D1.2a Conceptual Model (public version)

Document Submission Date: 15/04/2021

Work Package 1: End-user requirements and needs

Document Dissemination Level: PU

TRESSPASS - robusT Risk basEd Screening and alert System for Passengers and luggage
Funded by the Horizon H2020 Framework Programme of the European Union for Research and Innovation, Grant Agreement number: 787120

Abstract

This document is deliverable D1.2a – "Conceptual model", with dissemination level Public. It is a copy – with minor changes – of D1.2 dissemination level Confidential (i.e. only for members of the TRESSPASS consortium, including the Commission Services), submitted in April 2019.
It should be noted that this public version does not contain new information in comparison to the original version, and therefore does not reflect the actual implementation of the concept within TRESSPASS per submission date.

Within the scope of H2020 project TRESSPASS, a new so-called risk-based concept has been developed to perform security checks at border crossing points at Europe's external borders. As described in the Horizon 2020 call 'Risk-based screening at border crossing'[1] *"The concept of 'borders' has changed in recent times. The purpose and function of borders have been, and remain, to delineate and demarcate one sovereignty from another. However, borders must also allow for the smooth movement of people and goods. Maintaining the current level of checks is becoming increasingly expensive given the ever growing volumes of people and goods on the move, and* [checks are becoming] *increasingly more disruptive of flows"* (European Commission, 2015).

The call text further stated that border control "*would remain sustainable if thorough checks could be limited to fewer individual goods and people pre-selected further to a preliminary (and non-disruptive) risk-based screening of the flows*" (European Commission, 2015). In support of this the call requests asks for "*the development of technologies and capabilities which are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security (border checks), whilst respecting human rights and privacy*" (European Commission, 2015).

The risk-based concept described in this deliverable D1.2a addresses the main purposes and expectations of risk-based border management.

Indicator	Description
Effectiveness	Success-rate of stopping unauthorised travellers when they attempt to cross the border at the BCP
Flow-rate	Speed of the flow of travellers as they approach and cross the border at the BCP
Efficiency	Number of resources required at the BCP to achieve a certain degree of effectiveness and/or certain minimal flow-rate
Level of ethical compliance	Degree to which a BCP mitigates negative ethical impact on the travelling public and on the public in general – regardless of if they travel

The focus of risk-based BCPs can be one-sided, for example when only the (beneficial) effects on one of the factors effectiveness, flow-rate or efficiency are mentioned. Stakeholders can either knowingly or unknowingly have biased expectations of risk-based border crossing

[1] SEC-15-BES–2017: Risk-based screening at border crossing (HORIZON 2020 - Work Programme 2016-2017, Secure societies – Protecting freedom and security of Europe and its citizens)

points. In reality, these factors are intrinsically linked and need to be addressed in an integral manner.

This deliverable uses TRESSPASS D1.1 as input, and puts the identified requirements and needs in the context of the TRESSPASS RBBM concept. D1.2a fulfils almost all requirements stated in D1.1. It should be noted that in case deliverables D1.1 and D1.2a are in conflict, D1.2a has preference. In addition, this deliverable D1.2a defines additional requirements (in section 4.10) which arise from the TRESSPASS concept.

In chapter 5, the conceptual framework of risk-based border management is described. A conceptual framework is a way to organise ideas to achieve the research projects' purpose. The conceptual framework is described to ensure shared understanding and a common structure allowing integrating results. The following elements are part of the Conceptual Framework of RBBM: conditions and general design principles, basic concepts such as key terms and typical characteristics of BCPs, of travels and travellers, of threats, and of border management operations, and RBBM capabilities.

The way forward beyond D1.2a has also been defined. This is done in three disjunct manners. First, in terms of how other TRESSPASS tasks relate to this deliverable in Annex D. Second, in terms of the transition from rule-based border management towards risk-based border management in chapter 6. And third, what future developments beyond TRESSPASS might be possible, in Section 6.5.

Project Information

Project Name	robusT Risk basEd Screening and alert System for PASSengers and luggage
Project Acronym	TRESSPASS
Project Coordinator	National Center for Scientific Research "Demokritos", EL
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SEC-2016-2017 (SECURITY)
Topic	SEC-15-BES-2017 "Risk-based screening at border crossing"
Funding Instrument	Innovation Action
Grant Agreement No.	787120

Document Information

Document reference	**D1.2a**
Document Title	**Conceptual Model (Public version)**
Work Package reference	WP1
Delivery due date	N/A
Actual submission date	15/04/2021
Dissemination Level	Public
Authors	**Jeroen van Rest, Dirk Stolk, Ingrid Weima and Martijn Wessels (TNO)**
Contributors	-
Document Review Status	☒ Consortium ☒ WP leader ☒ Technical Manager ☒ Quality and Risk Manager ☒ Ethical Advisory Board ☒ Security Advisory Committee ☒ Project Coordinator

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
ANPR	Automatic Number Plate Recognition
API	Advanced Passenger Information
BB	Building Block (TRESSPASS)
BCP	Border crossing point
BM	Border management (TRESSPASS)
CBP	Customs and Border Protection (United States)
CCTV	Closed-circuit television
CD&E	Concept Development and Design
CIS	Customs Information System
CONOPS	Concept of Operations
CTA	Common Travel Area
DBT	Design Basis Threat
DHS	Department of Homeland Security
DPBD	Data protection by design
EC	European Commission
ECRIS	European Criminal Records Information System
EES	Entry-Exit System
eGate	Automated border control system
EIS	Europol Information System
ELSA	Ethical, legal and societal aspects
EPDbD	Ethics, privacy and data protection by design
ETIAS	European Travel Information and Authorisation System
EU	European Union
EURODAC	European Dactyloscopy database
EOROSUR	European Border Surveillance System
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the EU Member States
GDPR	General Data Protection Regulation
IBM	Integrated Border Management
ICT	Information and Communication Technologies
ID	Identity
KPI	Key Performance Indicator

ACRONYM	EXPLANATION
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone (of an identity page of a passport)
MS	Member State (EU)
NRM	Networked Risk Management
OSINT	Open-source intelligence
PIU	Passenger Information Unit
PNR	Passenger Name Records
RBBM	Risk-based border management (TRESSPASS)
RIA	Research and innovation action (EC)
RTP	Registered Traveller Programme
SBC	Schengen Borders Code
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents (Interpol)
TCN	Third Country National
TRL	Technology Readiness Level
U-R	User-requirement or need (TRESSPASS)
US	United States (of America)
VIS	Visa Information System
WP	Work package (TRESSPASS)

Table of Contents

1 INTRODUCTION

Within the scope of H2020 project TRESSPASS a new so-called risk-based concept has been developed to perform security checks at border crossing points at Europe's external borders. This chapter provides a brief introduction into the background of the project and into the specific scope of Task 1.2: the development of the TRESSPASS conceptual model for risk-based border control. This chapter describes the context of border management at border crossing points (BCPs), the main challenges in this field and the chosen direction of meeting this challenge by a risk-based border management approach for screening at BCPs. To this purpose, as an initial step towards risk-based border control, a conceptual model has been developed. The way in which this has been done in Task 1.2 is explicated. The chapter ends with a reader's guide.

1.1 Context

As described in the Horizon 2020 call 'Risk-based screening at border crossing'[2] *"The concept of 'borders'' has changed in recent times. The purpose and function of borders have been, and remain, to delineate and demarcate one sovereignty from another. However, borders must also allow for the smooth movement of people and goods. Maintaining the current level of checks is becoming increasingly expensive given the ever growing volumes of people and goods on the move, and* [checks are becoming] *increasingly more disruptive of flows"* (European Commission, 2015).

Border control *"means the activity carried out at a border, …, in response exclusively to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance."* (Regulation (EU) 2016/399, Article 2*)*

Border checks *"means the checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it."* (Regulation (EU) 2016/399, Article 2)

Figure 1-1 shows the currently foreseen problem. The condition is that the effectiveness of border control at BCPs should remain the same or at least at an acceptable level. If nothing will be changed in the border control processes, however, due to growing flows of traffic the flow-rate of travellers at BCPs is expected to decrease.

The call text states that border control *"would remain sustainable if thorough checks could be limited to fewer individual goods and people pre-selected further to a preliminary (and non-disruptive) risk-based screening of the flows"* (European Commission, 2015). In support of this the call requests asks for "*the development of technologies and capabilities which are required to enhance systems, equipment, tools, processes, and methods for rapid identification to improve border security* (border checks)*, whilst respecting human rights and privacy"* (European Commission, 2015).

[2] SEC-15-BES–2017: Risk-based screening at border crossing (HORIZON 2020 - Work Programme 2016-2017, Secure societies – Protecting freedom and security of Europe and its citizens)

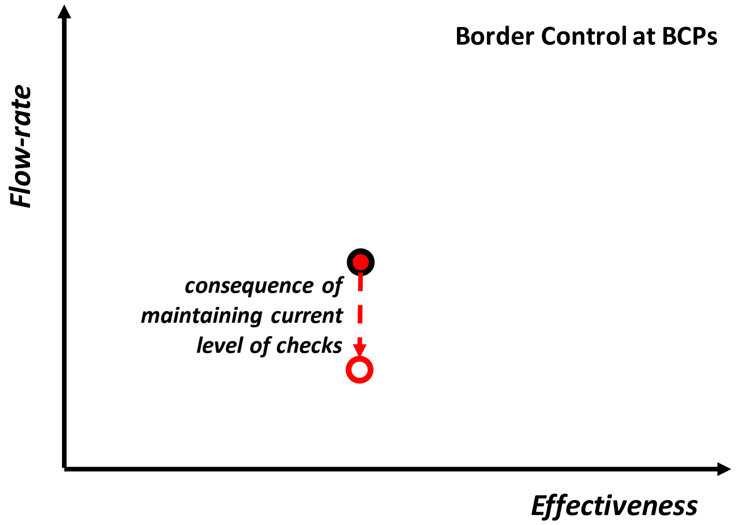


FIGURE 1-1 IMPACT OF MAINTAINING CURRENT APPROACH OF BORDER CONTROL ON THE FLOW OF TRAVELLERS

These technologies and capabilities should, amongst other things, result into (European Commission, 2015):

- *"Enhanced situational awareness for border control practitioners, enabling the timely and proper identification of potentially dangerous people and goods, and preventing smuggling and human trafficking;*
- *Improved risk-management coordination and cooperation between border control (passport/persons), customs (baggage/goods) and security in transport (pre-boarding security checks on persons and baggage);*
- *Improved solutions for remote detection of abnormal behaviours;*
- *Improved and people-respectful border automated screening systems;*[3]
- *More effective use of intelligence to reduce risks at borders."*

Risk-based approaches, such as risk-based screening, are typically used to select measures that are proportional to the actual threat, while maintaining or reducing the risk. This means: less stringent measures if possible, more stringent measures when needed. The implementation of such an approach at border crossing points implies that people (including their goods and vehicles) who clearly not pose a significant threat, invasive checks can be limited. Moreover, in case data can already be collected and analysed before travellers arrive at the BCP, less additional personal data of them has to be collected at the moment they actually arrive at the BCP. This will lead to less and shorter interruptions in the flow of people and goods, thus contributing to a smooth movement of people and goods at BCPs.

Considering the development of the requested technologies and capabilities in support of a 'risk-based border management' (RBBM) approach at BCPs, the overall objectives of TRESSPASS are to:

1. Develop a single cohesive risk-based border management concept;
2. Apply an ethics and data protection 'by design' approach;
3. Include the aspect of trustfulness of travellers as part of the concept;

[3] This should be done *"through close cooperation with actions resulting from SEC-18-BES–2017: Acceptance of 'no gate crossing point solutions'"* (European Commission, 2015). It concerns the H2020 project PERSONA.

4. Prepare three pilot demonstrations;
5. Demonstrate the validity of the RBBM concept in these pilots;
6. Prepare further developments of the developed RBBM concept.

The initial activities of TRESSPASS (i.e. WP1 – End-user requirements and needs) are mainly related to meet the first overall objective. It concerns the identification of the needs and requirements of border authorities and customs with respect to a future risk-based approach (Task 1.1), the development of a risk-based border management concept to enable faster and more effective control procedures at BCPs (Task 1.2), the development of scenarios of flows of travellers at BCPs and the identification of gaps between current border management and future risk-based border management (Task 1.3), and finally a review of EU's border management legal framework (Task 1.4). This specific report describes the results of Task 1.2 and thus focusses on the development of the RBBM concept to enable faster and more effective control procedures at BCPs.

1.2 Purpose and scope

The purpose of Task 1.2 is to develop a new border management concept based on the idea of risk-based screening of travellers[4] and their goods. This will be achieved, by defining the principles of the concept vis-à-vis alternative approaches, such as rule-based border control and intelligence-led border control. This includes the expected benefits and important conditions for implementation of a risk-based border management concept.

Relation with D1.1 – End-user requirements and needs

In Task 1.1 user-requirements and needs have been collected by a literature study and interviewing end-users from border authorities. These have been reported in deliverable D1.1, which has been used as input for Task 1.2. Requirements and needs that are relevant for the concept have been put in the context of the TRESSPASS RBBM concept. Furthermore, this deliverable D1.2a defines additional requirements (in section 4.10) which arise from the TRESSPASS concept.

The RBBM concept should fulfil the following conditions:

- It should be in alignment with the Guidelines for Integrated Border Management (IBM Guidelines), which concerns mitigating cross-border crime, national security and preventing illegal migration (note: this excludes threats posed by state-actors);
- It should reflect the different modalities: air, land and maritime;
- It should be flexible and adaptive for new trends and threats;
- It should respect human rights and privacy.

In addition, the scope of the RBBM concept should be in alignment with the overall scope of the TRESSPASS project. This means that the concept focusses on:

- BCPs at Europe's external borders[5]; therefore, the TRESSPASS concept does not consider people crossing borders outside BCPs such as e.g. refugees who cross the Mediterranean or Aegean Sea with the help of traffickers;

[4] In the context of TRESSPASS a traveller who want to cross the border at a BCP can be a passenger but also a driver or crew member of a vehicle, or a pedestrian.

[5] The distinguished external borders (land, sea, river, etc.) are sometimes referred to as green or blue borders. A green border generally refers to a land border; a blue border generally refers to rivers, lakes and maritime borders.

- Travellers, both entering and leaving Europe via BCPs, including their luggage; however, cargo is excluded from the concept.

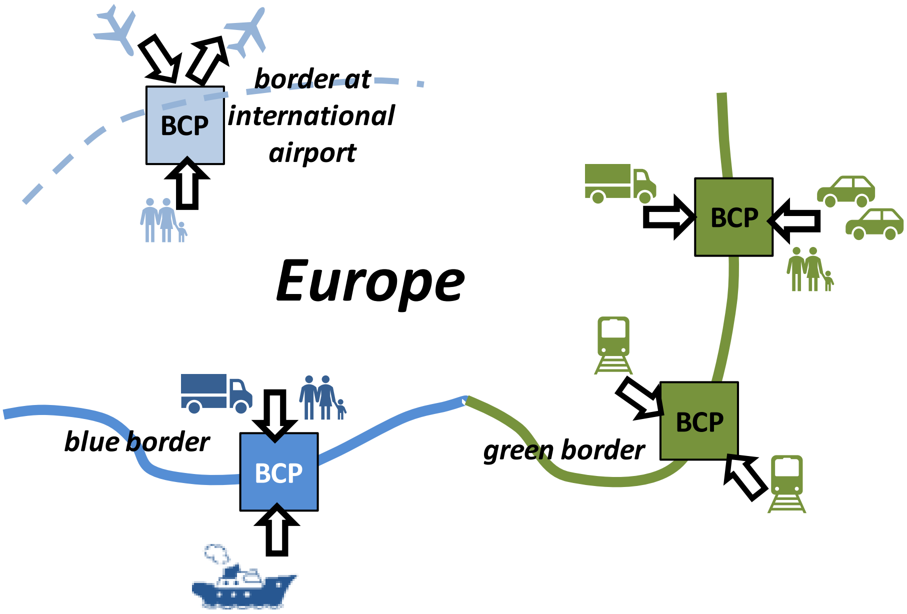


FIGURE 1-2 SCOPE: BORDER CONTROL OF FLOWS OF TRAVELLERS AT BCPS

Furthermore, the concept presumes:

- Normal traffic situations at the borders; it excludes excessive situations such as international tension at the external border (threat of military invasion) or a great surge of refugees towards a BCP that overwhelms that BCPs capacities (which e.g. happened at the borders of the Spanish enclaves in Morocco);
- No help of insiders (i.e. assistance of people who are active in border control) to malicious travellers at their attempt to cross the border at a BCP.

The primary focus of the RBBM concept is on border crossing processes. Other processes, such as those pertaining to travel security (e.g. aviation security) and BCP security (e.g. port security, attacks on queues at a BCP) are beyond its scope. Nevertheless, given the relationship between these processes (i.e. border crossing, travel security and BCP security), some attention will be given to strengthen mutual coordination of these kind of processes, which may, for example, generate information relevant to the border control process.

Having set the concept's boundaries, the application of an RBBM concept at EU level from a governmental, strategical, tactical and operational perspective will be described. The operational aspects, however, have only be touched in this task, because they will be elaborated in more detail in WP6 – Operational methods and acceptability.

This task provides the most important pillars and capabilities of the RBBM concept. Building on the findings of this activity as well as on the results of Task 1.1's surveys and interviews with customs and border authorities, the required capabilities in terms of people, processes, information, and technology to support the successful implementation of the TRESSPASS concept are defined.

1.3 Approach

The approach for D1.2a consisted of the following phases. Before TRESSPASS started, RNM and T1.2 task leader TNO had together explored the challenge and generic approach for risk-based border management, especially for the air modality, and with a local focus (Van Rest, J. and Weima, I., 2017). During the proposal phase, these insights were shared with, and enriched by the TRESSPASS consortium, which led to the TRESSPASS proposal.

In task T1.2 of TRESSPASS, document analysis, brainstorms, interviews, a large workshop, a series of internal design sessions and a gaming session with RNM were used to develop the TRESSPASS concept further. Firstly, by defining the scope of the concept vis-à-vis alternative approaches, such as information-based and rule-based border control, as well as by stressing its differences with current concepts. This includes the expected benefits and important conditions for implementation of a risk-based border management concept.

Second, having set the concept's boundaries, the consortium assessed the application of a risk-based border management concept at EU level from a political, strategic and tactical perspective. This was done in the workshop and this was part of the focus of the interviews. Another part of the focus of the interviews was on the operational aspects. The serious game that was played with RNM also helped to get an initial idea of how the operational aspects relate to the goals of the other governance levels.

Finally, this has lead to the most important pillars and capabilities of the risk-based border management concept. Building on the findings of this activity as well as on the results of T1.1 surveys and interviews with custom and border authorities, and T1.4 The legal and regulatory framework, the consortium has further defined the needed capabilities to support the successful implementation of the TRESSPASS concept.

1.4 Reader’s guide

Chapter 2 describes the current approach of border management in Europe, the way in which threats are dealt with, and provides an overview of new developments and initiatives. Chapter 3 describes the challenges in border management as a result of current problems and trends that will affect border management. A potential solution to meet these challenges is the RBBM approach. In Chapter 4 the main principles of this approach are explicated and are compared with the rule-based and intelligence-led approaches. Subsequently, in Chapter 5 the conceptual framework of RBBM is elaborated. In next chapter – Chapter 6 – the implications of and the conditions for a future transition towards RBBM are described. The final chapter – Chapter 7 – summarises the main results and provides an overview on how these results relate to future TRESSPASS activities. At the end of the main text all references are listed.

Detailed and background information is provided in various annexes. It concerns:

A. Glossary of terms
B. Fictional example of how threat representations evolve
C. Addressing end-user requirements and needs of deliverable D1.1
D. Connection of deliverable D1.2a with other TRESSPASS work packages and tasks

2 BORDER MANAGEMENT – CURRENT SITUATION

This chapter describes the current approach of border management in Europe, the involved stakeholders at various levels (from international policy till operational), and the way in which border control in general and at the border crossing points in particular is carried out. In addition a number of relevant developments and initiatives in border control is listed.

2.1 Main principles and goals of border management in Europe

In alignment with the European Border and Coast Guard Regulation the European Union's (EU) Integrated Border Management (IBM) *"aims at managing the crossing of EU's external borders efficiently and addressing migratory challenges and potential future threats at those borders. IBM contributes to addressing serious crime with a cross-border dimension (such as migrant smuggling, trafficking in human beings and terrorism) and ensuring a high level of internal security within the EU"* (Regulation (EU) 2016/1624, Article 4). In addition a key principle of IBM is to act in full respect for fundamental rights and in a manner that safeguards the free movement of persons within the EU. The European Border and Coast Guard Regulation mentions as main components of IBM: *"*[a] *border control,* [b] *prevention and detection of cross-border crime,* [c] *referral of persons who are in need of, or wish to apply for, international protection,* [d] *search and rescue operations for persons in distress at sea,* [e] *risk analysis for internal security and security of the external EU borders,* [f] *cooperation with third countries with a special focus on neighbouring countries and those which have been identified as countries of origin and/or transit for irregular migration, and* [g] *return of third country nationals who are subject to return decisions"* (European Commission, 2010).

As such IBM is supportive in achieving EU's goal of having open, but controlled and secure borders, by enhancing the coordination and cooperation among all relevant border authorities at national and international levels. IBM consists of the following elements (European Commission, 2010):

- Border control – checks and surveillance – as defined in the Schengen Borders Code (SBC), including relevant risk analysis and crime intelligence;
- Detection and investigation of cross-border crime in coordination with all competent law enforcement authorities;
- Coordination and coherence of the activities of EU Member States and institutions and other bodies of the Community and the Union;
- Inter-agency cooperation between border guards, customs, police, national security and other relevant authorities with respect to border management as well as international cooperation;
- The 'four-tier access control' model:
    - Tier 1: measures in third countries, especially in countries of origin and transit,
    - Tier 2: cooperation with neighbouring countries,
    - Tier 3: border control at the external borders for every person entering or leaving the Schengen area, which is in fact the core topic of the TRESSPASS' RBBM concept, and
    - Tier 4: control measures within the area of free movement within the Schengen area.

2.2 Involved stakeholders

Four main groups of stakeholders are distinguished: first, the traveller itself. Second, the general public, whether they travel or not, third public stakeholders that are responsible for border control on the one hand, and finally a group of various other stakeholders on the other hand. The latter group consists of travellers and carriers who want to cross EU's external borders to continue their trip, and public or private facilitators of the BCP infrastructure (e.g. port authorities) who need to cross the border for their work at the BCP premises.

2.2.1 The traveller

First of all there are the travellers who are willing to cross the EUs external border with their luggage and/or vehicles either to enter or to leave EUs territory, and therefore need to be checked by border authorities. Their main interest is to be able to cross the border with as less 'friction' as possible. This group includes travellers with 'bad intentions'.

Travellers can be pedestrians but most often they will arrive at the border by a certain means of transport such as a car, a plane or a ship. Either they are a passenger or they drive, fly or sail themselves as driver or crew member.

2.2.2 The general public

Second, the general public has several stakes in good functioning border management. (External) borders are an important risk mitigation measure. Terms in the public and political debate like 'fortress Europe' relate directly to this function of borders and of border control. Directly related to this, is the understanding that the type and quality of border control have direct impact on the flow of traveller and thus on economic factors.

Both these factors, the risk mitigation and the flow-rate, and also the privacy impact of border measures, are also connected to highly valued types of freedom of the general public, such as freedom of ideas and of movement.

2.2.3 Public stakeholders responsible for border control

With respect to public agencies IBM discriminates between three types of collaboration: intra-service (within organisations), inter-agency (between organisations), and international (between organisations of different countries). These three 'pillars of collaboration' refer to national and international coordination and cooperation among all relevant authorities and agencies involved in border security. By means of these three pillars EU's goal is to establish effective, efficient and coordinated border management, in order to reach the objective of open but well-controlled and secure borders.

An important challenge to achieve adequate international collaboration is that organisational structures and processes of cross border management differ between EU's Member States (and also between EU countries and third countries). In fact, each country has its own *"names and methodology of agencies responsible for border checks"* (European Commission, 2010, p. 29). However, *"the core task remains the same: to determine whether persons are authorised to enter or leave the territory of a state, including checking their means of transportation and the objects in their possession and processing them accordingly"* (European Commission, 2010, p.29).

Organisations of EU Member States (MS) that are involved in border checks deploy most of their personnel at border crossing points to check entry and exit of travellers and their goods, and in the vicinity of EU's external 'green and blue' borders for surveillance purposes. The remaining personnel is employed at regional or central headquarters (e.g. performing command and control or intelligence), at embassies in third countries (e.g. for processing visa requests), at locations within the MS as inland mobile surveillance units, and at international organisations or operation centres such as Frontex dealing with common border issues.

Figure 2-1 provides a schematic overview of the ways in which border management is organised in countries, and of the various types of intra-service, inter-agency and international collaboration. The picture shows five hierarchical levels:

- EU policy level where the EU and governments of MS make agreements on border management in Europe, and in the way how they operate in agencies like Frontex and Eurosur;
- National policy or governmental level where each MS decides on the implementation of border management within its country in alignment with EU's policies, and where bi-lateral agreements with countries inside and outside the EU are established;
- Strategic level where national authorities and services (a) command and control their respective agencies at tactical level (intra-service), and (b) coordinate their activities with their colleague-agencies at strategical level within their country (inter-service) and with other countries (international);
- Tactical level where command, control and coordination at BCPs and at the green and blue borders takes place;
- Operational level where border control (at BCPs) and border surveillance (at green and blue borders) actually is executed.

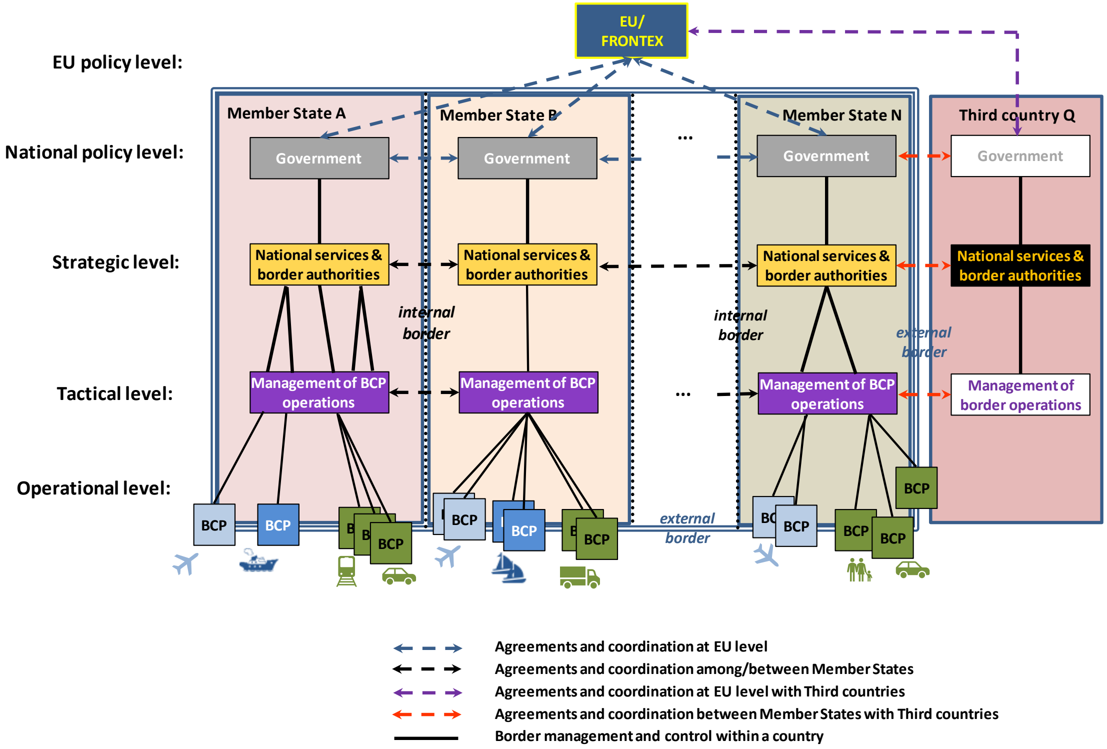

EU/ FRONTEX
EU policy level:
National policy level:
Strategic level:
Tactical level:
Operational level:
Member State A
Member State B
...
Member State N
Third country Q
Government
Government
Government
Government
National services & border authorities
National services & border authorities
National services & border authorities
National services & border authorities
internal border
internal border
external border
Management of BCP operations
Management of BCP operations
...
Management of BCP operations
Management of border operations
BCP
BCP
BCP
BCP
BCP
BCP
BCP
BCP
BCP
BCP
external border
Agreements and coordination at EU level
Agreements and coordination among/between Member States
Agreements and coordination at EU level with Third countries
Agreements and coordination between Member States with Third countries
Border management and control within a country

FIGURE 2-1 SCHEMATIC OVERVIEW OF PUBLIC STAKEHOLDERS AND THEIR RELATIONS

The RBBM concept that is developed within TRESSPASS mainly focusses on the BCPs at Europe's external borders (tier 3).

2.2.4 Other stakeholdersrs

This group of stakeholders includes professional carriers that transport passengers by plane, ship, bus or train across the external borders. Carriers of planes, ships and trains can be forced to transport passengers back when their entrance in the EU is refused by the border authorities.

It also concerns public or private organisations who host, facilitate or work at the BCP infrastructures. Think of owners of an international airport or port authorities. They are not responsible for border control, but they are interested in a smooth flow of traffic and travellers at their facilities. Furthermore, although they will stay at the BCP, their personnel might need to pass border control without unnecessary delays to do their work.

2.3 Journey of a traveller in view of border control

The journey of a traveller begins at the moment that he (or she) starts planning his trip. Information that he has to provide offers border management authorities the opportunity to collect and analyse data. Ideally, this is done long before the traveller actually arrives at the BCP.

The journey of a traveller, either being a passenger or a crew member, can typically be subdivided in four travel stages:

- Pre-travel: the stage in which the traveller plans his journey, applies for a visa, and/or buys a ticket; this stage ends when the traveller is on the way to the BCP;
- Approach BCP: this stage starts at the moment it becomes clear that the traveller is on the way and will arrive at the BCP, and it lasts until his arrival at the BCP; the duration of this stage depends on the distance to the BCP and the mode of transport;
- At BCP: this is the stage in which the traveller has arrived at the BCP and in which he will be checked by the border authorities;
- Post BCP: this stage starts as soon as the traveller has been allowed to cross the external border.

Travellers can travel alone – e.g. as a passenger on a ferry, or as a single person driving a car or flying small plane – but also as a group. Examples are a car with three occupants or a school class aboard an airplane. As a group these travellers often have booked their train, bus, ferry or air tickets together. Apart from the fact that during their journey they are expected to arrive at the BCP together, this can also provide information in advance of their journey that is of interest for border control. For instance, if one person of the group has a criminal past.

2.4 Checks, decision making, infrastructure and information systems at BCPs

A BCP is described as any crossing point at land, sea, river, lake or air borders, authorised by the competent authorities for crossing a state border In total there are approximately 1.800 BCPs at EUs external borders of the Schengen area.[6] In fact, as depicted in Figure 1-2, there exist three types of BCPs: land BCPs, seaports (maritime) and international airports (air).

[6] From the presentation on smart borders by Anna Herrera de la Casa (DG Home, Unit C3 – TransEuropean Networks for Freedom and Security & relations with eu-LISA), Madrid, 25 June 2014.

At the BCPs border control takes place (IBM tier 3), which is described in the IBM Guidelines as *"an activity carried out at a border in response exclusively to an intention to cross that border or the act of crossing that border, regardless of any other consideration. It covers:*

- *checks carried out at authorised border crossing points to ensure that persons, their means of transport and the objects in their possession may be authorised to enter the territory of the country or authorised to leave it;* [and]
- *surveillance of borders between authorised border crossing points and the surveillance of border crossing points outside the fixed opening hours to prevent persons from circumventing border checks."* (European Commission, 2010, p.10)

Within TRESSPASS only the first activity is covered, because border surveillance is beyond the scope of the project (see Section 1.2).

2.4.1 Border checks and decision options at BCPs

In alignment with IBM tier 3 everyone who wants to cross EUs external border has to be checked.[7] In TRESSPASS deliverables D1.4 and D9.6 a check is conceptualised as "*performing the access and egress control function based on the revelatory function with regard to the movement of persons and the goods they bring along with them (including the means of transport) at the external borders of the EU*". This check is done by qualified border officials who have the required knowledge and skills for checking and verifying the validity and authenticity of all necessary documents (e.g. passports or visa), consult criminal databases, inspecting luggage and vehicles (e.g. to detect weapons, drugs or stolen goods), and detecting suspicious behaviour and/or circumstances. This is a risk mitigation measure, which can be visualised in a risk reduction overview (Havinga, H. N. J., & Sessink, O. D. T. 2014).

Checks reveal information from a traveller to a relatively high degree of reliability. Obtaining a high degree of reliability typically requires time (check duration) and interaction. The impact on the flow of travellers is further discussed in section 0.

All persons who want to cross the border will be subjected to identity checks performed by border officials. Travellers are required to show a valid travel document. In addition, border officials check whether the traveller's name is on a watchlist. In case of non-EU travellers, so-called Third Country Nationals (TCNs), additional checks are carried out. These checks are depending on the agreements between Europe and the concerned TCN's country. If a visa is required its validity will be checked. In fact, at the point of entry the purpose and duration of the stay in Europe should be clear, as well as the fact whether one can afford his stay.

