FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

Common Integrated Risk Analysis Model

Common Integrated Risk Analysis Model
Summary booklet

Version 2.1

European Border and Coast Guard Agency

Plac Europejski 6
00-844 Warsaw, Poland
T +48 22 205 9500
F +48 22 205 9501
frontex@frontex.europa.eu
www.frontex.europa.eu

ACKNOWLEDGMENTS

The Common Integrated Risk Analysis Model 2.1 has been updated by CIRAM-certified analysts from the Member States in close cooperation with the Frontex Risk Analysis Unit. Numerous people contributed to its development, and their assistance is hereby acknowledged with gratitude.

Introduction

CIRAM establishes a clear and transparent framework for risk analysis and should serve as a benchmark for analytical activities. Analysis based on CIRAM will enable decision-makers to reduce and mitigate risk where resources and capabilities are limited. CIRAM seeks to promote a common understanding of risk analysis and contribute to greater coherence in the management of the EU's external borders.

The development and implementation of CIRAM is based on **Article 29 of Regulation (EU) 2019/1896 (European Border and Coast Guard Regulation)**, which states:

> *The Agency shall monitor migratory flows towards the Union, and within the Union in terms of migratory trends, volume and routes, and other trends or possible challenges at the external borders and with regard to return. For that purpose, the Agency shall, by a decision of the management board based on a proposal from the executive director, establish a common integrated risk analysis model, which shall be applied by the Agency and the Member States.*

What does CIRAM mean?

While the legislator did not provide a definition of the terms, the following understanding has been developed within the European Border and Coast Guard (EBCG) community*:

* As defined in Article 4 of Regulation (EU) 2019/1896.

„Common“ refers to a framework, developed by Member States and Frontex, which shall be applied at both national and EU levels.

„Integrated“ refers to Frontex's aim to ensure a uniform and high level of control over all external borders. An integrated approach to risk analysis suggests cooperation with other law-enforcement bodies / border authorities and other authorities dealing with migration issues, such as customs authorities, immigration offices and national police.

„Risk Analysis“ means the systematic examination of components of risks to inform decision-making.

„Model“ means an analytical framework which provides a common vocabulary and structure for risk analysis in the EBCG community. It is not an algorithm providing absolute outcomes.

The four-tier access control model

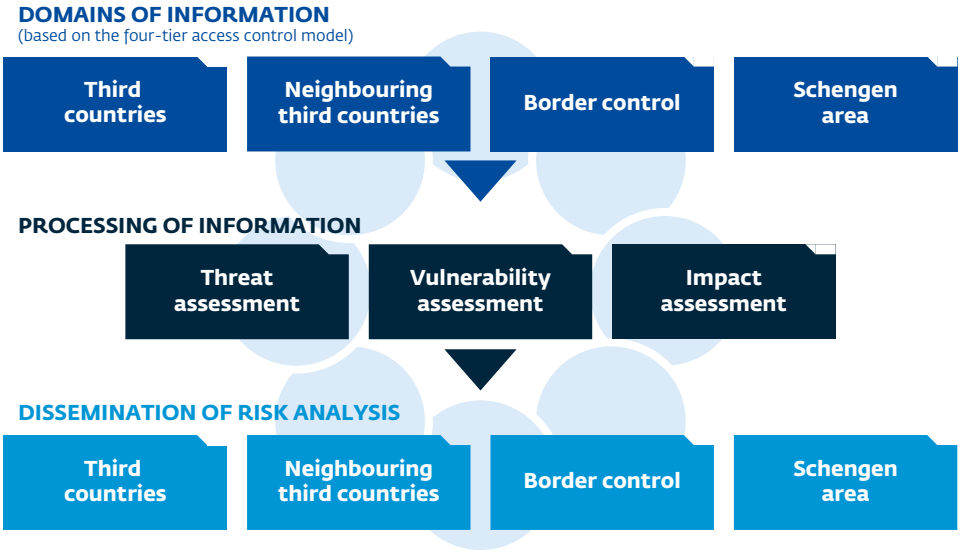
The four-tier access control model* includes:

1. measures in third countries,
2. cooperation with neighbouring third countries,
3. border control and
4. control measures within the Schengen area including return.

