Customs Perspectives on Detection of Deliberate Regulatory Violations in Global Supply Chains - the Role of Information and Data in Risk Identification

Discussion Paper presented at:

UNECE-OSCE Roundtable on Inland Transport Security, Vienna, Austria, 13.12.2011

Hintsa J., Männistö T., Urciuoli L., Ahokas J.

Cross-border Research Association, Lausanne, Switzerland

Agenda

- Setting the scene: ”risk-based”
- Paper intends to create common grounds for productive discussions between public and private sectors
- Recommendations

”Risk” – what?

Risk management

Risk assessment

Targeting

Risk rules

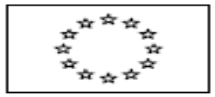
Profiling

High risk indicators

… Identification!

EU Internal Security Strategy and Common risk management framework

Common risk management framework, CRMF, has its basis laid out in the Internal Security Strategy, ISS, of the European



EUROPEAN COMMISSION

Brussels, 22.11.2010
COM(2010) 673 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The EU Internal Security Strategy in Action: Five steps towards a more secure Europe

As part of Objective 4 of the ISS document - Strengthen security through border management – CRMF basics are explained in Action 3: Common risk management for movement of goods across external borders.

EU Internal Security Strategy and Common risk management framework (cont.)

- Significant legal and structural developments have taken place in recent years to improve the security and safety of international supply chains and movement of goods crossing the EU border. **The Common Risk Management Framework (CRMF), implemented by customs authorities, entails continuous screening of electronic pre-arrival (and pre-departure) trade data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately**. The CRMF also provides for application of more intensive controls targeting identified priority areas, including trade policy and financial risks. It also requires systematic exchange of risk information at EU level.
- A challenge in the coming years is to **ensure uniform, high-quality performance of risk management, associated risk analysis, and risk-based controls in all Member States**. In addition to the annual report on the smuggling of illicit goods referred to above, the Commission will develop EU level customs assessments to address common risks. Pooling information at EU-level should be used to reinforce border security. In order to strengthen customs security to the required level at external borders, the Commission will work in 2011 on options to improve EU level capabilities for risk analysis and targeting and come forward with proposals as appropriate.

Business – government communication: pretty much one-way street today?

Here you are, Mr. Government agency!
-My facilities
-My IT systems
-My pre-departure data
-My declaration
-My end-of month accounts etc.

Now, can I get anything back from you?

Thanks Ms. Supply chain operator.

Sure, you get many things back from me, including:
-Do-not-load –messages
-Flagging for physical inspections
-Phone calls about missing or unclear information and data
- Audit visits etc.