In exceptional situations the Schengen Borders Code (Regulation (EU) 2016/399, Article 9) offers the opportunity to the BCP command to temporary relax the checks. It concerns circumstances *"where unforeseeable events lead to traffic of such intensity that the waiting time at the border crossing point becomes excessive, and all resources have been exhausted as regards staff, facilities and organisation* [taking into account that] *border checks on entry movements shall in principle take priority over border checks on exit movements"*.

[7] *"All persons shall undergo a minimum check in order to establish their identities on the basis of the production or presentation of their travel documents. Such a minimum check shall consist of a rapid and straightforward verification, where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorising the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting."* (Regulation (EU) 2016/399, Article 8).

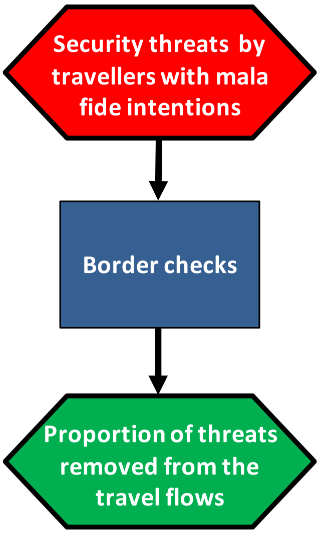

Security threats by travellers with mala fide intentions
Border checks
Proportion of threats removed from the travel flows

FIGURE 2-2 RISK REDUCTION OVERVIEW FOR BORDER CHECKS

When checking persons and their luggage and/or vehicle border control officials have the following options:

- Permit a person to enter or leave the country unconditionally;
- Permit a person to enter or leave the country under certain conditions, such as
    - permission to enter only for a temporarily stay in Europe, or
    - permission to leave only after having settled unpaid taxes or fees;
- Refuse a person to enter or leave the country for a legitimate reason (e.g. in case of missing documents or in case of a 'persona non grata' who wants to enter the EU);
- Hold or detain a person in case he/she:
    - presents falsified documents,
    - is on a watchlist (e.g. for terrorist activities or missing persons),
    - shows suspected intentions or activities,
    - possesses stolen or suspected (forbidden, dangerous) goods or animals,
    - drives, flies or sails a stolen vehicle;
- Transfer of a person who makes a request for asylum to the immigration officials; and
- Put the person in quarantine in case of a serious infectious disease.

In addition, (first line) border control officials have the option to carry out a closer inspection (second line) before taking one of the decisions listed above.[8] They will do so anyhow when they need or want to know more or have any doubts about a person, his luggage and/or vehicle. But they can do so for other reasons as well. For instance, by executing closer inspections randomly or unexpectedly. Thus introducing a form of surprise in the border control process to keep potential malicious travellers in suspense, but also as a kind of validation of the current approach of border checking.

[8] The Schengen Borders Code states: *"'second line check' means a further check which may be carried out in a special location away from the location at which all persons are checked (first line)"* (Regulation (EU) 2016/399, Article 2).

2.4.2 Rule-based decision making

It should be noted that the current decision-making process on who has to be checked often is strictly rule-based. As depicted in Figure 2-3 every traveller who wants to cross the border at a BCP has to be checked by the border authorities indiscriminately; i.e. according to the same rules. In practice non-EU citizens likely will receive a more thorough check at EU's external borders than EU citizens, because of specific requirements such as required visa.[9]

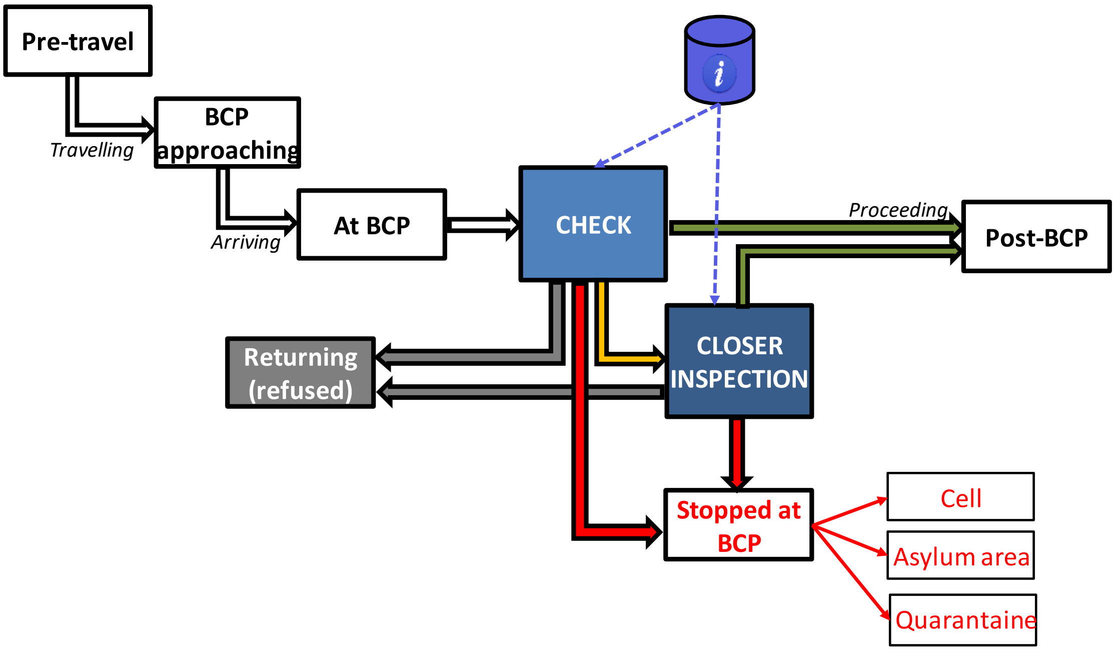


FIGURE 2-3 OVERVIEW OF A TRAVELLER'S JOURNEY AND DECISION OPTIONS OF BCP AUTHORITIES

In Figure 2-3 the white arrows represent the flows of travellers before they arrive at the BCP. The colour white represents the fact that nothing is known about the travellers and their journey until they arrive at the BCP. To check or inspect flows of travellers border officials at BCPs make use of information systems that are described in Section 2.4.5 (blued dotted lines). In alignment with the decision options that are described in Section 2.4.1, the check will result in a permission to proceed (green arrow), a closer inspection (orange arrow), a certain kind of 'isolation' (red arrow) or a refusal (grey arrow). The closer inspection will result in the final decision: permission to proceed (green), isolation (red) or refusal (grey).

2.4.3 Intelligence-led decision making

As an extension of rule-based decision making, at certain BCPs (especially at airports) the checking process is supported by collecting and screening information of travellers before they actually arrive at the BCP. The purpose of intelligence-led decision making is to improve the organisation of the checking process based on validated information and knowledge that has been gathered through, for instance, checks at the gate or special attention given to certain types of (suspected) vehicles. As a consequence the overall flow of travellers can be

[9] For instance, questions can be asked to verify one's background and identity, or to inform about the duration of and the reasons for his stay in Europe and to check to what extent he can pay it.

smoother (i.e. a higher flow-rate). Figure 2-4 shows the expected benefits of the intelligence-led approach (yellow dots) in comparison to the rule-based approach (red dots).

Although the checks at the BCP are similar as those in the rule-based approach, a potential extra benefit of the intelligence-led approach is an increase in the effectiveness of border control. This because border guards have more information at their disposal when checking travellers.

It should be noted, however, that despite the above-mentioned benefits of the intelligence-led approach the problem that increasing flows of traffic pose on border control, in the long-term will not be solved. Because the checks remain the same, the flow-rate of travellers at BCPs is expected to decrease (represented by the downward yellow arrow).

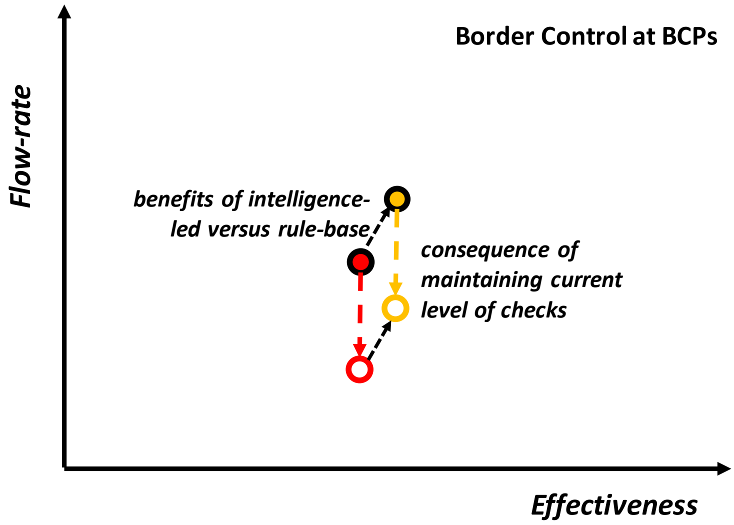

Border Control at BCPs
Flow-rate
Effectiveness
benefits of intelligence-led versus rule-base
consequence of maintaining current level of checks

FIGURE 2-4 BENEFITS OF AN INTELLIGENCE-LED APPROACH IN COMPARISON WITH A RULE-BASED APPROACH

The information gathered during the Pre-travel and the Approach BCP stages is depicted in Figure 2-5 by black dotted lines. This kind of information is provided by carriers and/or authorities from the own or other countries. This information is enriched by comparing it with intelligence data (e.g. the political, social and economic context of countries of origin), and with information that is present in the systems that are listed in Section 2.4.5. The results of this so-called screening process are used in the checking process, enabling border officials to give special attention to 'suspected' (coloured orange) and malicious (coloured red) persons; this can e.g. be facilitated by filtering flows of travellers that arrive at the BCP.

Screening and Check

In the context of border management, a screening is a rough assessment of the potential risk posed by a traveller. Screening is typically carried out without delaying the traveller. On the other hand a check is an assessment with a high degree of accuracy that is achieved by an (invasive) inspection of the traveller; this will typically cause some delay for the traveller. Where a check actually inspects a traveller, a screening does not do so.

One should note that the time available for screening purposes depends on the moment in which information becomes available. Some types of information become available quite early, for instance, when tickets are bought or visa are requested (Pre-travel stage). Other information becomes only available at the time of departure from abroad to the BCP (Approach BCP stage). Many relevant indicators for screening travellers cannot directly be observed directly. Instead, they have to be assessed in an indirect manner from other (observable) aspects. This is called profiling, which is discussed in the next section.

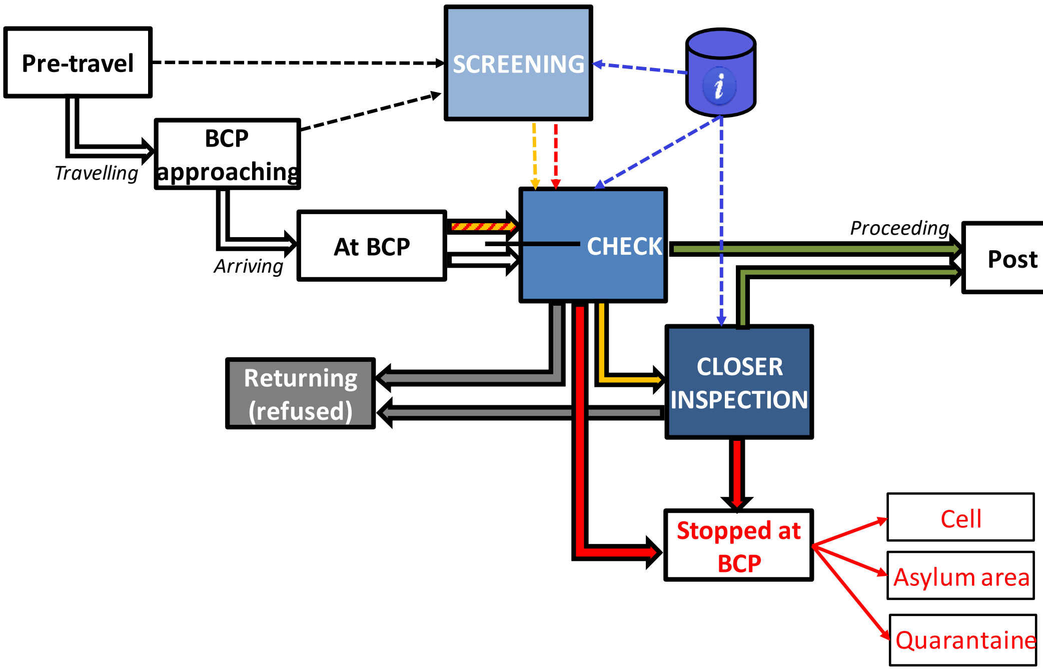


FIGURE 2-5 INTELLIGENCE-LED BORDER MANAGEMENT AT BCPS

A by-product of gathering information for a screening for border crossing, can be that it also generates useful information for other types of screening or checks, such as for travel security. This may be relevant to optimise the design of specific BCPs, but should not be leading in the selection of risk indicators for screenings for border crossings.

2.4.4 Profiling

Profiling is considered as an extrapolation of a certain characteristic of a person, a group or a situation based on other information of the respective subject (Van Rest, J.H.C., Roelofs, M., Van Nunen, A., and Don, S.B., 2014). Profiling can be used to draw attention to suspicious patterns (or the absence of normal patterns). As such profiling is a very powerful tool. However, profiling neither measures nor observes. It is merely a method using statistically founded assumptions. A hit or no-hit can be the reason for additional observation or inspection, but should never be used as evidence or to give weight to other evidence. When used incorrectly, profiling can lead to exclusion, discrimination, a fake sense of security and inefficiency.

In the context of BCPs, profiling is currently applied in practice by border authorities in the various travel stages of the traveller. It is often subject to the ‘four-eyes’ principle. Typical types of current profiles include:

- ‘Business-as-usual’: this type of profile describes normal travellers, and is based on experiences in the course of time (e.g. a year to be robust against seasonal patterns). A no-hit on this profile that cannot easily be explained, will result in a further inspection.
- ‘Known modus operandi’: this type of profile describes observable aspects of known modus operandi. A hit on this profile will also result in a further inspection, unless it can be easily explained.

- ‘Specialist profile’: this type of profile is based on individual expertise of experienced specialists. The purpose of this type is to ensure that even unknown types of modus operandi, which include those of well-prepared adversaries, can be spotted. A hit will always result in further inspection.

Profiling is currently done – often unaided – in situ at desks (e.g. at the passport check), at the entrance of security checkpoints (e.g. to select travellers for different screening levels), near queues, and during mobile patrols near BCPs. Profiles are taught through training and by sharing experiences between border guards. It is also done remotely, in a back-office, using automated tools.

Note that tens or even hundreds of different profiles can be active at one BCP. These can be required for various purposes and therefore can be owned by the respective stakeholders such as border guards, law enforcement agencies and custom authorities.

2.4.5 Information systems

In support of their activities (both rule-based and information-led) border officials have a number of international information systems for border management and law enforcement at their disposal. These are:[10]

- Second version of the Schengen Information System (SIS II) records entry of and alerts on Third Country Nationals for the purpose of refusing their entry into or stay in the Schengen Area. SIS includes information on, for instance, lost identity documents, stolen cars and European arrest warrants.
- Visa Information System (VIS) facilitates the verification that a person presenting a visa is its rightful holder. This is done by using biometric data to confirm a visa holder’s identity allows for faster, more accurate and more secure checks.
- European Dactyloscopy (EURODAC) the EU’s asylum fingerprint database of asylum applicants and of TCNs who have either crossed the EU’s external borders irregularly, or who are irregularly staying in Europe.
- European Criminal Records Information System (ECRIS) provides criminal record information on convictions of EU nationals.
- Europol Information System (EIS) provides criminal information and intelligence covering all of Europol’s mandated crime areas, including terrorism Europol databases (Europol, no date).
- Interpol’s database of Stolen and Lost Travel Documents (SLTD) enables border guards to quickly ascertain the validity of passports, identity documents, and visas.

In addition to the above-listed systems border officials at air BCPs possess:

- The Advance Passenger Information (API) is information supplied by carriers to authorities that are responsible for carrying out checks on persons at external borders. It is sent to authorised BCPs through which these persons will enter the territory of a Schengen Member State. Carriers are obliged to transmit this by end of check-in (Council Directive 2004/82/EC, Article 3).[11]

[10] Information on these systems can e.g. be found in “EU Information Systems, Security and Borders”; EC DG Home; December 2017.

[11] Art.3 of Council Directive 2004/82/EC (Directive on the obligation of carriers to communicate passenger data)

- The Passenger Name Record (PNR) that concerns information provided by passengers and collected by airlines, in the normal course of their business, for enabling reservations and carrying out the check-in process (Directive (EU) 2016/681).

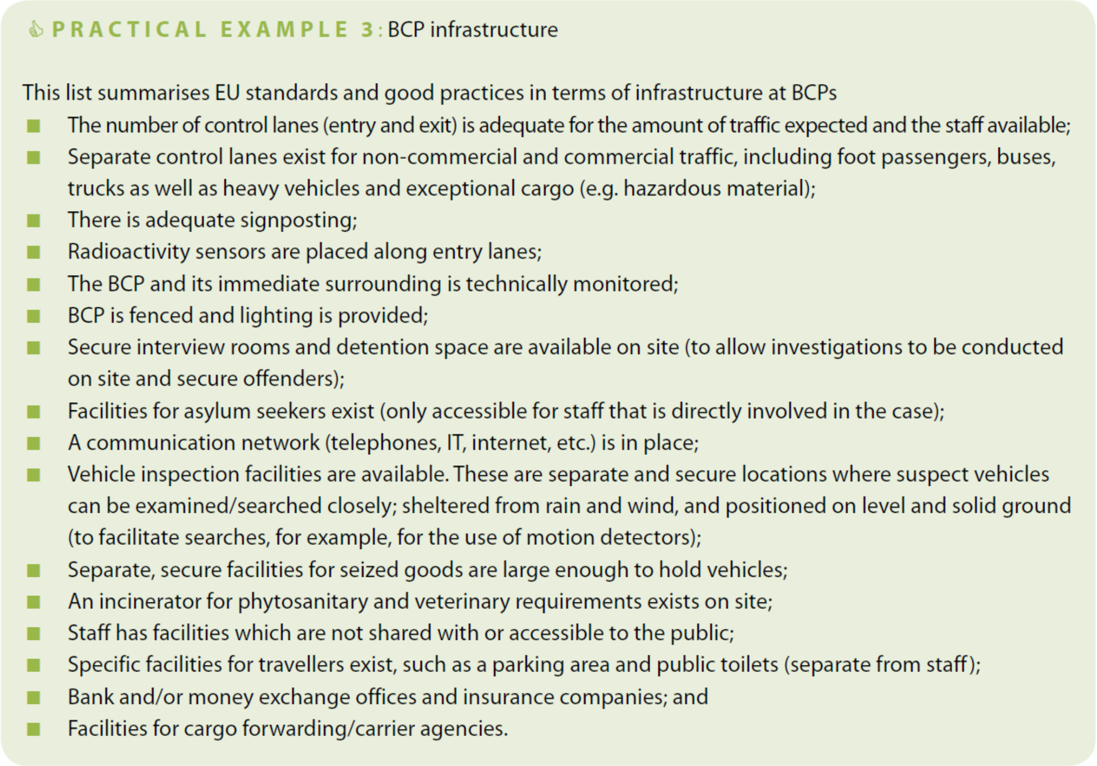
Border officials at maritime BCPs do not have API or PNR; they, however, possess:

- International Maritime Organisation (IMO) Crew-Passenger list that provides information about the number and composition of the crew on the arrival in and/or departure of a ship from a port of an EU Member State.

Furthermore, border officials at BCPs of individual countries can use various national systems.

2.4.6 BCP infrastructure

Figure 2-6 is derived from the IBM Guidelines (European Commission, 2010, page 51). It provides an overview of infrastructural requirements at a typical land BCP giving an impression of the environment in which the TRESSPASS concept and its future solutions will operate. In fact, despite the differences in modes of transport, the requirements of a maritime or an air BCP are roughly the same.



PRACTICAL EXAMPLE 3: BCP infrastructure

This list summarises EU standards and good practices in terms of infrastructure at BCPs

- The number of control lanes (entry and exit) is adequate for the amount of traffic expected and the staff available;
- Separate control lanes exist for non-commercial and commercial traffic, including foot passengers, buses, trucks as well as heavy vehicles and exceptional cargo (e.g. hazardous material);
- There is adequate signposting;
- Radioactivity sensors are placed along entry lanes;
- The BCP and its immediate surrounding is technically monitored;
- BCP is fenced and lighting is provided;
- Secure interview rooms and detention space are available on site (to allow investigations to be conducted on site and secure offenders);
- Facilities for asylum seekers exist (only accessible for staff that is directly involved in the case);
- A communication network (telephones, IT, internet, etc.) is in place;
- Vehicle inspection facilities are available. These are separate and secure locations where suspect vehicles can be examined/searched closely; sheltered from rain and wind, and positioned on level and solid ground (to facilitate searches, for example, for the use of motion detectors);
- Separate, secure facilities for seized goods are large enough to hold vehicles;
- An incinerator for phytosanitary and veterinary requirements exists on site;
- Staff has facilities which are not shared with or accessible to the public;
- Specific facilities for travellers exist, such as a parking area and public toilets (separate from staff);
- Bank and/or money exchange offices and insurance companies; and
- Facilities for cargo forwarding/carrier agencies.

FIGURE 2-6 BCP INFRASTRUCTURE – EU STANDARDS AND GOOD PRACTICES

At BCPs flows of travellers can be filtered by the border authorities based on one or more specific characteristics of the traveller (e.g. EU versus non-EU citizen). As a result of filtering, travellers will be directed at the BCP to different lanes to be checked by border guards (see also Section 0).

The Schengen Borders Code (Regulation (EU) 2016/399, Article 10) states that at air BCPs (international airports) *"Member States shall provide separate lanes, … in order to carry out checks on persons,* [….] *Such lanes shall be differentiated by means of the signs bearing* (agreed) *indications"*. For maritime and land BCPs Member States *"may provide separate* *lanes"* (Regulation (EU) 2016/399, Article 10). In fact, at land BCPs this is often done by discriminating between types of vehicles (in addition to EU/non-EU).

Flow of travellers

As described in Section 1.1, ensuring the continuity of the flow of travellers (and traffic) is an important aspect of border control. The **flow-rate** is the average speed of travellers when they cross the border at the BCP. As such it is an indicator for the continuity of the throughput of travellers at the BCP. Border checks have several negative effects on the flow of travellers and goods. From the point of view of the traveller, these effects can be called 'hindrance', while from the perspective of the travellers' flow they can be called 'friction'.

2.4.7 Base flow and friction

The speed at which people approach a BCP – the **base flow-rate** – varies between modalities and depends also on other factors such as the physical capabilities of the traveller. For instance, children and elderly tend to walk less quickly than healthy adults. So, existing BCPs already have many measures in place to facilitate the continuity of the various flows of travellers, e.g. by having created separate lanes for inherently slower travel groups.

The theoretical limit to which a BCP can facilitate border crossing in terms of flow-rate, is to have zero **friction** on the base flow-rate. For a land BCP this would imply that cars can remain driving at their normal speed (within the speed-limit), and that pedestrians and bikers can continue unimpeded. For an air, rail or maritime crossing, this would mean that travellers (typically passengers) can walk in or out the vehicle unimpeded.

2.4.8 Impact of check-duration on flow of travellers

The duration of a check is the time that a traveller occupies the resources for the check and thereby blocks the use of those resources for other travellers. This definition must be precise, because there are many ways in which the duration of checks are already optimised. Travellers can prepare a check by collecting and disclosing information, by altering their clothing, etc. A transition to risk-based checks is not about such optimisations, but about the selection of travellers for certain types of checks.

Depending on the function of a check, it can take anywhere between less than a second up to minutes or even longer. There is currently no unambigious overview of types of checks and their duration. Obviously, if a rule-based check does not take a significant amount of time, then there will be hardly any gaining of time by a transition to risk-based border checks.

Most checking procedures consist of two or more passes: a first line check and a secondary check. A quick first line check (of the flow) is done using highly optimised technologies and procedures. When a traveller fails this check, then he is subjected to the second more accurate check. This secondary check typically takes more time, which means the traveller also blocks the respective resources (including staff) longer for other travellers.

2.4.9 Impact of check-interaction on flow of travellers

Travellers and their goods must remain relatively stationary for the duration of the check. So even if a check takes a short amount of time, the traveller will still experience an interruption of his speed, and as consequence there will be at least some friction in the flow of travellers. In addition, he has to (to some degree) participate with the check in a conscious manner. This is a form of hindrance, and can negatively impact the traveller's experience.

2.4.10 Filters

A single BCP can accommodate different traveller types. To facilitate the flow of travellers, and to make sure that the proper screenings and checks are applied to travellers, a BCP consists of filters. A filter typically facilitates a type of traveller. The types depend on various factors, such as nationality, tasks and registration on traveller programmes. Examples of traveller types are (non-)EU travellers, frequent travellers or staff working at the border or working in the transport sector.

The physical part of these filters are implemented at the BCP, but procedurally these filters start before the traveller arrives at the physical BCP, and may extend after passing the BCP, this is conceptualised as the **integral filter**.

Each individual traveller has a specific starting point for his/her journey: they decide to enter in a specific integral filter. For example by requesting a visum, or by accepting a work schedule from their employer if they are staff. An integral filter can be considered as a combination of screening and checking efforts to determine whether the traveller can legitematly cross the BCP. Whereas a screening of travellers requires no physical interference, a check does. Hence, a check with everything it entails can be regarded as a minimal **physical filter**.

Figure 2-7 provides a schematic overview of an integral filter.

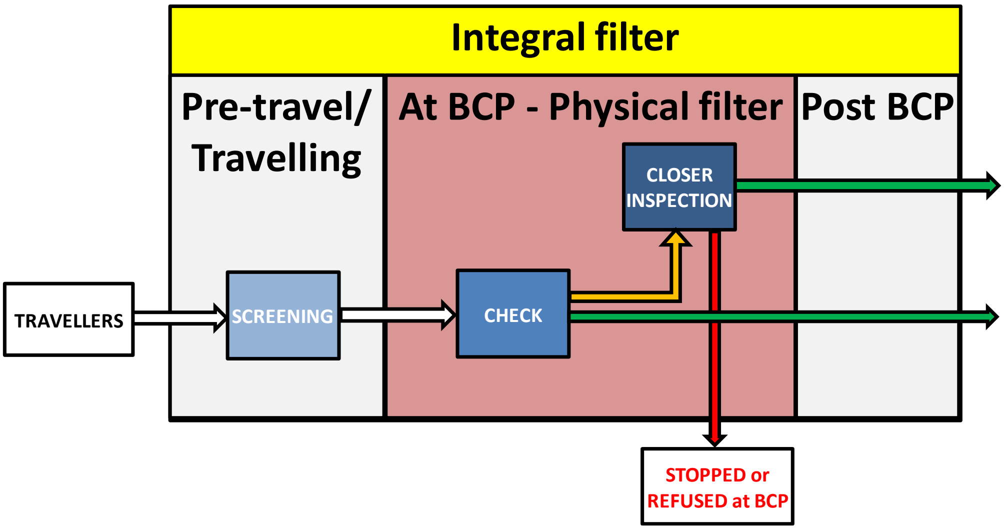


FIGURE 2-7 SCHEMATIC OVERVIEW OF AN INTEGRAL FILTER

In fact, a BCP conists out of multiple integral filters: depending on the type of traveller (e.g. EU or non-EU), a traveller enters a specific integral filter that consists out of different types of screening methods and/or checks (see Figure 2-8). As screening of travellers can be conducted before they arrive at the BCP, the integral filter exceeds the physical boundaries of a BCP.

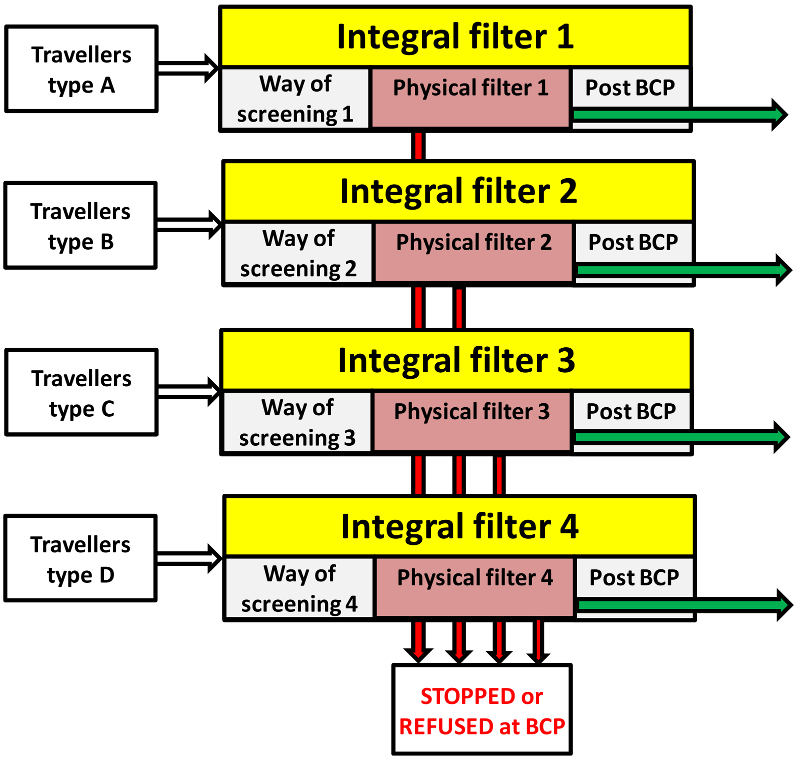


FIGURE 2-8 SCHEMATIC OVERVIEW OF FILTERING FLOWS OF TRAVELLERS BEFORE AND AT A BCP

2.4.11 Derivatives of flow-rate

Another relevant aspect is the subjective experience of the flow-rate. Travellers who move slowly but steadily may have a better subjective experience than travellers who move faster on average, but have to stop frequently in between.

There is also the difference between the physical throughput of travellers moving through a physical area, versus the flow of the same travellers through a process of a filter. The flow of the process should keep up with the flow through the area, otherwise people reach the point where they have to be diverted to a check (or not) before they are screened.

These insights about derivates of flow-rate can be combined in smart ways, depending on the preferences of BCP authorities and transport operators. For example, checks can be repeated, so that travellers that failed a first check can be directed to successive checks, while still allowing them to physically move forward.

2.5 Developments and initiatives

In addition to existing information systems there are several developments and initiatives to improve border control at BCPs that are or can become of interest to TRESSPASS. It concerns developments with respect to information systems (for instance to improve their usability and interoperability), while other address the mobility issues caused by increasing flows of travellers. Several solution directions are explored. First, BCPs can opt to automate larger parts of the process with the use of technology. Second, they can opt to systemically use information to make more efficient use of border officials. These solution directions are already in place at some BCPs, or are under development.

2.5.1 Developments of European information systems

Currently, the following information systems are proposed or are already being developed in Europe:[12]

- ECRIS-TCN, which is an extension of ECRIS, will enable the exchange of information on criminal activities committed by TCNs or stateless persons;
- Entry-Exit System (EES) registers dates and places of entry and exit, and calculates the maximum length that visa holders and visa exempted TCNs are authorised to stay. Furthermore, the EES provides information on refusals of entry;
- European Travel Information and Authorisation System (ETIAS) keeps track of visitors from countries who do not need a visa to enter the Schengen Zone for up to 90 days.

In addition, DG Migration & Home Affairs of the European Commission initiated the proposal for the European Search Portal: an EU Interoperability framework for border management systems (Figure 2-9). The objectives of this initiative are to: (1) ensure that end-users have fast, seamless, systematic and controlled access to the information that they need to perform their tasks, (2) detect multiple identities linked to the same set of biometric data, (3) facilitate identity checks of TCNs on the territory of a Member State by police authorities, and (4) facilitate and streamline access by law enforcement authorities to non-law enforcement information systems at EU level.

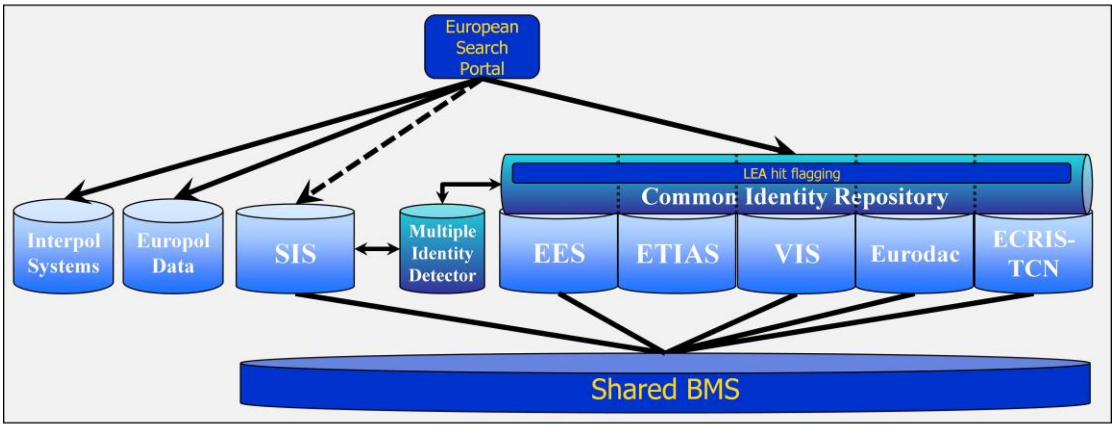


FIGURE 2-9 PROPOSAL FOR EU'S INTEROPERABILITY FRAMEWORK FOR BORDER MANAGEMENT SYSTEMS (RINKENS, 2018)

2.5.2 Other developments

Both inside and outside Europe there are also other interesting initiatives, which are briefly described in this sub-section.