* As explained in the European Council document on the Updated Schengen Catalogue on External Borders Control, Return and Readmission, 15250/2/08, REV 2, LIMITED.

It forms the core of Integrated Border Management. In simplified terms, the model requires that a set of complementary measures be implemented across the different tiers. For risk analysis the four-tier access control model indicates the different domains in which analysts seek information. The model indicates that the analytical products will be useful for all authorities that are active in one or more tiers. In this sense, the four-tier access control model is a powerful reference to the integrated dimension of risk analysis.

Graphic 1: CIRAM diagram



Overview of risk

For the management of the external borders, risk is defined as the magnitude and likelihood of a threat that may affect the management of the external borders, given the measures in place at the borders and within the EU, which will impact on the EU's internal security, or the functioning or security of the external borders, or which will have humanitarian consequences.

From this definition of risk, risk analysis is defined as the examination of the following three components, the outcome of which is recorded in the form of a risk assessment*:

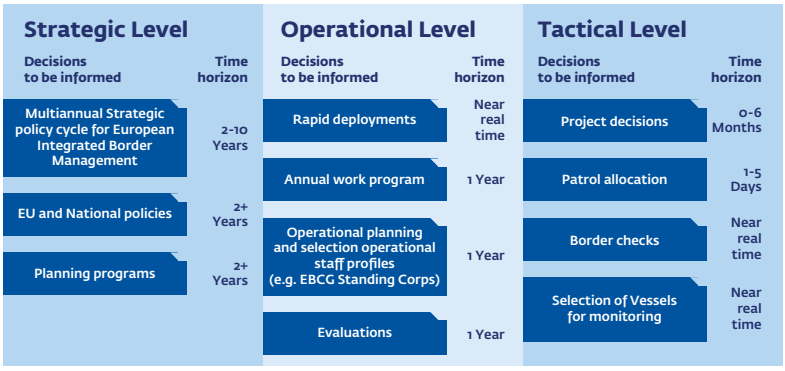
1. the threat;
2. the vulnerability to the threat;
3. въздействието, ако възникне заплахата.

* This definition of risk does not apply to all processes of Integrated Border Management. For other definitions of risk see, e.g., Article 3 of Regulation (EU) 2018/1240 (ETIAS regulation).

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

The assessment should have a clearly defined scope and purpose. It should cover a specific period and assess the threat over a specified future period, consistent with the level of decision-making it is to inform.

Graphic 2: Examples of decisions and time horizons for the EBCG



Support for decision-making

While it will never be possible to eliminate risk, by enabling decision-makers to take informed decisions, risk analysis will contribute to closing the gap between a risk and the capability of an IBM system to reduce and mitigate it.

The scope of recipients and levels of decision that can benefit from this intelligence-driven approach to risk analysis is quite broad. From policy makers to first-line border guards, all actors within IBM structures not only benefit from the support of relevant analytical products, but also play a decisive role in the quality of the intelligence, as they are key elements of information collection within their organisations.

The intelligence requirements for the strategic, operational and tactical levels are expected to be different. They vary in terms of output for decision-making, inquiries to be made, data to be used, the analytical approach to be performed, and the variety of tools and techniques to be used.

There is no clear rule differentiating the approaches for the strategic, operational and tactical level assessments. This division of levels should adapt to the specifics and structures of different national IBM contexts.

Nevertheless, some specificities can be identified:

Strategic level assessments should focus on:
- understanding the development of phenomena;
- creating a general and global picture,
- delivering an outlook;
- providing recommendations on the development of capabilities and capacities;
- defining requirements of resources;
- supporting decisions on the budget.

Operational level assessments should involve aspects / products regarding:
- the dynamics of a threat;
- internal factors and findings from Vulnerability Assessment are of relevance to allow assessments of resources and their reallocation;
- focus on border section.

Tactical level assessments need to treat aspects / products related to:
- risk indicators;
- risk profiles (for perpetrators, victims and the m.o.);
- a defined geographical area and time;
- external aspects (at the border).