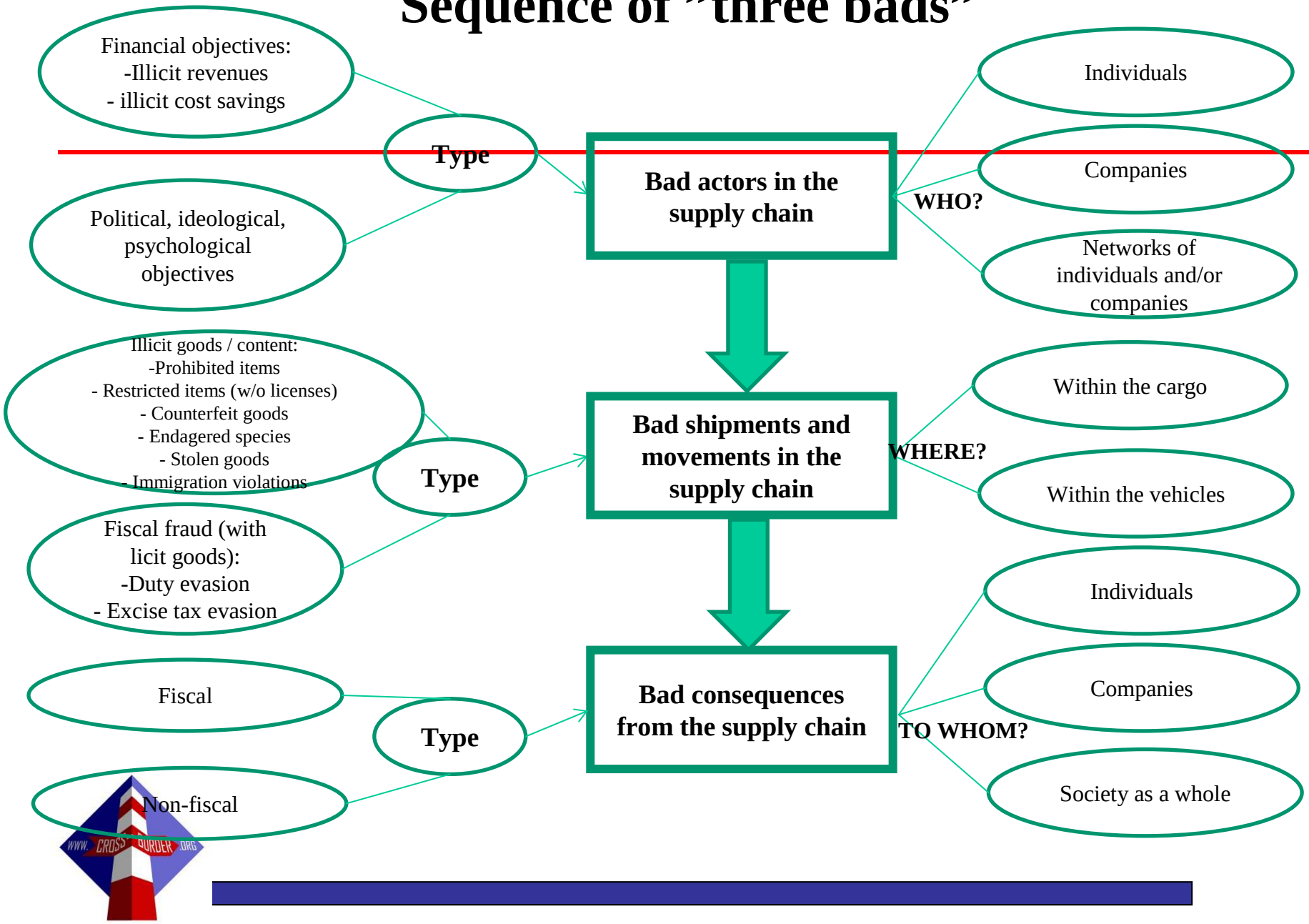
More information: email cbra@cross-border.org ; tel. +41-22-548

Discussion paper:

Customs Perspectives on Detection of **Deliberate Regulatory Violations** in Global Supply Chains - the Role of Information and Data in Risk Identification

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Sequence of ”three bads”



More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Taxonomy on customs related illicit activites – four main categories

- The first category includes events where bad actors smuggle restricted and prohibited goods across borders in order to circumvent prohibitions, license requirements, quotas, and anti-dumping restrictions.
- The second category concerns shipping of cargo to forbidden destinations. In this category, the bad actors violate regulations regarding embargoed countries, organizations and individuals.
- The third category encompasses actions where the bad actors evade duties and taxes, which collection is the customs' responsibility. Tax and duty fraud can be either partial or complete.
- The fourth category of customs related illicit activities relates to false reimbursement claims for refundable VAT, export subsidies, and drawbacks .
- *The two latter categories, the duty fraud and the false reimbursement claims, are purely profit-driven illicit activities. In comparison, the smuggling of prohibited and restricted goods and the shipping of cargo to forbidden destinations can be motivated by fiscal benefits and sometimes by political and ideological reasons.*

Taxonomy on customs related illicit activites – nine criminal (sub)MOs

1. Complete avoidance of customs controls
2. Undervaluation
3. Overvaluation
4. Under-declaration of quantity
5. Misrepresentation of tariff code
6. Misuse of authorizing documentation
7. False declaration of country of origin
8. False declaration of country of destination
9. False declaration of consignee