2.5.2.1 Passengers Information Units

Each European country is required to implement the rules of the PNR directive of 27 April 2016 by establishing Passenger Information Units (PIUs): specific entities responsible for the collection, storage and processing of PNR data. *"The rules apply to flights arriving from third countries to the European Union Member States. Member States can decide to apply these measures to flights departing from and arriving to an EU Member State (intra-EU flights)."*

[12] See also "EU Information Systems, Security and Borders" (European Commission, 2017).

These units should (Migration and Home Affairs, no date):

- Compare PNR data against relevant law enforcement databases and process them against pre-determined criteria, in order to identify persons that may be involved in a terrorist offence or serious crime;
- Disseminate PNR data (booking, luggage, contact, payment) to national competent authorities, Europol and PIUs of other Member States, either spontaneously or in response to duly reasoned requests.

In case of travellers who are suspected of terrorism or serious crime,[13] information can be added. For instance about their appearance and potential abnormal or dangerous behaviour.

2.5.2.2 Registered Traveller Programme

The purpose of the European initiative for a Registered Traveller Programme (RTP) is to speed up, facilitate and reinforce border check procedures by using smart technologies that give frequent TCN travellers the option of pre-screening, so that they would be able to use the automated border control systems like Member States' nationals.

2.5.2.3 Local Border Traffic Regime

This regime is a derogation from the general rules governing the border control of persons crossing the external borders of Schengen States, which facilitates border crossing for border residents (Council Regulation (EC) 1931/2006). The Local Border Traffic Regime enables EU states to conclude bilateral agreements with their neighbouring non-EU countries so that the border residents can travel back and forth without a Schengen visa and, therefore, without any impediment trade, social and cultural interchange in the region concerned. It is therefore specifically of interest for land BCPs. It has been established for border residents who frequently need to cross the external borders.

2.5.2.4 CBP Preclearance

Customs and Border Protection (CBP) Preclearance provides border inspection and clearance of commercial air passengers and their goods at locations in foreign countries on behalf of the United Stated (US).[14] A preclearance inspection is essentially the same inspection an individual would undergo at a US port of entry and preclearance travellers do not have to undergo a second CBP inspection upon arrival in the US.

CBP Preclearance is focused solely on traveller processing (not on cargo). Processing includes any belongings (e.g. luggage, clothing, currency) a traveller intends to bring into the US. Preclearance does process immigration issues related to applying for admission.

As stated on the website of DHS preclearance operations are believed to

> *"assist efforts in identifying terrorists, criminals, and other national security threats prior to their boarding an aircraft bound for the United States, and is a critical step in DHS's continued efforts to enhance national security and facilitate growing international travel and commerce.* […] *In addition to enhancing security, Preclearance*

[13] To that purpose a list of types of malicious acts is used.

[14] Actually, it concerns mainly airports in Canada and in the Caribbean, under which Aruba (Netherlands), and only two in Europe at the airports of Dublin and Shannon (Ireland).

> *has the potential to increase capacity and create growth opportunities for airports and air carriers in the United States and abroad, while improving the passenger experience. Preclearance generates the potential for significant economic benefits for the United States and our international partners by facilitating travel through all gateways, creating an overall increase in clearance capacity, and maximizing aircraft and gate utilization."*

2.5.2.5 Seamless Flow

A promising development is the use of biometrics to facilitate processes at a BCP. An example of this is Seamless Flow that is currently being developed at Schiphol Amsterdam Airport. The aim of Seamless Flow is to *"enable a smooth passenger process whereby the required checkpoints can be passed easily, quickly and document-free"* (Van Dijk, 2017). The principle of Seamless Flow is that travellers who voluntarily register their biometric markers, e.g. fingerprints and facial scans, at the start of their journey may pass checkpoints at the airport more smoothly. Apart from the airport, other vital stakeholders in Seamless Flow are carriers (travel data) and national authorities (passport data).

It is expected that by automating process steps at checkpoints, controlling passenger flows will improve. Data from the checkpoints will supply more precise and real-time information, pinpointing where travellers are in the travel process. Because data are available earlier in the process, the border guards will have more time to conduct additional screenings when needed. In addition, it creates the opportunity to intervene on the traveller at more locations than just only at the border.

2.5.2.6 H2020 projects

There are various related projects in the domain of border control, and of which results are or can be of interest for TRESSPASS. One of these projects is iBorderCtrl (Intelligent Portable Control System) that focusses on combining state-of-the-art technologies for biometric verification, automated deception detection, and document authentication with a tool for risk assessment.[15] The main objective is to enable faster and thorough border control for TCNs who want to crossing the external borders at land BCPs. This project aims to achieve this goal by using pre-registration, and by reducing the subjective control (and thus workload of border officials) and increasing the objective control with automated means that are non-invasive and do not add to the time the traveller has to spend at the border. The results, such as portable devices, will be tested in three pilots at BCPs in Greece, Hungary and Latvia (iBorderCtrl, 2019).

Another relevant project that recently started, is PERSONA (Privacy, Ethical, Regulatory and SOcial, No-gate crossing-point solutions Acceptance). This project aims to fulfil the need for processing an increasing amount of border crossings and decreasing the pressure on border control systems by developing flexible, automated and scalable border security solutions. PERSONA strives to better manage personal information and to support the automated checking and analysing of various entry and exit data. It will include networks of sensors that

[15] The Risk Based Assessment Tool (RBAT) implements a risk assessment routine which aggregates and correlates the risks estimations received by the processing of the travellers' data and documents supporting the decision-making of the border guard.

collect information needed for border checks, without increasing the risk of loss of privacy (PERSONA, 2019).

2.5.3 Synthesis of developments

Notwithstanding the fact that the solutions and developments described in previous sections are necessary for future border management, they are potentially insufficient to handle the increasing flows of travellers. If BCPs remain exclusively dependent on rule-based principles for their border management, the foreseen challenge of mobility issues may be only postponed or temporarily addressed, but not mitigated in the long-term. The introduction of risk-based management practices can be a sustainable solution for this long-term issue. It can help to facilitate a better flow of people and their goods. This results in more throughput by separating people in at least two groups, and conducting:

- Minimal (relaxed) checks to travellers who are expected to pose no or very limited risk; and
- Thorough checks to travellers who are expected to pose a high risk.

In addition more groups and types of checks can be defined for risk situations in between.

It is expected that all three solution directions – i.e. extending the use of information, implementing new technology and risk-based border management – are required as they are depending on each other. The systematic use of information and (developing new) technology are main building blocks for BCP management, and can provide input for a risk-based border management approach.

3 Border Management – Challenges

This chapter lists needs and expectations that have been expressed by stakeholders who are involved in border management at BCPs. In addition an overview is provided of developments and trends that will or might affect border management in the (near) future. These two aspects – needs and trends – pose a number of challenges to the development of the risk-based concept.

3.1 End-user needs and expectations

Within Task 1.1, end-users' needs for and expectations of border control in general were identified through a review of the existing literature, a survey of border authorities, and a number of interviews with end-users. Their needs have been categorised by a number of key themes: identification and assessment of risks and threats, processes and functions, collaboration and cooperation, technology (IT systems, tools and data), training and simulation, and legal and ethical issues.[16]

In alignment with the call text, because of the increasing numbers of travellers stakeholders want a modernisation of the border control ecosystem. Potential solutions that have been mentioned by the end-users are the establishment of a common border control infrastructure and equipment at BCPs, the engagement of border officials in joint controls and operations, and lastly, the adoption of innovative solutions for identifying and managing threats. Several solutions were mentioned, such as the 'trusted passengers concept' – by using a database of travellers that have been 'pre-screened' – or the introduction of a pre-registration/ enrolment screening process[17] of travellers to enable the classification of travellers into risk categories ahead of their arrival at BCPs. The use of complementary information from open sources (OSINT) can be used for early determination of intent, capability, possession and/or identity of malicious travellers.

Various stakeholders expressed a need for the integration and adoption of technologies to improve early behavioural detection for cross-checking purposes and for applying these in a 'threat prediction system' that combines threats, modus operandi and risk indicators. The data that are fused in such a system can come from various sources (e.g. passport or ID card readers, fingerprint readers, eGates and CCTV systems).

Furthermore, there is a need to improve multi-agency cooperation and information sharing at international level, as is illustrated by the PIU's. Beyond sharing operational data to assess threats posed by specific travellers (such as API and PNR data), this need also extends to tactical data which describes (changes in) modus operandi, risk, profiles, information on aggregated (ab)normal travel-patterns and on vulnerabilities of specific BCP's. This can be achieved by standardisation of data sources, including dedicated technology to share these data, and by organising networking events or joint training to promote collaboration.

[16] More detailed information on these needs is provided in the TRESSPASS deliverable D1.1 – "End-user requirements and needs".

[17] This requires a registration/enrolment platform for travellers, which could be combined with a multi-lingual 'collaboration and information' portal for travellers to cover their lack of knowledge for border control processes (duties, rights and implications).

3.2 Trends influencing border management

3.2.1 *Global trends*

Apart from the needs and expectations that are mentioned in the previous section, there is a number of trends in society and in technology that are important because they have the potential to influence border management at BCPs in the short or longer run. In its report on future border management, PwC (2015) analysed the impact on border management of the five global megatrends: demographic and social change, shift in economic power, rapid urbanisation, climate change and resource scarcity, and technological breakthroughs. With respect to border control at BCPs the PwC study foresees the following impact:

- Increasing mobility of people due to globalisation leads to increasing volumes of legitimate and illegitimate travellers, and thus to an increasing pressure on border crossing infrastructures. Therefore, in alignment with the goal of the TRESSPASS study, governments need *"to think about new ways to regulate travel in partnership with operators to effectively 'offshore' controls and to use technology solutions to track movements, secure identity and automate decision-making"* (PWC, 2015, p.6).
- Exponential growth of the movement of goods and services caused by open market conditions. As a consequence *"governments need to respond to increasingly evident challenges such as the smuggling of illicit goods"* (PWC, 2015, p.6).
- Shifts in global power that result *"in a burgeoning middle-class in developing nations and increases export production and opportunities for the movement of people and goods, which in turn, are capable of being exploited by criminal enterprises"*.
- Promising opportunities in the domain of border control because of significant technological breakthroughs in the fields of:
    - Data analytics that support screening activities by having created risk profiles based on data that is collected from multiple public and private stakeholders;
    - Biometrics enabling to verify the identity by using fraud independent biometric data.

Furthermore, the general trend of decreasing amounts of people that are employed within the public sector needs to be mentioned. To what extent this decrease is present in the case in staffing border control in the various member states is not clear. However, the aim for more efficiency – more output with less resources – is quite universal: *"Governments are asked to do more, do it better, and do it with the same amount of taxes"* (McKinsey, 2007). This implies the ever-increasing importance of applying new technology, such as the constant need for further developments in automation (digitalisation).

With respect to the scope of TRESSPASS it can be concluded there are two important trends. First, the increasing numbers of travellers that will cross EU's external borders due to globalisation, the still increasing world population, the political instability in many countries outside Europe resulting into increasing (irregular) migration. Second, the changes in type and size of threats. Here, one may think of changes in terrorist activities all over the world, and of the increasing professionalisation, and the adaptiveness of organised crime (e.g. rapidly changing modi operandi). Furthermore, one may think of threats related to public health change (epidemics). Due to the growing mobility and numbers of travellers from all over the world infectious diseases, will spread faster and more easily.

3.2.2 Towards pre-border screening

As described in deliverable D1.1 *"new technologies should help Member States to deal with increasing travellers flows, without necessarily increasing the number of border guards, and to promote mobility between the Schengen zone and third countries in a secure environment. It is therefore necessary to work towards integrated solutions for improved accessibility to data for border management and security, in full compliance with fundamental rights."* There is a preference of moving towards pre-border screening of travellers. The steps in border control then could be:

1. Pre-border check with help of an application to verify the identity of travellers, including answers to a number of questions;
2. Guiding travellers through different control lanes along border guards (note: lanes can be assigned to travellers based on information that has been gathered in advance);
3. Asking, if needed, additional questions by the border guard.

As proposed by the EC in the Smart Borders package *"the automation of the steps and procedures also allows guards to fully concentrate on assessing the individual profiles"* and *"implementation would allow for an increased rate of traveller checks in a given time interval at first-line control without necessarily having to increase the number of border guards"*. The information systems that are required for such an approach should be interoperable as much as possible.

3.3 Synthesis of challenges for border management

With respect to border control, there is the 'conflicting' matter of protecting the national security that requires sound border control on the one hand, and stimulating mobility on the other hand, which demands the smooth movement of people (for comfort and acceptance) and of goods (for economic reasons). This means that innovative solutions at BCPs should improve effectiveness and/or the smooth flow of travellers. Furthermore, it is required to fulfil the needs for improvement, and to take into account the trends that are dealt with in the previous section (Section 3.2.1).

To meet these challenges, TRESSPASS is investigating the opportunities for management approaches at BCPs that make use of so-called risk-based screening of flows of travellers. In fact, it fits with the trend towards pre-border screening. One of the core principles is that the screening is extended – in comparison to traditional approaches – with a risk assessment (RA) of each traveller.

Figure 3-1 illustrates how the risk-based approach works. Each traveller is risk-assessed through the analysis of data that is gathered in advance of his arrival and at the BCP. These data are compared with so-called risk profiles. Based on this assessment, the severity of the check of each traveller is determined, for example, minimum check (green), regular check (white), or extensive check (red/orange).

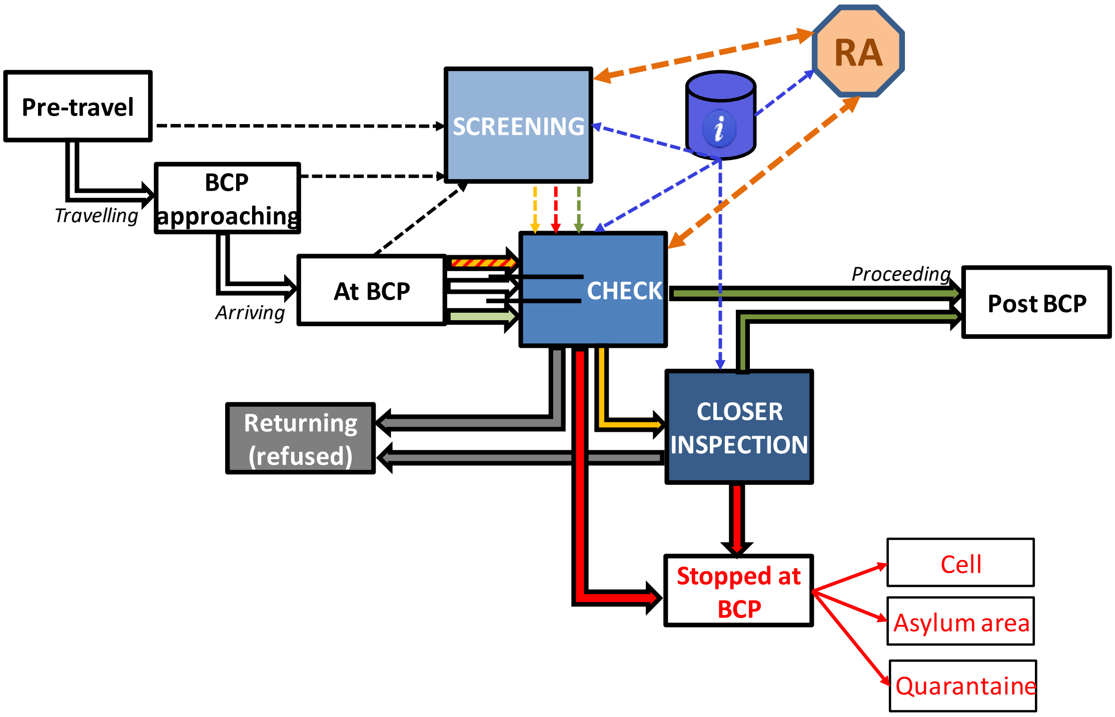


FIGURE 3-1 RISK-BASED BORDER MANAGEMENT AT BCPS

Similar as to intelligence-led and rule-based BCP, a risk-based BCP consists out of multiple integral filters. But, whereas an intelligence-led filter consists of a rather predetermined continuation of screening methods and checks (based on existing rules how to screen and check specific traveller types), in a risk-based filter travellers are subjected to tailored checks based on the outcome of one or more screenings. Figure 3-2 illustrates a risk-based filter at a BCP.

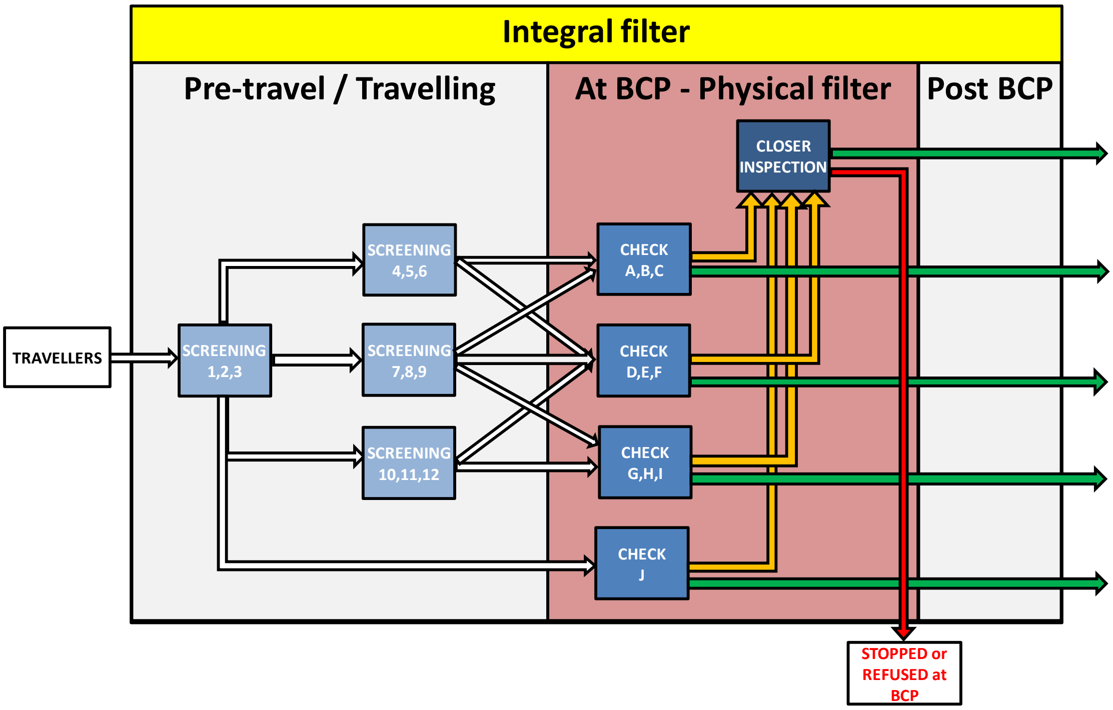


FIGURE 3-2 SCHEMATIC OVERVIEW OF A RISK-BASED FILTER AT A BCP

So, a risk-based BCP (and filter) typically consists of a wider variety of types and levels of checks, and these checks are preceded by a more extensive set of screening methods.

The mission of the TRESSPASS project is the elaboration and initial testing of the risk-based approach on its effectiveness and feasibility. In addition there are some other challenges to be kept in mind as well. These are:

- The concept should encompass border control of travellers at BCPs of different types of borders and modes of transport: land (cars, trains, trucks, bicycles, pedestrians, etc.), maritime (several types of sea transport), and air.
- Information exchange is one of the core principles of risk-based border management. However, the General Data Protection Regulation (GDPR) poses certain restrictions on the exchange of personal data that has to be taken into account by the concept (see also deliverable D1.4 – "Analysis of the legal and regulatory framework").
- National governments have a stake. Although the concept is developed for Europe, national governments can have more strict regulations or laws which could undermine the basic principles of risk-based border management (i.e. international cooperation and data exchange). Section 6.2 goes into the possible consequences of this issue more deeply.

In Chapter 4, the main principles of the risk-based border management concept are explained in more detail.

4 RISK-BASED BORDER MANAGEMENT AT BCPS

This chapter provides an introduction into, and a global explication of, a risk-based approach for border control at BCPs. Based on the general risk management norms (NEN-ISO 31000, 2018) and border management documents (CIRAM, Frontex, 2012; IBM, European Commission, 2010)[18], the premise and key elements of risk-based border management at BCPs are described. The general understanding of RBBM that is described in this chapter is used as foundation of the conceptual framework that is presented in Chapter 5.

This chapter starts with identifying the expected benefits of RBBM and which border management challenges, either current or future, this approach aims to solve. Hereinafter, the main elements and basic principles of RBBM are described. The risk-based concept for a BCP is defined and illustrated with a number of characteristic examples. A dedicated section describes how risk-based decision-making progresses throughout different governance-levels, and what this implies for the BCP's information needs. Finally, a number of prerequisites for RBBM are listed.

4.1 RBBM and its potential benefits

As described in Section 2.4, a BCP is a crossing-point authorised by the national authorities for crossing an external border of Europe. Its main purpose is to ensure that unauthorised travellers or goods are prevented from crossing Europe's borders by means of effective border control. As stated in the call text (see Section 1.1) it *"must also allow for the smooth movement of people and goods"* (European Commission, 2015). Therefore, the RBBM approach aims to facilitate these tasks by increasing both the effectiveness of border control and the flow-rate of travellers at the BCPs.

Risk-based approaches are used to select mitigation measures that are proportional to the situation specific risk assessment of a situation, person or object. In the case of border management, this would be a traveller. It is typically introduced under the condition of maintaining or even reducing its residual risk with regard to the original rule-based approach. For example, in civil aviation security (EC Regulation 300/2008) "*Member States should also be allowed, on the basis of a risk assessment, to apply* ***more*** *stringent measures than those laid down in this Regulation."* (emphasis added).

In border control this would mean: minimal checks if possible, more stringent checks when needed. To achieve this, the type of checks should be based on a situational threat assessment of each individual traveller, based on actual information on threats and vulnerabilities. This implies that for people and goods that are found to pose an insignificant threat in that situation, the number of invasive checks at BCPs can be limited. It is expected by border officials and policymakers that this is the case for the vast majority of people and goods, because most travellers do not pose any threat, and because border officials and policymakers assume that RBBM can be designed in such a way that the threat can be accurately assessed

[18] IBM (2010) is the official Guideline for Intergrated Border Management in Europe. CIRAM (2012) is the Common Integrated Risk Analysis Model that provides a methodological framework for risk analysis in border management.

for a large amount of travellers[19]. As a consequence, this will lead to fewer and shorter interruptions in the flows of travellers and goods, and to more freedom for most travellers.

The intended benefits of a risk-based approach in comparison to the current rule-based and intelligence-led approaches are:

- More effective (i.e. better risk reduction at) border control at border crossing points, among others because of more (local) adaptivity in case of changing trends and actual threats and vulnerabilities within internationally agreed conditions;
- Smoother flows of travellers (i.e. reducing friction of flows); and
- More proportional checks which are expected to lead to more support for border security measures with travellers, the general public and policymakers.

It is expected that these benefits can be realised without increasing operational costs, i.e. without decreasing efficiency. This expectation is based on the assumption that capacity that can be saved from checking low risk travellers can be allocated to checking high risk travellers.

By applying RBBM in Europe, Member States and BCP operators will get more freedom to design dedicated filters at their BCPs (see Section 2.4.5). It should be noted, however, that this freedom implies that Member States and BCP operators should be aware of their responsibility for the effects of those new designs – both, with regard to a design's intended and unintended effects. Apart from operational costs, the latter also includes a design's ethical, legal and societal impact on the travelling public (see Figure 4-1). Three kinds of impelling principles should always be weighed against the anchoring principle of ethical compliance.

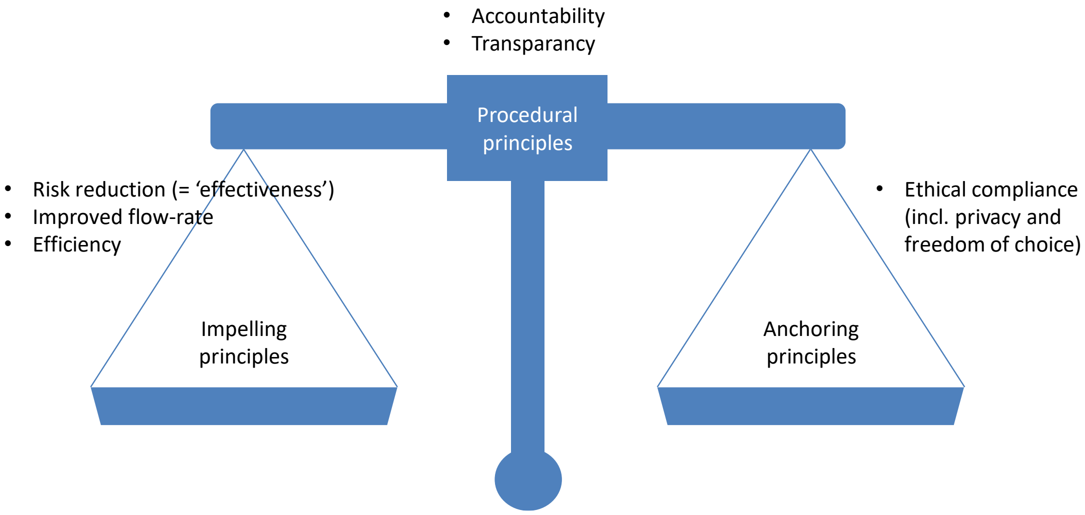


FIGURE 4-1 EFFECTS OF RBBM HAVE TO BE CONSIDERED INTEGRALLY. INSPIRED BY (WRR, 2011).

Table 4-1 provides an overview of the indicators that describe the performance of a BCP. Next sub-sections describe the main effects of RBBM on these indicators – risk reduction, flow-rate and efficiency – and on some other derived or related terms including the ethical compliance.

[19] The difference between threat posed by a traveller, and actual benefits gained by a specific (risk-based) BCP-design is covered in section 4.5.2.

TABLE 4-1 BCP PERFORMANCE INDICATORS

Indicator	Description
Effectiveness	Success-rate of stopping unauthorised travellers when they attempt to cross the border at the BCP
Flow-rate	Speed of the flow of travellers as they approach and cross the border at the BCP
Efficiency	Number of resources required at the BCP to achieve a certain degree of effectiveness and/or certain minimal flow-rate
Level of ethical compliance	Extent to which a BCP mitigates negative ethical impact on the travelling public and on the public in general

The focus of risk-based BCPs can be one-sided, when only the (beneficial) effects on one of the factors effectiveness, flow-rate or efficiency are mentioned. Stakeholders can either knowingly or unknowingly have biased expectations of risk-based border crossing points. In reality, these factors are intrinsically linked and need to be addressed in an integral manner.

Risk-based border management can lead to a reduction in residual risk: Excluding travellers from checks based on screenings that are less reliable than the check is per definition less effective (i.e. a worse type of risk reduction) than including all travellers in the checks. This is further illustrated by examples of specific risk-based concepts in section 4.8.2. However, one cannot deduce that risk-based border control therefore has a higher residual risk. Quite the opposite, risk-based border management is about proportional measures, which implies that it is possible to combine risk-based concepts that together generate equivalent or better residual risk, for example by combining a risk-based concept that more stringently checks unknown persons of interest with another risk-based concept that excludes from checks travellers with a low risk profile. This is the topic of TRESSPASS task T2.1.

The main beneficiaries of a transition to risk-based BCPs depend amongst other things on the specific risk-based BCP concept. There is no guarantee that travellers, border agencies or BCP operators benefit economically from such a transition. The only guarantee is that, if introduced and operated well, travellers will experience proportional checks.

4.1.1 Impelling principles (purpose, effectiveness and efficacy)

As stated before, the purpose of BCPs is to facilitate legitimate border crossings by checking whether travellers and their goods are authorised to enter and/or to leave Europe. The purpose of these checks is to prevent unauthorised travellers passing the border. The effectiveness of a BCP can be considered as the extent to which these goals are achieved. So, the first element of effectiveness is the **contribution to risk reduction**. This is what is typically meant when the effectiveness of borders, BCPs and checks is discussed.

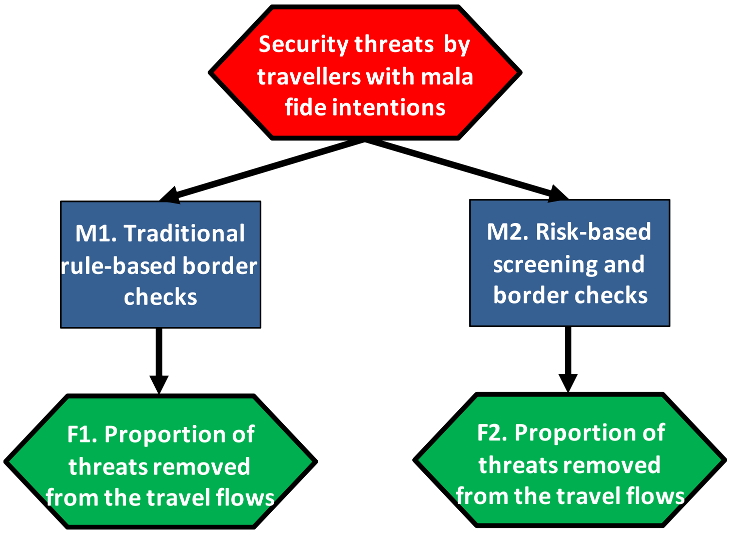

Security threats by travellers with mala fide intentions
M1. Traditional rule-based border checks
M2. Risk-based screening and border checks
F1. Proportion of threats removed from the travel flows
F2. Proportion of threats removed from the travel flows

FIGURE 4-2 RISK REDUCTION OVERVIEW DESCRIBING RISK-BASED VERSUS TO RULE-BASED BORDER CHECKS

The second element is **the contribution to flow-rate**. Risk-based concepts that reduce the average time spend in checks (see section 2.4.8), and that reduce the interaction required with travellers (see section 2.4.9), have significant economic benefits for the economies of the areas that depend on the flow of people and goods that are facilitated by the BCP. This economic benefit is often an important justification for the transition from traditional to risk-based BCPs.

When discussing effectiveness in a R&D project such as TRESSPASS, it is essential to be clear about the validity of the results the project in order to avoid raising unrealistic expectations. TRESSPASS cannot research the effectiveness of RBBM or of risk-based BCPs, but only the efficacy.

The efficacy of a border check is whether it works under ideal (i.e. typically controlled and/or carefully scoped) circumstances. In the context of (risk-based) BCPs, efficacy is typically used to describe two different situations:

First, efficacy is used to describe capabilities that are under development. For example, TRESSPASS is a research project at TRL7. TRESSPASS will use pilots with a mix of operational and simulated data (e.g. through the use of red teams) to investigate the *efficacy* of risk-based border crossing points. However, because TRESSPASS itself will not implement and operate risk-based BCPs in practice, it cannot study their *effectiveness*.

Second, efficacy is also used to describe the workings of a part in a wider context. For example, suppose a border check works at 100% accuracy, but as a side-effect, it has a very high chilling effect: many normally authorised travellers are afraid to use the BCP because of the way the border check works. In such a scenario, this border check may be *effective* for its own purpose. But its *efficacy* in wider perspective, i.e. its contribution to the purpose of the BCP which is also to facilitate border crossings, is very low. In a second example, data collection technologies may be very effective in the limited sense that they collect reliable information, but if they assess indicators that have a very low contribution to risk assessment, or only for a very small set of travellers then it is not effective in the wider sense.

4.1.2 Unintended effects and anchoring principles of RBBM

To assess the unintended effects of a technical system design or concept is a crucial step towards increased responsibility and more informed decision making. Unintended (or side-)

effects can be positive or negative and it is hard to define the scope of what aspects should be taken into account. Figure 4-3 illustrates how these unintended effects can also be seen as risks created by the BCP-design itself.