Threat

Threat is defined as a force or pressure that may affect the management of the external borders. It is characterised by its magnitude and likelihood.

At the core of risk analysis is the identification of current and future threats that influence the management of the external borders.

A description of a threat typically includes a description of the *modus operandi*, the perpetrator's goals, motives and capabilities (who, where, when, how many), trends and predictions, and any factors that affect the magnitude and likelihood of the threat. The exact components are based on an examination of the threat to identify the variables that influence it, as well as any possible correlations among them.

Threats should be measured so that they can be compared and prioritised. As the purpose of analysis is to inform decision-making, which will determine future actions, analysis of a threat is by nature forward-looking and should make reference to the likelihood and magnitude of the threat for a given time horizon.

Vulnerability

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.

Among the prime factors used to identify vulnerability are the geographical attributes of the border areas, analysis of operational activities, including capabilities to mitigate the threat, such as numbers of staff and their skills, the deployment of equipment and the management of priorities and policies. Assessment of these factors should indicate to decision-makers vulnerabilities in relation to specific threats so as to enable a swift response to events.

Vulnerability concerns matters that, due to their nature, allow for more accurate measurements and estimations than when assessing threat and impact.

Vulnerability in CIRAM in relation to Vulnerability Assessment of Article 32 of Regulation EU 2019/1896.

Regulation EU 2019/1896 establishes Vulnerability Assessment (VA)* as one of the quality control mechanisms that monitors and assesses the capacities of the Member States. VA has its own Common Vulnerability Assessment Methodology (CVAM). The Regulation EU 2019/1869 defines several interfaces between risk analysis and VA.

* Articles 3(1)(k) and 32 of Regulation (EU) 2019/1896.

Impact

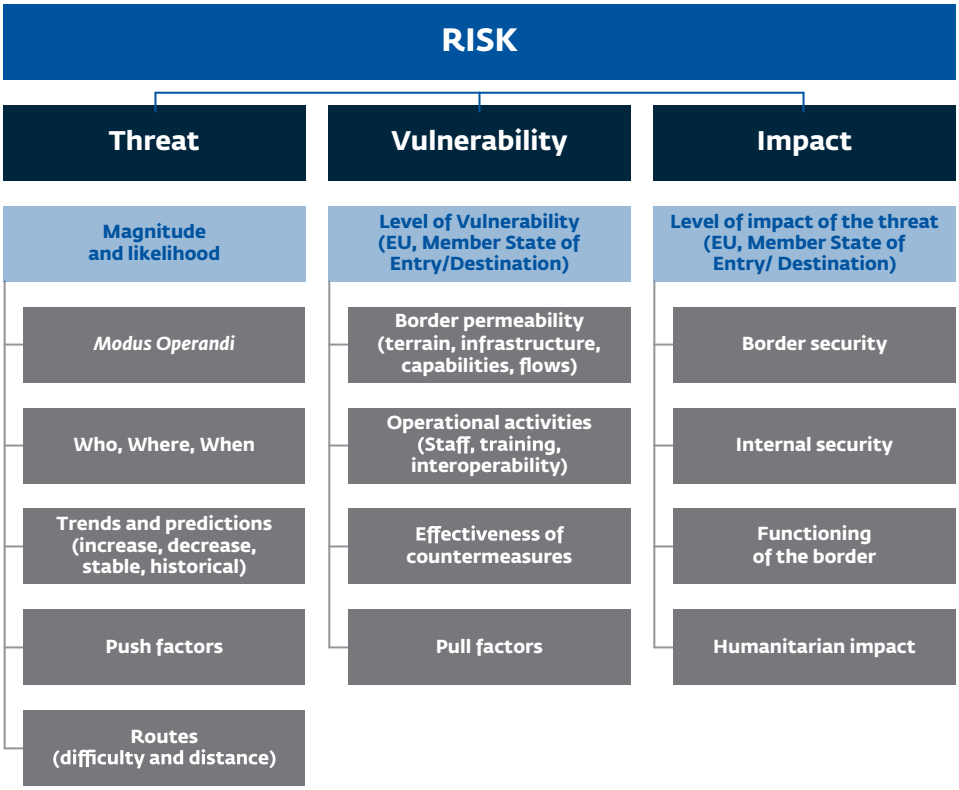
Impact is defined as the effects of a threat on the EU's internal security or the functioning or security of the external borders. Impacts can also be analysed in terms of humanitarian consequences.

