English

FRONTEX

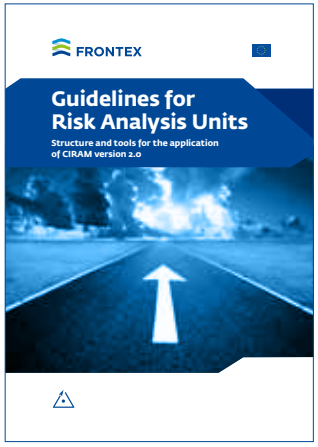
Common Integrated Risk Analysis Model

Summary booklet

Optimised for screen viewing

version 2.0

Reference number: 17600 / 2013 en



The Common Integrated Risk Analysis Model (CIRAM) developed by Frontex is described in two documents. The first (left) describes the overall model, while the second (right) focuses on its practical implementation by outlining the structure and tools for the application of the model. This booklet is a summary of these two documents.

Contents

Introduction

The purpose of the Common Integrated Risk Analysis Model (CIRAM) is to establish a clear and transparent methodology for risk analysis in order to facilitate efficient information exchange and cooperation in the field of border security. The CIRAM seeks to promote a common understanding of risk analysis and contribute to greater coherence in the management of the external borders. The development and implementation of the CIRAM is a legal obligation according to Article 4 of Frontex's regulation.

Article 4 of Frontex regulation (EC 2007/04)

Risk analysis

The Agency shall develop and apply a common integrated risk analysis model. It shall prepare both general and tailored risk analyses to be submitted to the Council and the Commission. The Agency shall incorporate the results of a common integrated risk analysis model in its development of the common core curriculum for border guards' training.

What does CIRAM mean?

While the legislator did not provide definition of the terms, the following understanding has been used to develop version 2.0:

"Common" refers to a methodology, developed by Member States and Frontex, which can be applied both at national and EU level.

"Integrated" refers to Frontex's aim to promote integrated border management ensuring a uniform and high level of control over the external borders. An integrated approach to risk analysis offers a bridge with other law-enforcement bodies / authorities active at the borders and other authorities dealing with migration issues, such as customs authorities, immigration offices and national police.

"Risk Analysis" refers to the systematic examination of components of risks to inform decision-making.

"Model" refers to an analytical framework which provides a common vocabulary and structure for risk analysis in Member States. It is not an algorithm providing absolute outcomes.

Overview of risk

For the management of the external borders, **risk** is defined as the magnitude and likelihood of a threat occurring at the external borders, given the measures in place at the borders and within the EU, which will impact on the EU internal security, on the security of the external borders, on the optimal flow of regular passengers or which will have humanitarian consequences.

Risk in the context of the management of the external borders can thus be viewed as having three components: (1) the threat that will be assessed in terms of magnitude and likelihood; (2) the vulnerability to the threat – in other words the level and efficiency of response to the threat; and (3) the impacts – in other words the impacts, should the threat occur, on the EU internal security, on the security of the external borders, as well as the humanitarian impacts and the bearing on the efficient management of bona fide border crossing.