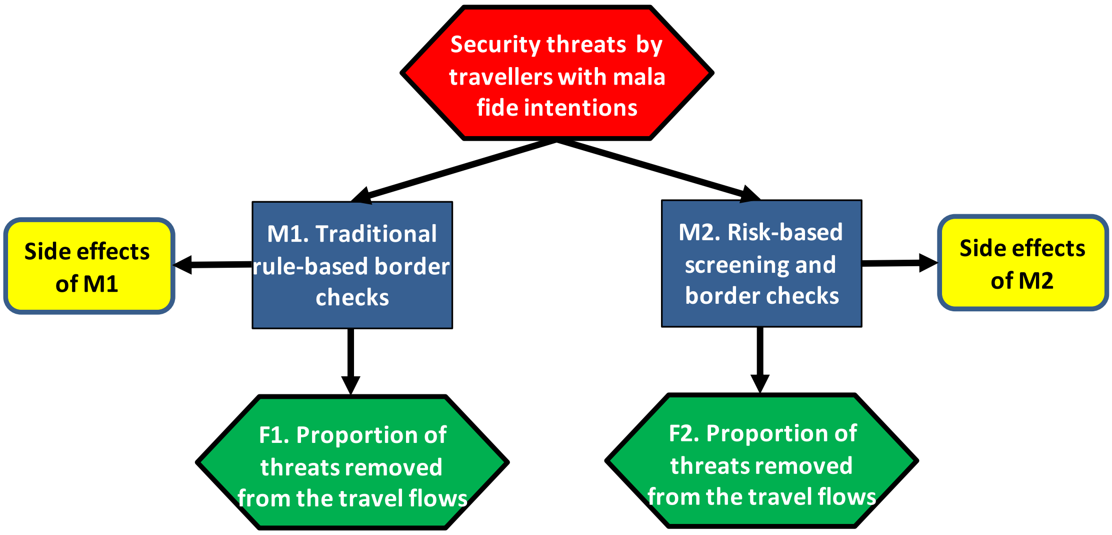

Security threats by travellers with mala fide intentions
Side effects of M1
M1. Traditional rule-based border checks
M2. Risk-based screening and border checks
Side effects of M2
F1. Proportion of threats removed from the travel flows
F2. Proportion of threats removed from the travel flows

FIGURE 4-3 RISK REDUCTION OVERVIEW OF BORDER CHECKS AND PLACE HOLDERS FOR POTENTIAL SIDE EFFECTS

For introducing RBBM, examples for unintended effects could be that:

- Bona fide travellers plan less time for crossing a border, which decreases the chance that they also use commercial functions around the BCP (restaurants, hotels and entertainment);
- Mala fide travellers experience a different deterrence effect (see next section);
- travellers waiting before the check become a less attractive target of terrorists when queues are shorter or more dispersed.
- Legitimate travellers experience a different chilling effect (see next section) (EFF, 2003):
  - more severe impact, because all travellers are subject to additional collection and processing of personal data as more information is required for the screening and risk classification activities,
  - less severe impact, because fewer travellers have to undergo stringent second line checks at the BCP, such as opening the luggage for customs or being interviewed by border guards.

These side effects are highly relevant for stakeholders, including the travelling public, so they should be taken into account when designing risk-based BCPs. Many of these unintended effects are not unique to the introduction of RBBM. Hence, it makes sense to assess relevant side effects of a risk-based BCPs in comparison to existing BCPs (or realistic best-case or worst-case scenarios for current, rule-based checks), not in isolation (cf. TRESSPASS deliverable D9.6 p. 13-14).

Regarding the anchoring principles, in TRESSPASS, a value sensitive design for RBBM has been applied (cf. section 6.3.2 in this document). This means that unintended effects with regard to ethical, legal and societal aspects (ELSAs), such as privacy and data protection issues, are taken into account "by design". In order to do so, relevant ELSAs for RBBM have been identified in deliverable D9.6, which will subsequently allow the formulation of ethical design requirements, e.g. privacy requirements[20]. Table 4-2 gives an overview over the relevant ethical side-effects that will be analised in TRESSPASS.

TABLE 4-2: RELEVANT ELSAS FOR RBBM

ELSA category A: Privacy and data protection	ELSA category B: unfair distribution of impact across different social groups	ELSA category C: restrictions of societal freedoms and liberties
Intrusion into spatial privacy	Disproportionate impact due to infeasibility of standard checks	Accosting travellers
Intrusion into bodily privacy	Disproportionate impact due to accumulation of false alarms	Lack of accountability
Intrusion into private life	Disproportionate impact due to false or incomplete external data	Restriction of self-determination and misuse of data
Disclosure of information	Impact on non-travellers	Lack of transparency

4.1.3 Chilling and deterrence

Two types of subjective effects are of particular relevance because they explain links between three of the four main performance indicators: risk reduction, flow-rate and the ethical compliance. These are the chilling and deterrence effect.

4.1.3.1 Chilling effect

The chilling effect is the effect that people refrain from legitimate actions because of a (perceived) threat of negative consequences. In the context of border checks, refugees might be deterred from requesting asylum at a BCP because of a (perceived) threat of detention of themselves and/or their children. If this subjective chilling effect of the risk-based checks at a BCP makes legitimate travellers (meaning they would be authorised by border control if they attempted to) refrain from attempting to cross a border, then this should be considered a serious negative impact. First, it could be considered a violation of fundamental rights and freedoms. Second, it is arguably a dampening effect on the flow-rate of travellers, in the aggregated economic sense. Therefore, the evaluation of risk-based border crossing points must take changes in this effect into account.

The chilling effect, and changes therein, relate directly to one of the three main intended purposes of RBBM: more proportional checks which are expected to lead to more support for border security measures with travellers, the general public and policymakers. If RBBM leads

[20] As outlined by van Rest et al. (Van Rest, Jeroen, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen, 2014), when privacy requirements are formulated early-on in the design process, privacy problems can be taken into account “by design” by making use of best-practive privacy design patterns specific to these problems.

to a reduced chilling effect, then this support may even be expressed by travellers by opting more for risk-based BCP's, as opposed to traditional rule-based BCP's.

4.1.3.2 Deterrence effect

The deterrence effect is the effect that leads adversaries to refrain from illegitimate actions (Morall and Jackson, 2009). It can be caused by a fear of punishment, or by the perception that the chance of success is low. Deterrence is a complicating factor for RBBM. Without deterrence, a determined adversary (e.g. terrorists, criminals or irregular immigrants) would not perceive a barrier to make an attempt to cross a (risk-based) BCP, and the number of attempts of illegitimate travellers would be higher than it is with deterrence.

Stakeholders that want to use risk-based paradigm to better facilitate travel flows, rely on the assumption that only a small percentage of travellers constitute a threat. So for them, deterrence becomes much more important than in traditional 'rule-based' approaches.

Current theories of what contributes to deterrence include uncertainty about defensive capabilities (Morall, A. R. and Jackson, B. A., 2009). Security-through-obscurity[21] and unpredictability are therefore good security (in the wide sense) practices. Specifically, hiding what you know, and what your capabilities are, is considered one of the best ways to deter opponents. Obviously, this does not match with good practices for the protection of privacy, such as the sixth foundational principle of privacy-by-design: visibility and transparency – keep it open (Cavoukian, 2009; D9.6, p.31). This is a challenge that will be addressed in TRESSPASS deliverables D2.1 and D6.3.

The deterrence effect, and changes therein, relate directly to one of the three main intended purposes of RBBM: more effective (i.e. better risk reduction at) border control at border crossing points, among others because of more (local) adaptivity in case of changing trends and actual threats and vulnerabilities within internationally agreed conditions. If RBBM leads to an improved deterrence effect, then less illigitimate travellers attempt a border crossing, thereby improving the security of member states. It must be noted however that currently, border checks do not legally have a preventive (e.g. through deterrence) function.

4.1.4 Checking capacity and efficiency

Efficient BCPs require relatively few resources in relation to reach a certain effectiveness and flow-rate. The influx at the BCP varies over time. So the resources used are governed by the average number of travellers passing the check-point over time. The available resources directly impact on the flow-rate. Peaks in the influx will temporarily overload checks, delaying and interrupting the flow of travellers. Traditional business intelligence can help determine expectations in the influx of travellers. In addition, intelligence-led border checks can help assess in advance which travellers might require more checking resources (e.g. because they typically need a secondary check, or further processing such as detainment). This helps to further organise capacity in a timely manner and reduces unnecessary overcapacity of resources during the off hours. However, this does not constitute a risk-based border check yet as all checks are identical and every traveller is subjected to every check.

[21] Security through obscurity means that the enemy does not know the inner workings of a system, and that this leads to a disadvantage for him. However, it is not wise to rely solely on obscurity: the system should also be secure if the enemy knows the inner workings of a system. In addition, if friendly forces do not know the inner workings, then they cannot help improving the system.

A transition to risk-based border checks would require that based on intelligence obtained from one or more screenings, a traveller would receive a different type of check: either less or more stringent than the default check, requiring either more or less checking resources. Based on the interviews and other interactions with border agencies and Frontex, it is learnt that they assess that a high percentage of travellers would then require less checks, thereby reducing the required checking capacity at the cost of some increased screening capacity.

Whether this leads to more efficiency depends on the rule-based starting point and on the specific risk-based concept. For many combinations of screening and checking, it may not be efficient for the border agency to increase the screening in order to reduce border checks. That could be acceptable if the concept significantly improves the flow-rate which would benefit businesses in the vicinity of the BCP and indirectly the economies of the respective countries.

4.2 The main elements that support trust in RBBM

When considering a risk-based approach at BCPs, trust amongst and between stakeholders is of vital importance. A mutual trust relationship is essential between the general public, border agencies, commercial operators and travellers, all of whom are impacted by introducing the risk-based paradigm.

As this border management approach relies on extensive gathering and collection of data and information on travellers by border agencies, they should be trusted that this is done for the purposes legally defined for border checks, that it is an effective measure and that it is done proportionally and carefully with regard to the rights and freedoms of travellers.

If such a trust network fails or is, for whatever reason, not sufficient, border guards will experience opposition when introducing new data sources.[22] Consequentially, they may need to resort to other legal means at their disposal to obtain information, with or without the cooperation from the commercial operators surrounding BCPs and travellers. This might include more intrusive forms of surveillance which would further erode trust, creating a negative spiral. This also puts commercial service providers (carriers) in a difficult situation. On the one hand, they need to protect their clients' interests, including their privacy. On the other hand, they are morally obliged to help protect national security. Hence, trust needs to be accounted for when designing (and testing) a risk-based border management concept. TRESSPASS deliverable D6.3 will address trust as part of the acceptability criteria for RBBM, taking also the increased relevance of deterrence into account.

Therefore, the main elements of RBBM must connect the source of the risk (i.e. unknown individuals amongst the group of travellers) with the owner of the risk and to public interest (i.e. the state[23] as the guarantor of security) in a carefully designed risk management process which allows both for sufficient deterrence for adversaries and for sufficient transparency to the proper stakeholders. This is described in TRESSPASS deliverable D2.1.

Furthermore, in order to transparently asses and demonstrate the proportionality and carefulness of introducing a given risk-based BCP design, the effects on the travelling public

[22] For example, authorities that want to introduce new types of requests (e.g. social media) can count on significant opposition from civil rights groups. https://www.accessnow.org/cms/assets/uploads/2017/02/JointLetterUSBorderSearches-final.pdf

[23] Depending on the context, 'the state' may not only refer to specific Member States, but also the European Union.

must be considered in connection with relevant societal norms and values, i.e. the state as the guarantor of freedoms and liberties. This is done in TRESSPASS deliverables D9.7 and D9.8.

As RBBM requires the traveller to be conceptualised into a risk framework, which is subjected to a risk management process, this in turn requires the operationalisation of risk into risk indicators, that can be assessed in a sufficiently accurate way for each traveller. Next section describes in general terms how this is done.

4.3 Risk management: risk, threat, vulnerability, impact

To implement RBBM, it is important to establish a uniform understanding of the key elements of risk management. NEN-ISO defines **risk** as the *"effect of uncertainty on objectives"* (2018, p.1). In the context of border control risk can be considered as the effect that people, who (including their goods) are unauthorised to pass the border, do pass the border because of some failure in border control.

Risk management can be defined as the *"coordinated activities to direct and control an organization with regard to risk"* (NEN-ISO 31000, 2018, p.1). In the context of RBBM, this organisation is the state (i.e. the risk owner), not the border guard agency, or Frontex, or any international organisation.

When organisations adopt a risk management approach, it is assessed to what extent their goals by which threats potentially are imperilled.[24] Then, it is decided whether and to what extent measures should be taken to minimise the chance of these threats from occurring, or to reduce the impact of these threats. IBM describes risk management as follows:

> *"risk management is about systematically taking all measures necessary to prevent or limit the likelihood of risks occurring; it is the process of coming up with solutions to deal with the identified threat. In managing risk a balance must be struck between costs and benefits, as clearly it is not cost effective to address all risks equally. Criteria are needed to decide what constitutes an acceptable or unacceptable level of risk."* (European Commission, 2010, p. 93, emphases added).

Several key concepts can be distilled out of IBM's definition of risk management. First of all, a conceptual understanding is needed of the difference between a 'threat' and a 'risk'. Further, it should be clear what is meant by solutions for these potential threats (i.e. risk mitigation). This description also stresses the importance of selectively mitigating certain risks, and that it should be decided what levels of risks are acceptable or not, as not all risks can be addressed equally. In the next sub-sections, these concepts have been elaborated.

CIRAM (Frontex, 2012) describes risk as a function of three variables: threat, vulnerability and impact.[25] As CIRAM is already a directive to risk-based border management, it is wise for TRESSPASS's conceptual framework to build upon these existing definitions and

[24] The scope of the objectives can vary: they can be on the level of a (sub-)process of the organisation, but also on a general organisational level. The latter is the case in the context of TRESSPASS: it focusses on continuing, well-functioning BCPs throughout Europe.

[25] CIRAM (Frontex, 2012) argues that all three elements of a risk (threat, vulnerability, impact) cannot be assessed separately: *"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 and ideas for the assessment of the other two components."* (p.13).

understandings. Where needed, the conceptualisations are adapted to make them more applicable to risk-based border management at BCPs.[26]

4.3.1 Threat

A **threat** is *"defined as a force or pressure acting on the external borders"* (CIRAM, 2012, p.20). In the context of border management, examples of such threats are traffickers of drugs or terrorists that seek to enter Europe. These threats are always directly related to one of the objectives within the scope of the organisation: the threats potentially endanger achieving or maintaining the organisation's objectives. It is important to note that risks are not only caused by external threats (e.g. crime). The internal threats – in which case, a better term is 'vulnerabilities' – of an organisation, e.g. lack of proper training of border officials or insufficient financial means (IBM, 2010, p. 93) can also be a risk factor.

CIRAM (2012) further argues that a threat is *"characterised by its magnitude and likelihood"* (p.20). **Magnitude** can be understood as the size of the threat that is measured in one of the units described in the following examples. To illustrate, *"for counterterrorism, the units may be the number of suspected terrorists. All measurements should refer to a certain period of time (for example month, quarter or year)"* (Frontex, 2012, p.22). Furthermore, CIRAM adds that the assessment of a threat often requires multiple indicators to fully grasp its magnitude. Another element of CIRAM's notion of threat is the **likelihood** that the threat manifests, i.e. *"chance of something happening"* (NEN-ISO 31000, 2018, p.2). There is a difference between the threat manifesting (e.g. an illegitimate traveller presenting himself at a BCP), and a risk manifesting (e.g. an illegitimate traveller crossing the border). Hence, the likelihood that the risk occurs depends not only on the chance of the threat happening, but also on the **vulnerabilities** of the BCP (described in Section 4.3.2).

In the TRESSPASS RBBM concept, a threat is determined by the pressure generated by illegitimate travellers to cross the border at a BCP, including legitimate travellers who illegitimately bring certain goods with them. This means that anything surrounding that traveller, such as his travel group, may be relevant context.

4.3.2 Vulnerability

A **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, 2012, p.27). Hence, these are the measures that are in place to mitigate potential threats (i.e. risks). For BCPs, this can be regarded as the quality of the checks that are in place. Examples of the quality of the checks can be the accuracy of detecting illegal goods in luggage of travellers via technology at BCPs, or the quality of training received by border officials who must have the right skills and knowledge to perform their tasks. When these measures are at the right level, the magnitude (e.g. the amount) and likelihood of travellers that do pose a threat will pass the checks unnoticed is being reduced in comparison to a situation with less or no checks.

[26] CIRAM (Frontex, 2012) gives a general description of risk-based border management. However, as TRESSPASS exclusively focusses on risk-based border management *at BCPs* and therefore requires further specification for the development a conceptual framework that can be utilised at BCPs. Therefore, also definitions of ISO 31000 (2018) are visited.

In the TRESSPASS RBBM concept, the vulnerability of a BCP is the lack of quality of the check (the ability of refusing and stopping unauthorised travellers to cross the border at the BCP).

4.3.3 Impact

Impact can be described *"as the effects of a threat on the internal security and on the security of the external borders. Impact can also be analysed in terms of the effects on the optimum flow of passengers at the borders, and in terms of humanitarian consequences"* (Frontex, 2012, p.30).[27] Hence, focussing on this first meaning, the impact of a risk needs to be understood as the 'consequences'[28] that the threat has on one of the goals of border management, being the *"protection of internal security"* (European Commission, 2010, p.20). For instance, when the BCP fails to stop people with terrorist intent, this can have severe consequences for the EU and its Member States.

In the TRESSPASS RBBM concept, the impact of a risk is determined by the effects of the pressure generated by illegitimate travellers on the internal security after border checks have been conducted at the external borders.

4.4 Risk management: ownership, acceptance and mitigation

The three elements of risk (threat, vulnerability, and impact) need to be assessed to determine whether measures should be undertaken to mitigate this risk. The assessment of risks can be regarded as the **risk analysis** and has the purpose to *"comprehend the nature of risk and its characteristics including, where appropriate, the level of risk"* (NEN-ISO 31000, 2018, p.12). Risk-based border management is heavily reliant on relevant and sufficient information. This information can be processed, analysed and combined to create intelligence that provides input for risk management, especially when analysing the risks. As CIRAM (Frontex, 2012, p.16) describes: *"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"*. Thus, a risk-based border management approach should invest in proper collection, analysis, and dissemination of information. This is especially important for the different decision-making processes within RBBM.

Based on the risk analysis results, the **risk owner** needs either to accept the existing level of risk, or establish measures to **mitigate the risk** to such an extent that he considers the **residual risk** to be acceptable. The paragraphs below are dedicated to conceptualise these key constructs.

4.4.1 Risk owner

The risk analysis reveals the nature, the characteristics and the level of risks. These results need to be evaluated in order to show whether risks are acceptable (and thus current measures can be maintained) or require additional mitigation. This is described as the risk evaluation, which *"involves comparing the results of the risk analysis with the established risk*

[27] The impact of the border checks on the travelling public is analysed as part of WP9.

[28] The term *impact* in CIRAM (Frontex, 2012) corresponds with ISO's notion of *consequence*, being the *"outcome of an event affecting objectives"* (NEN-ISO 31000, 2018, p.2).

criteria to determine where additional action is required" (NEN-ISO 31000, 2018, p.12).[29]The risk evaluation is done by the so-called risk owners, who *"have the accountability and authority to manage risk"* (NEN-ISO 31000, 2018, p.7).

In the TRESSPASS RBBM concept, the risk owner is the state that owns the BCP, or a collective of states (such as the EU) for its external borders. For the sake of simplicy, this deliverable focusses on the state as risk owner. In concrete risk-based concepts, this will be more refined.

4.4.2 Risk acceptance

The risk owner has the following options: (a) accept the risk and take no further measures, (b) eliminate the risk (if possible and sensible[30]), and (c) reduce the risk by taking further measures that decrease the size or likelihood of the threat and/or reduce its impact (NEN-ISO 31000, 2018, p.13). The description of these options should also include relevant other factors, in the case of border management their impact on flow, their required capacity and their ethical impact.

Ideally, risk acceptance for RBBM includes a description in terms of effectiveness: how many of the travellers that pose a certain threat need to be stopped at the BCPs (e.g. '98% of the smugglers needs to be stopped'; 2% is an acceptable miss-rate). However, expressing risk acceptance is also one of the main challenges of RBBM, as it can be difficult to know what the total amount of travellers is that pose a certain threat to society and try to cross the border at a BCP.

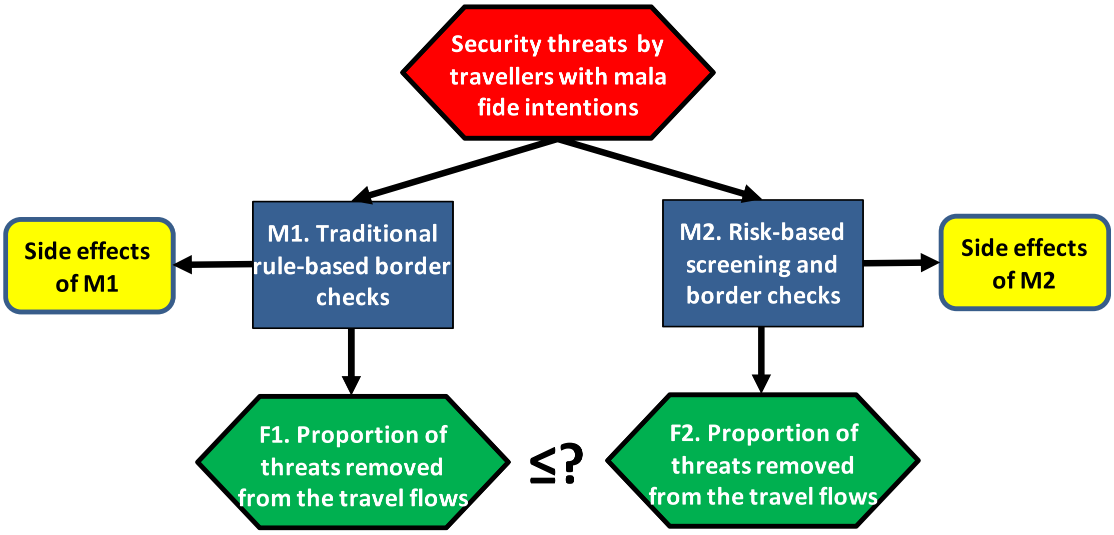

Security threats by travellers with mala fide intentions
Side effects of M1
M1. Traditional rule-based border checks
M2. Risk-based screening and border checks
Side effects of M2
F1. Proportion of threats removed from the travel flows
≤?
F2. Proportion of threats removed from the travel flows

FIGURE 4-4 COMPARISON OF RISK REDUCTION OVERVIEW BETWEEN RULE-BASED AND RISK-BASED BORDER CHECKS

In reality, it is difficult to make a realistic estimation with regards to the amount of travellers that pose a threat. Hence, risk acceptance will often be expressed in relative terms: 'we want to be at *least as* effective when implementing an RBBM concept, in comparison to our current approach' or 'we want to be *more* effective when implementing an RBBM concept in

[29] Which actor is mandated to be the risk owner in RBBM is a matter of governance. In Section 4.4.1 the notion of risk ownership has been elaborated.

[30] E.g. by closing the BCP, the threat of terrorists entering Europe via that BCP is eliminated (assuming border surveillance works 100%), but for reasons of mobility this obviously is not a sensible solution.

comparison to our current approach'. The risk reduction overview (see e.g. Figure 4-4) may be useful to describe which risk mitigation measures should be compared with each other.

For instance, a BCP stops on average 100 travellers a month that pose a specific threat.[31] As a consequence, every traveller is checked on this specific threat leading to long queues of travellers at the BCP. To increase the travel flow, one can decide to implement an RBBM concept (in which not every traveller is being checked) under the condition that still at least approximately 100 travellers who pose the specific threat are stopped each month.[32] In this case, risk acceptance is being expressed in relative terms ('approximately as good').

If (objective) quantitative numbers are too hard to obtain then it could still be very useful to describe risk reduction in qualitative terms.

4.4.3 Risk mitigation and residual risk

Measures that are implemented at BCPs mostly aim at a reduction of the vulnerability: having sufficient checks to ensure that the people that pose a threat are stopped at the BCPs. However, as the premise of RBBM is to check people by (the type of) checks in accordance to their risk-profile, the level of risk acceptance should also be converted into the accuracy of the screening methods that are implemented: how many of the malicious travellers who intend to cross the border at the BCP need to be checked and stopped before or at the BCP (e.g. a chance of arrest of 95% is acceptable). The accepted inaccuracy contributes to the **residual risk**: the risk that remains after the implementation of the measures to decrease the vulnerability (and thereby the magnitude and/or likelihood of a risk still to occur).

Thus, risk mitigation measures consist of both the quality/effectiveness of the checks, and the accuracy of the screening methods that are in place to ensure that the right (i.e. acceptable) level of (remaining) risk is achieved.

4.4.4 Iterative process

Due to societal factors, flows of people and goods change over time. Adversaries adapt to changing vulnerabilities and new technology that is frequently being introduced. An up-to-date BCP concept requires an evolving risk management process that is flexible and iterative. This can be achieved by continuously revising the risk-based filters that are established.

Adaptive adversaries: When malicious (or mala fide) travellers figure out how (risk-based) filters work, they may alter their modus operandi to circumvent checks. For instance, if drug traffickers are aware that children will not be checked on the possession of drugs at BCPs, they might start using groups of unwitting children as mules. Hence, the learning ability of malicious travellers should be taken into consideration when designing the risk profiles of travellers and corresponding checks.

[31] This is a hypothetical example.

[32] Formulating a relative level of risk-acceptance is based on the notion that in the current approach, there is no 100% accuracy. Therefore, the risk-based concept neither has to result in 100% accuracy. The challenge with this approach to formulate a relative level of risk acceptance is that when the RBBM concept over time results in significantly less travellers that prove to pose a specific threat are being stopped, it can be hard to determine whether this is due to concept failure, or that there are less travellers that pose the specific threat try to cross the BCP. This should be kept in mind when evaluating the effectiveness of RBBM measures.

4.5 Operationalisation of risk into risk indicators

In this section, the generic operational context of RBBM is described, i.e. the relation between a screening and a check. Next, it is described how the abstract idea of risk as introduced in the previous sections is operationalised into risk indicators that can be applied to precise situations, specifically to definite travellers as they present themselves at a BCP. This is essential to understand the type of practical challenges that need to be overcome in order to realise the full potential of RBBM.

Risk and Trust: In this report, as well as in this chapter, the principles of RBBM have mainly been elaborated by means of the concept of risk. However, also the concept of trust – i.e. the assessment that someone is a bona fide traveller – is part of RBBM. In fact, trust can be considered as the opposite form of risk. In addition to risk indicators that are used to assess whether someone is potentially mala fide, also bona fide or trust indicators can be defined to assess whether someone can be trusted as being a bona fide traveller. This is elaborated in detail in deliverable D2.3.

4.5.1 Checks based on the outcome of screening

In the context of RBBM, the function of a screening is to determine the risk profile for a traveller, which is used to determine what kind of check the individual must undergo. However, a screening is merely a rough assessment of the risk posed by a traveller, and therefore, it is less accurate than a check. Over-reliance on the accuracy of screenings can lead to an unrealistic idea of the residual risk. This is a serious pitfall, because a typical precondition in the transition to risk-based border crossing points, is that the residual risk may not deteriorate.

For instance, a concept can be implemented that increases the flow-rate of travellers by only extensively checking travellers that match certain risk profiles – i.e. assessed by screening as being potentially mala fide –, whilst travellers that do not match these profiles are allowed to pass with no or limited checks – i.e. assessed as bona fide or neutral respectively. However, the possibility remains that people who should be stopped at the BCP are not recognised as a potential threat, as screening methods most likely do not work with perfect accuracy. Hence, suchlike concepts potentially decrease the effectiveness of the BCP (see arrow 1 in Figure 4-5).

To compensate for this, however, another concept needs to be implemented which increases the effectiveness, but thereby also cancels out some of the gained benefits in terms of flow-rate (see arrow 2 in Figure 4-5). When accumulating different risk-based concepts, the overall effectiveness and flow-rate of BCPs – two of the main intended nett benefits – may be assumed to have increased. [33]

[33] The expected impact of implementing RBBM management for both the flow-rate and the effectiveness of the BCP as depicted assumes that the efficiency of the BCPs remain constant: the same amount of border officials is being used. Obviously it is possible to improve the efficiency of the BCPs when for instance the flow-rate is being increased, but this can have in turn negative consequences for the flow-rate when the amount of border officials is being downscaled.

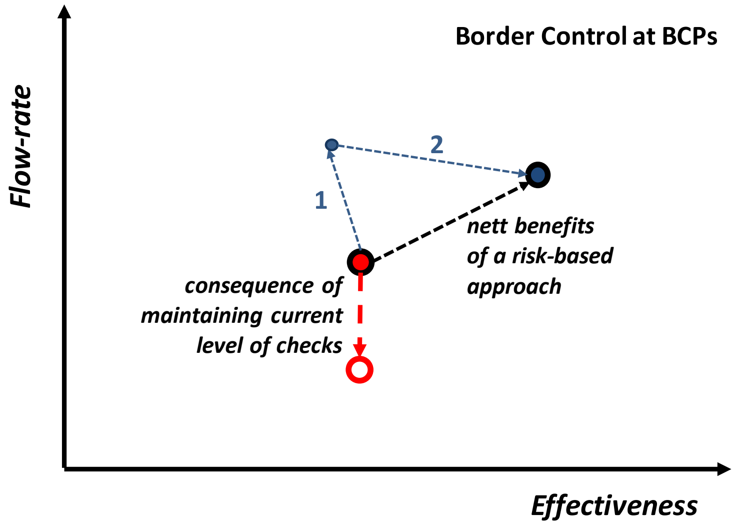


FIGURE 4-5 EXPECTED IMPACT OF RISK-BASED BORDER MANAGEMENT AT BCPS

What is the minimal amount of checks that is required?

The answer depends on the legal status of the two involved states. For example, if both states are part of the Schengen Area, travellers usually do not have to show travel documents as there are no systematic border checks. However, when entering the Schengen Area from a non-Schengen country, identity checks through travel documents against certain checklists are required for all travellers.

This (rule-based) requirement could in theory also be subjected to a risk assessment. For example, if there is reliable information that the respective traveller will only be in the Schengen Area for a very short time, and he will not interact with other people [note: it seems highly unlikely that this is possible] while he is in the Schengen-area, it might be acceptable that his identity is not checked. That could be the case if the state accepts the risk that e.g. this was a wanted fugitive. For now, this remains purely a theoretical exercise.

4.5.2 Parallel models of the same threat

Within the cyclical process as described in Section 4.4.4, the threat that is posed by people at the BCP must be described – and be kept up-to-date – before a risk-based border crossing point concept can be developed or adapted. However, in a risk-based BCP, there will be several closely related – but different – models of the threat in use. Table 4-3 provides an overview of these.

TABLE 4-3 THREAT DESCRIPTIONS

Threat description type	Where does it reside?
The **generic threat** that is generated by actual adversaries and other real world factors (e.g. drug traffickers). Adversaries will typically actively hide information about this threat.	In the real world
The **intelligence report of a threat** that is the outcome of an intelligence process: data gathering about the threat, processing this	On paper

Threat description type	Where does it reside?
data into relevant pieces of information and analysing and combining them into an intelligence report on the threat.	
The **design of the basis threat (DBT)** as authorised by the risk owner of the border (i.e. the Member State). The owner of a border can decide to deviate from the intelligence report, which will change his residual risk.	On paper
The **threat indicators as part of a screening** that are implemented (through training or through programming) into a border security screening.	At a BCP
The **threat assessment that is made of a concrete passenger (group) (or red team) as part of a screening**, by a border guard (or automated system).	At a BCP
The **threat indicators to be used in a check** that are implemented (through training or through programming) into a border security check.	At a BCP
The **threat assessment that is made of a concrete passenger (group) as part of a check**.	At a BCP
The **threat posed by a specific passenger as part of his travel group**.	In the real world
The **approximation of the threat** as posed by red teams.	In the real world

It is easy to confuse them with each other. For example, the statement "99% of travellers poses no threat" concerns the first and last variants: the generic and specific threats in the real world. Nevertheless, the cost-benefit equation of a change from rule based to risk-based border management is concerned with the assessment made of the threat by the border guards as part of the screening (not the check), combined with situations when the associated incident actually occurs. This assessment depends on many other factors. And it is very likely not to approach the real life prevalence at all or only at the trade-off of false negatives, undermining the overall effectiveness (see Section 4.1.1).

Annex B provides a fictive example of how the concept of threat changes as it progresses through the NEN-ISO 31000 process. The annex illustrates the importance of both a good design of the threat, and a good design of risk indicators.

Accuracy: A high priority requirement for any RBBM concept is knowing the accuracy of both the screenings and the checks involved. Screenings and checks will never be perfect. There will always be false positives and false negatives. But only by knowing the accuracy of the screenings and checks, it is possible to manage the residual risk in other ways, and to obtain the intended benefits of RBBM.

4.5.3 Specification of risk indicators

For accurate filters, specific indicators are required for screenings and checks. Without specific indicators, screenings and checks will not be sufficiently accurate. These indicators must also be assessible, i.e. it must be realistic within the context of a BCP to assess their values with the required accuracy for each traveller. This section and next section deal with this topic.

The use of specified risk indicators – and bona fide indicators; see remark on risk and trust at the beginning of Section 4.5 – must also be ethical and legal. Within a risk-based legal framework, legality is based on purpose, proportionality and subsidiarity, which also requires a sufficient level of specificity. This is described further in Section 6.3.2 and in TRESSPASS deliverable D1.4. The ethical impact of using risk indications is analysed using the framework developed in TRESSPASS deliverables D9.7 and D9.8.

A further benefit of specifying risk indicators and risk profiles, is that they can be exchanged with partners. For example, if a state has determined that a specific risk profile accurately describes a type of traveller that poses a certain threat, and that this type of traveller is often encountered in flows from specific states, then these states can share the risk profile to allow for earlier detection of such threats.

Certain types of risk indicators are described in databases that require information about the identity of a person as a search key, such as travel documents or biometrics. This includes information regarding missing persons or migration in SIS, or information regarding the current itinerary in PNR records. Detecting such a 'known person of interest' is based on using the identity to check travellers.

However, for many types of threats, the identity of the person of interest is not (reliably) known beforehand. This requires also detecting the 'unknown person of interest'. This is more complex, as it requires a conceptualisation that relates risk, threat, and optionally vulnerability, to risk indicators. Risk indicators can be anything that describes a relevant aspect of a traveller, the only hard requirement is that it improves the risk assessment for a traveller, i.e. that it helps distinguish risk from non-risk.

