Policy background for customs risk management: Practitioners' Guidance Document

Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements

February, 2017

This document is for general information only. It is not legally binding.

Policy background for Customs Risk Management – Practitioners' Guidance Document

Table of Contents

Practitioners Guidance Document

I. Introduction

This document presents the result of work of an expert working group set up under the Customs 2020 programme. The group consisted of the practitioners from various Member States and the Commission in the area of customs risk analysis, targeting data analytics, and experts with the knowledge of the EU customs IT architecture.

The purpose of the document is to provide additional information regarding the key customs risk management challenges arising from:

- the current EU strategic and policy framework ,
- the current and future operational needs faced by customs authorities in their daily work, and
- future opportunities from emerging technologies in the field of big data analysis.

The document provides an insight into a number of customs risk management themes which have an important data analytics dimension, for the benefit of interested parties in both the research community and the technology industry, as well as for the Member States public authorities. It explains the **needs and interests of customs operational risk management** of international goods supply chains.

While it is hoped that this document will help understanding the current environment from the customs risk management perspective, it should be emphasised that the document is for general information only.

II. Customs Risk Management of the International Supply Chains – Strategic view

THE CONTEXT

The EU customs risk management policy and strategic objectives as defined in the EU Strategy and Action Plan (adopted by the Commission under COM (2014) 527 final) were endorsed by the Council in December 2014. The Strategy covers all threats and risks connected with international goods movements. It aims to mitigate them at the most opportune time and place in the supply chain (‘*assess in advance, control where required*’), to improve operational risk analysis capacities, to improve access to and exploitation of risk and intelligence information from non-customs authorities and to improve targeting of high risks and facilitation of legitimate trade through strengthened cooperation with economic operators.

For EU customs authorities to be able to implement the strategy they need to be equipped with high performing information systems capable to capture huge volumes of data provided by economic operators with different roles in the supply chain. In addition, customs need to be equipped with sophisticated electronic systems to evaluate, analyse, identify and mitigate the entire range of risks (e.g. from explosives posing imminent threats to the transport and supply chain security, to different types of security, health and safety risks requiring control intervention at the EU external borders (e.g. smuggling of weapons, explosive precursors, narcotics, cigarettes, dangerous goods) and risks to the financial and economic interests of the EU and its Member States).

PROBLEM STATEMENT

EU customs implement risk management and controls under the common Union framework by deploying their national risk management capacities and expertise. The Strategy acknowledges the need to work further on increasing the risk analysis operational capacities at the national and EU level.

Two main challenges need to be addressed: overcoming capacity variances across the EU Member States to be able to implement common risk criteria and standards, and capability to more effectively tackle trans-national threats. Capacity variances arise due to the existence of 28 different national electronic risk analysis systems and differences in expertise across the EU Member States. More broadly, as the Strategy reflects very well, the customs authorities of the Member States need to significantly improve the capacity, tools and methods (organisation) to address transnational risks posed by cross-border crime and terrorist organisations.

The Strategy calls for the ramping up of the EU level risk analysis capacities to be able to address these challenges, and of the work commenced on developing the common trade data repositories that will provide a foundation for future common and /or shared analytics capacities for the national customs authorities.

RELATED POLICY INITIATIVES AND RESEARCH ACTIONS

Customs are legally required to provide a key contribution to the broader security context, including the implementation of the European Agenda for Security, and efforts towards delivering an effective and genuine Security Union.

The need for establishing the interaction/interoperability between the customs systems and processes managing the risks connected with flows of goods and the systems developed to protect the EU borders (control of persons) and internal EU security is strategic.

In particular, attention is needed in identifying possible solutions in the area of inter-agency information sharing in order to plug the knowledge gaps due to the silo approach taken in the past resulting in the fragmented systems.

The on-going work of the High Level Expert Group tasked to progress on delivering Stronger and Smarter Information Systems for Borders and Security (COM(2016)205, 6 April 2016) is of relevance. The final report of this high level group is due to be adopted by the end of April 2017.