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Type of customs realted illicit activity		Smuggling of restricted and prohibited goods				Shipping cargo to forbidden destination		Tax and duty fraud		False reimbursement claims
Modus operandi \ Evasion of		Absolute prohibiti	Licensing equirements	Quota	Anti-dumping policies	Country mbargo	Denied & restricted party controls	Taxes & duties completely	Taxes & duties partially	-
1	Complete avoidance of customs controls		x	x	x		x	x		
2	Undervaluation									
3	Overvaluation				x					x
4				x			x		x	
5			x	x	x	x	x	x	x	x
6	Misuse izing docun tion	x	x	x	x	x	x	x	x	
7	False declaration of country of origin		●	●	●	●		●	●	
8	False declaration of country of destination		x			x				
9	False declaration of consignee		x			x	x			

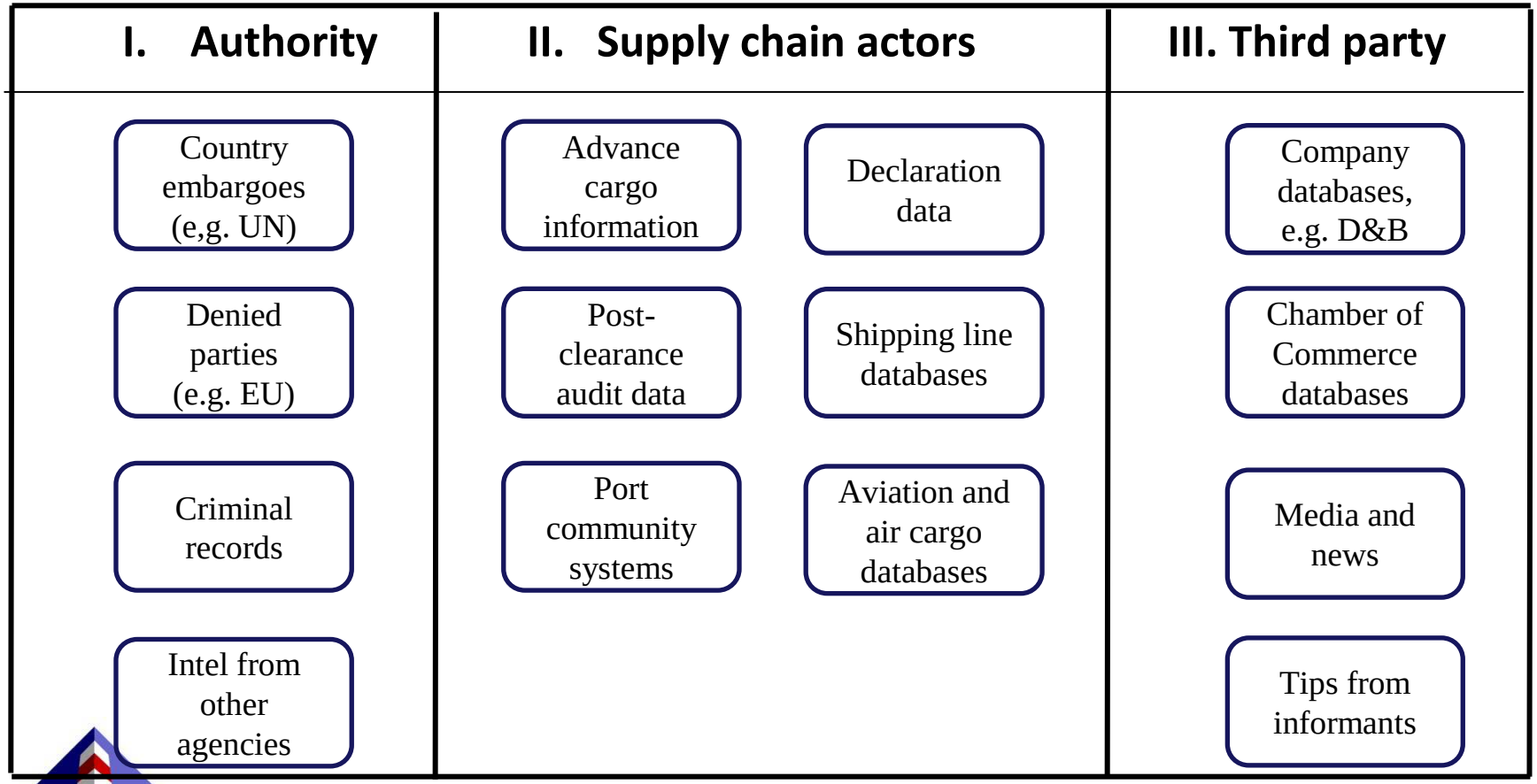
Smuggling of restricted and prohibited goods