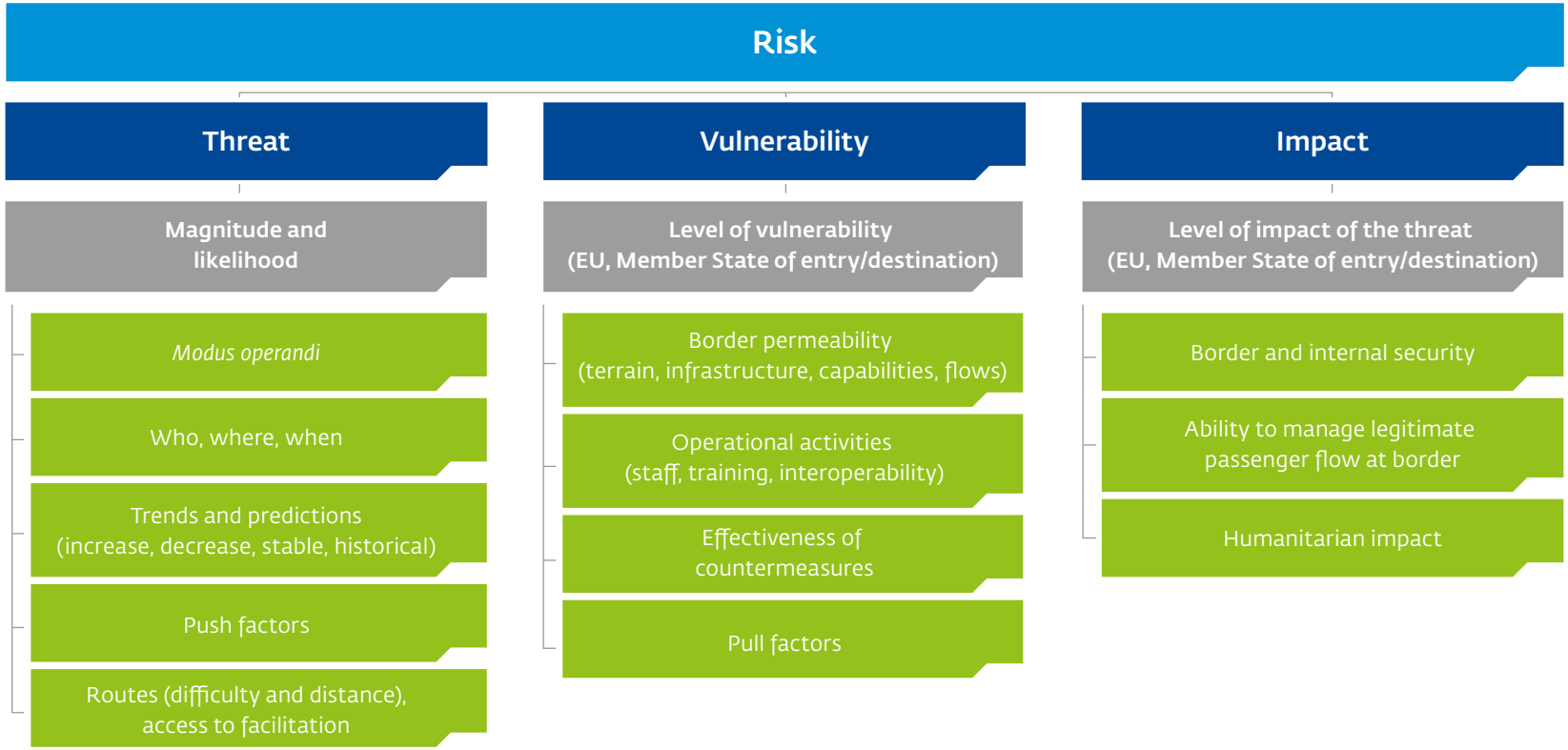
The three components are not isolated, and are not to be assessed in rigid sequence. Rather, each component is seen as a different angle from which to study the risk, the assessment of one component providing material for the assessment of the other two components.

Risk analysis implies a reference period – a day, a week, a month or a year – consistent with the level of decision-making it is to inform. For example, risk analysis at BCP level will be developed in order to facilitate short-term decisions, such as the mobilisation of resources for the day or the week ahead, while risk analysis to inform the decision process of the Frontex Management Board will have an annual timeframe.

Risks are identified and assessed, in view of their level of threat, vulnerability and impact, and then communicated to the decision-makers. While the analysts are responsible to identify and assess the threat, decision-makers are responsible, within the remit of their decision-making capacities, to manage the risks.

Example: Frontex's strategic risk analysts communicate risks to the Management Board, so that it can take informed decisions about annual budget allocation among a variety of risks. Risk analysts at border crossing point (BCP) level communicate operational risks to the head of the BCP, so that he or she can take informed decisions when allocating staff for controls and surveillance.

Defining likelihood precisely, for example by using probability methods, is often not possible. However, it is useful to consistently use the same vocabulary to refer to similar state of likelihood.


Risk
Threat
Vulnerability
Impact
Magnitude and likelihood
Level of vulnerability (EU, Member State of entry/destination)
Level of impact of the threat (EU, Member State of entry/destination)
Modus operandi
Who, where, when
Trends and predictions (increase, decrease, stable, historical)
Push factors
Routes (difficulty and distance), access to facilitation
Border permeability (terrain, infrastructure, capabilities, flows)
Operational activities (staff, training, interoperability)
Effectiveness of countermeasures
Pull factors
Border and internal security
Ability to manage legitimate passenger flow at border
Humanitarian impact

Threat

Threat is defined as a force or pressure acting on the external borders. It is to be characterised by its magnitude and likelihood.