A variety of relevant research actions are on-going (such as FP7 CORE, SEC-21-GM-2016-2017: Pan European Networks of practitioners and other actors in the field of security, FP6 Kermit on image and text analysis).

III. Existing and future customs IT systems and architectures and relevant on-going customs risk analysis projects

CUSTOMS IT SYSTEMS, REFERENCE DATABASES AND SUPPORTING TOOLS

EU customs information systems, and their overall ecosystem, include:

- Customs declaration systems
  - The advance cargo information system: ICS, and its on-going reform ('ICS2' with the national and common data repositories),
  - The import declaration systems with the national and common data repositories (SURVEILLANCE III)
  - Transit (NCTS) national and common data repository
  - Export (ECS) declaration systems
  - EU database of container status messages (Council Regulation 515/97)
- Customs reference databases (TARIC, EORI/EOS, ECICS, CS/RD, COL …)
- Customs risk analysis systems at the national level

- Customs supporting tools for risk analysis and targeting (e.g. AMT (Automated Monitoring Tool), Contraffic, Open Source intelligence tools)
- Future (to be developed) common and shared capacities

CUSTOMS RISK ANALYSIS PROJECTS

There are a number of issues which make research in the area of security particularly complex, for example the operational sensitivity of the issues involved and the fact that some of the results which emerge from the research cannot always be made public.

In this context, the working group under the Customs 2020 programme indicated that a number of projects in the area of risk analysis capacity increasing are under-way to analyse and explore operational risk management needs. They form a part of the implementation of the EU customs risk management strategy, such as in the area of data-mining, improving advance cargo risk analysis and targeting for security risks by linking advance cargo data and data of container movements (container status messages). Such projects are "*Limited*" for internal customs administration use only, which means that further detailed information cannot be made available. Customs administrations are nonetheless already aware of, and participate in these projects, with the support of the Commission's Joint Research Centre (JRC).

IV. Operational risk management needs

The strategic need for a better visibility of legitimate and illicit supply chains (horizontal across modes and countries and vertical through deeper understanding of the actors/parties involved) and for an enhanced knowledge of known and unknown risks goes beyond the traditional risk analysis methods used by the customs. This requires collection, integration and processing of supplementary (structured and un-structured) data from various sources (open or other governmental), new methods, state-of-art tools, etc. This is subject of course to full compliance with data protection rules and information security procedures.

Practitioners (active in the expert working group set up under the Customs 2020 programme) identified the following general needs (all valid for real-time[1] and historical data analysis, and which may fall under more than one domain):

DATA COLLECTION, ORGANISATION AND STORAGE DOMAIN

[1] Real-time can vary across different application domain and/or operational context (e.g. between less than a second to several hours)

- Linking different datasets relevant for the supply chain process using data sources, such as from logistics, financial, tax and open source (free or payable)

- Developing standardized methods (protocols) and architectures (distributed and/or centralised) for storage, organisation, cleaning, anonymization, encryption and exploitation of large volumes of data collected through the shipment life cycle, from more than one Member State. Particular attention would be given to the protection of sensitive data (e.g. personal, law enforcement)

- Identifying the relevant open sources (free or payable) and developing solutions to extract and integrate information in customs operational risk analysis. Information extracted from dark web is also relevant in this context.

ANALYTICAL DOMAIN

- Cargo supply chain data often contain information in free text fields. Methods that address text mining in order to help overcome multi-language issues (translation, transliteration, entity matching using data created or stored in different alphabets).

- New text mining tools to contribute to the real-time processes which distinguish natural from legal persons

- Improving the effectiveness of detection and selection of risk shipments via automated processes and evaluation through learning from past events and control results (positive and negative) by identifying networks/connections from different data sources, identifying, anomalies (e.g. identity hijacking, rip-off, misclassification, undervaluation). This can be achieved by deploying or – where necessary – advancing the statistical, mathematical models used in customs and other application domains. Special emphasis should be given to a strict control of false signals.