There are different potential sources for inspiration of risk indicators: historical modus operandi recorded in legal documents, experienced border agency staff, even works of fiction such as written into movies and books. Obviously, these sources have different value in terms of how specific, traceable and accurate they are (Van Rest, Roelofs and Van Nunen, 2014).

The conceptualisation needs to be able to cover input from all such sources, and must be extendible to accommodate accumulating insight. In this report, the initial conceptualisation is partly inspired by Smith and Brooks (2012) in which is stated that a threat consists of intent and capability. Intent requires desire and expectation, and capability requires access to resources and to knowledge. Resources can include weapons, money, tools, etc. Knowledge may require access to specialised people, written manuals or blueprints, etc. The context of the threat, such as the travel group of a traveller, is also relevant, because it may give the traveller access to knowledge or resources. In this manner, risk indicators can be specified, and successively be grouped into risk profiles. This is discussed in more detail in Section 5.3.3 and this is the topic of Task 2.2.

The concept of vulnerability can also lead to useful risk indicators. In the context of RBBM, a vulnerability is the lack of capacity of a filter to detect a threat. So, if there is knowledge of a modus operandi that exploits a vulnerability, then signs of that modus operandi could also be useful risk indicators. For example, suppose there is a known modus operandi that exploits identity theft using falsified travel documents. if it is also known that certain BCPs are less capable of detecting falsified travel documents than others. That means that travellers whose identity was checked in 'weaker' BCPs, pose a larger risk, and vice versa for 'stronger' BCPs.

4.6 Assessing risk indicators

This sub-section describes in general terms how specified risk indicators can be assessed. Some indicators can be constructed from the direct observation of aspects of the traveller, such as what he does or does not carry with him. A risk indicator that someone has a lack of funding to support his living could be constructed from a lack of cash, or a debit card.

Other indicators cannot be directly observed, such as indicators related to his intent or his knowledge. This requires indirect assessment methods based on the observation of related, but different aspects. This is called profiling.

The values of these indicators can rarely be reliably assessed from clear and unambigious observations. Rather, they have to be assessed (sometimes calculated) from multiple less reliable observation. This is called 'fusion'. There are significantly different types of fusion. In this deliverable the following distinction is used:

- Sensor fusion uses multiple sensors to create one improved observation. For example two camera's observing the same person at the same time from different angles can provide a facial image without occlusion from the nose.
- Data fusion uses multiple types of data to assess one technical variable with improved reliability. For example, an RFID tracker may track luggage of a traveller while he is carrying it, and a video tracking system may track both the traveller and his luggage. Combining this information in a reliable track of the traveller, and the moment when he forgets his luggage somewhere, is called a form of data fusion.
- Information fusion uses multiple types of information to make more abstract assessment of relevant aspects. For example, the identity information on a travellers identity document, his verbal identity claim, the identity information on his smartphone and the way the traveller identifies himself on social media can all technically be different, but still within legal 'margins of error' due to e.g. spelling conventions, social norms and ease of use. Such differences should, through the use of fusion, still refer to one single identity.

4.6.1 Assessing intent

When assessing the threat posed by a traveller, intent is often an important part of the conceptual model of the the threat. It is supposed to be a, or *the*, main factor that determines human behaviour. For example, in 'folk psychology'[34], the relation between desire and action is described using the 'intentional chain'*:* desire → intent → action → outcome (see Figure 4-6).

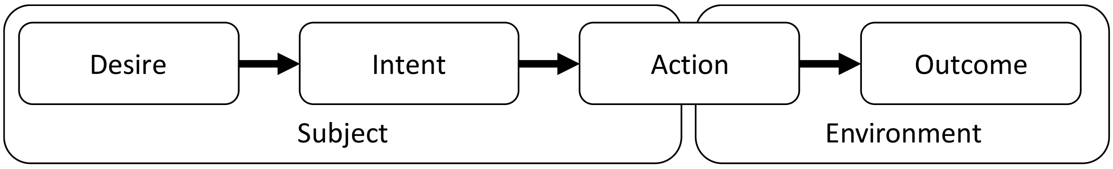


FIGURE 4-6 THE INTENTIONAL CHAIN LINKS DESIRE TO EXPECTED OUTCOME

[34] Folk psychology is the way laymen in everyday life reason about the behaviour and mental state of people. This simplified type of psychology sometimes also finds its way into official policies (Kashima, Y., McKintyre, A., & Clifford, P. 1998).

This simplified model is also applied in the legal domain, i.e. there is a legal difference between desire, i.e. a wish that is not expressed into a mental state of action, versus intent, i.e. a commitment to action, and versus action, i.e. actually doing something. This line of reasoning is also followed in the closely related domain of aviation security (ECAC, 2016).

However, there are several complicating factors regarding this simplified model and the assessment of intent:

- The current belief in the scientific psychological community is that the relation between self-image, attitude, belief, desire, intent and other psychological constructs is much more complex than can be described with the intentional chain.
- Behaviour is the reaction of an agent (an autonomous entity) to a stimulus, often moderated by internal factors such as memory. So, an action cannot be solely attributed to the internal state of intent, but must always be considered in a wider context, which is also not represented in the intentional chain.
- There are other psychological constructs that can lead to actions or behaviour such as emotions or mental strain, so an observed action cannot solely be attributed to an intent.
- As a psychological construct, intent is (for now[35]) – not a directly observable quantity. Intent can therefore only be assessed in indirect manners and by approximation, which is by definition a type of profiling.
- Intent and its related concepts are still very much subject to active research, so new insights are continuously becoming available in the form of innovative interviewing techniques (Ormerod and Dando, 2015) and sensing technologies (Poppe et al, 2014).
- The ethical and legal frameworks regarding the assessment and use of intent, and related methods (e.g. profiling) and technologies (e.g. behavioural analytics) are highly dependent on the situational context (making ethical and legal compliance a moving target); there is no established consensus on how to approach this problem. This is further complicated by a firm negative perception of profiling activities.

There is not one single solution for assessing mental state ('intent') or capability from travellers for risk-based BCPs, nor is it realistic to believe that such a singular solution can presently be developed. The TRESSPASS strategy is therefore to develop methodologies and tools that can be used to design and implement various highly specific ways of assessing relevant mental states of subjects, which also fits the general philosophy of a risk-based approach: adaptive to the local situation. Additionally, existing frameworks for ethical and legal evaluation of such methods are developed further to allow for more informed decision making in RBBM.

4.6.2 Profiling and behaviour detection for RBBM

Profiling is essential for detecting unknown persons of interest, i.e. persons that pose a threat, but which cannot be derived solely from their identity. As described in Section 2.4.4, profiling is already done within the context of intelligence-led border management. Profiling is the assessment of relevant hidden aspects of travellers based on other, observable aspects (Van Rest, J.H.C., Roelofs, M., Van Nunen, A., and Don, S.B., 2014). Figure 4-7 illustrates for example

[35] There is ongoing research into mind-reading which may offer more direct methods for the assessment of intent, e.g. using Functional Magnetic Resonance Imaging (FMRI). This is still very premature and is likely to be highly invasive in initial implementations, requiring cooperation of the subject, sensors directly attached to their body and extended periods of calibration and analysis (Simpson, J. R., 2008).

that hidden aspects mental state and capability may be derived from observable aspects identity and behaviour.

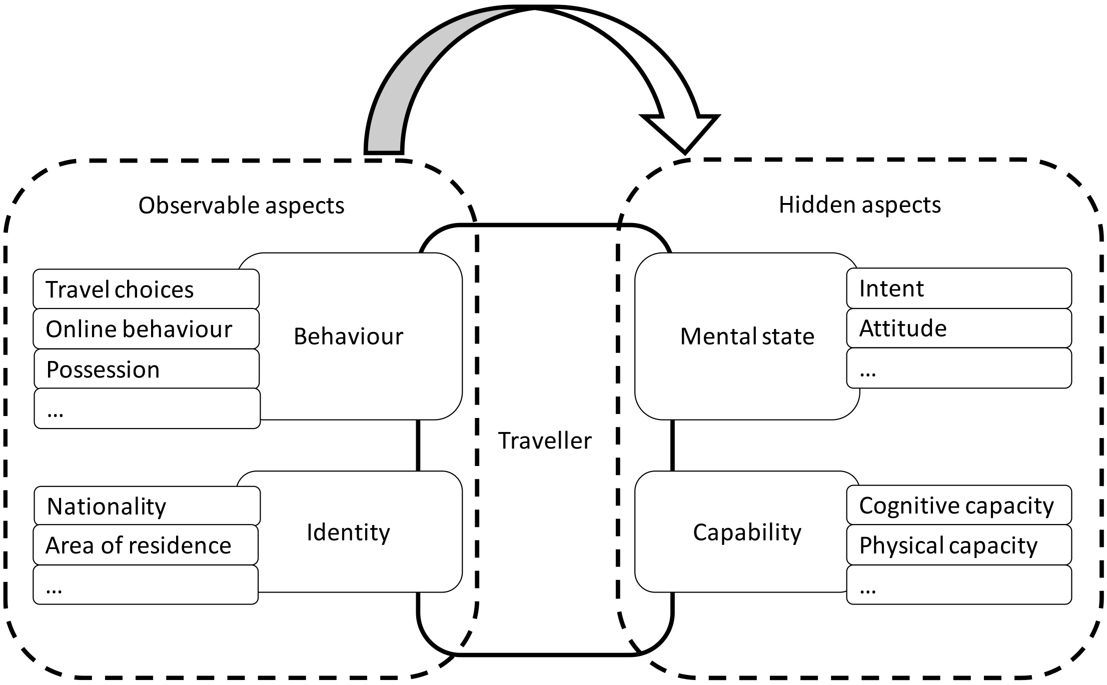


FIGURE 4-7 PROFILING FOR BCPS ASSESSES HIDDEN ASPECTS OF TRAVELLERS FROM OBSERVABLE ASPECTS

TRESSPASS will improve on current practice by gathering and describing good-practices (including from an ethical and legal point of view) with regard to profiling (in WP2, WP6 and WP9), and by developing methodologies and supporting tools that implement those good practices (in WP3, WP4 and WP5). The methodological approach taken by TRESSPASS will result in more transparent BCP designs, making the evaluation of the effectiveness of BCPs easier. In addition, the development of advanced simulation tools (WP7) will allow border guards and custom agencies to verify and validate current and new risk-based methods for profiling within BCP designs.

Intelligence-led border management and RBBM may use algorithms for profiling. The GDPR and the Law Enforcement Directive require that such algorithms be transparent and the results should be traceable to relevant inputs and formal policies.

4.6.3 Behaviour detection

Behaviour detection is one of the most promising inputs for profiling. In the context of risk-based BCPs, behaviour[36] can be relevant for different reasons (Van Rest, Roelofs and Van Nunen, 2014), such as:

- It is required behaviour for executing a modus operandi;
- It has a high correlation with incidents (but we don’t understand the causality yet);

[36] Behaviour is the reaction of a person on a stimulus. This (re)action can be covert or overt, conscious or subconscious, internal or external, and voluntary or involuntary (Van Rest, J.H.C., Roelofs, M., Van Nunen, A., and Don, S.B., 2014).

- It arises from 'mental strain' from maintaining a deception or cover hostile intent or dangerous capabilities.

In TRESSPASS, this generic and broad definition of behaviour has been used in order to be flexible for a wide range of behaviour, and thereby to be relevant for a wide range of travel modalities, tiers and threats.

Relevant behaviour can occur long before a booking is made, and continues beyond the actual border crossing. The TRESSPASS specification of potentially relevant behaviour is listed here:

- Choices made regarding the travel, such as origin and destination, travel legs, travel group(s), travel modalities, time of departure, and food preferences along the way;
- Choices made regarding appearance, such as clothing, tattoos, and hairstyle;
- Choices made regarding possessions, such as luggage, and clothing;
- Choices made regarding communications and online possessions, such as verbal and written utterances, including online communications and social media;
- Choices made regarding movement and gestures, such as walking patterns and posture;
- Unconscious reactions to stimuli, such as can be introduced by border guard or custom authorities in desk, queue or interview settings[37].

The relevance of this kind of behaviour depends on a different type of reasoning (Van Rest, Roelofs and Van Nunen, 2014). These are some examples:

- Behaviour can be instrumental for a modus operandi. For example, in human trafficking, the victim cannot be trusted with his or hers own passport by the trafficker. Therefore, a behavioural indicator of human trafficking is that someones passport is provided to authorities by another person, which implies choices made regarding possession and travel groups.
- Behaviour can be moderated by the unconscious, due to mental strain of attempting to hide or simulate certain behaviour in order to attempt to fool authorities. For example, the ECAC study group focusses on behaviour that stems from a fear of discovery (ECAC, 2016).
- Behaviour can be difficult to explain by what is normal at the BCP. For example, people may buy a ticket to a cheap destination, pass the border at the BCP, but not actually board the plane or train, and return back to the state of origin. This may be a sign of a new type of modus operandi which may require further investigation. It could be a way to show respect to arriving people, by greating them already at the gate. It could also be a way to attack travellers when they least expect it, e.g. for pickpocketing.

4.7 Data gathering through interaction and observation

The previous sections operationalised risk indicators and described how these are assessed (e.g. through profiling and behavioural analyses). This section describes in generic terms the relationship between the traveller, the data pipeline and the risk indicators. This is the final step needed before the functional design of a BCP can be done (in WP2).

[37] Aviation security may also apply behaviour detection. The ECAC behaviour detection study group (BDSG) states that it focusses specifically on unconscious reactions to stimuli (BDSG 2016).

4.7.1 Data records: Online record and BCP record

As presented in Table 4-4 there are dozens of types of potential data sources and related processing technologies that can provide the information that is input (through profiling) to the risk assessment process of a traveller.

TABLE 4-4 RELATION BETWEEN ASPECTS OF A TRAVELLER, TYPES OF DATA, SOURCES AND PROCESSING, AND RISK ASPECTS

Traveller			Data pipeline		Risk				
Person is (body)	Person behaves		Data source	Data processing (if distinctive)	Intent	Capability	Possession	Identity	Travel group
	Person acts	Person carries							
		Identity documents	Passport					x	
			Identity card					x	
Hard biometrics			Face	Fixed	o			x	
				On the move	o			x	
			Iris	Fixed	o			x	
				On the move	o			x	
			Finger-print		o			x	
			Palm vein		o			x	
	Soft bio-metrics		CCTV	Appearance (suspect search)	o	o			
				Walking pattern	o	o			
	Booking		API		x				
			PNR		x				x
		ICT device	Laptop/Tablet/ Phone/ Wearable		o	x	x	o	o
	Physical behaviour near BCP		Interview	Trained professional	x	x	o	o	o
				Analytics	x	x	o	o	o
			CCTV	Trained professional	x	x	o		o
				analytics	x	x	o		o
	Online behaviour		Social media		x	x	o		o
			Online presence		x	x	o		o
		Handheld luggage	Baggage screening system		x	o	x		
		On body items	Security scanner		x		x		
		Cargo Luggage	Cargo scanner		x	o	x		

Traveller			Data pipeline		Risk				
Person is (body)	**Person behaves**		**Data source**	**Data processing (if distinctive)**	**Intent**	**Capability**	**Possession**	**Identity**	**Travel group**
	Person acts	**Person carries**							
Temperature			Infrared		**o**	**o**	**x**[38]		

Legend: **x** = risk indicator can be derived directly / **o** = can contribute to risk indicator
Note: Travel group is included under 'Risk' to illustrate how also relevant factors beyond the traveller him/herself can be incorporated.

These data sources will record data from travellers at different times and places. It may be difficult to keep an overview of the data sources and their individual contribution to the effectiveness of filters. Especially in a situation where they are locally combined in risk profiles. It may be useful to group them in some manner. In the current situation, the passenger name record (PNR) already describes – to a certain degree of accuracy and completeness – the travel itinerary. In TRESSPASS it is proposed to create two other types of records:

- **Online record**, consisting of relevant indicators composed of online sources, and through web intelligence;
- **BCP record**, consisting of relevant indicators composed of behavioural cues at or around the BCP.

A trip from a traveller that covers three countries, and passes two BCPs would then be described by one PNR record, one online record and three BCP records. Together, this could be called the 'travel record'.

4.7.2 Ways of collecting data

A risk-based BCP must be able to find relevant pieces of data regarding these aspects from travellers and link these pieces of data to the correct traveller (i.e. assign them the correct travel record) – while they are in some state of 'flow'. For some types of data and traveller interactions (such as behaviour, movement or communication patterns) and for some situations (such as travellers in a physical flow), this can be difficult. Therefore, in TRESSPASS recognition[39] of people between different times and places will be done by (re)using mature hard biometrics and Automatic Number Plate Recognition (ANPR) where viable, and complement these with soft biometrics ('suspect search') where needed. TRESSPASS distinguishes between three different ways to get information about travellers.

The first way to get information from travellers is simply to ask them for it based on the traveller's cooperation. If travellers consent to providing information, they will be allowed to go through checkpoints faster. However, no amount of trust will convince actual hostile adversaries to provide accurate and timely information, so in all contacts authorities must be

[38] Temperature may be an indication of illness (fever) (e.g. Ebola) (Carter & Meisel, 2014).

[39] Recognition is different from identification. Identification is to establish someone unique identity, out of all possible people. Recognition does not require a link to someone's unique identity, and is typically only from a limited group of people. Recognition is therefore typically easier and less invasive than identification.

prepared to deal with lies, including misdirection, incomplete statements and other attempts to conceal the truth. This is the topic of Section 4.7.4.

The second way is to ask for or demand relevant information from businesses that travellers directly and indirectly use (for their travel)[40]. However, there is a lot of relevant information for which the required legal, organizational and technical provisions have not yet been made. Relevant technologies are new types of encryption (e.g. homomorphic encryption) and hashing that allow for the sharing of relevant information without sharing personal or classified data.

The third way is to obtain information through observation. This is a focal point of the TRESSPASS project. There are three significantly different settings:

1. **When travellers are in a flow of travellers** (e.g. walking, or driving in a car) it is possible to observe their behaviour and possessions remotely, often assisted by automated means (e.g. video analytics). Non-cooperative (soft) biometrics will be required to systematically and efficiently link relevant observations to the right traveller.
2. **When travellers are stationary, but not in a controlled environment and still part of the primary flow of travellers** (e.g. at a desk, in a checkpoint or at a self-service kiosk, or queued up in a security check line) it is possible to observe their behaviour in more detail, to be able to distinguish certain preselected involuntary and physiological types of behaviour that may reveal information about the mental state and capabilities of the traveller.
3. **When travellers are stationary and in a controlled environment, not being part of the primary flow of travellers anymore** (i.e. in an interview room) it is possible to observe their behaviour in most detail. Many different interviewing techniques are available and more are still subject of research. Part of the challenge is knowing which interview technique is suitable for which situation, and which types of information are relevant for that interviewing technique (VicarVision, no date; Bouma et al, 2016).

The stationary setting may be less relevant for RBBM, because ideally the screening has been completed before travellers queue up. Otherwise, the flow-rate will almost certainly decrease.

4.7.3 Assessing relevant aspects from travellers while they are on the move

A risk-based BCP will have to be able to assess relevant aspects of travellers while they are on the move. Otherwise, merely gathering data for a screening already interrupts the flow, undermining the potential of RBBM to facilitate the base flow-rate.

Example: In order to screen travellers approaching a land BCP in a car, they would have to claim an identity, and to provide authentication of that claim. In addition, depending on the claimed identities, the risk-based BCP could require that the amount of claimed identities is validated against a count of the number of people in the car. It would be beneficial for the flow, if both the identities and the count of people can be done while the car is on the move.

[40] This includes travel operators, operators of transport hubs, but potentially also social media companies and other businesses. This would typically be based on specific laws, and regulations, such as for example is arranged for API and PNR data.

There are several methods to assess aspects of travellers while they are on the move. Modern ICT can help obtain input directly from moving travellers. An app on a smartphone can be used to collect information from travellers while they are walking, or sitting on a train, plane, or on a boat, or when they are passenger in a car.

Another method is to use advanced sensors that can assess relevant aspects and attribute them to the right travel record. Typically, the accuracy of such sensors is hampered by the movement of the subject. E.g. biometrics on the move are less accurate than biometrics in a fixated setting. Depending on the outcome described in deliverable D2.2, relevant aspects to be assessed on travellers on the move could be related to the possession of large amounts of money, the possession of drugs, weapons or explosives or the hiding of people in a car. Another relevant aspect could be the temperature of travellers arriving from a location with an elevated risk of infectious disease.

Multiple sensors that can detect small traces of relevant materials could be combined to determine threats for moving travellers (Van Rest, J., Bovenkamp, E., Eendebak, P., Baan, J., & van Munster, R. 2009).

The land border scenario could benefit a lot from technologies that assist travellers on the move because their base flow is relatively high. The following is a hypothetical example.

Example: Ten kilometres before the BCP, road signage alerts travellers that they have to verify identities in relation to their number plate. This can be done using an app on a smartphone that also has a biometric authentication ability, e.g. fingerprint, voice and / or face recognition.

With this information, travellers can be screened while the car is moving at its original speed. If only trusted identities are claimed in a trusted car, then the vehicle can keep moving at high speed while passing the green fast lane of the land BCP. Otherwise, the car is directed to the white lane, where it has to slow down to 30 km/h. Five kilometres before the BCP, the number of people in the vehicle is assessed using advanced sensors, and this is linked to the number plate information. The number of people is validated against the number of claimed identities. If these numbers are the same, and if the screenings of those travellers have been completed and do not reveal any threats, then the car can be directed to the ‘green lane’. Otherwise, the car is directed to a checkpoint where the travellers are checked. Depending on the risk indicators, this may require them to leave the car.

4.7.4 Assessing the veracity of statements made by travellers

As described in Section 4.5.2, the accuracy of information directly affects the effectiveness, the travel flow and the efficiency of filters. There are many modi operandi conceivable that among other things require a traveller who does not give sincere answers to questions posed. So, if a check at a BCP is not able to adequately authenticate the veracity of statements made by travellers, this constitutes a major vulnerability. This is in itself not new for RBBM, but if RBBM leads to more use of intent, capability and other ‘hidden’ aspects of travellers to create risk indicators from, then this vulnerability becomes much more important.

There are different strategies to authenticate the veracity of statements made by travellers:

- The first strategy is to compare statements to other (reliable) sources. For example, a statement made by a travelling companion can be compared with statements from other travelling companions. Statements about places that have been visited in the past can be compared with maps.

- The second strategy is to confront the traveller with inconsistent statements. Many types of interviewing techniques apply this strategy.
- The final strategy presented here, is to look for behavioural cues that are indicative of mental states of the traveller (e.g. cognitive load, emotion) which can ultimately be related to the sincerity of answers to questions posed to them.

The second and third strategies do not directly lead to the truth. They may only give hints as to what the traveller claims versus what he actually believes being the truth. But just having a good indication that a traveller makes an (in)sincere statement is already very useful in both screenings and checks.

The use of technology to look for relevant behavioural cues is very contentious, but given the potential benefits, must be explored. In controlled environments the best known accuracy is currently beyond 70% (Van Der Zee, S., Poppe, R., Taylor, P. J., & Anderson, R. 2015; Van Der Zee, S., Poppe, R., Havrileck, A., & Baillon, A., 2018). This is useful for steering the direction of an interview, but is in most legal frameworks not sufficient as 'proof' of something. In fact, even bona fide travellers can have many types of motivation to conceal the truth or to make incorrect statements. For instance, because they have the feeling that this will help them to pass the BCP faster.

In many legal contexts, citizens have the right not to incriminate themselves. In the US this is described in the fifth amendment of the constitution. In the EU, Article 6 of the European Convention on Human Rights gives citizens the right to a fair trial. The text of this article does not mention self-incrimination, but the European Court of Human Rights has interpreted this in case law to include the right to remain silent (Berger, 2007). However, in both cases, this is a right. So, if both parties agree to admit the outcome of a so-called lie detector as evidence, it may still be used. However, the purpose of RBBM is not about finding evidence, but about assessing indicators to select appropriate checks. The legal base for such screenings depend on the purpose and context within which it is used. For instance, screening for aviation security has another legal base than screening for admission to certain sensitive jobs. Most laws will require that proportionality and subsidiarity have to be assessed per application scenario. In Task 3.1 TRESSPASS investigates the use of indicators for mental constructs that are related to the sincerity of statements made.

The TRESSPASS approach is to assist human professional interviewers with technology that helps observing relevant behaviour cues from subjects in interview settings. This means that travellers will be addressed by human professionals, not by automated avatars. Second, the actual assessment of sincerity and accuracy will always be made by a human professional, never by a machine. Third, by assisting professionals with the more mundane aspects of observing interviewees, these professionals can have more attention on the actual content and direction of the interview, rather than on 'counting behavioural cues'. The hypothesis is that this leads to more proportional and more effective interviews when necessary, fitting the overall RBBM paradigm.

4.7.5 Assessing the quality of risk indicators in simulation and in practice

Just like in rule-based border management, it is essential to verify the specificity of the indicators for the threat, and to verify the quality of the assessment methods against the stated ambition level. Section 4.5.2 describes that the operational ability to reliably separate threat from non-threat determines the actual effects of a risk-based BCP, rather than a high level threat or generic threat assessment.

So, it is essential to monitor the actual quality of risk-based filters. This is especially important if on the one hand they are supposed to produce an equivalent remaining level of risk as rule-based filters, and on the other hand the flow-rate must be improved based on less stringent checks. In fact, assessing the effectiveness of security measures is a fundamental challenge in security research. This may among other things require 'red teaming'. It is especially difficult if also subjective factors such as deterrence and chilling can have effect (see section 4.1.3), which is the case in border management. This challenge is addressed in TRESSPASS WP7 (Simulation, evaluation and training tools) and WP8 (Pilots).

4.8 Definition and examples of risk-based BCP concepts

Based on the main elements of RBBM, it is possible to define a risk-based concept and to give some examples. Within one BCP filter, multiple risk-based BCP concepts can be active simultaneously (see Section 4.5.1). By combining multiple concepts into one filter, negative and positive effects on effectiveness, flow-rate and efficiency may be outweighed. A typical expectation is, however, that combinations of risk-based filters can be chosen in which the cumulative effect is that all will be improved.

4.8.1 Definition of a risk-based BCP concept

A risk-based border crossing point concept is defined by the following elements:

- The type of travellers (target group) for which the concept is meant for, defined by aspects such as entering or leaving Europe, crew member or passenger, nationality, being a registered traveller or not;
- A risk acceptance statement that describes which risk is accepted (tolerated) for travellers who belong to the target group;
- Changes in the risk reduction of border control for the target group;
- Changes in the screening capabilities and capacities;
- Changes in the checking capabilities and capacities;
- Changes in flow-rate;
- The legal base;
- The applicability of the concept.

The following sub-section provides a number of examples of risk-based BCP concepts following this structure. The legal base is still to be determined, so that is omitted here.

4.8.2 Examples of risk-based border crossing point concepts

Table 4-5 summarises the effects of these examples. It illustrates that risk-based concepts can improve either of the three main types of effects, but also that there is always a trade-off: there is no risk-based concept that improves on all three effects. It further shows that filters can be designed that are composed of combinations of such concepts.

The legal base for applying RBBM and for collecting data is not yet included in these examples. For instance, the case based on a national registered traveller programme that has access to relevant information for all travelling participants may currently not be legal.

By studying these examples closely, their respective vulnerabilities can also be found. For instance, for the first case concerning crew on short trips outside Schengen, a vulnerability is that such crew is especially targeted by organised crime to e.g. smuggle goods or money.

These examples were encountered from interaction with border guard agencies, some of which are TRESSPASS partners, and other are made up specifically for this deliverable.

TABLE 4-5 SUMMARISED EFFECTS OF EXAMPLES OF RISK-BASED CONCEPTS

Example-name	Change in risk reduction (effectiveness)	Change in flow-rate	Change in efficiency
Crew of a short-distance return-trip outside Schengen	Slight decrease	Improvement	Improvement
Travellers that passed strong BCPs	Slight decrease	Slight improvement	Slight improvement
Human trafficking	Increase	No change	Slight decrease
Infectious disease	Slight decrease	Improvement	Improvement
National Registered Traveller Programme: outbound travellers	Slight decrease	Large improvement	Large improvement
Arrival of residents from trusted non-Schengen countries	Decrease	Improvement	Improvement
eGates for departing travellers from third countries	Decrease	Improvement	Improvement

4.8.2.1 *Example – Crew of a short distance return-trip outside Schengen*

This fictive example was provided by a partner in TRESSPASS. It covers the staff of airliners that regularly fly to the UK, and have very short turn-around times.

Target group:	Crew of a carrier that is screened periodically by their trusted employer (i.e. a trusted carrier), and that does not cross the border at the port of destination (i.e. at the connecting BCP outside the Schengen Area).
Risk acceptance statement:	The Schengen state of arrival accepts the risk that screened staff on short distance connections poses any threat.
Change in risk reduction:	The risk reduction is slightly less because there might be screened crew that is still a threat.
Change in screening capability:	To assess whether staff was indeed only travelling the short-distance return-trip. Other screening has periodically to be done by their employer (not per trip).
Change in screening capacity:	Screenings of the trusted carrier and of the border agency must be re-aligned of these changes.

Change in checking capability:	The border check is omitted for such a crew.
Change in checking capacity:	A slight reduction in required checking capacity.
Change in flow-rate:	The flow-rate at crew filters is increased because less staff needs to be checked.
Applicability:	Neighbouring countries where transport operator staff has a low incentive to become a threat, and which has a very short layover such as ferries and air-connections on short routes.

4.8.2.2 Example – Travellers that passed strong BCPs

This fictive example was originally made up for the H2020 project D4FLY. It is not based on threats, but on vulnerabilities. A potential positive side-effect of this risk-based concept is that it generates pressure on states to keep the quality of their travel document authentication up-to-date.

Target group:	Travellers who have passed a BCP that has strong authentication checks for travel documents, and who actually have been subjected to such a strong check.
Risk acceptance statement:	The state of arrival accepts the risk that travel documents, although they have been checked at a strong BCP, still turn out to be false.
Change in risk reduction:	The risk reduction is slightly less because there still might be travellers who passed a strong BCP by using forged travel documents that would have been detected by the present BCP.
Change in screening capability:	To determine whether a traveller has passed a strong BCP, and that his travel documents have been checked. This information must be obtained from other BCPs.
Change in screening capacity:	This kind of screening can easily be automated. If that is the case, obtaining information from other BCPs does not require additional operational screening capacity.
Change in checking capability:	Travellers from countries with strong authentication of travel documents do not have to be checked as thoroughly again.
Change in checking capacity:	This can save a small amount of time per identity check using travel documents.
Change in flow-rate:	The flow-rate at filters is increased because authentication takes less time.
Applicability	Travellers from countries with strong authentication of travel documents can be included in this filter. A side effect of this risk-based concept may be that there is increased

	pressure on states to keep the quality of the travel document authentication up to date.

4.8.2.3 Example – Human trafficking

This is a fictive example of a risk-based concept for an unknown person of interest, in this case, the person is ‘of interest’ because he is related to human trafficking. This example illustrates that persons are only ‘of interest’ for a specific reason.

Target group:	All travellers.
Risk acceptance statement:	The state of departure does not accept the risk that human traffickers succeed in moving victims across its border.
Change in risk reduction:	Introducing this kind of screening and checks will lead to more human traffickers and victims being found.
Change in screening capability:	To assess whether travellers carry their own travel documents, and whether their online record shows a lack of freedom of movement or a lack of basic necessities such as food, water, sleep or care.[41]
Change in screening capacity:	This requires dedicated capacity to design and maintain relevant risk indicators.
Change in checking capability:	This introduces an interview for selected travellers.
Change in checking capacity:	This interview requires dedicated and specialised capacity.
Change in flow-rate:	The flow-rate at filters can be kept constant if the indicators can be assessed in a timely and accurate manner.
Applicability:	This can be applied in each state, both inbound and outbound, including transfer. It may be applied especially on travel routes which have a higher expected frequency.

4.8.2.4 Example – Infectious disease

This fictive example has been used in a serious game session (see Section 6.4) to explain the concept of RBBM. It assumes a scenario where connected states have been infected with a serious disease, and where invasive and time-consuming checks have been implemented to stop infected travellers. This risk-based concept would be an alternative to that situation.

Target group:	All incoming travellers from a country where is an epidemic.
Risk acceptance statement:	The state of arrival does not accept the risk that a significant number of infected travellers enter the country, but it does

[41] These indicators of human trafficking are merely examples taken from the US Customs and Border Protection (CBP, 2019). Some of these indicators can be assessed during a screening, others will require a check.

	accept travellers who have an increased body temperature for another obvious reason.
Change in risk reduction:	Slight decrease: some infected travellers may still be running (despite being ill), which would cause them to be excluded from a check. Their infection would not be detected.
Change in screening capability:	To assess whether a traveller has been running at the BCP. If he did, then accept that as an explanation for an elevated temperature, instead of being infected.
Change in screening capacity:	This screening requires determining the walking speed for travellers who arrived from specific countries and comparing their speed with a certain norm.
Change in checking capability:	Take a blood-sample.
Change in checking capacity:	This requires dedicated and specialised capacity, an invasive procedure and takes significant time.
Change in flow-rate:	This will improve the flow-rate as opposed to time-consuming checks on all travellers.
Applicability:	This can be applied in each state, on inbound travellers from countries where is an epidemic.