Identifying threats means being able to summarise, in the most appropriate form for decision-making, the data and information that have been communicated to or collected by the analysts. There are many techniques to identify threats and several techniques complement each other.

An exhaustive description of all threats would be too long to assist decision-making. As a rule of thumb, it is preferable to communicate to decision-makers between five and ten threats. Sometimes, only one threat will be considered.

The description of the threat typically includes the description of the *modus operandi*, the perpetrator's goals, motives and capabilities (who, where, when, how many), the trends and predictions, the push factors affecting its magnitude and likelihood.

The analysts should provide the decision-makers with some measurement of the magnitude of the threat, so that different threats can be compared and priorities can be established. For example, the magnitude of the threat of illegal border-crossing along the external borders varies widely, from several thousands per month during crisis periods in the Mediterranean area, to less than ten per year along some sections of the external border. When precise measurements are not possible, relative scales or levels can be used.

As the purpose of the analysis is to inform decision-making so that the decisions will have effects in the future, the analysis of the threat is by nature forward-looking and should make reference to a likelihood for a given time horizon. Assessing the likelihood of a threat is part of the information that will help making decisions.

For example, the analyst should state that the threat of illegal border-crossing between BCP X and BCP Y is very likely, given evidence from the past and intelligence currently available, whereas it is unlikely between BCP Y and BCP Z. This information enables decision-makers to allocate resources as well as to the area between BCP X and BCP Y as a priority.

Vocabulary assessing the likelihood of a threat

State of likelihood	Measures of probability (often not available)	Phrases of likelihood
Certain	100% – certainty	Without a shadow of doubt No doubt
Almost certain	93% (give or take 6%)	Will Virtually certain Highly likely High degree of probability Extremely high probability
Probable	75% (give or take 12%)	Likely Probable Reasonable likely
Chances about even	50% (give or take 10%)	Equal chance Medium probability
Probably not	30% (give or take 10%)	Unlikely Low probability Doubtful Slim
Almost certainly not	7% (give or take 5%)	Virtually impossible Almost impossible Slight chance Highly doubtful Very unlikely Highly unlikely Extremely unlikely Little prospect Improbable Remote possibility Extremely low probability
Impossible	0% – impossibility	Zero chance Nil No chance

Vulnerability

Vulnerability is determined by the capacity of a system to mitigate a threat.

Vulnerability is not the vulnerability of the criminal groups, which is a definition often used in criminal intelligence literature. It is rather a description of the degree of ability of the systems in place to detect or prevent a threat.

Among the prime factors that will affect the vulnerability are the geographical attributes of the border areas, which may vary from desert areas to dense urban areas. It is also important to know if the number of staff available for surveillance along a particular border section is in the range of tens or hundreds. Knowing the capacity in place enables the analyst to determine the reasons for trends observed in regularly collected data. For example, an increase in detections of illegal border-crossing may be due to an increase in the number of attempts by migrants, or due to an increase in the number of staff able to detect the migrants.

Vulnerability concerns matters that can often be carefully studied and for which estimate can be reasonably accurate, for example by relying on staff records or on the inventory of equipment at BCP level. In practice, simple indications of change over time may suffice to indicate in which direction the measures in places are evolving.

The analysts should have the tools to indicate to decision-makers which border sections are most vulnerable to specific threats so as to enable a swift response to events. Similarly, the decision-makers should understand the vocabulary used by the analyst to assess the level of vulnerability. It is therefore important that the analyst defines the different levels of vulnerability, as in the example proposed below.

Example of qualitative estimates of level of vulnerability for different aspects of vulnerability

Level	Border permeability	Operational capacities and legal responses	Pull factors: High unemployment rate, large communities in Member States, perceived easy fraudulent access to international protection and social welfare benefits
Very High Vulnerability	Terrain or natural conditions of the external borders are exploited by the threat	No competencies or legal responses are available to address this threat	All these factors present
High Vulnerability	Terrain or natural conditions of the external borders are favourable to this threat	A very limited number of competencies or legal responses are available to address this threat	Several factors present
Medium Vulnerability	Terrain or natural conditions do not condition the development of this threat	A moderate number of competencies or legal responses are available to address this threat	One of these factors present
Low Vulnerability	Terrain or natural conditions prevent the development of this threat	Sufficient numbers of competencies or legal responses are available to address this threat	None of these factors present

Impact

Impact is defined as the effects of a threat on the internal security and on the security of the external borders. Impacts can also be analysed in terms of their effects on the optimum passenger flow at the borders, and in terms of their humanitarian consequences.

