor tip 4×4. În cadrul acestui sistem, informațiile / datele sunt evaluate pe baza a două dimensiuni, prima fiind credibilitatea sursei informațiilor / datelor, iar a doua valabilitatea informațiilor / datelor. Aceste două dimensiuni sunt evaluate pe baza unei scale cu 4 niveluri, după cum urmează:

Evaluarea credibilității sursei

Clasificare	Descriere
A	Nu există nicio îndoială cu privire la autenticitatea, credibilitatea și competența sursei; dacă informațiile sunt furnizate de o sursă care, în trecut, s-a dovedit a fi de încredere în toate situațiile
B	O sursă care a furnizat informații, care s-au dovedit a fi de încredere în majoritatea situațiilor
C	O sursă care a furnizat informații, care s-au dovedit a nu fi de încredere în majoritatea situațiilor
X	Credibilitatea sursei nu poate fi evaluată

Evaluarea valabilității informațiilor/datelor

Clasificare	Descriere
1	Informație a cărui exactitate nu este pusă la îndoială și de multe ori este confirmată de alte surse
2	Informație cunoscută personal de sursă, dar care nu este cunoscută personal de funcționarul care o transmite mai departe și este probabil adevărată
3	Informație care nu este adevărată
4	Informație care este necunoscută faptic

De exemplu, informațiile provenite de la o sursă sigură (clasificată ca fiind de nivel A) și evaluate ca fiind corecte (clasificate ca fiind de nivel 1), vor fi numite informații „A1". Informațiile furnizate de o sursă care nu poate fi evaluată și care sunt necunoscute faptic, vor fi numite informații „X4".

Exemple de produse dezvoltate de Unitatea Frontex de Analiză de Risc

ARA – Analiza de risc anuală

Raport anual cu privire la situația migrației ilegale în anul precedent, perspective și recomandări de viitor folosite în sprijinul planificării activităților operaționale ale Frontex pentru anul următor.

SARA – Analiza de risc semestrială

Actualizare semestrială a ARA, inclusiv, dacă este necesar, evaluarea și ajustarea recomandărilor.

FRAN trimestrial

Raport trimestrial care furnizează feedback și analiza tendințelor de migrație ilegală, pe baza schimbului de informații din cadrul FRAN.

TRA – Analiza de risc specifică

Raport analitic care se concentrează pe un fenomen sau o zonă geografică specifică; de exemplu, migrația ilegală a populației din Irak în UE sau impactul crizei financiare asupra migrației ilegale în UE.

TFA – Evaluarea tactică specifică

Raport analitic care sprijină planificarea unei operațiuni comune specifice.

WAR – Raport analitic săptămânal

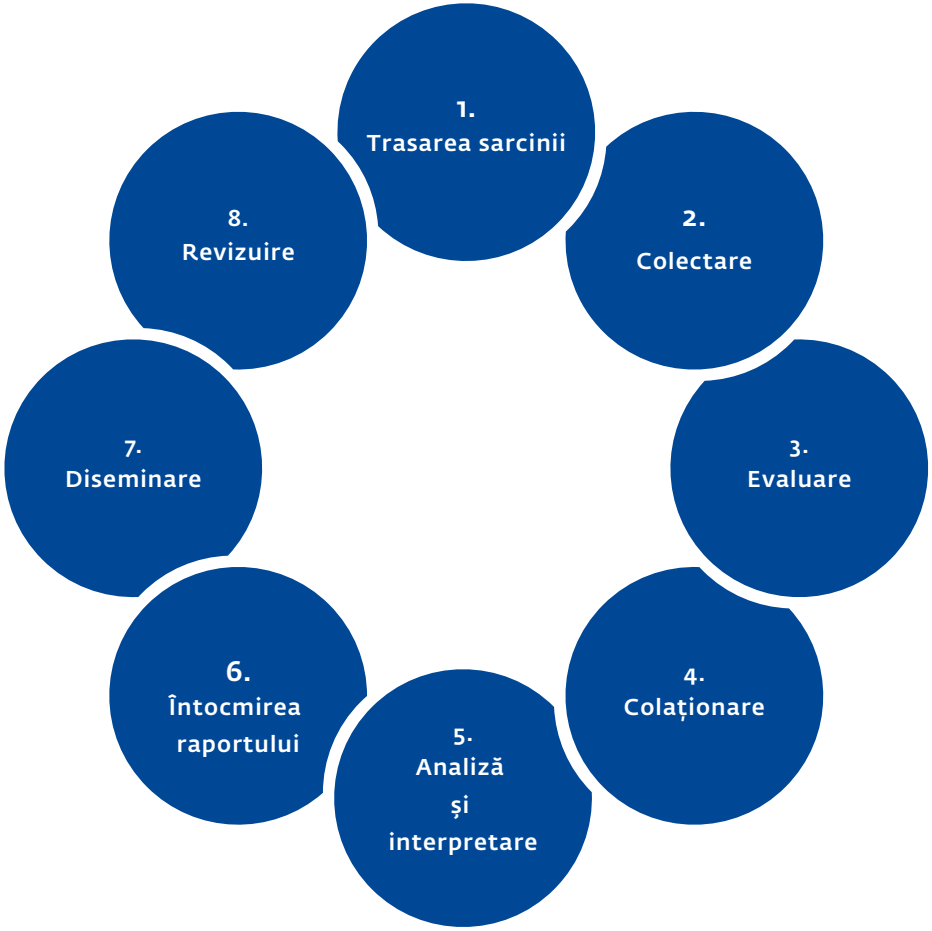
Analiză săptămânală a informațiilor colectate în timpul unei anumite operațiuni comune, pentru echipa operațională și autoritățile statului gazdă.