4.8.2.5 Example – National Registered Traveller Programme: outbound residents

This fictive example came up during TRESSPASS board meetings. It is limited to outbound residents, because recent data must be available for screenings, which may be difficult to obtain from abroad.

Target group:	All departing travellers who are a resident of the departing state.
Risk acceptance statement:	The state of departure accepts the risk that residents who are participating in a national RTP pose a threat.
Change in risk reduction:	Slight decrease: residents that participate in a national RTP could mislead screenings.
Change in screening capability:	To assess RTP-participants based on information obtained through their consent from a relevant selection of sources, e.g. online sources, financial records, etc.
Change in screening capacity:	This requires a significant screening capacity.
Change in checking capability:	Regular border checks.
Change in checking capacity:	A considerable decrease of required capacity because outbound residents require less checks.
Change in flow-rate:	This will significantly do increase the flow-rate.

Applicability:	This can be applied in each state on outbound residents.

4.8.2.6 Example – Arrival from residents of trusted non-Schengen countries

States may have such strong economic incentives to improve flow-rate of certain types of travellers (e.g. coming from economically important states), that they may be willing to accept all risk posed by those inbound travellers. In such cases, screening is not needed, see the fictive example below.

Target group:	All inbound travellers who are residents of states that normally help to mitigate threats.
Risk acceptance statement:	The state of arrival accepts the risk that residents who are arriving from trusted third countries still pose a threat.
Change in risk reduction:	Decrease: residents from trusted third countries could evade risk mitigate measures in their respective countries.
Change in screening capability:	None
Change in screening capacity:	No change
Change in checking capability:	Checks are omitted.
Change in checking capacity:	A significant decrease of required capacity because inbound residents from trusted third countries – potentially a large fraction of all travellers – require less checks.
Change in flow-rate:	This will improve the flow rate significantly.
Applicability:	This can be applied in each state, on inbound residents of trusted third countries.

4.8.2.7 Example – eGates for departing travellers from third countries

States may have such strong economic incentives to improve flow-rate of certain types of travellers, that they may be willing to accept all risk posed by those outbound travellers. In such cases, no screening is needed. For example, the risk of overstay may be accepted (for travellers from specific states).

Target group:	Departing travellers from (specific) third countries.
Risk acceptance statement:	The state of departure accepts the risk that outbound travellers from third countries pose a threat, e.g. having overstayed their visa.
Change in risk reduction:	Decrease: because residents from third countries can overstay their visa.
Change in screening capability:	None: no screening is required.

Change in screening capacity:	None.
Change in checking capability:	Regular visa checks
Change in checking capacity:	A decrease of required capacity because outbound residents from third countries – potentially a large portion of all travellers – require less checks.
Change in flow-rate:	This will improve the flow-rate.
Applicability:	This can be applied in each state on outbound residents of third countries.

4.9 Decision-making in RBBM

4.9.1 Rule-based versus risk-based decision-making

A risk-based border management concept requires decision-making which is diverging from traditional rule-based or intelligence-led decision-making. According to Simon (1965, in: Van Rest & Weima, 2017), decision-making consists of three separate phases: collecting information which leads to the realisation that a decision is necessary, generating alternatives and describing them in a meaningful way, and choosing one of the alternatives, i.e. making the actual decision.

For rule-based decision-making, which is applied in rule-based and intelligence-led border management, the decisions are based on pre-existing regulations and guidelines. Consequently, only information is gathered that is necessary to apply the proper rule to a traveller. For instance, information that is needed to determine whether the traveller has a Schengen-nationality or not, to decide what type of checks need to be applied. Another example is the use of databases (see Section 2.4.5) to find out whether the traveller is on a watchlist (based on identity) and has to be detained. Obviously, through intelligence-led border management – and by using other types of information as well – the situational awareness can be increased, but existing rules and directives still need to be honoured. Thus, decisions that are made in rule-based border management are straight-forward: based on general rules and regulations. Therefore, one can wonder whether this is really a matter of 'decision-making' or rather of 'acting according to protocol'.

On the other hand, risk-based border management is focussing on conducting a risk analysis as input for decision-making. This kind of analysis results in the assessment of different levels of risks, upon which to decide whether or not these risks are acceptable. If not, measures of risk mitigation should be undertaken. As already described in previous section, the mitigation measures lead to residual risks, which need to be accepted by the risk-owner. Hence, the type and level of checks that individual travellers receive is determined by the risks that the risk owner is willing to accept, instead of a set of predetermined rules and directives.

Multiple actors can be made risk-owner for border management. For instance, Frontex can be assigned with the risk-ownership for the whole Schengen area or individual Member States can become responsible for managing the (remaining) risks of their own BCPs. Multiple options are discussed in Section 4.9.4 together with their implications and consequences.

RBBM does not completely neglect rule-based decision-making. In fact, risk-based and rule-based border management will co-exist in the multi-level governance of border-management. The risk-owner determines which levels of risks should be mitigated, which on their turn are implemented in concrete protocols and directives for border officials. They will be instructed to only check those travellers who match the determined risk-profiles. As a consequence, the decision-making at the operational level of BCPs – by border officials – remains rule-based.

4.9.2 Additional information needs

Risk-based decision-making also requires more and other types of information to be collected in comparison to rule-based decision-making. Whereas the rule-based approach mostly uses information to gain situational awareness and to verify that the proper rule is applied to a traveller, risk-based border management requires information for a situational risk assessment. It concerns information to determine the level and types of risks that an individual BCP is facing, and – depending on the risk acceptance by the risk owners – to determine the risk of each individual traveller based on among others his identity, capability, possession and intent.

These increased information needs result in more types of data that needs to be collected, and for the technological and human resources to do so. For instance, to determine whether a traveller who booked an airline ticket online has a terrorist intent, it might be necessary to screen his online behaviour (e.g. via social media). Hence, this requires additional data sources (social media) and technology or professionals to interpret and assess the collected data.

This additional need for information also results in an urgency to establish records with information about the traveller within the three travel stages before and at the BCP. Section 4.7.1 introduced, besides the Passenger Name Record (PNR), also the ‘online record’ and the ‘BCP record’.

In the pre-travel stage only information can be retrieved through the internet or by consulting databases into the online record, whereas actual behaviour can only be observed when the traveller is approaching or arriving at the BCP (e.g. when he is entering an airport). The more a traveller behaves in a relevant manner at the BCP, the more information must be gathered in this BCP-record (see Section 4.7.1). By accumulating the insights that are gathered in the various travel stages the risks can be better estimated.

4.9.3 Basic principles of risk-based decision-making

In risk-based border management, the performance of BCPs can be evaluated by four different indicators as defined in Table 4-1: risk reduction (i.e. effectiveness), flow-rate, efficiency and ethical compliance. Each of these indicators can be the (initial) driver to change or implement risk mitigation measures.

Example for increased risk reduction (i.e. effectiveness): When intelligence sources indicate that there is a potential threat caused by travellers who are infected with a new type of serious infectious disease, additional types of checks may be required to prevent infected travellers from entering Europe (unnoticed).

Example for increased flow-rate: When a country wants to improve its economic attractiveness, then the flow-rate is an important distinguishing feature. If a risk-based BCP can be developed that allows for increased flow, with equivalent residual risk, then this can be a powerful economic driver for changes in the border control.

Example for increased efficiency: When it becomes more difficult to attract suitable staff for checks, there might be the need to increase the efficiency of checks. If less travellers have to be checked then this may generate a gain in efficiency.

Example for increased ethical compliancy: When a privacy impact assessment of an existing border control concept generates a lot of red flags because of disproportional measures in relation to travellers that 'have obviously no bad intentions', then this may be a driver to look for a different, more proportional border control concept.

The process of risk-based decision-making is graphically depicted in Figure 4-8. Independent of the driver – effectiveness, flow-rate, efficiency or ethical compliance – for changing the current methods and checks of the BCPs, the risk-owner should always address the requirements for all four performance indicators, as this offers essential specifications and guidelines for the development or revision of the RBBM concept (i.e. the set of screening methods and checks).

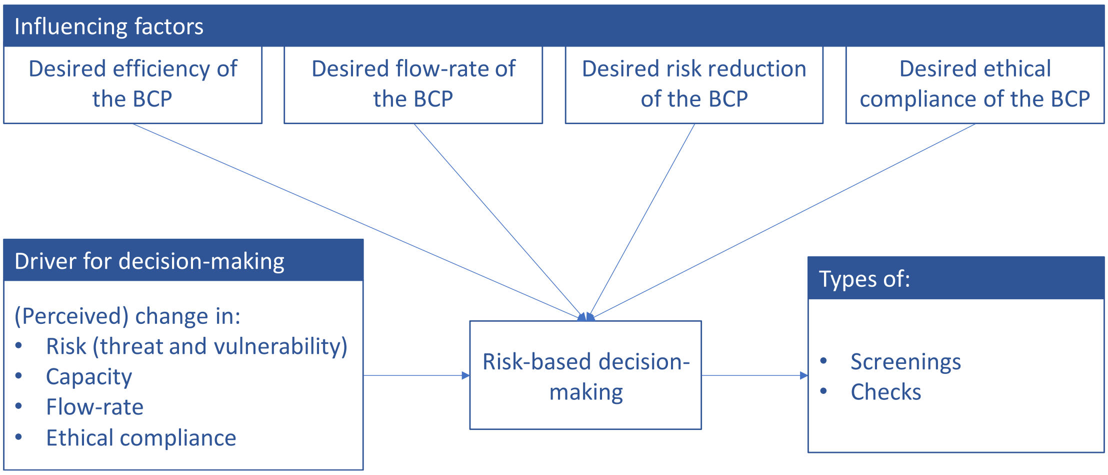

Influencing factors
Desired efficiency of the BCP
Desired flow-rate of the BCP
Desired risk reduction of the BCP
Desired ethical compliance of the BCP
Driver for decision-making
(Perceived) change in:
• Risk (threat and vulnerability)
• Capacity
• Flow-rate
• Ethical compliance
Risk-based decision-making
Types of:
• Screenings
• Checks

FIGURE 4-8 RISK-BASED DECISION-MAKING PROCESS

4.9.4 Governance in relation to risk-based decision making

Similar to the current border management approach, multiple governance levels need to be involved. The different levels all play a vital role in executing risk-based border management and in the decision-making processes that are part of it. The following paragraphs elaborate on the different tasks, responsibilities, and types of decision-making (i.e. rule-based or risk-based) that are present. Table 4-6 provides a summary of these elements per governance level.

TABLE 4-6 GOVERNANCE IN CASE OF RBBM

Level	Tasks	Responsibilities in RBBM	Type of decision-making
EU and/or National	Deciding how to react on (changes in levels of) risk(s). Determine whether there needs to be changes to the effectiveness, efficiency or flow-rate of BCPs.	Risk-owner (accepting risks)	Risk-based
Strategic	Providing input for the risk-owner to make a decision on the risk acceptance.	Risk analysis Formulating risk-profiles that match the preferred levels of residual risk.	Risk-based
Tactical	Designing and implementing RBBM concepts in alignment with the requirements formulated at the EU/national level (i.e. effectiveness, efficiency, and on the changing demands at the strategic and EU/national level. Monitoring whether the concept fits the requirements. Monitoring whether the risk profiles are still adequate and up-to date.	Risk mitigation	Risk-based and Rule-based
Operational	Executing the rules that are part of the designed and implemented RBBM concept, in which it is determined what (level/type) of check(s) each individual traveller receives.	Risk mitigation	Rule-based

4.9.4.1 EU and/or National level

The EU and/or the individual Member States are responsible for the functioning of the BCPs. This will not change in case RBBM will be implemented. However, when border agencies are permitted[42] to implement the RBBM approach, the EU and/or national level also has a specific

[42] 'Permitted' is intentionally used. The EU/National level is mandated to determine how border management is being conducted. This level of governance needs to decide whether or not to use RBBM. Without this formal approval, the lower levels cannot legitimately implement operational RBBM concepts in their practices. As is the case with many agencies of member States, they are part of certain governmental departments (e.g. ministries) which are under the responsibility and supervision of the national political sphere. These lower levels need to align their border management approach with the

role to fulfil in this process. This level of governance is required to express what (level of) risks is acceptable, and/or what residual risk should be achieved by the border agencies. [43]

Consequentially, the decision-making process is mainly risk-based: the levels of all potential threats need to be reviewed and determined whether or not measures should be taken to mitigate these risks. Furthermore, the EU/National level needs to express where these measures should comply to and result in: what the residual risk of the concept is (i.e. the effectiveness of the concept), how efficient the concept should be (in terms of the used personnel and resources), and what the flow-rate.

This requires capabilities in terms of arguing why certain levels of risk should be achieved and maintained, and taking responsibility for the residual risks. Hence, this diverges from the current border management approach in which only quality demands for the BCPs are formulated.

4.9.4.2 Strategic level

The strategic level consists of the highest organisational levels of border agencies, which are responsible for the overall strategy for border control at BCPs. This governance level is obliged to safeguard that proper functioning of BCPs is continued and sustained over time. To do so, long term planning is required to ensure that current and future challenges are addressed. The expected trend of increasing traveller migration flows is an example of suchlike future challenges. In RBBM, the strategic level is the link between the EU/national level, and the tactical level of border management: entities at the strategic level need to ensure that the expressed level of residual risk is guaranteed by the implementation of proper measures and checks at BCPs. To do so, the strategic level should formulate the risk-profiles of travellers that should be stopped.

In RBBM, the strategic level is mostly concerned with risk-based decision-making as their actions are guided by the assessment of risks, and to anticipate on future hazards that can become a concrete threat over time (to ensure the continuity of the BCPs). The strategic level needs to be involved with the risk evaluation on EU and national level (e.g. by providing input), but simultaneously needs to direct its attention to potential future threats to take preventive measures (e.g. designing and implementing training programmes for border officials).

When at the strategic level long term strategies are formulated, this should be done by incorporating what of the three performance indicators (effectiveness, efficiency and flow-rate) are potentially endangered by changing risks, and discuss this with the EU/national level when new RBBM concepts should be designed or implemented to preserve the continuity and well-functioning of the BCPs. Therefore, the strategies that are formulated should be grounded in risk-based thinking and decision-making.

regulations coming from the EU and/or national level. Consequentially, (political) approval is required for border agencies to implement and execute a risk-based border management concept that results in structural check-differentiation of individual travellers based on their risk profile.

[43] In the conceptual framework, no distinction is made yet between the tasks and responsibilities of the EU and national level of the governance structure. It needs to be (politically) decided whether the stated tasks or responsibilities should be located at the EU or national level, or that they should be divided amongst both levels. Although this decision is beyond the scope of the TRESSPASS project, this topic is briefly addressed in chapter 6. Furthermore, this distinction is not relevant for understanding the rationale behind risk-based border management and decision-making.

4.9.4.3 Tactical level

The tactical level is concerned with designing, implementing, and maintaining measures to fulfil the needs of the EU/national level: the expressed (remaining) risk should be achieved by the mitigation measures. This is done under coordination of the strategic level. Furthermore, the tactical level is involved in maintaining the daily operations of the BCPs. For instance, entities at the tactical level need to ensure that the border officials receive proper training and/or to ensure that sufficient BCP posts are staffed by sufficient border officials. They also provide instructions to the border officials (i.e. BCPs).

The decision-making process at the tactical level is mostly rule-based, as this level is responsible for implementing the decisions that are made on the EU/national and strategic level. For example, they need to ensure that travellers that fit the high-risk profile receive more stringent checks, and if not, receive less checks.

Nevertheless, this level also provides feedback and input to strategic decision-making, and therefore also needs to participate in the process of recognising future risks and challenges. The tactical level needs to understand the manner in which long term strategies are formulated in terms of risks. Also, this level should indicate when they think the risk-profiles that are formulated in the higher governance levels are outdated or should be revised. For instance, when new practices or modus operandi are recognised in daily practices. Thus, this level also needs to adopt risk-based thinking to a certain degree.

The tactical level needs a general understanding of the diverging understanding of ‘risk’ on national/policy level and strategic level. The national/policy level understands risks in terms of threats that potentially endangers interests of the state (i.e. security within Europe). The strategic level needs to convert the articulated risk acceptance by the national/policy level in terms of strategic goals to fulfil. Simultaneously, the strategic level is responsible for the (long-term) continuation of the BCPs, they need to ensure that they can deliver on the desired residual-risk articulated by the national/policy level.

This leads to two different types of risks: 1) *the risk of compromising security within European borders*, and 2) *the risk of not having the right capabilities and capacities to ensure or achieve the desired level of (residual) risk.* The first type is mostly applicable to the national/policy level, whilst the latter is under the responsibility of the strategic level. Therefore, the tactical level needs be aware of these diverging understandings of risk when communicating- and providing feedback- to the strategic level.

4.9.4.4 Operational level

The operational level consists of the border officials that perform the checks and measures that are designed and implemented by the tactical level. They are given certain instructions on what the relevant risk profiles are, and how to act according to the different risk-profiles of travellers: which travellers to check, and which not. Therefore, the decision-making process of border officials in an RBBM approach is similar to their current rule-based decision-making process: they need to execute the prescribed protocols and guidelines.

4.10 Prerequisites for RBBM

The previous paragraphs reveal multiple prerequisites that should be fulfilled for giving RBBM a chance to succeed. At least, the following requirements need to be met (not meant as an ordered list). These must be considered additional requirements for the TRESSPASS architecture and pilots.

1. **Risk ownership:** An actor in the governance structure of border management should be mandated with being the risk-owner of the residual risk of the BCPs. This actor is then accountable for the effectiveness, efficiency and flow-rate of the BCPs, and also needs to be able to express what the minimum requirements for these three performance indicators are.
2. **Defining risk profiles:** In order to be able to execute the RBBM concepts, actors must be able to translate the threat that ought to be mitigated into risk-profiles of travellers.
3. **Determining the effectiveness, efficiency and flow-rate of the BCPs:** To evaluate whether the BCP works conform the risk acceptance expressed by the risk owner, there should be measures determined to monitor the effectiveness, efficiency and flow-rate of the BCP.
4. **Formulating needs and requirements for information for risk-profiles:** In order to determine whether an individual traveller matches the determined risk-profiles, sufficient information should be accessible. However, the needs and requirements for this information should be expressed beforehand (when developing the RBBM concepts for a BCP) in order to make these concepts feasible. Hereby, a balance should be struck between the available data and the technological resources that are already in place at existing BCPs, and to express what additional data is necessary (e.g. what technology can be helpful or what data sources should be made accessible). Further, the trustworthiness of the data (sources) should also be evaluated (e.g. whether the data is reliable, up-to-date, complete).
5. **Having sufficient information to perform adequate risk analyses:** For the risk-owners to make knowledgeable decisions in respect to what levels of risks are being accepted, they need to have access to adequate information on the three main elements of a risk: the threat (together with its magnitude and likelihood), the vulnerability of the BCP, and the impact of the threat. Hence, the intelligence cycle of the border management agencies should be well-functioning for RBBM to work adequately.
6. **To work in an accountable and transparent manner where this does not conflict with the purpose of border control:** The way (personal) data is processed and for which purpose must be made clear for travellers. For the sake of clarity the ‘BCP record’ can be used as a term for the information gathered about travellers at a BCP. This should be a traceable and distinct part in the RBBM information management systems.
7. **Be robust against insincere statements made by travellers**: no amount of trust will convince actual hostile adversaries to provide accurate and timely information, so in all contacts authorities must be prepared to deal with this, including misdirection, incomplete statements and other attempts to conceal the truth.

5 Conceptual framework of RBBM

5.1 Conditions for RBBM at BCPs

The concept should fulfil the requirements that have been described before. Therefore, the concept must:

- Focus on both the effectiveness and the flow-rate of RBBM at BCPs; in addition the efficiency (i.e. efficient use of resources) is a relevant issue.
- Provide insight into risks and vulnerabilities at Member State and European level.
- Facilitate risk assessment at Member State level.
- Be adaptive and flexible to changes, such as new threats and changes in legislation.
- Be applicable for all Member States for border control for travellers that enter or leave Europe, and for all types of BCP (air, land and maritime).
- Facilitate the interaction about risk management between all involved organisations at the different management levels (EU/member state, strategic, tactical and operational level).
- Be designed in such a way that tasks and interactions are appropriate for the level (strategic etc.) at which they are executed.

5.2 Basic concepts

This section provides an overview of the main charcateristics of some key elements within the conceptual framework. These elements are: the BCP and border control activities, the traffic-flows, the travellers, and the threats.

5.2.1 BCP and border control characteristics

A BCP is the location where travellers cross the border. There are three types of BCPs: air, land and maritime.

With the resources that border authorities have at their disposal each traveller (including his luggage and vehicle) is checked, while traffic-flows/flows of travellers are guided as smooth as possible along the check-points. Therefore, the basic design of a BCP consists of a process that separates travellers from the flow who need to be refused (and therefore should return), or diverged into another process (e.g. asylum) or even taken into custody. The design can make use of filters (i.e combining screening and types of checks and regulating different flows of travellers).

With respect to national security and organised crime issues, checks aim to isolate persons:

- Who have committed, or are suspected of having committed, malicious acts such as crimes or activities affecting national security (‘wanted persons’, black list, people who staid too long, etc.).
- Who seem to have intentions for committing malicious acts or carrying out activities that might affect national security and/or indicate criminal activities.
- Who could endanger public health (e.g. in case of ebola).

Current, non-risk-based BCPs implement rule-based checks to filter the flows of travellers and their luggage. However, these rule-based checks do not take the actual risk into account and therefore create disproportional disruptions. In a concrete (risk-based) BCP, there may be multiple screening, checks and inspection steps, for example for different agencies, threats or jurisdictions. Risk-based screening is expected to especially be relevant for BCPs with high volumes of traffic and/or travellers.

5.2.2 Traffic-flow characteristics

A traffic-flow consists of vehicles or persons (i.e. travellers) who arrive at the BCP. Such a flow can be inbound (to enter Europe) or outbound (to leave Europe). The traffic-flow is the number that arrives per time-unit in a certain direction (inbound or outbound). It will very during the day, and depends also on the type of day (working-day, weekend, holidays' season).

The type of traffic-flow depends on the modality of transport which is dependent on the type of BCP (air, land or martime), and on the fact whether the flow consist of vehicles (e.g. cars) with one or more passengers inside who want to cross the border, or of persons who are walking to the BCP's checking area (e.g. crew members or passengers of an aircraft or cruise-ship). Therefore, the base-flow-rate of the traffic flow – which is the average speed of the travellers – depends on the transport modality.

5.2.3 Traveller characteristics

A traveller is a person, including his luggage, who who wants to cross the border at the BCP. He can do so as pedestrian or with his own vehicle (e.g. car or boat), or as a crew member (e.g. of an airplane) or as a passenger (e.g. of a train). He can travel alone but also as a member of a group of persons (e.g. three persons in one car).

The journey of a traveller consists of four phases: Pre-travel, Approach BCP, At BCP, and Post BCP. The amount of information that border authorities will get or can retrieve from a traveller increases during the first three stages, and also depends on the preparations of the traveller (e.g. booking a flight) and on issues that he has to fulfil (e.g. a request for a visa).

The following categories of information are distinguished: (a) Identity, (b) Capability, (c) Behaviour, (d) Mental state, (e) Luggage, and (f) Vehicle. In the course of the TRESSPASS project the characteristics within each of these categories will be elaborated.

5.2.4 Threat characteristics

A threat is a situation that a traveller (including his goods and vehicle) who is illegitimate to cross the border – and therefore needs to be refused or stopped by the BCP officials – arrives at the BCP. Threat characteristics are parameters that are used to characterise all kinds of threats (including their impact) and the various modi operandi of 'malicious' (mala fide) travellers in their attempt to cross the border at the BCP. Certain parameter values or combinations of parameter values can be used as risk indicators.

In Task 2.1 the threats will be classified and will be elaborated in more detail in the so-called Design Basis Threat. In Task 2.2 will go into more detail on the issue of determining risk indicators.

5.3 Capabilities

To adequately perform border management in general and risk-based border management in particular, the involved border control authorities need to have a certain number of capabilities. A capability is understood as the ability to adequately execute a certain task or function with the available resources (personnel and materiel), where adequately means that the output is 'of good quality', 'delivered in-time' and 'as long as needed'.[44]

As described in Section 2.2.3 there are several hierarchical levels of organisations involved in risk-based border management. At each level has its specific category of capabilities, while each category on its turn consists of a number of capabilities. The categories are:

- Policy-making capabilities at EU and national level to coordinate and agree at European level on high-level aspects of RBBM at BCPs in Europe (such as threats to be mitigated to ensure national security), and to decide at MS level in each individual country on implementation of risk-based border control.
- Strategic capabilities by stakeholders at strategic level of each MS (national services and border authorities) to coordinate and set goals for agencies at tactical level based on the implementation as decided on at EU and MS policy, and to ensure continuity of RBBM processes in the MS.
- Tactical capabilities by stakeholders at tactical level of each MS – i.e. the services that manage and coordinate overall operations at BCPs – to command, control and coordinate operations at BCPs.
- Operational capabilities by stakeholders at operational level to execute or facilitate risk-based border control at BCPs.

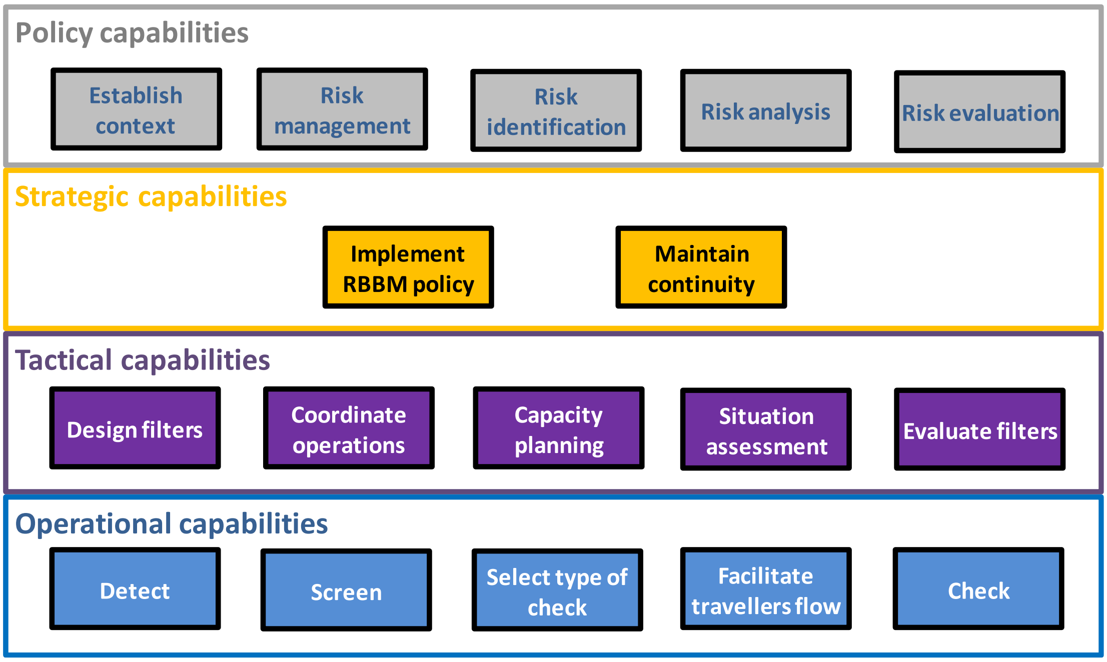


FIGURE 5-1 RBBM – OVERVIEW OF REQUIRED CAPABILITIES

Figure 5-1 provides an overview of all capabilities that are distinguished in TRESSPASS' conceptual framework and that are required for a risk-based approach for border control at BCPs at the external borders of Europe. Next sub-sections deal with the various capabilities within the four capability categories. Each of the seventeen capabilities is explicated by a

[44] By analogy with Joseph W. Pfeifer and Ophelia Roman, The Journal of the NPS Center for Homeland Defense and Security, Volume XIV – 2018.

short description and its purpose, the results (output), the required input, and the staff that is responsible for executing the capability.

5.3.1 Policy capabilities

The objectives of policy capabilities in risk-based border management by the EU and Member States are:

1. Deciding upon the general context and overall strategy in which RBBM has to be applied at the BCPs in the various MS and to ensure a uniform understanding of risk management and related definitions of terms – such as risk, threat, vulnerability and impact – in the domain of border control at BCPs.
2. Articulating clear commitment to apply risk management in border control at BCPs, including the objectives and the definition of risk criteria.
3. Elaborating the overall identified strategy into the various risks that should be mitigated by border control at BCPs (types of threats, their impact, risk indicators).
4. Determining the level of risks, their nature and the magnitude of their consequences, and the ways in which the risks should be mitigated by effective border control at BCPs (detection, screening and checks) including the required effectiveness of mitigation.
5. Evaluating the risks and deciding either to which extent risks should be mitigated by effective risk-based border control because they are unacceptable, or that risks not have to mitigated because they are acceptable or cannot be mitigated at all (unavoidable risks).

5.3.1.1 Establishing context

Determine the general context and ensure a common understanding of applying risk management for border control operations at BCPs. This includes decision making on the overall strategy (e.g. the strategy to fight cross-border crime, and the key drivers and trends affecting border control), and articulating a clear commitment to apply RBBM.

Input:	Positive attitude of the EU and participating countries towards RBBM.
Output:	Commitment and overall strategy for applying RBBM at BCPs.

5.3.1.2 Risk management

Determine the objectives of applying RBBM at BCPs and specify the risks that should be mitigated by border control. This includes clear definitions of threats, impact, risks in the domain of border management and consensus on (a) the risk criteria that will be used in border control operations, and (b) the ways in which the risks should be mitigated by effective border control at BCPs (detection, screening and checks).

Input:	Overall strategy (from Establishing context) and Risk evaluation report (from Risk evaluation).
Output:	Risk criteria and General guidelines for RBBM.

5.3.1.3 Risk identification

Elaborate the overall identified strategy by identifying and describing the various types of threats, and risks caused by travellers who passed the border but should have been refused or stopped at the BCP.

Input:	Overall strategy (from Establishing context), and Risk criteria (from (Risk management).
Output:	Overview of threats.

5.3.1.4 Risk analysis

Comprehend the nature, likelihood and severity of the risks that are posed by the identified types of threats, and identification of indicators of these threats. These risk indicators are classified into the categories Identity, Possession, Intent and Capability.

Input:	Risk criteria (from Risk management) and Overview of threats (from Risk identification).
Output:	Overview of risks, including risk indicators.

5.3.1.5 Risk evaluation

Evaluate the determined risks and decide to which extent these risks should be mitigated by effective risk-based border control at BCPs, and communicate the results to all organisations (at all levels) involved in border control.

Input:	Risk criteria (from Risk management) and Overview of threats (from Risk identification), and Overview of risks (from Risk analysis).
Output:	Risk evaluation report.

5.3.2 Strategic capabilities

The objectives of strategic capabilities in risk-based border management of each MS are:

1. Implementing the RBBM strategy as has been agreed upon at EU and MS level and has been elaborated by organisations at the policy level of the MS.
2. Monitoring and maintaining risk-based border control in the MS to ensure continuity, and to modify the implemented RBBM policy if needed (e.g. by taking corrective measures).

5.3.2.1 Implementing RBBM policy

Implementing the strategy for RBBM within the MS. This is achieved by developing MS-specific guidelines and instructions for RBBM and by providing these to organisations at tactical level of the MS. In addition, it includes the provision of sufficient resources to implement risk-based border control at tactical and operational level. Finally, it includes adjustments of the implemented RBBM policy in case this is needed for continuity of RBBM operations.

Input:	Overall strategy and General guidelines for RBBM (from Risk management), and Adjustment needs (from Maintaining continuity).

Output:	MS-specific guidelines and instructions for RBBM, and RBBM resources.

5.3.2.2 Maintaining continuity

Ensure continuity of RBBM within the MS by monitoring MS' border control activities, and by reporting adjustment requirements of the implemented policy if needed (e.g. in case of a lack of resources, or when there are shortcomings in guidelines).

Input:	Evaluation report (from Evaluating filters).
Output:	Adjustment needs.

5.3.3 Tactical capabilities

The objectives of tactical capabilities in risk-based border management of each MS are:

1. Elaborating the decisions on risk-based border management that have been made at policy and strategic level in so-called risk-based filters that are established at the various BCPs.
2. Coordinating border control operations between organisations at tactical level within the state and with similar organisations in other countries.
3. Executing capacity planning for border control operations, including command and control of border control of these operations (i.e. at the BCPs in the state).
4. Assessing the overall situation of risks, threats and flows of travellers on a regular basis, and take appropriate measures if needed.
5. Evaluate the results of border control operations at the BCPs and reporting the evaluated results to the strategic level, and re-designing border control operations and filters if needed.

5.3.3.1 Designing filters

Elaborate the MS's guidelines and intructions for RBBM (e.g. the risks that should be mitigated by border control) into filters (see Section 2.4.10) that should be established for screening, profiling and checking flows of travellers at the various BCPs.

Input:	Overall strategy and General guidelines for RBBM, Risk criteria, Overview of threats, and Overview of risks and risk indicators (from Risk management), MS-specific guidelines and instructions for RBBM (from Implementing RBBM policy).
Output:	Filter designs.

5.3.3.2 Coordinate operations

Coordinate border control operations between organisations at tactical level within the state and with similar organisations in other countries with respect to the implementation of RBBM at BCPs.