Maintaining the border and internal security of the EU is the primary rationale that underpins the work of Frontex and Member States' border authorities. Risks are consequently assessed by their impact on the border and internal security.

The assessment includes an appraisal of the impact on the ability to manage passenger flow in order to ensure optimal flow levels of persons crossing the border, as stipulated in the Schengen Borders Code.

Border guards are also often the first authorities in contact with the person in need of international assistance. Fundamental rights guide and inform Frontex's operational and analysis activities and as such the humanitarian impact of risks identified by the Risk Analysis Unit is carefully considered.

If quantitative or qualitative assessments are not available, impact can be measured through the description of outcomes arising from inductive analysis ('educated guess') or scenario analysis. As in other types of assessment, it is useful to clearly define the different level of impact used in the assessment.

Example of qualitative estimates of level of impact related to illegal migration

Impact	Critical	Very Important	Important	Low
Loss of human lives	A majority of instances (e.g. >75%) put human lives at risk protection	A high number of instances (e.g. 20%<x<75%) put human lives at risk	A moderate number of instances put human lives at risk (<20%)	Does not affect human lives

Assessment of risk

Expressing the risk level numerically, for instance in percentages, is likely to convey a false sense of precision to the decision-makers. Quantitative estimates of risk levels will only apply for particular cases where a large amount of data is available and outcomes can be validated over time. In the case of border management this is most likely not the case and analysts should primarily rely on qualitative descriptions of risks.

In most cases, it is recommended to rely on qualitative assessments and to classify risks in categories of significance. It is the responsibility of the analyst to choose the number of levels of risk and document her / his judgements on risk.

Levels of risks can be described with varying terminology, but the examples below provide some advice. Descriptions of risk levels are a key outcome of the risk analysis process and are vital in aiding the decision-making process. Analysts should keep in mind that their work influences decisions and should strive for as much clarity in describing and explaining risks as possible.

Example of three risk levels

Level of risk	Description
Low	Acceptable risk. The impact can be dealt with, and the vulnerability is acceptable, but the threats must be monitored to discover changes that could increase the risk level.
Medium	Tolerable risk, but the impact is not easily dealt with given current capacity in place. A small increase of the magnitude of the threat could jeopardise the effectiveness of the response. The development of the threat must be monitored on a regular basis, with consideration to whether necessary measures have to be implemented.
High	Not acceptable risk. The impacts cannot be dealt with adequately with the given capacities and before risk reducing treatment has been implemented.

Data and information collection

To be effective, risk analysis depends upon having access to sufficient data and information. Data / information collection is a co-operative effort between the analytical units and other entities gathering the data. Data / information may be received from a variety of sources and may be restricted or publicly available.

Data (metric) are most often used to describe patterns and trends in a threat assessment, as well as the magnitude of a threat, but can also be included as part of a vulnerability assessment or an impact assessment.

At national level, potential sources of readily-available data include:

- specialised databases such as VIS, SIS, Eurodac;
- databases recording passenger flow;
- records of numbers of officers.

At Frontex level, since 2008, the Frontex Risk Analysis Network has been collecting data on a monthly basis regarding: detections of illegal border-crossing between BCPs, detections of clandestine entry at BCPs, detections of suspected facilitators, detections of illegal stay, refusals of entry, asylum applications, detections of false documents, return decisions issued, and effective returns.

Information (non-metric data) is essential to identify and characterise risks, threats, vulnerability and impacts.

At national level, potential sources of readily-available information include:

- national databases recording passenger information (country of origin, reason for arriving, travel information, type of vehicle when crossing the border, etc.;
- law-enforcement databases including those of wanted persons, criminal records, records of apprehended persons, intelligence, stolen documents, etc.;
- reports providing analysis or situational pictures and open sources.

At Frontex level, since 2008, the Frontex Risk Analysis Network has been collecting bi-monthly analytical reports providing Member States with summary analysis regarding four topics: third-countries, the situation at the border, illegal stay within the EU, and institutional changes at national level.