Ciclul informațional

Informațiile prelucrate constituie baza analizei de risc, fiind definite ca orice informații, primite sau transmise, care au legătură cu una din componentele riscului, respectiv, o amenințare, o vulnerabilitate sau un impact.

În contextul controlului de frontieră, informațiile prelucrate se referă cu precădere la informațiile referitoare la anumite evenimente legate de trecerea frontierei (în special activități ilegale), care pot fi utilizate în scopuri operaționale. ‚Exemple de informații prelucrate privind securitatea frontierei ar putea fi informații despre migranți care intenționează să treacă ilegal frontiera sau informații despre anumite transporturi de droguri.

Procesul de structurare a informațiilor prelucrate este numit ciclu informațional. Acesta este un ciclu care poate fi definit și care asigură eficacitatea activităților de aplicare a legii prin intermediul unui sistem de verificări și echilibrări.



Înființarea unității de analiză de risc în statele membre

Fiecare stat membru este încurajat să înființeze și să mențină o unitate de analiză de risc.

Funcția unei unități de analiză de risc este de a colecta informații referitoare la securitatea frontierei și în sens mai general, securitatea internă a UE. În aceste scopuri, unitățile de analiză de risc vor elabora și disemina rapoarte și evaluări analitice. Acestea vor cuprinde tendințele generale sau specifice, rutele, modurile de operare și mijloacele de transport utilizate pentru activități infracționale și posibila implicare a rețelelor de crimă organizată.

Unitățile de analiză de risc au responsabilitatea de a transmite informații despre care se presupune că pot avea un impact în afara frontierelor Statelor Membre, atât asupra Frontex, cât și asupra statelor membre afectate. Cooperarea este indispensabilă pentru gestionarea eficace a frontierelor externe.

Managementul eficient al unității de analiză de risc este esențial pentru calitatea activităților analitice. Astfel, conducătorii unităților de analiză de risc au o serie de responsabilități de conducere, care cuprind printre altele:

- direcționarea și gestionarea resurselor;
- menținerea relațiilor cu alte agenții / departamente interesate;
- îndeplinirea rolului de punct de legătură între autoritățile naționale și internaționale;
- asigurarea coeziunii, cooperării și schimbului de informații / informații prelucrate;
- contribuția la planificarea activităților și stabilirea priorităților;
- dezvoltarea de soluții pentru eventuale probleme sau deficiențe;
- actualizarea și modificarea metodelor de lucru ale unității;
- asumarea altor inițiative care pot îmbunătăți funcționarea unității de analiză de risc.

Tehnici de evaluare

O gamă diversă de tehnici de evaluare poate fi utilizată pentru diferite scopuri analitice. Alegerea tehnicii depinde de datele și informațiile disponibile, de nivelul factorului de decizie care trebuie să fie informat și de timpul acordat pentru efectuarea analizei, precum și de gradul de familiarizare a analistului cu tehnicile. Câteva din metodele cele mai utilizate și mai polivalente sunt descrise mai jos, pentru a servi drept îndrumare, dar lista nu este exhaustivă. Analiștii trebuie să aleagă tehnica pe care o cunosc cel mai bine și prin care au obținut anterior cele mai bune rezultate. Diferitele tehnici pot fi aplicate pentru a crea diverse produse analitice, de exemplu evaluări ale amenințării, vulnerabilității sau ale impactului.

Brainstorming: aceasta este o tehnică de imaginație aplicată care implică stimularea conversației libere în cadrul unui grup de specialiști. Accentul semnificativ pe care această tehnică îl pune pe imaginație și pe influențarea reciprocă a ideilor face ca aceasta să fie deosebit de utilă în situații în care nu există date disponibile sau în care se dorește renunțarea la un mod de gândire predominant.

Solicitarea de opinii calificate: această metodologie asigură o cale de a implica în mod structural experții în domeniile principale de interes pentru securitatea frontierei (migrație ilegală, infracționalitate și terorism). Aceasta cuprinde o abordare nuanțată care vizează extinderea fondului de cunoștințe și este în principal calitativă prin natura sa. Anumite metode cantitative pot fi combinate (de exemplu, cerându-le experților să clasifice amenințările).

Analiza tiparelor și a tendințelor: o abordare care poate combina diferite instrumente. Accesul la date istorice (statistici cu privire la evenimentele anterioare) este important pentru această metodologie.