Input:	Overall strategy and General guidelines for RBBM, Risk criteria, Overview of threats, and Overview of risks and risk indicators (from Risk management), MS-specific guidelines and instructions for RBBM (from

	Implementing RBBM policy), and Situation overview (from Situation assessment).
Output:	Harmonised operations at tactical level.

5.3.3.3 Capacity planning

Execute capacity planning for border control operations, including command and control of border control of these operations (i.e. at the BCPs in the state). This is achieved by providing guidelines on performing risk-based border control, by dedicated instructions on the use of filters, screening, risk-profiles and checking of travellers and their goods, and by allocating resources.

Input:	Overview of risks and risk indicators (from Risk management), RBBM resources, and MS-specific guidelines and instructions for RBBM (from Implementing RBBM policy), Filter designs (from Designing filters), and Situation overview (from Situation assessment).
Output:	Resources and Instructions for executing operational capabilities (i.e. Detecting, Screening, Selecting type of check, Facilitating flows of travellers, and Checking).

5.3.3.4 Situation assessment

Assess the overall situation of risks, threats and flows of travellers on a regular (e.g. daily) basis, and take appropriate measures if needed. For instance, because of a sudden threat or new modus operandi to cross the border (with some characteristic risk indicator).

Input:	Set of data that characterise the flows of travellers at the BCPs (size of the flows, nationality, modes of transport, etc.), Threat reports (trends) related to threats that should be mitigated and are relevant for border control operations.
Output:	Situation overview.

5.3.3.5 Evaluating filters

Evaluate the results of border control operations at the BCPs and reporting the evaluated results to the strategic level, and re-designing border control operations and filters if needed.

Input:	Output of all operational capabilities (i.e. Detecting, Screening, Selecting type of check, Facilitating flows of travellers, and Checking).
Output:	Evaluation report.

5.3.4 Operational capabilities

The objectives of operational capabilities in risk-based border management are:

1. Checking travellers, who intend to enter or to leave Europe via a BCP, whether they are legitimate to pass the border or not, and if not to take the appropriate measure (i.e. refuse border crossing or stopping the person at the BCP); to this purpose the checks are tailored to the individual risks that travellers pose.

2. Facilitating – in accordance with the designed filters – the flows of travellers at a BCP in such a way that benevolent travellers, who pose no risk, can smoothly pass the border (i.e. without delays and invasive checks).
3. Conducting - in support of both previous objectives – dedicated detection and screening activities of travellers and their goods, and selecting appropriate types of checks to be applied.

5.3.4.1 Detecting

Notice observable and hidden aspects of a traveller concerning his identity, behaviour, capability or mental state that (might) point out to a suspected situation that might pose a threat.[45] To this purpose a special method – the risk-based approach – including dedicated equipment and ICT tools are used. Detection can be executed by analysing travellers' data that become available during his travel stages (Pre-travel, BCP approaching, and At BCP). It is obvious that at later stages more data concerning the traveller and his goods can be collected.

Input:	Resources and Instructions (from Capacity planning), and Situation overview (from Situation assessment). Set of data that are required to characterise the identity, behaviour, capability and mental stage of a traveller, and an overview of deviant values with respect to identity, behaviour, capability or mental state.
Output:	Aspects related to identity, behaviour, capability or mental state that are of interest for screening and checking a traveller, because they either directly point out a threat (e.g. smuggling goods) or point out a situation that might be a threat because of the deviant or suspicious aspect values (e.g. deviant behaviour while approaching the BCP).

5.3.4.2 Screening

Investigate whether the aspects that characterise the identity, behaviour, capability and mental stage of a traveller meets one or more risk-profiles; if so, indicate the applicable risk profiles.[46]

Input:	Resources and Instructions (from Capacity planning), Situation overview (from Situation assessment), and Set of risk-profiles (from Coordinate operations), Information of aspects that has been collected (from Detect), and Information that is available in various information systems (see Section 2.4.5).
Output:	Applicable risk-profiles of the traveller.

[45] Definition by analogy with Cambridge dictionary: "to notice something that is partly hidden or not clear, or to discover something, especially using a special method or special equipment".

[46] Definition by analogy with Cambridge dictionary: "test or examine to discover if there is anything wrong with someone".

5.3.4.3 Selecting type of check

Determine the type of check that should be applied to the traveller and his goods, based on his risk-profile(s), including risk-related data that are relevant for checking the traveller. In case the traveller fulfils more risk-profiles, the severest check will be selected.

Input:	Resources and Instructions (from Capacity planning), and Applicable risk-profiles (from Screening), and data of interest that have been determined (from Detecting).
Output:	Type of check that should be applied to the traveller and his goods, including relevant risk-related data to be used during the first-line check.

5.3.4.4 Facilitating the flow of travellers

Facilitate the flows of travellers by (1) assigning each traveller to the lane that, according to the designed filters, is dedicated to the type of check that should be applied to him, and (2) optimising the flow-rate of travellers given the available resources.

Input:	Resources and Instructions (from Capacity planning), Filters (from Designing filters), Situation overview (from Situation assessment), Type of check for each traveller (from Select type of check), and daily instructions and information on volumes of flows of travellers (Coordinate operations).
Output:	Smooth flows of travellers who have been assigned (based on their profile) to the appropriate lanes within the filters of the BCP.

5.3.4.5 Checking

Conduct the first-line check to ensure that a traveller and the goods (and vehicle) in his possession are authorised to enter or to leave Europe. This check is done in accordance with the type of check that has been assigned to the traveller. If he is authorised, the traveller and his goods may pass the border. If not, there are two decision options: (1) the traveller is refused to cross the border because he is not allowed to pass, or (2) he is stopped at the border because either he is applying for asylum, or he is suspected of a certain crime or terrorist activity (national security), or he is suspected of having a certain disease that might affect public health. In case, a decision cannot be made by this first-line check, the traveller will be send to the second-line check for additional interrogation to take a final decision.

Input:	Resources and Instructions (from Capacity planning), Situation overview (from Situation assessment), The type of first-line check that should be applied to the traveller, including the risk-profile and relevant risk-related data (from Select type of check).
Output:	One of the following options: (a) the traveller (including his goods) is allowed to pass the border, (b) the traveller is refused to pass the border and therefore should return, (c) the traveller is stopped at the border and is transferred – depending on the above-mentioned reasons to the asylum, the judicial, or the public health authorities.

5.4 Interoperability aspects

As stated in Section 5.1, one of the conditions for RBBM is that interaction between all involved organisations at the various management levels, as indicated in Figure 2-1, is facilitated. Within TRESSPASS this means that collaboration and information exchange between the organisations involved in executing the capabilities that are described in the previous section (Section 5.3) is needed. To achieve this in an effective way, proper interoperability is essential.

There are various definitions of interoperability, for instance:

> *"The ability of diverse systems and organizations to work together i.e. to inter-operate."* [ISO 22397]
>
> *"Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems."* [European Interoperability Framework]

It is clear from both defintions that interoperability has various dimensions. The European Interoperability Framework defines four aspects types of interoperability, namely:

- Legal interoperability to align legislations of collaborating countries;
- Organisational interoperability, which aims at coordinating processes in which different organisations achieve a certain agreed and mutually beneficial goal;
- Semantic interoperability, needed for preserving the precise meaning of terminology, exchanged information, so it has the same meaning for all parties;
- Technical interoperability of equipment and ICT systems.

All these aspects of interoperability are key to ensure that all capabilities involved in RBBM are connected well. Thus enabling effective collaboration cross border (between countries in Europe), cross level (between the various organisations levels in RBBM), and cross sector (between organisations at the same level, such as border guards and customs). Because of its importance Task 2.5 is dedicated to elaborate the interoperability aspects in more detail.

To illustrate the different types of interoperability, several fundamentally different types of cooperation between states are provided below.

Sharing BCP-records: *During their trip, travellers may pass through multiple BCPs. This is already described in their PNR record, which is shared with PIUs. In the TRESSPASS-concept, each BCP will also generate a BCP-record: a description of relevant information regarding the travellers passage through the respective BCP. This BCP-record may be relevant also for other BCPs. Sharing BCP-records might, just like API and PNR data, become a part of RBBM within a cooperating set of states, if a variant can be determined that is ethically compliant.*

Sharing profiles: *Border guard agencies may learn distinguishing features between illegitimate travellers and legitimate travellers. They will design profiles based on those features that work for them, and which might also work for other BCP's, perhaps even for BCP's* *in other modalities or in other countries. Sharing profiles for evaluation and learning purposes may be an important part of the increased adaptivity that is expected from RBBM.*

Sharing risk-based concepts: *A state may develop a risk-based concept that works very well for them. For example a concept that is based on proximity to a particular trusted neighbouring country, such as The Netherlands with the UK. Other neighbouring countries, such as Greece and Turkey, or Spain and Marocco, may want to implement similar concepts by learning from each other.*

Equivalent residual risk: *A state may accept a particular type of risk evaluation and related residual risk in light of certain economic benefits. If this state is part of an international agreement, such as Schengen, then this agreement may (in the future) stipulate how its participants may reach agreement on taking on less, or additional risk and under which conditions. One condition might be that while risk mitigation measures may differ, the states should all have equivalent residual risk for specific types of threats or vulnerabilities.*

6 Implications of RBBM

In Chapter 2 today’s pre-RBBM situation is described, while Chapter 3 presents an overview of the challenges of the current situation. Chapters 4 and 5 discuss the intended situation in which an RBBM approach is applied. This chapter describes the implications of the decision to implement RBBM at BCPs in Europe. It first compares rule-based, intelligence-led and risk-based border management. With that information, authorities of a Member State can assess their current situation with respect to border control. Next, the difference between the current, and the intended situation is described, and it is described what needs to change in order to obtain the intended situation. Finally, this chapter describes in general terms how these changes – the transition from the current to the intended RBBM situation – can be realised.

The information in this chapter is based on logical deduction from the operational starting point (differentiated checks based on the outcome of screenings), and on interaction with the end-user partners within the TRESSPASS consortium. Expectations are that interaction with more types of stakeholders in the course of the TRESSPASS project will lead to a more refined insight into the implications of RBBM.

6.1 Comparison between rule-based, intelligence-led and risk-based border management

This section compares rule-based, intelligence-led and risk-based border management. This will help stakeholders to better understand the main differences between these different management approaches. In addition, using this information, a Member State can assess to what extent it is ready to start working towards RBBM.

Table 6-1 compares RBBM with the current (rule-based and intelligence-led) approaches. Risk-based border management diverges on multiple key elements in comparison to the traditional rule-based and intelligence-led approaches. Obviously, the main difference between the current and the risk-based approach is the premise that all travellers receive a check that matches their (lack-of) individual risk-profile, instead of subjecting travellers to certain checks because of general rule-based characteristics (e.g. EU or Non-EU).

Table 6-1 Comparison between border control approaches

Topic	Rule-based	Intelligence-led	Risk-based
Type of checks	Dependent on general characteristics, such as EU/Non-EU)	Dependent on general characteristics, such as EU/Non-EU)	Dependent on risk-profile of the traveller
Fraction of travellers that is checked	All travellers are checked	All travellers are checked	All travellers are checked on identity (see Section 4.5.1), besides that, trusted (bona fide) travellers might not be checked anymore.

Topic	Rule-based	Intelligence-led	Risk-based
Regulations	Regulations stipulate operational rules that all BCPs must follow.	Regulations stipulate rules that all BCPs must follow. Exceptions can be made for busy moments.	Regulations leave room for a local risk-based approach.
Decision-making	Rule-based	Rule-based	Based on risk acceptance
Information needs	General traveller information is required to determine the required type of check (based on EU law)	General traveller information is needed to determine required check (based on EU law), and additional information is needed to gain situational awareness (mostly for planning or instructing personnel)	Information is required on specific risk indicators to determine the type and level of checks for each individual traveller, and information is needed on changes in risks, threats and trends to determine proportionality under EU law
Purpose of screening	N/A	To assess how much capacity is required for this traveller	To assess the risk of a traveller, and thus which checks a traveller needs to undergo
Performance indicators	Flow-rate, efficiency, and the quality of checks	Flow-rate, efficiency, and the quality of checks	Flow-rate, efficiency, quality of checks, and the risk reduction

6.2 Implications and needs at the various governance levels

This section describes the difference between the current situation and a situation with RBBM. This is done at the various relevant governance levels: (inter)national, strategic, tactical and operational. This provides an answer to the question ‘what is lacking for RBBM?’.

The two most important changes that RBBM requires are:

1. To apply screenings that generate a meaningful risk level per traveller, including the assessment of ‘unknown persons of interest’, and being able to deal with unreliable information, including insincere verbal statements by travellers.
2. To take responsibility for the risk management process on the national level.

TRESSPASS deliverable D1.3 will analyse the gap between the current state of the art and possible future risk-based border control. Understanding the implications is best done by experiencing them. One way to do so is to play the TRESSPASS serious game (see Section 6.4).

6.2.1 Implications and needs at (inter)national level

The basic idea of RBBM is to ensure that the travellers receive a check that corresponds with their risk profile. In itself, this should generate trust in the functioning of border management. Ideally, this results into less stringent checks for most of the travellers (as most travellers are not malicious). However, this can also skew the perceptions of travellers in respect to the BCPs: they perceive the BCPs as less effective because only few travellers are extensively checked. As a consequence, the public opinion can start questioning and doubting the security of Europe and the BCPs, which can affect the legitimacy of border agencies. This will be addressed in TRESSPASS deliverable D6.3.

So, perhaps the most important change for this level is to take responsibility for the residual risk of a risk-based BCP. This may seem difficult, but it can be done relatively easy if the tactical level can show how the cumulative residual risk for a state in a specific instantiation of RBBM (e.g. by combining different risk-based concepts into one filter or BCP) is no more than what it was in a the pre-RBBM situation.

RBBM requires a legal base that allows for checks based on the outcome of a risk assessment, i.e. a screening. If there is no current legal base for this discretion, then it may be desirable to adapt directives and / or regulations in order to create a legal ground to be able to do this. This is further described in TRESSPASS deliverable D1.4.

In order to allow risk owners on all levels to take responsibility and make informed decisions that also take the ethical implications of introducing an RBBM approach into account ‘by design’, TRESSPASS deliverables D9.7 and D9.8 will define a framework for the assessment of ethical, legal and societal impact on the travelling public.

The check as part of a BCP also has a deterrence side effect. This is relevant for RBBM as RBBM is affected by the perceived threat. Deterrence affects threat, so an increased deterrent function of BCPs would increase the prevention effect of BCPs. As described in Section 4.1.2, deterrence can be increased by raising the uncertainty with adversaries of the workings of a risk-based BCP, which can be obtained with the flexibility of RBBM. It may be useful to alter EC Regulation 2016/399 to also give BCPs a preventive function.

The geographic location, economic position and political landscape of states all influence the type of travellers that use their BCPs. So states face different risks from travellers. This is a major motivation for states to consider RBBM, as it allows for more flexibility and for local variations to allow for different checks based on screenings. This raises the question if there should be limits to that variability and flexibility. For example, states may be bound to internal or external agreements and legislature that creates a lower limit to the amount of risk that they are allowed to take. A state’s decision to consider RBBM implies that it must also define the risk evaluation criteria within which it can operate itself, and the criteria that are implied for a specific cooperation.

The networked nature of international travel and of international treaties implies that risk taken by one state, may alter the risk for another state. For example, if two states have agreed on open borders, and if a specific risk profile is considered a low threat in the first state, but a high threat for the second state. This can be solved by international coordination, e.g. by sharing the risk evaluation of a risk-based filter with partners. Depending on the nature of the international cooperation, approval from partners may be required, e.g. facilitated by international agencies such as Frontex. The complexity of this is illustrated in Figure 6-1, and is also discussed briefly at the end of section 5.4.

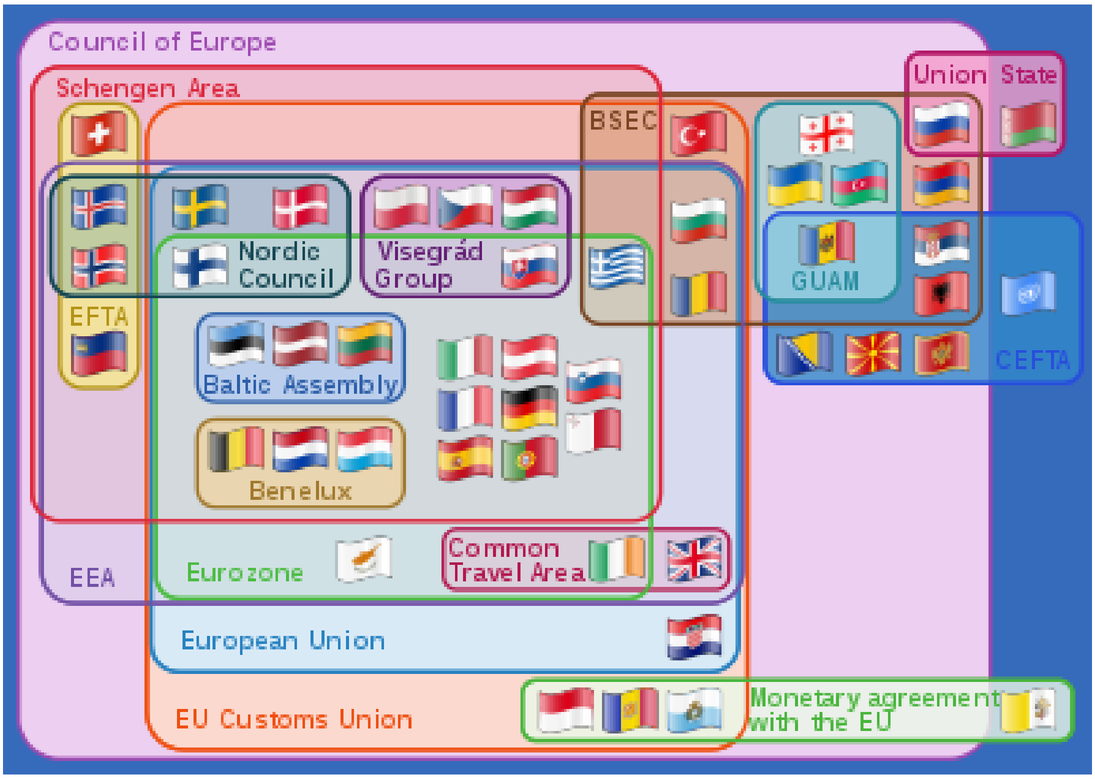


FIGURE 6-1 RELATIONS BETWEEN VARIOUS MULTINATIONAL EUROPEAN ORGANISATIONS AND AGREEMENTS (REDDIT)

6.2.2 Implications and needs at strategic level

The strategic level is concerned with the long term continuity of the state's border management, including the changes that are required to secure that long term continuity.

Introducing RBBM is such a strategic change: depending on the threats that require mitigation, specific risk-based concepts need to be implemented into established or novel BCPs. These concepts often demand changes in practices of BCPs in comparison to the current rule-based or intelligence-led border management approaches. As the need for information expands and changes, BCP tactics and operations often needs to be adapted.

For instance, when other types of information are required that are currently not collected, new data sources need to be consulted which potentially requires novel technological resources (e.g. data scrapers, observational technology) or human resources (e.g. additional skills and training).

For RBBM concepts to work and to be able to collect information that is necessary to know whether a traveller matches a certain risk-profile or not. There can be legal barriers or restrictions that need to be overcome for a risk-based concept to be implemented. Hence, this should be taken into consideration when developing RBBM concepts. Often, experimental settings provide a temporary opportunity to validate whether the concept (by using data sources that are normally restricted) can work in practice. When successful, it can be decided whether border management agencies might be granted access to the data sources, and under what conditions (for instance, to ensure the proportionality and subsidiarity of the concept). This is discussed in TRESSPASS deliverable D1.4.

In addition this can imply that the physical space or infrastructure of the BCPs needs to be altered in order to collect the required information.

6.2.3 Implications and needs at tactical level

The tactical level is concerned with the design and implementation of risk-based filters. To this end, they must have the ability to evaluate the effects of alternative filter designs and to compare them. This is in itself not new, as under rule-based and intelligence-led border management, BCP operators and border guard agencies could already design BCP filters and evaluate them on traveller flow and efficiency (see Section 2.4), and -if they so desired- a host of side effects (see Section 4.1.2).

But RBBM adds another parameter: the detection power of a filter, including possibly the deterrence factor. It is important for this tactical level to agree with the risk owner about the risk criteria, as completely eliminating any risk is impossible, also in the current situation.

How to integrate deterrence in the risk management process and trust framework without increasing the chilling effect? BCPs have a deterrence effect on adversaries, which may have to be increased to compensate for reduced detection power of checks. In such cases, deterrence of risk-based filters must be assessed in such a way that the outcome can be used as input to the risk evaluation and trust framework. This is described in TRESSPASS deliverables D2.1 and D6.3.

Therefore, the tactical level needs methods and tools that help evaluate risk in a clear manner, such that it can be explained to relevant stakeholders. This may involve evaluating the quantitative effectiveness of the pre-RBBM approach but there may also be tools that can show the difference merely using a qualitative approach.

The tactical level needs intelligence about the 'rise and fall' of relevant threats and vulnerabilities. This intelligence is essential in order to be able to make sure that the effectiveness of BCP operations does not drop below acceptable levels. This intelligence should therefore be collected in a coherent tactical management dashboard containing an actual risk overview / situation assessment.

The tactical level also benefits from accurate information about the duration of checks, specifically for the duration that travellers occupy the resources of a check (see also Section 2.4.8).

6.2.4 Implications and needs at operational level

Recent changes in rule-based border management have shown that small changes, e.g. weighing the relevance of one risk indicator in a different manner, can have large implications for the flow of travellers. So, the increased flexibility of RBBM can have significant effects on the operational level.

Existing methods such as behaviour detection and profiling will still be used, but now in a broader context. Frontline operational staff has to be taught how to the assess new types of risk indicators, and their feedback must be taken into account in a learning loop.

If the appropriate priority was not given thus far to the assessment of the information provided by intelligence, it will be necessary to do so for RBBM. In intelligence-led border management, it may sometimes not have been clear how information could help allocate resources better. In RBBM, the risk-based framework provides a more specific context and provides more direction for the underlying short-term intelligence cycle (i.e. per traveller).

There will be an increased time-pressure on the operational level to finish traveller screenings on time. If screenings are not finished on time, then travellers cannot be directed to differentiated checks, thereby negating the potential benefits of RBBM.

6.3 Transition to RBBM

This section describes how a transition to RBBM can be implemented on relevant governance levels. The only starting point in this section is that RBBM is not yet implemented.

The previous section described in great detail that RBBM is fundamentally different from both rule-based and intelligence-led border management. This directly implies that a transition to RBBM is not possible with the flick of a switch. A transition is a systemic change of the relation between border management stakeholders, and will require time and dedicated and coordinated change-management in and between multiple actors.

6.3.1 Change management for RBBM

This section describes the conditions for a controlled and safe transition to RBBM, which together guarantee both the continuity of border management during such a transition, and the realisation of the transition. They come down to answering three basic questions: (1) Do I want RBBM?, (2) Am I allowed to do RBBM?, and (3) Am I able to introduce and operate RBBM? To affirm these questions a number of conditions should be fulfilled.

Question 1: Do I want RBBM?

Conditions:

1. The risk-owner (i.e. the state) should be aware of the actual status of border management. He should know on which rules border management is based, and should be aware of the implications of the current approach on reduced flexibility, efficiency and flow-rate.
2. The risk-owner should have a basic understanding of the principles of RBBM. This should include a general idea of the possibilities RBBM offers and awareness of the challenges involved in introducing RBBM.
3. The risk-owner should be willingness to explore RBBM for the proper reasons, i.e. reasons that RBBM may actually be able to deliver on.
4. The transition towards RBBM should be initiated and governed at the level of the risk-owner. This is required, because lower levels simply do not have sufficient mandate to decide about introducing RBBM.

Question 2: Am I allowed to do RBBM?

Conditions:

5. The intended type of RBBM should have a legal foundation. This includes that it respects international agreements (see deliverable D1.4).
6. The intended type of RBBM uses a value-sensitive-design approach. It takes human values such as ethics and privacy into account during the entire life cycle of applied ICT systems.

Question 3: Am I able to introduce and operate RBBM?

Conditions:

7. The (parts of) organisation(s) involved in change management
    a. should have sufficient mandate,
    b. should be able to deliver sufficient power ('momentum') to drive the change towards RBBM, and
    c. should be properly positioned with respect to the 'regular' management.
8. The introduction of RBBM will continuously be monitored.

6.3.2 Value sensitive design for RBBM

The GDPR and the Law Enforcement Directive 2016/680 (LED) require data protection by design (DPBD) for new border management developments such as RBBM. DPDB is an example of 'value-sensitive design'.[47] Such design principles envision that ethics, privacy and data protection are operative throughout the entire life cycle of technologies:[48] from the early design stage to their deployment, use and ultimate disposal. This is done by applying a design process that covers all life cycle stages and by applying ethical, privacy and data protection design patterns which are well understood and are the known best-practice for the particular purpose they are used for, and domain they are used in. The resulting design documents and systems should limit all the ethical, privacy and data protection invading activities to the minimum according to the foundational principles (Cavoukian, 2009) of privacy by design, data protection, non-discrimination and other fundamental values.

TABLE 6-2 TRESSPASS ETHICS, PRIVACY AND DATA PROTECTION BY DESIGN (EPDPBD)

EPDPbD foundational principles Index	During TRESSPASS project	Beyond TRESSPASS project (future systems)
Proactive not Reactive; Preventative not Remedial	By having an ethics specialist responsible for ethical relevant issues, TRESSPASS creates a working environment where data protection, privacy other ethical issues can be pro-actively worked on, instead of in a reactive manner with only an external ethical board. The deliverables (containing sections) on ethics and	TRESSPASS will advise technical partners on relevant issues and offer an impact assessment method in deliverables D9.6-D9.8. Ethical guidelines for end users and decision makers will be developed as part of deliverable D9.9.

[47] Value sensitive design (VSD) is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner. (Friedman, B., Kahn Jr, P. H., Borning, A., & Kahn, P. H. (2006). Value Sensitive Design and information systems. Human-Computer Interaction and Management Information Systems: Foundations. ME Sharpe, New York, 348–372).

[48] van Rest, Jeroen, et al. "Designing privacy-by-design". Annual Privacy Forum. Springer Berlin Heidelberg, 2012.

EPDPbD foundational principles Index	During TRESSPASS project	Beyond TRESSPASS project (future systems)
	privacy will be a direct result of this approach.	
Privacy as the Default	TRESSPASS will use simulated data (WP7) for a large part of the R&D activities as well as for the evaluation. Volunteers will only participate in remaining validation activities on an opt-in basis (consent). The consortium is considering using regular travellers as data subjects only for more mature validation activities that cannot be done with volunteers.	The TRESSPASS simulator will be available for future development and (re)design of risk-based BCPs. For ethical impact assessment (D9.7-D9.8), TRESSPASS will make use the simulator for assessing the ethical impact and for supporting ethically informed decision making by end users.
Privacy Embedded into Design	Ethics specialists are embedded in every relevant work package.	
Full Functionality – Positive-Sum, not Zero-Sum	This table regarding EDPbD will be the starting point for all design decisions.	TRESSPASS will advise end users on ethics and data protection by design in D9.6 and provide an impact assessment method in D9.7 and D9.8.
End-to-End Security – Lifecycle Protection	The TRESSPASS project does research for security while ensuring the privacy of data subjects which were needed for the project.	
Visibility / Transparency	By using the DBT method (Task 2.1), TRESSPASS will ensure that all requirements are grounded in actual security and research needs, and that full functionality will remain the goal during the design and development process.	TRESSPASS will advise end users on ethics and data protection by design in relation to the DBT in D9.7 and D9.8.
Respect for Users	Any personal data that is gathered during the project	TRESSPASS will develop a project baseline for

EPDPbD foundational principles Index	During TRESSPASS project	Beyond TRESSPASS project (future systems)
	phase will be deleted when it is not needed anymore for the project.	research ethical questions D9.2 and support the consortium in meeting all relevant standards of responsible research. D9.3-D9.5 will periodically report on research ethical aspects.

A challenge when applying such principles to very innovative technologies, is that it is not yet known which ethical and data protection design patterns are in fact best-practice: there is no experience with applying them in practice yet. Moreover, what works in one domain (e.g. aviation security) may not work in another (e.g. smuggling). Based on the ethical framework for design and evaluation of traveller screening technologies developed in the project XP-DITE, WP9 will identify the relevant ethical, legal and societal risks relevant to risk-based border management. A method for evaluation will allow a comparative impact assessment of different implementations of risk-based border management with regard to the specific design basis threat (thus, integrated with WP2's approach to risk-based border management). On the basis of this method for evaluation, WP9 will offer an additional view for more informed decision making for the design and implementation of risk-based screening and provide input to the technical work packages on how to use opportunities to minimise the ethical and data protection impact of the TRESSPASS solutions.

6.3.3 Required steps and good practices

States will have different starting points, different types of purposes with RBBM and they may have different levels of ambition. A custom-tailored, comprehensive and detailed set of steps cannot be made within the scope of TRESSPASS, but a generic set of steps and related good practices is given in this section. These steps can take two to five years to take, depending on the exact starting position, the level of engagement and the ambition level.

Starting position: Having intelligence-led border management is not a precondition to start a transition to RBBM, as both transitions can theoretically be combined. But it is a good practice to first make a transition towards intelligence-led border management. This will require the related border agencies to become familiar with screenings and profiling, and it will alert their ICT services to the relevance of collecting local information around the BCP.

The required steps are:

- **Step 1**: Use concept design & experimentation (CD&E) to develop a set of specific risk-based concepts. This will help to create awareness of the potential benefits, and it will help make clear which specific types of information are going to be required, and the legal framework for doing so;
- **Step 2**: Organise the challenge in disjunct 'building blocks' (see Section 6.3.3.2), and execute them in a programmatic manner governed by proper change management;
- **Step 3**: Implement the results of the building blocks;
- **Step 4**: Operate, evaluate, adapt and improve;

Note: TRESSPASS deliverable D10.6, the Sustainability report (roadmap), will describe how the TRESSPASS solutions can be introduced and sustainably will be used in relevant user communities.

6.3.3.1 Step 1: Concept development & experimentation

The first step of the transition is to develop a number of risk-based concepts that address the local challenges and sketch valuable, meaningful benefits (see Section 4.8.2 for some examples). This activity requires multi-disciplinary skills and capabilities.

CD&E is a structured method that helps organisations to develop complex integral concepts for a wide variety of challenges. It is based on the idea that complex solutions arise from the confrontation, experimentation and integration of ideas that over time lead to realistic solutions. CD&E as such is a generic method. Therefore, an adaptation for TRESSPASS has been made by developing the initial version of the so-called 'TRESSPASS risk-based BCP design game' (see Section 6.4). This game is completely compatible with the value sensitive design approach as described in Section 6.3.2. Playing this game in successive iterations with subject matter experts and with representatives of local stakeholders will therefore lead to realistic, proportional, and desirable risk-based concepts.

6.3.3.2 Step 2: Programmatic approach based on building blocks

A Member State that decides to move to RBBM faces a complex transition. This transition can be decomposed into *'building blocks'* (BB) which each address coherent, relatively independent parts of the transition. They are different from the functional elements of RBBM: building blocks only cover missing or lacking aspects.

Just like RBBM has to be approached in an integral manner, building blocks have too. As depicted in Figure 6-2 six generic building blocks have been identified. These building blocks serve as starting point for developing state-specific building blocks.

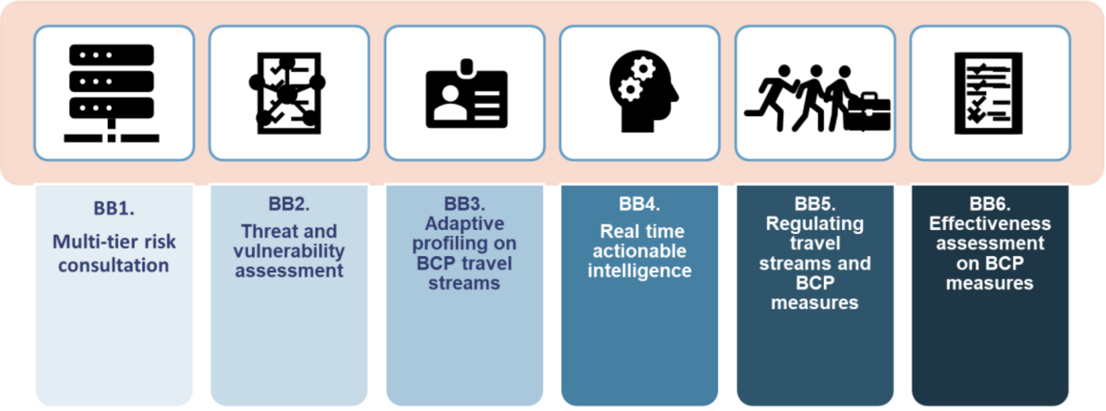

BB1.
Multi-tier risk consultation
BB2.
Threat and vulnerability assessment
BB3.
Adaptive profiling on BCP travel streams
BB4.
Real time actionable intelligence
BB5.
Regulating travel streams and BCP measures
BB6.
Effectiveness assessment on BCP measures

FIGURE 6-2 RBBM – BUILDING BLOCKS THAT ARE REQUIRED FOR INTRODUCING A RISK-BASED APPROACH IN A STATE

The building block are:

- **Multi-tier risk consultation (BB1)**: Identifying and evaluation risk in a networked environment requires a different paradigm than the traditional focus on singular risks. Accepting that 100% security at the border is impossible, does not mean that every false negative (i.e. missed threat) will actually lead to the manifestation of an incident. The state has the possibility to use information gathered at the BCP to manage risk later in the causal chain, e.g. by providing information to national police, the intelligence service or to international partners. This multi-tier risk model is the basis for Integrated Border Management, and works both nationally and internationally.