Information evaluation grading system

There are many information evaluation systems in place, but the most common one is the 4×4 information evaluation grading system. In this system: the information / data is evaluated against two dimensions, the reliability of the source of information / data and the validity of the information / data. These two dimensions are evaluated against a 4-level scale, as follows:

Evaluation of the reliability of the source

Grading	Description
A	There is no doubt of the authenticity, trustworthiness and competence of the source; if the information is supplied by a source who, in the past, has proved reliable in all instances
B	Source from whom information received has in most instances proved to be reliable
C	Source from whom information received has in most instances proved to be unreliable
X	The reliability of the source cannot be assessed

Evaluation of the validity of the information / data

Grading	Description
1	Information whose accuracy is not in doubt
2	Information known personally to the source but not known personally to the official passing it on
3	Information not known personally to the source but corroborated by other information already recorded
4	Information not known personally to the source and cannot be corroborated

For example, information coming from a reliable source (graded as A) and evaluated as accurate (graded as 1) will be referred to as "A1" information. Information from a source that cannot be assessed and that is factually unknown will be referred to as "X4" information.

Examples of products developed by Frontex Risk Analysis Unit

ARA – Annual Risk Analysis

Annual report on the situation of illegal migration in the previous year, outlook and recommendations for the future, supporting the planning of Frontex operational activities for the following year.

SARA – Semi-annual Risk Analysis

Mid-year update of ARA, including, if necessary, review and fine-tuning of recommendations.

FRAN Quarterly

Quarterly report providing feedback and analysis of illegal migration trends based on the information exchange within the FRAN.

TRA – Tailored Risk Analysis

Analytical report focusing on a specific phenomenon or geographical area; e.g. Iraqi illegal migration to the EU or impact of the financial crisis on illegal migration to the EU.

TFA – Tactical Focused Assessment

Analytical report supporting the planning of a specific Joint Operation.

WAR – Weekly Analytical Report

Weekly analysis of information collected during a particular Joint Operation, for the operational team and hosting authorities.

© Frontex 2010

Intelligence cycle

Intelligence is placed at the heart of risk analysis by defining it as any information, received or generated, that is related to one of the components of the risk, i.e. related to a threat, vulnerability, or impact.

In the context of border control, intelligence typically refers to information about specific border crossing events, in particular illegal activities, that can be used for operational purposes. Examples of intelligence in border security could include information about migrants who intend to cross the border illegally or information about particular drug shipments.

The structured intelligence process is referred to as the Intelligence Cycle, a definable cycle that ensures the efficiency of law-enforcement activities through a system of checks and balances.

Establishing risk analysis units in Member States

Each separate Member State is encouraged to establish and maintain a risk analysis unit.

The function of a risk analysis unit is to gather information affecting the security of the border and more generally the internally security of the EU. For such purposes, risk analysis units will elaborate and disseminate analytical reports and assessments. This will include general or specific trends, routes, *modi operandi* and means of transportation used for criminal activities, and the possible involvement of organised criminal networks.

Risk analysis units are responsible for passing on information which might conceivably impact beyond their Member States' borders both to Frontex and the affected Member States. Co-operation is indispensible to the effective management of the external borders.

Effective management of the risk analysis unit is crucial to the quality of analytical activities. As such, risk analysis unit leaders are tasked with a range of management responsibilities including:

- Directing and managing resources;
- Liaising with other stakeholder agencies / departments;
- Acting as contact between the national and international authorities;
- Ensuring cohesion, cooperation and exchange of information / intelligence;
- Contributing to planning activities and setting up priorities;
- Developing solutions for any problems or deficiencies;
- Updating and modifying the working methods of the unit
- Undertaking any other initiatives that may enhance the risk analysis units functioning.

© Frontex 2012

Assessment techniques

A diverse range of assessment techniques can be used for different analytical purposes. The choice of a technique depends on the data and information available, the type of decision that needs to be informed and the time given to develop the analysis as well as the analyst's familiarity with the techniques. A selection of some of the most commonly used and versatile methods are described below as a means of guidance, but the list is not intended to be exhaustive. Analysts should chose the technique they are most comfortable with and which has previously produced the best results for them. The different techniques can be applied in producing various intelligence products such as threat, vulnerability or impact assessments.