Shipping cargo to forbidden destinations

Tax and duty fraud

7. False declaration of country of origin

Information sources to identify bad actors and bad shipments



Flexibilities in ”data timing” and ”data filing”

	A) Operator files automatically	B) Operator files per customs request	C) Customs accesses operator systems	D) Combinations of A), B) and C)
1. ”In advance”				
2. ”Real-time”				
3. ”Afterwards”				
4. ”Continuous”				
5. Random				
6. Combinations of 1/2/3/4/5				

Examples of data elements which may be used for risk identification purposes (CASSANDRA project - ICS/ECS + SAD)

- Consignor
- Consignee
- EORI number
- Country of consignment
- Country (ies) of transit (routing)
- Country of destination
- HS code
- Notify party
- Container owner
- Transport charges
- Method of payment
- Licence
- Country of Origin
- Procedure code
- Duty override code

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Illustration of ”high risk indicators”

Supply chain actor / stage	Illustration on what might be considered as “high risk indicators”
Shipper	
Commodity	
Country of origin	
Carrier	
Container	
Routing and transshipments	
Importer	

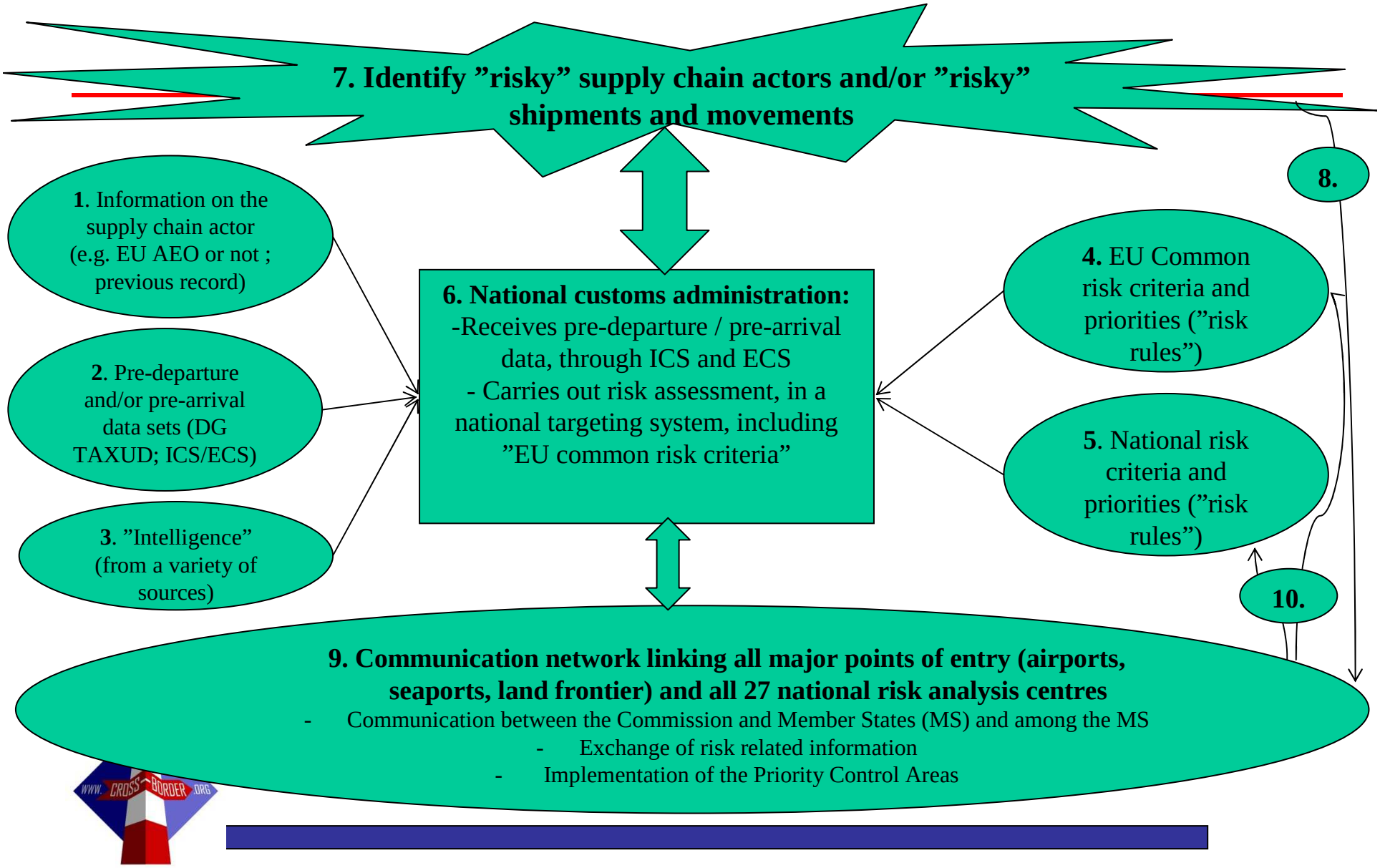
More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Illustration of ”high risk indicators” (cont.)

Supply chain actor / stage	Illustration on what might be considered as “high risk indicators”
Shipper	- Shipper has not exported the specific commodity before - Shipper information cannot be found from commercial registers or from the Internet
Commodity	- Hazardous materials which may be used for terrorist acts: e.g. Sulphur Dioxide and Iridium 192 - Common materials which may be used for concealment purposes: e.g. sugar and auto parts
Country of origin	- High level of corruption in the country - Non-existing (or low) level of export controls: e.g. pre-cursor chemicals, narcotics, and dual use goods.
Carrier	- Specific crew associated with organized crime - Carrier history of frequent violations of customs enforced regulations
Container	- Goods description does not match with the container type or with the total weight of the container. - Discrepancies in seal numbers (documents versus actual seal)
Routing and transshipments	- Routing of shipment is not cost effective - Transshipment cost paid with cash
Importer	- The frequency of imports does not support a “sustainable business”. - A suspect employee is working for the importer.