- **Threat and vulnerability assessment (BB2)**: Under a rule-based approach, the identification of threats and vulnerabilities was done in a centralised manner. In RBBM, local actors have a degree of freedom to act on local situations: threats and vulnerabilities. This requires an increased capability to assess threats and vulnerabilities. This development will present challenges for the supporting intelligence cycle.
- **Adaptive profiling on BCP travel streams (BB3)**: RBBM increases the focus on actual threats, instead of generic threats that are only described in generic rules. Profiling is essential for detecting an important type of threat: unknown persons of interest. In RBBM, profiling may be done more adaptive than under intelligence-led border management, which requires better cooperation with partners, better information exchange, better intelligence processes, better tools, training and work methods.
- **Realtime actionable intelligence (BB4)**: The tactical level needs intelligence in a slow loop about the “rise and fall” of relevant threats and vulnerabilities. This intelligence is essential in order to be able to make sure that the effectiveness of BCP operations does not drop below acceptable levels. This intelligence should therefore be collected in a coherent tactical management dashboard containing an actual risk overview / situation assessment and that provides ‘actionable intelligence’ on the tactical level, for example to dynamically alter threat profiles.
- **Regulating travel streams and BCP measures (BB5)**: The ability to filter and facilitate flows of travellers is required to realise the benefits of RBBM. If trusted travellers still queue up for stringent checks because the signage is wrong, and if unauthorised travellers can slip through relaxed checks, then all the work done in screening is done for nothing. In addition, specific types of checks may have to be designed for specific types of threats. A specific focus should be on secondary checks based on advanced interview methods, because this is where the funnel of failed screenings and failed checks all lead to. If the latest check is the weakest link, then the filter can never be effective.
- **Effectiveness assessment on BCP measures (BB6)**: The operational ability to reliably separate threat from non-threat determines the actual effects of a risk-based BCP. It is crucial for trust in risk-based BCPs that the risk owner can proof how effective it is in detecting threats, and to know how accurate this proof is. This requires the local availability of reliable and trusted assessment methods, including perhaps also methods to assess the deterrence effect. This is required both on the tactical level for the quick loop, and on the level of the risk-owner for the slow policy loop.

The building blocks can also be mapped on ISO 31000 as has been done in Figure 6-3. This gives some more context regarding the origin and the purpose of the building blocks.

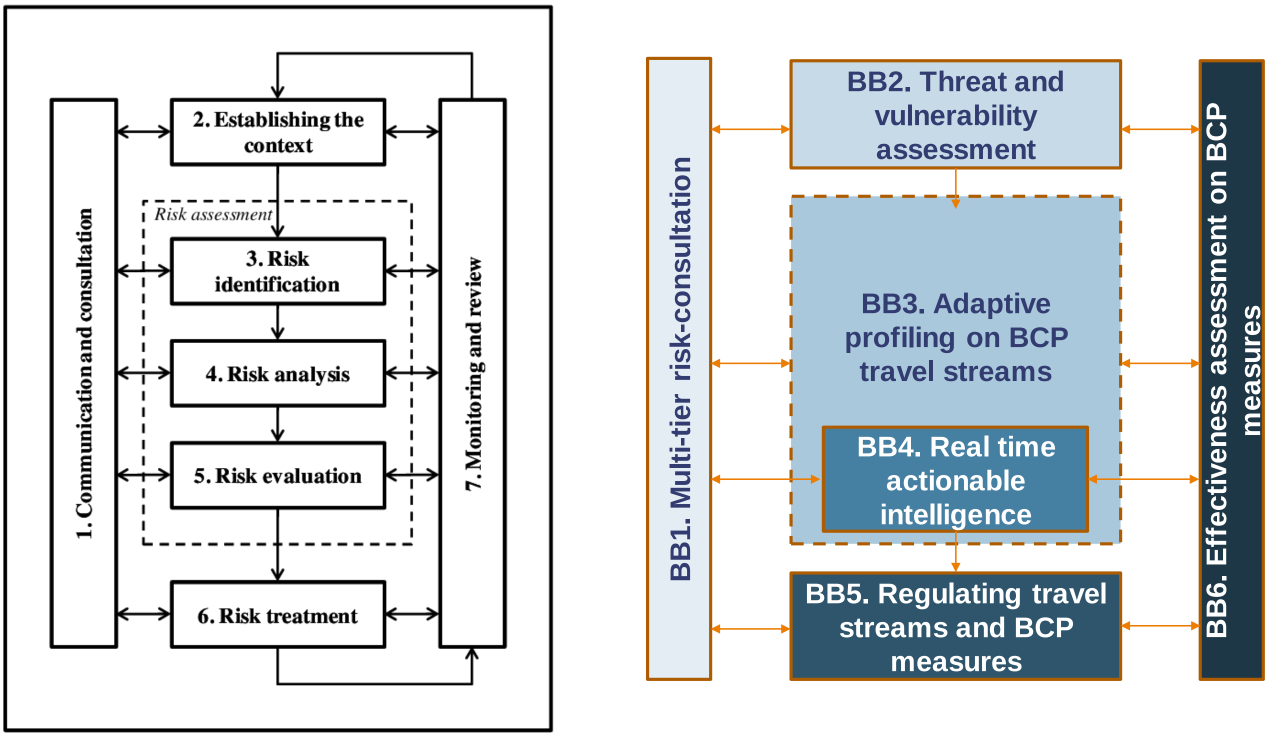

2. Establishing the context
Risk assessment
3. Risk identification
4. Risk analysis
5. Risk evaluation
6. Risk treatment
1. Communication and consultation
7. Monitoring and review
BB1. Multi-tier risk-consultation
BB2. Threat and vulnerability assessment
BB3. Adaptive profiling on BCP travel streams
BB4. Real time actionable intelligence
BB5. Regulating travel streams and BCP measures
BB6. Effectiveness assessment on BCP measures

FIGURE 6-3 ISO 31000 RISK MANAGEMENT AND TRESSPASS RISK-BASED BUILDING BLOCKS

6.3.3.3 Step 3: Implement the results of the building blocks

Implementing the results of the risk-based building blocks requires cooperation between -at least- the state as risk owner, a border guard agency, and a BCP operator. Often, this BCP operator is a private party, which typically makes the implementation a public-private endeavour under management of the state.

6.3.3.4 Step 4: Operate, evaluate, adapt and improve

The evaluation of risk-based concepts is required to be able to demonstrate that the transition itself is done in safe manner, and also to be able to gradually adapt and improve them. This means that the building block ‘Effectiveness assessment on BCP measures’ should be developed as one of the first.

Specific attention should be given to the evaluation of components that rely on variants of profiling. First, because the ELSA implications of profiling are substantial, second because the expected benefits are substantial, third because profiling is difficult to ‘get right’ (if there is such a thing), and fourth because it is notoriously difficult to evaluate properly.

6.4 TRESSPASS risk-based BCP design game

One of the challenges of developing the RBBM concept is to understand, develop and explain operational concepts that can be eventually implemented in the daily operations of BCPs. Concept development requires extensive coordination and interaction between multidisciplinary actors at all governance levels, which can be difficult to achieve. Furthermore, as concept development relies on a high degree of iteration of steps, this process can be perceived as chaotic. To provide guidance to this concept development, a serious game is being developed. The purpose of this game is to develop the information view of an operational concept (i.e. establishing a concept in which it is established what data and resources is required to effectively identify travellers that match a certain risk profile). By playing this game, an unstructured set of ideas and perspectives of different actors and experts can be structured and aligned. This will eventually result in a concept that is suitable for operationalisation and experimentation.

The TRESSPASS serious game is an initial adaption of the generic CD&E process. It serves multiple purposes:

- Facilitate understanding of what is RBBM;
- Help developing risk-based concepts;
- Help explaining risk-based concepts to stakeholders, both local and international.

The game was played by TNO with end-users and experts of the Royal Netherlands Marechaussee[49] (The Hague, 13 February 2019), which was considered as being a very useful session to explain the main principles of a risk-based concept. In Task 2.4 the game will be elaborated and will be adjusted based on experiences of applying it. In that task also a full description of the game will be provided in deliverable D2.4 (“Design of risk-based BCPs”). It will be used in the TRESSPASS pilots (WP8), but can also be used by other parties (e.g. Frontex) that are considering to implement RBBM at BCPs.

Currently, it is very difficult to estimate the variability in risk-based concepts that will arise. Will there be five different risk-based concepts which are basically the same everywhere? How would that be different from the current rule-based situation? Will there be fifty risk-based concepts, basically adapted to the needs of specific states? Or will there be thousands, adapted to specific filters for specific modalities for specific states? It will be essential, anyhow, to have an international discourse about risk-based concepts. Perhaps including a level of coordination or a centralised governance. This discourse, coordination and governance will need tools to describe, develop and evaluate risk-based concepts. The TRESSPASS serious game may be one of those tools.

6.5 Beyond TRESSPASS: Networked risk management

Suppose RBBM is implemented in a cooperating group of states, and suppose it works as intended. States design risk-based filters that are optimised for the local situation. By design this is a solution direction based on distributed intelligence (distributed over different states), focused on local optimisation for local interests (individually for each state).

The distributed nature makes RBBM extremely scalable. Large groups of nations can agree on residual risk, and use local knowledge to design optimal filters. See also section 5.4.

Local optimisation may have the best support from local stakeholders, but it cannot lead to solutions that are best overall, i.e. that are most efficient, most effective or best for the flow-rate. For example, will the local optimization in all separate Schengen states, also lead to better border management when considering the whole Schengen area?

To better understand this issue, one needs to turn towards the theory of Networked Risk Management (NRM; Joosten & Smulders, 2014). NRM adds to the traditional approach of risk management in the sense that it helps to understand how the management of risks works in a complex environment. In complex environments, such as the Schengen area (with a wide variety of stakeholders, threats and challenges), it becomes harder to understand what actor

[49] The organisation that is responsible for border control in the Netherlands.

has the overall responsibility. When this clear hierarchy is absent, NRM helps to understand how the management of risks then can be done.

In networks, risk management is mostly about aligning the 'obligations' and 'expectations' of different stakeholders (i.e. nations and agencies). Obligations are the responsibilities of (a group of actors), and the total collection of obligations are conceptualised as a scope. In this context, a risk is when obligations in the scope are not met by the responsible actor(s). In a networked environment, actors can have expectations to other actors (both with their relative scopes) to meet their own scope. These expectations can be considered as a risk, because when they are not fulfilled, the own obligations are not met (Joosten & Smulders, 2014). Therefore, it is in a networked environment extremely important that the expectation of actor A in actor B, is experienced as an obligation by actor B. If there is a misalignment, problems can occur in the form of unmet obligations.

In the context of RBBM in the Schengen area, this requires extensive coordination and cooperation between different Member States. Member States need to be able to express the (residual) risks they deem acceptable, and what not. These expectations of all Member States, located at either the border of Schengen or in the middle of the area, need to provide insight in the (residual) risks they accept. Hence, when operational RBBM concepts are implemented, they should not only adhere to the interests (i.e. obligations) of the respective country they are located, but also to all different member states (i.e. expectations) as there is free travel flow within Schengen. Therefore, if every nation can construe their own RBBM concepts to mitigate risks, the concepts needs to be conform the expectations of whole Schengen.

This can be coordinated by a central border management agency such as Frontex, but if this process is too rigid and sluggish, this might result in less flexibility and capacity to react on shifting risk-levels. This is the challenge beyond TRESSPASS.

7 CONCLUSIONS

This deliverable (D1.2a) defines the principles of the TRESSPASS RBBM concept vis-à-vis alternative approaches, such as rule-based border control and intelligence-led border control. This includes the expected benefits and important conditions for implementation of a risk-based border management concept.

The way forward beyond D1.2a has also been defined. This is done in three disjunct manners. First, in terms of how other TRESSPASS tasks relate to this deliverable in Annex D. Second, in terms of the transition from rule-based border management towards risk-based border management in chapter 6. And third, what future developments beyond TRESSPASS might be possible, in Section 6.5.

REFERENCES

Berger, M. (2007) ‘Self-incrimination and the European Court of Human Rights: Procedural issues in the enforcement of the right to silence’, *European Human Rights Law Review*, 5, pp. 514-533.

Bouma, H., Burghouts, G., Den Hollander, R., Van der Zee, S., Baan, J., Ten Hove, J., Van Diepen, S., Van den Haak, P. and Van Rest, J. (2016) ‘Measuring cues for stand-off deception detection based on full-body nonverbal features in body-worn cameras’, *Proceedings Volume 9995, Optics and Photonics for Counterterrorism, Crime Fighting, and Defence XII,* pp. 1-20.

Carter, B. and Meisel, A. (2014) *Is it worth screening for Ebola at airports?* [Online]. Available at: https://www.bbc.com/news/magazine-29787746 (accessed 27 March 2019).

Cavoukian, Ann. “Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices”. Information and Privacy Commissioner of Ontario, Canada (2009).

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082&from=EN (accessed 27 March 2019).

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&from=EN (accessed 27 March 2019).

ECAC Behaviour Detection Study Group (2016) “ECAC Strategy paper on behaviour detection”. Available at https://www.ecac-ceac.org/behavior-detection-study-group-bdsg

Electronic Frontier Foundation (EFF). (2003) *Biometrics: Who’s Watching You?* [Online]. Available at: https://www.eff.org/wp/biometrics-whos-watching-you (accessed: 27 March 2019).

European Commission. (2010) *Guidelines for Integrated Border Management in European Commission External Cooperation* [Online]. Available at: https://europa.eu/capacity4dev/ibm-eap/document/1-guidelines-integrated-border-management-european-commission-external-cooperation-european (accessed 27 March 2019).

European Commission. (2015) *Risk-based screening at border crossing (ID: SEC-15-BES-17)* [Online]. Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/sec-15-bes-2017 (accessed: 27 March 2019).

European Commission (2017). *EU Information Systems Security and Borders* [Online]. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_eu_information_systems_security_and_borders_en.pdf (accessed: 27 March 2019).

Europol. (No date) *Information Exchange* [Online]. Available at: https://www.europol.europa.eu/activities-services/services-support/information-exchange/ (accessed 27 March 2019).

Finn, R. L., Wright, D. and Friedewald, M. (2013) 'Seven types of privacy'. In Gutwirth, S. Leenes, R. De Hert, P. (eds) *European data protection: coming of age*. Dordrecht: Springer, pp. 3-32.

Frontex. (2012) 'Common Integrated Risk Analysis Model a comprehensive update (version 2.0)'. Available at https://frontex.europa.eu/intelligence/ciram/

Havinga, H. N. J., & Sessink, O. D. T. (2014, September). Risk reduction overview. In International Conference on Availability, Reliability, and Security (pp. 239-249). Springer, Cham.

iBorderCtrl Consortium (2019) iBorderCtrl. Available at: https://www.iborderctrl.eu/

Interpol. (No date) *Border management* [Online]. Available at: https://www.interpol.int/en/How-we-work/Border-management (accessed 27 March 2019).

Joosten, R. and Smulders, A. (2014) *Networked Risk Management: How to successfully manage risks in hyperconnected value networks*. TNO.

Kashima, Y., McKintyre, A., & Clifford, P. (1998). The category of the mind: Folk psychology of belief, desire, and intention. Asian Journal of Social Psychology, 1(3), 289-313.

McKinsey. (2007) 'Global trends affecting the public sector' [Online]. Available at: https://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Public%20Sector/PDFS/McK%20on%20Govt/Inaugural%20edition/TG_global_trends.ashx (accessed 27 March 2019).

Migration and Home Affairs, EC. (No date) *Passenger Name Record (PNR)* [Online]. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en (accessed 27 March 2019).

Morall, A. R. and Jackson, B. A. (2009) *Understanding the role of deterrence in counterterrorism security*. Santa Monica: Rand

NEN-ISO 31000. (2018) *Risk management – Guidelines*.

Ormerod, T. C. and Dando, C. J. (2015) 'Finding a needle in a haystack: Toward a psychologically informed method for aviation security screening', *Journal of Experimental Psychology: General*, *144*(1), pp.76-84.

PERSONA Consortium (2019) PERSONA project. Available at http://persona-project.eecs.qmul.ac.uk/

Poppe, R., Van Der Zee, S., Heylen, D. K., & Taylor, P. J. (2014) 'AMAB: Automated measurement and analysis of body motion'. *Behavior research methods*, *46*(3), pp.625-633.

PWC. (2015) 'The future of border management: maintaining security; facilitating prosperity' [Online]. Available at: https://www.pwc.com/m1/en/publications/documents/the-future-of-border-management.pdf (accessed 27 March 2019).

Regulation (EU) No. 2016/399 of the European Parliament and of the Council of 9 march 2016 on a union code on the rules governing the movement of persons across borders (Schengen Borders Code) [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0399&from=EN (accessed 27 March 2019).

Regulation (EC) No. 1931/2006 of The European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1931&from=EN (accessed 27 March 2019).

Rinkens, R. (2018) 'EU Interoperabilityframeworkfor border management systems' [PowerPoint presentation]. *Unit B3 – Information Systems for Borders and Security*.

Simpson, J. R. (2008). Functional MRI lie detection: too good to be true?. Journal of the American Academy of Psychiatry and the law online, 36(4), 491-498.

Smith, C., & Brooks, D. J. (2012) *Security science: The theory and practice of security*. Waltham: Butterworth-Heinemann.

US Customs and border protection (CBP) (2019) Human trafficking. Available at https://www.cbp.gov/border-security/human-trafficking

US Customs and border protection (CBP) (2019) Preclearance locations. Available at https://www.cbp.gov/border-security/ports-entry/operations/preclearance

Van Der Zee, S., Poppe, R., Havrileck, A., & Baillon, A. (2018). A personal model of trumpery: Deception detection in a real-world high-stakes setting. arXiv preprint arXiv:1811.01938.

Van Der Zee, S., Poppe, R., Taylor, P. J., & Anderson, R. (2015, January). To freeze or not to freeze: A motion-capture approach to detecting deceit. In Proceedings of the Hawaii international conference on system sciences, Kauai, HI.

Van Dijk, W. (2017) *Passenger experience: Enabling a seamless flow* [Online]. Available at: https://www.internationalairportreview.com/article/75108/seamles-pass-flow/ (accessed 27 March 2019).

Van Rest, J., Bovenkamp, E., Eendebak, P., Baan, J., & van Munster, R. (2009). Sensors and tracking crossing borders. In In Proceedings of the 4th Conference on Safety and Security Systems in Europe.

Van Rest, J., Roelofs, M. and Van Nunen, A. (2014) *Deviant behaviour - Socially accepted observation of deviant behaviour for security - extended summary*. TNO.

Van Rest, J. and Weima, I. (2017) *Sturen op risico's: een verkenning in het veiligheidsdomein bekeken vanuit het grensproces op luchthavens*. TNO.

VicarVision. (No date) *Reading Faces* [Online]. Available at: http://www.vicarvision.nl/technology/reading-faces/ (accessed 27 March 2019).

Wetenschappelijke Raad voor het Regeringsbeleid (WRR; Dutch Scientific Council for Governmental Policies) (2011). IOverheid (Vol. 86). Amsterdam University Press.

LIST OF FIGURES

LIST OF TABLES

ANNEX A GLOSSARY OF TERMS

This annex provides an alphabetical overview of terms, definitions and descriptions, including their sources *[between square brackets]*. Terminology regarding risk management (ISO 31000) is concentrated in Section 4.3.

Border – *[Schengen regulation]*

Border checks means the checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it.

Border control *[IBM Guidelines]*

An activity carried out at a border in response exclusively to an intention to cross that border or the act of crossing that border, regardless of any other consideration. It covers: (a) checks carried out at authorised border crossing points to ensure that persons, their means of transport and the objects in their possession may be authorised to enter the territory of the country or authorised to leave it; and (b) surveillance of borders between authorised border crossing points and the surveillance of border crossing points outside the fixed opening hours to prevent persons from circumventing border checks.

Border crossing point (BCP) *[IBM Guidelines]*

Any crossing point – at land, sea, river, lake or air borders – authorised by the competent authorities for crossing a state border.

Border guards / border police *[IBM Guidelines]*

Any public agency officially assigned in accordance with national law to border crossing points or along the border or the immediate vicinity of the border to perform checks and surveillance.

Bottom-up and top-down information flow *[IBM Guidelines]*

Describes the information flow within a given organisational unit starting at either the central or the operational level, as well as within hierarchical structures from operational to governmental level (bottom-up) or from governmental level to operational level (top-down).

Carrier *[IBM Guidelines]*

Any natural or legal person whose profession it is to provide passenger transport.

Check *[TRESSPASS]*

A check is a revelatory activity regarding a relevant aspect of a traveller, done by an authorised border agency in order to determine with a high degree of certainty if a traveller can be authorised to cross the border.

Database *[IBM Guidelines]*

Comprehensive collection of data organised for convenient access, generally automated for electronic analysis.

External borders *[IBM Guidelines]*

Specifically refers to the EU Member States' land borders, including river and lake borders, sea borders and airports, river, sea and lake ports, provided that they are not internal borders (of the EU).

Filter *[TRESSPASS]*

A filter is a combination of screenings, checks and flow facilitation at a BCP. A single BCP can accommodate different traveller types. To facilitate the flow of travellers, and to make sure that the proper screenings and checks are applied to travellers, a BCP consists of filters.

Flow-rate *[TRESSPASS]*

The flow-rate is the average speed of travellers when they actually cross the border at the BCP.

Base – [TRESSPASS]

The speed at which people approach a BCP is the base flow-rate. This varies between modalities and depends also on other factors such as the physical capabilities of the traveller. The base flow-rate can be much higher (in the case of a car approaching a land border) than the flow-rate at the actual border, where the traveller has to slow down in order to be screened and / or checked.

IBM strategy *[IBM Guidelines]*

A catalogue of the governmental and operational objectives a country wants to achieve in order to establish a more comprehensive, effective and efficient system of border management.

Personal data *[IBM Guidelines]*

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Processing of personal data *[IBM Guidelines]*

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, blocking, erasure or destruction.

Profiling *[TRESSPASS]*

Profiling is considered as an extrapolation of a certain characteristic of a person, a group or a situation based on other information of the respective subject (Van Rest, J.H.C., Roelofs, M., Van Nunen, A., and Don, S.B., 2014). Profiling can be used to draw attention to suspicious patterns (or the absence of normal patterns). As such profiling is a very powerful tool. However, profiling neither measures nor observes. It is merely a method using statistically founded assumptions. A hit or no-hit can be the reason for additional observation or inspection, but should never be used as evidence or to give weight to other evidence. When used incorrectly, profiling can lead to exclusion, discrimination, a fake sense of security and inefficiency.

Schengen agreement *[IBM Guidelines]*

The signatory states to the Schengen agreement have abolished all internal borders in lieu of a single external border, where border control for the Schengen area is carried out in accordance with harmonised legislation and identical procedures. Schengen cooperation was incorporated into the EU legal framework by the Treaty of Amsterdam of 1997.

Schengen area *[IBM Guidelines]*

Represents a territory where the free movement of persons is guaranteed in accordance with the Schengen Agreement of 1985. The Schengen area has gradually expanded to include nearly every EU Member State and also includes non-EU Member States (e.g. Iceland, Norway and Switzerland.

Screening *[TRESSPASS]*

A screening is a revelatory activity regarding a relevant aspect of a traveller, done by an authorised border agency in order to determine with a limited degree of certainty if a traveller can be authorised to cross the border. Under RBBM, the outcome of a screening can lead to a different type of check, or even no check which would make the screening the basis for an authorization.

Third country *[EU terminology]*

Non-EU Member State.

Visa Information System (VIS) *[IBM Guidelines]*

Consists of a central information system, of an interface in each Member State, and of a communication infrastructure between the central system and the national interfaces. The main purposes of the VIS are to improve the implementation of the common visa policy, and to strengthen consular cooperation and consultation between the central visa authorities of the EU Member States.

ANNEX B REPRESENTATIONS OF THE CONCEPT OF THREAT

The concept of threat changes as it progresses through the ISO 31000 threat management process (see Section 4.5.2). Changes propagate and accumulate in every step of its life cycle. This is illustrated in the table below based on a fictive example of an infectious disease. This fictive example is based on a classic risk-based BCP filter: a flow of travellers which passes through a screening and a check at a BCP.

Threat description type	Example
The actual **generic threat**	2,1% of all travellers are infected with the B4N8 virus. This virus infects the blood and visual cortex, and makes patients roll their eyes. Children that have not reached puberty are immune.
The **intelligence report of a threat**	1%-5% of the travellers is infected with the B4N8 virus that makes them roll their eyes. Babies and toddlers are immune.
The **design of the basis threat (DBT)**	Travellers who are infected with the B4N8 virus, which make them roll their eyes; note: babies are immune.
The **threat indicators to be used in a screening**	People that have problems looking straight ahead and for which their passport states they are older than 2 years must be considered to be possibly infected.
The **threat assessment that is made of a concrete passenger (group) (or red team) as part of a screening**	Everyone older than 2 years old that does not look the border guard straight in the eyes when spoken to, is selected for additional checks.
The **threat posed by a specific passenger as part of his travel group**.	A member of a cultural minority is crossing the border. He is not a carrier of the B4N8 virus. But in his culture it is inappropriate to look people in the eyes, so he does not at the border neither. As a consequence, he will be selected for further checks every time.
The threat indicators to be used in a check	The count of infected cells in the bloodstream.
The threat assessment that is made of a certain group as part of a check	A medical professional takes a blood sample from a traveller and uses a specialised device to count the infected cells. This procedure takes 10 minutes and is 99,5% reliable.
The **approximation of the threat**	A 'red team' partly consisting of children of age three and older is walking with their caps over their eyes.

Note: The example starts with a description of what is actually happening. So, the first row is not even part of the ISO 31000 process.

The risk management process first considers this threat because of an intelligence report in the second row. This report is merely an approximation of the real world facts. In a good intelligence process it is known what potential sources for biases are, and what the options are to reduce those biases, but the intelligence process is resource intensive and trade-offs have to be made.

The owner of the border in this example wants to be on the safe side. He understands that 100% safety is not possible, but he does not want to be accused of taking on too much risk. In this example he more than doubles the prior probability that a traveller is infected (from 2.1% to 5%).

BCP system designers have to make sure that the threat indicators can actually be assessed in operational scenario's, i.e. reliably, repeatedly and with the appropriate workload for the operators. In this example, they propose some shortcuts. Unfortunately, it is ignored that the passport age may deviate substantially from the biological age due to cultural, legal and other factors. In addition, "rolling with eyes" was too vague and too difficult to specify so they attempted to approximate this by stating "not looking straight ahead" which is a much broader specification.

Border guards are professionals, but they are also just human. In this example, the training was too long ago, and the specific instructions were not remembered precisely anymore. In addition, the 'behaviour detection' training to detect outgoing jihadist fighters interfered with the 'behaviour detection' training for detecting infected travellers, as both contained indicators regarding the way travellers looked at the border guard when spoken to.

The actual threat posed by a specific traveller determines the actual risk. In this example, this traveller and other of his cultural minority systematically display the indicators that the border guards are looking for, while this is not even a proper indicator of the actual threat. This BCP is biased and ineffective.

The indicators to be used in a check are much accurate, but also much more invasive. In this case, it is the count of infected cells. It is obvious that there will be significant societal pressure on the BCP to exclude travellers from this check.

The check itself takes a lot of time, and is not even 100% accurate. Even with a highly invasive check, infected travellers will be missed, and/or healthy travellers will be stopped.

The red team is hired through a tender, where cost was a big difference maker. The contractor was able to sell fieldtrips for primary school children as red team exercises to the BCP. He expects the BCP to validate whether his 'red teams' were sufficiently representative of what they needed, and never received a complaint. The BCP operator and respective border guard claim they are validated regularly and claim high success rates.

The members of the red team give their best impression of infected people. They look down all the time which creates chaotic situations when they bump into each other and into other travellers. When they are 'caught' by border guards, they get some candy and lemonade. School staff has learnt how this works, and helps to make sure that each child is 'caught' and gets his 'fair' reward.

This fictive example illustrates how the threat is modelled slightly different in every successive step of the process. The formal DBT is already an approximation of an approximation, but at least that is a description that mandated decision makers have explicitly taken responsibility for. In order to have an effective and unbiased BCP, it is essential that each successive model of the threat is compared to the DBT, and that differences are identified, accounted for and reduced as much as possible.

ANNEX C ADDRESSING END-USER REQUIREMENTS AND NEEDS

In this version of D1.2a, dissemination level Public, the former Annex C (that appeared in D1.2, dissemination level Confidential) has been omitted. It should be noted that all relevant end-user requirements that have been identified in Task 1.1 have been addressed.

ANNEX D CONNECTION OF D1.2A WITH TRESSPASS TASKS

The table in this annex provides an overview of all tasks of the TRESSPASS project and how they are linked – either as input or output – with the contents of this deliverable.

Task id	Task name	Link with D1.2a
T1.1	End-user requirements	Annex C Addressing end-user requirements and needs
T1.2	Developing a new risk-based border management concept	Chapter 4
T1.3	High level scenarios (including gap analysis)	Section 6.2 gives a starting point for the gap analysis
T1.4	Legal and regulatory framework	Section 6.2 describes some generic relations to legal and regulatory frameworks. Section 6.3.2 covers value-sensitive-design.
T2.1	Method for Design Basis Threat	Section 4.2
T2.2	Risk indicators	Section 4.5, 4.6
T2.3	Risk assessments at border crossing points	Sections 4.6, 5.3.1 and 6.2.4 describe risk assessment at BCPs.
T2.4	Design of risk-based border crossing points	Chapter 4 gives more specifics on what the design should lead to.
T2.5	Multilevel and multinational risk-based cooperation	Section 5.3 and Section 5.4
T3.1	Sensors	Section 4.6
T3.2	Data Modelling & Ingestion Server	Too technical for D1.2a, requires more elaboration from WP5 and others.
T3.3	Interfaces to Legacy Systems/External Databases	Too technical for D1.2a, requires more elaboration from WP5 and others.

Task id	Task name	Link with D1.2a
T3.4	Information Exchange capabilities	Section 5.3.3
T4.1	Data and information fusion for advanced intelligence extraction	Sections 4.5.3, 4.6 and 4.7.1
T4.2	Web intelligence	Section 4.7
T4.3	Real time behaviour analytics	Section 4.6.3
T4.4	Red teaming	Section 4.7.5
T5.1	System Architecture & Use Cases	Chapter 4, and especially the requirements listed in section 4.10
T5.2	Data Visualisation (UI Services)	Too specific for D1.2a, requires more elaboration from WP5-6 and others.
T5.3	Dynamic Risk Assessment	Section 5.3.3
T5.4	Operational and Tactical Decision Support System (C2 services)	Sections 5.3.3 and 6.2.3
T5.5	International Alert System	Section 5.3.3
T5.6	Integration Plan of the overall system prototype	Too technical for D1.2a, requires more elaboration from WP5 and others.
T5.7	Integration of all subsystems and platforms into a risk-based border management system	Too technical for D1.2a, requires more elaboration from WP5 and others.
T5.8	Overall Prototype Technical Testing and Validation	Too technical for D1.2a, requires more elaboration from WP5 and others.
T5.9	Information Security	Too technical for D1.2a, requires more elaboration from WP5 and others.
T6.1	Operational observation studies for validating and support CONOPS definition	Section 6.3.3.1 and section 5.3.
T6.2	Consolidation of CONOPS framework and scenario definition (evolving model)	Section 6.3.3.1 and section 5.3.
T6.3	Integration of acceptability data into design criteria	Section 4.1

Task id	Task name	Link with D1.2a
		Section 6.3.2
T6.4	Identification of KPIs for the future implementation and validation of the TRESPASS solution including post-project	Section 4.1 Section 6.3
T7.1	Simulation Environment	Section 4.1 for the specification of relevant performance indicators, and sections 6.3.3.4 and 6.4 for the assessment of the quality of risk-based concepts.
T7.2	Technical component models	Too technical for D1.2a, requires more elaboration from WP5 and others.
T7.3	Fast simulation and analytical analyses	Too technical for D1.2a, requires more elaboration from WP5 and others.
T7.4	Training	Too specific for D1.2a, requires more elaboration from WP6 and others.
T7.5	Shared evaluation platform for risk-based border control systems (BCSEP)	Section 4.1 for the specification of relevant performance indicators, and sections 6.3.3.4 and 6.4 for the assessment of the quality of risk-based concepts.
T8.1	Planning and End-User Training	Chapter 4, especially the requirements listed in section 4.10 and section 6.3.3.1
T8.2	Pilot Netherlands	Section 6.3.3.1 and section 6.4.
T8.3	Pilot Poland	Section 6.3.3.1 and section 6.4.
T8.4	Pilot Greece	Section 6.3.3.1 and section 6.4.

Task id	Task name	Link with D1.2a
T8.5	Lessons Learnt	Section 6.3.3.1
T9.1	Research Ethics and accompanying ethical research	Not relevant for D1.2a
T9.2	Identification of relevant ethical, legal and societal risks	Section 6.3.2
T9.3	Framework for assessment of direct ethical, legal and societal impact	Section 6.3.2
T9.4	Ethical guidelines for decision makers	Section 6.3.2