Impact assessment includes consideration of both immediate impacts and those that might arise later. Consideration should also be given to small incidents which, taken individually, do not have a large impact, but when aggregated might have detrimental effects on the EU's internal security or the functioning or security of the external borders.

The measurement of impacts will depend on the threat identified. If quantitative or qualitative assessments are not available, impact can be measured through a description of outcomes arising from inductive analysis or scenario analysis.

Threat, vulnerability and impact are the building blocks of risk. Risk analysis is reflected in the diagram below. The elements shown in the diagram in grey colour are non-exhaustive. They are examples of variables to consider.

Graphic 3: Risk analysis diagram



Intelligence cycle

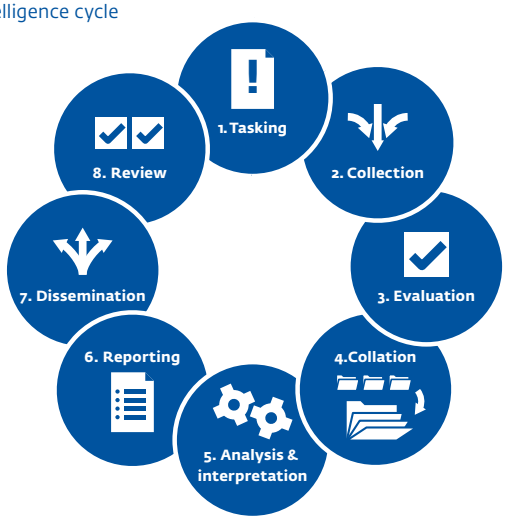
In every organisational setting, the intelligence activities which lead to the development of analytical products follow a 'standard' cycle or process chain. Frontex and Member States' risk analysis units use intelligence processes, skills and techniques to produce actionable information to increase the probability of success.

This is achieved by adopting a common structured intelligence process that comprises collecting, analysing and distributing actionable intelligence. This is the core process when conducting analytical activities within IBM and contributes to efficient border management by producing appropriate and timely products.

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

The basic premise of the Intelligence cycle is that the systematic exploitation of information leads to effective products which enable decision-makers to address risk.

Graphic 4: Intelligence cycle



Recommendations

If tasked, risk analysis should produce recommendations for decision-makers on developing and implementing measures to address risks. These measures should prevent risks from materialising or mitigate their impact if they do. Analysts may also develop action plans. In any event, an analytical product should always contain actionable information*.

Recommendations aim to assist decision-makers to select and implement appropriate measures.

* Such recommendations are part of the analytical conclusions and are to be distinguished from the Frontex Executive Director's recommendations mentioned in Articles 32 and 41 of Regulation (EU) 2019/1896.

CIRAM implementation

Each Member State is encouraged to establish and maintain risk analysis capacity in the form of a unit, network and/or system. The function of risk analysis capacity is to implement CIRAM and the Intelligence cycle by ensuring the acquisition of data, the application of the assessment methods, the provision of the proper tools and the involvement of risk analysts. The implementation of CIRAM and the Intelligence cycle is ensured by specialised training. Risk analysis capacities are also responsible for establishing respective cooperation networks.

At EU level, the situation at the external border is monitored by the EUROSUR framework. This also provides for exchange of information and operational cooperation within the European Border and Coast Guard in order to improve situational awareness and to increase reaction capability.

The Frontex Risk Analysis Network (FRAN), brings together representatives from the European Commission, JHA Agencies and Member States involved in risk analysis and border management.

Efforts are being made at EU level to complement the FRAN by establishing regional networks in the pre-frontier area and cooperation with third countries.

FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

European Border and Coast
Guard Agency

Plac Europejski 6
00-844 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
Warsaw, December 2021