- Predicting and quantifying (new) risks in terms of potential (financial) losses and/or damages.

- Analysis and exploitation of images and/or sensor signals (e.g. vehicle pictures, x ray images, radiation signals, positioning signals, image recognition on container scan images) for automatic verification of consistency against information stored in the national systems (e.g. national vehicle registration databases, customs declarations).

- Enhancing detection of anomalous transactions (e.g. identity hijacking, rip-offs, under-valuation, mis-classification) using historical and/or real-time data. Deploying or where necessary advancing the statistical, mathematical models used in customs and other application domains. Special emphasis: a strict control of false signals.

- Automated capacity to extract information from electronic documents (e.g. structured, unstructured) to facilitate customs documentary risk based controls by cross-checking and validating the customs declaration data and/or identifying possibly falsified documents.

OPERATIONAL TOOLS AND WORKING METHODS DOMAIN

- Enhanced flexible tools and organisation to implement new operational methods and knowledge into the process of risk management such as development, testing, configuring of algorithms and evaluating their outcomes

- New approach(es) for systematic collaboration with other authorities (e.g. border, law enforcement, security/ intelligence) to support operational risk analysis (e.g. integration of actionable data from other authorities into the risk analysis processes of customs (e.g. interfaces with the information systems such as SIS II), bringing the operational knowledge from multidisciplinary expertise into data analysis)

- Develop a solution to support verification of proper declaration of shipments by cross-checking advance cargo information against other information sources (e.g. vessel stowage plan, (air)port inventory systems)

Work in relation to all the above mentioned needs must of course take account of the necessary data security, integrity, and reliability and confidentiality requirements.

For effectiveness, any strategic customs risk management theme should be addressed in an integrated way, bringing together innovative solutions and practices across more than one of the domains above where relevant and appropriate.

V. Additional Information on customs risk management interests

MAPPING OF THE RELEVANT INFORMATION SOURCES AND DATA SETS

WCO and EU provides (customs) data models and data definitions.

Mapping of all relevant data sources, identification and organisation of relevant data sets from these sources, and a comprehensive description of metadata, would help in addressing the needs listed in the previous chapter.

POSSIBLE IT ARCHITECTURE(S)

In general terms, the expert working group under the Customs 2020 programme considered that the validation of a proof of concept by the customs services in their operational context represents a necessary condition for any future IT architectural solution(s) to be eventually considered for implementation (at EU level).

The group also considered that for acceptance and wide development future solution(s) would benefit from:

- Detailed references describing how the non-functional needs, such as data security, integrity, reliability and confidentiality requirements;
- A realistic vision for the governance of data access by different actors, flexibility, scalability, configurability, interfaces/interoperability, will have to be implementable within the customs IT ecosystems and their requirements;
- Deployment plan for production and operation environment.

VALIDATING VIABILITY OF SOLUTIONS

For sound assessment and conclusions, test scenarios should be based on use cases covering a representative range of risks as faced by customs (e.g., drugs smuggling, cigarette smuggling, smuggling of/illicit trade in weapons and explosives, dual-use goods, abuse of licit trade to support terrorism financing, money laundering, counterfeit goods, goods posing risks of people's health and safety, financial risks) and other relevant law enforcement authorities, also taking into account technical feasibility and recommendations from the research community (e.g. lack of appropriate data).

OTHER FACTORS:

The expert working group under the Customs 2020 programme indicated a number of other factors as important for future initiatives in this area, namely:

- commitment from the top management of the participating public administration,
- provision/supply of relevant data (such as national customs data from more than one Member State), and

- provision of the operational expertise (practitioners of the risk management, targeting, data analysts, investigations, and IT expertise).

The nature of the challenge is such that, in addition to customs, other authorities, representing the geographical, transport and trade specifics across the EU supply chains concerned, could meaningfully contribute.