Sondaje: acestea se concentrează în principal pe analiza vulnerabilităților (utilizând o abordare științifică pentru a extrapola cu privire la numărul total de persoane pe baza tehnicilor de capturare / recapturare. De exemplu numărul de infractori care trec frontiera capturați în raport cu numărul total de infractori care trec frontiera în perioada respectivă. De asemenea, aceste informații sunt utile pentru analiza amenințărilor.

Glosar de termeni-cheie

Analiză: studiul riscului, al amenințării, al vulnerabilității sau al impactului, care duce la identificarea, descrierea și evaluarea acestora.

Evaluare: opinia analistului cu privire la importanța riscurilor, amenințării, vulnerabilității sau a impactului identificat.

Frontiere externe: se referă la frontierele statelor membre ale UE cu statele care nu sunt membre ale UE. Prin extensie, se referă, de asemenea, la frontierele dintre statele asociate la Acordul Schengen și statele care nu sunt membre UE. De exemplu, frontiera dintre Polonia și Ucraina este o frontieră externă și prin extensie, frontiera dintre Norvegia și Rusia este, de asemenea, o frontieră externă. În schimb, frontiera dintre Suedia și Norvegia sau cele dintre Franța și Regatul Unit (pe cale feroviară), Ungaria și România sau Spania și Portugalia, nu sunt frontiere externe.

Impact: impactul este definit de efectele unei amenințări asupra securității interne și a securității la frontierele externe. Impacturile pot fi analizate luând în calcul efectele asupra fluxului optim de persoane la frontieră, și în funcție de consecințele umanitare.

Indicator: acesta se referă la un element unic de date care acționează ca reper sau indiciu, care exprimă o sugestie, condiție sau stare. De exemplu, un indicator poate sugera un eveniment specific sau o activitate în curs de desfășurare sau un set de condiții pentru producerea evenimentului respectiv sau poate sugera posibile intenții ale unei ținte. Pentru a fi utili și convingători, indicatorii sunt cel mai bine dezvoltați, colectați și evaluați ca „seturi”.

Informație: material neevaluat de orice tip, inclusiv care provine din observații, rapoarte, presupuneri și zvonuri, fotografii și alte surse, care după ce sunt preluctate, pot produce informații prelucrate.

Informație prelucrată: orice informații primite sau transmise, care au legătură cu una din componentele riscului, respectiv cu o amenințare, vulnerabilitate sau impact. Mai precis, în contextul controlului de frontieră, informațiile prelucrate (intelligence) se referă, în mod normal, la informații despre anumite evenimente de trecere a frontierei (în special, activități ilegale) care pot fi utilizate în scopuri operaționale.

Risc: pentru managementul frontierelor externe, riscul este definit ca magnitudinea și probabilitatea de apariție a unei amenințări la frontierele externe, care ar avea un impact asupra securității interne a UE, asupra securității frontierelor externe, asupra fluxului optim de persoane la frontierele externe sau care ar avea consecințe umanitare, având în vedere măsurile existente la frontiere cât și în interiorul UE.

Unitatea de Analiză de Risc (UAR): reprezintă,în cadrul managementului frontierelor externe, o unitate organizațională (celulă, secțiune etc.) care este însărcinată cu desfășurarea activităților aferente analizei de risc, pentru a asigura informarea conducerii cu alerte / evaluări / rapoarte de risc, privitoare la aspecte care au legătură cu securitatea frontierei, migrația ilegală, traficul de persoane și contrabanda.

Traficul de migranți: spre deosebire de definiția traficului de persoane și conform definiției din Convenția ONU împotriva criminalității organizate transnaționale (denumită ONU CRT), termenul de „trafic de migranți" se referă în general la tranzacția consensuală în care un transportator și persoana transportată sunt de acord să evite controlul de imigrație din motive reciproc avantajoase.

Traficul de persoane: pe scurt, traficul de persoane este comerțul ilegal de persoane în scopul exploatării sexuale comerciale și / sau muncii silite. Convenția ONU CRT definește pe larg traficul de persoane.

Amenințarea este definită ca forța sau presiunea care acționează la frontierele externe. Trebuie caracterizată prin magnitudine și probabilitatea de apariție. Analistul trebuie să descrie care din procesele sau factorii, atât de pe teritoriul UE, cât și din afara teritoriului UE, influențează magnitudinea și probabilitatea amenințării.

Vulnerabilitatea este determinată de capacitatea unui sistem de a combate / răspunde la o amenințare. Vulnerabilitatea se referă la factorii de la frontieră sau de pe teritoriul UE care pot mări sau reduce magnitudinea și probabilitatea amenințării.

FRONTEX

Agenția Europeană pentru
Gestionarea Cooperării Operative
la Frontierele Externe ale Statelor Membre
ale Uniunii Europene

Rondo ONZ 1
00-124 Varșovia, Polonia
T +48 22 205 95 00
F +48 22 205 95 01

frontex@frontex.europa.eu
www.frontex.europa.eu

Unitatea de Analiză de Risc

Numărul de referință: 17600/2013 ro

Varșovia, Noiembrie 2013