Brainstorming: Brainstorming is an applied imagination technique that involves stimulating free-flowing conversation amongst a group of knowledgeable participants. The heavy emphasis that the technique places on imagination and cross-pollination of ideas renders it particularly useful in instances where there is no data available or where the breaking free from a prevailing mindset is desirable.

Expert elicitation: This methodology provides an avenue for structurally engaging experts in the core areas of concern for border security (irregular migration, crime and terrorism). This includes a nuanced approach towards expanding the pool of knowledge and is mainly qualitative in its nature. Some quantitative methods can be combined (for instance, by asking experts to rank threats).

Pattern and trend analysis: An approach that can combine different tools. Having access to historical data (statistics on past occurrences) is important for this methodology. Trend analysis can be done using qualitative methods, whereas pattern analysis is based on quantitative techniques (for instance, the number of irregular migrants that cross certain borders during particular times).

Surveys: This mainly focuses on exploring vulnerabilities (using a natural science approach to extrapolate about the overall population based on capture / recapture techniques, i.e. the number of cross-border criminals captured versus the total number of cross-border criminals that pass in that given period). This information is also useful for analysing threats.

Glossary of key terms

Analysis: the study of risk, threat, vulnerability or impact that leads to their identification, description and assessment.

Assessment: the analyst's judgment on the importance of identified risks, threat, vulnerability or impact.

External borders: the borders of EU Member States with non-EU states. By extension it also applies to the borders between Schengen Associated Countries and non-EU states. For instance, Poland's border with Ukraine is an external border, and by extension the border between Norway and the Russian Federation is also an external border. By contrast, the border between Sweden and Norway or between France and the UK (via train), Hungary and Romania or Spain and Portugal are not external borders.

Impact: Impact is defined as the effects of a threat on the internal security and on the security of the external borders. Impacts can also be analysed in terms of the effects on the optimum flow of passengers at the borders, and in terms of their humanitarian consequences.

Indicator: a single data item that acts as a pointer or clue conveying a sense of suggestion, condition or status. For example, an indicator can be suggestive of a particular event or activity taking place, or of a set of conditions for such an event to occur, or suggestive about the possible intentions of a target. To be useful and persuasive, indicators are best developed, gathered and assessed as "sets."

Information: unevaluated material of every description, including from observations, reports, allegations and rumour, photographs and other sources which, when processed, may produce intelligence.

Intelligence: any information, received or generated, that is related to one of the components of the risk, i.e. related to a threat, vulnerability, or impact. More practically, in the context of border control, intelligence typically refers to information about specific border-crossing events, in particular illegal activities that can be used for operational purposes.

Risk: For the management of the external borders, **risk** is defined as the magnitude and likelihood of a threat occurring at the external borders, given the measures in place at the borders and within the EU, which will impact on the EU internal security, the security of the external borders, on the optimal flow of regular passengers or which will have humanitarian consequences.

Risk Analysis Unit (RAU): For the management of the external borders, an organisational unit (cell, section, etc.) that is tasked with conducting risk analysis activities in order to provide the management with risk alerts / assessments / reports on issues relating to border security, irregular migration, human trafficking and smuggling.

Smuggling of migrants: In contrast to the definition of Human Trafficking and as defined by the UN Convention Against Transnational Organized Crime (termed UN TOC), the term "smuggling of migrants" generally refers to consensual transactions where the transporter and the transported person agree to circumvent immigration control for mutually advantageous reasons.

Trafficking in human beings: the illegal trade of human beings for the purposes of commercial sexual exploitation and / or forced labour. The UN TOC Convention defines it in length.

Threat: a force or pressure acting on the external borders. It is to be characterised by its magnitude and likelihood. The analyst should describe which processes or factors both inside and outside the EU affect the magnitude and the likelihood of the threat.

Vulnerability is determined by the capacity of a system to mitigate a threat. Vulnerability is understood as the factors at the borders or in the EU that might increase or decrease the magnitude or likelihood of the threat.

FRONTEX

European Agency for the Management
of Operational Cooperation
at the External Borders of the Member States
of the European Union

Rondo ONZ 1
00-124 Warsaw, Poland
T +48 22 205 95 00
F +48 22 205 95 01

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

Risk Analysis Unit

Reference number: 17600/2013 en

Warsaw, November 2013