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

EU Common Risk Management Framework



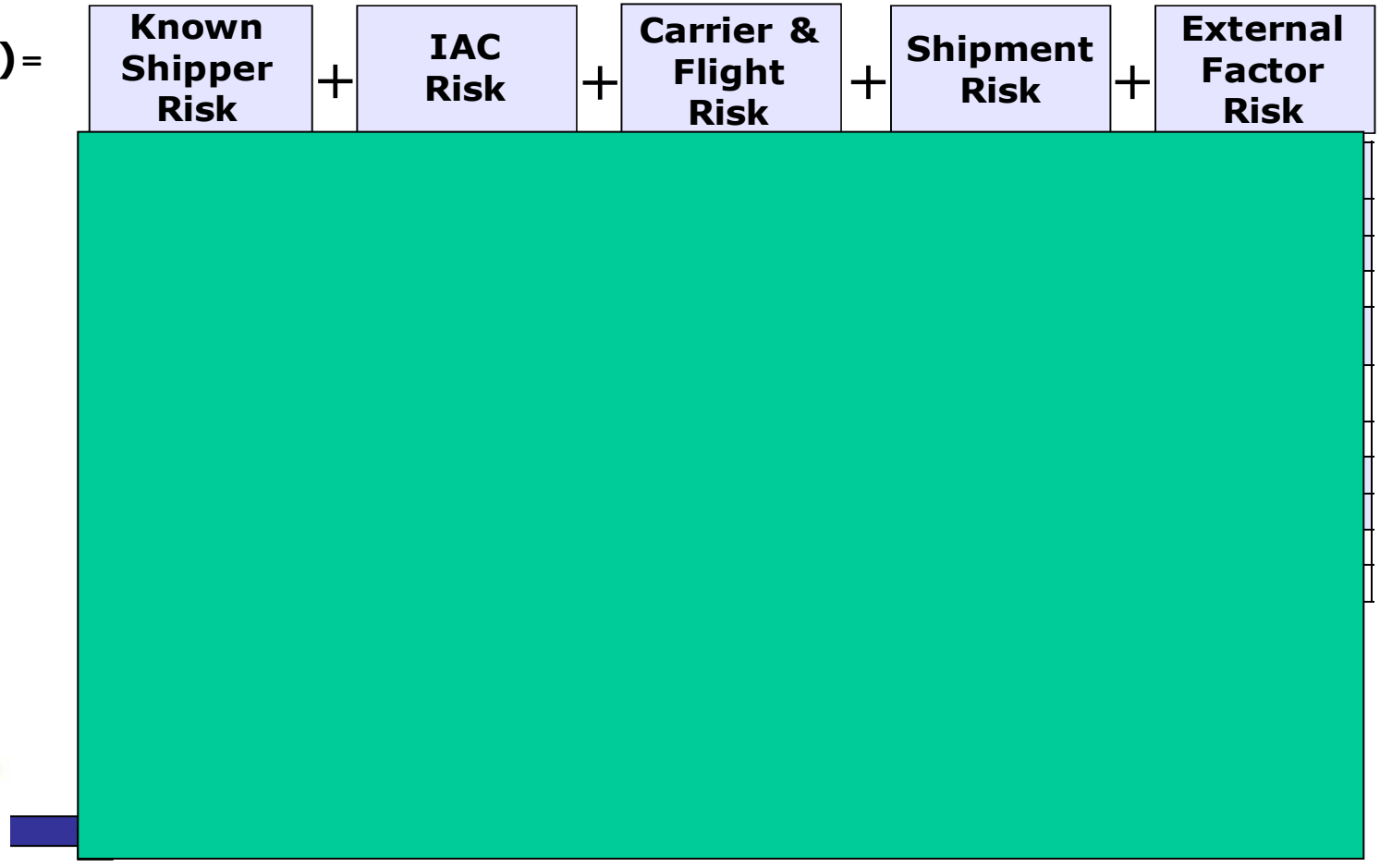
More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Illustration of US TSA "risk scoring"

ƒ(current) = Random Inspection + IAC + Shipper

(Not currently based upon risk assessment) (Approved: Y/N) (Known: Y/N)

ƒ(pilot) =



IAC = Indirect Air Carrier

Illustration of US TSA "risk scoring" (cont.)

ƒ(current) = Random Inspection + IAC + Shipper

(Not currently based upon risk assessment) (Approved: Y/N) (Known: Y/N)

ƒ(pilot) =

Known Shipper Risk	**IAC Risk**	**Carrier & Flight Risk**	**Shipment Risk**	**External Factor Risk**
Contact Name	Contact Name	**Inspection Results/ Vulnerabilities**	**Dimensions (LxWxH)**	**Current Threat Conditions**
Company Name	**Company Name**	Flight Route	**Weight**	**Watch List**
Address	**Address**	Cargo – Passenger Relationship	**Origination**	**Country of Origin**
Employee Names	Employee Names	**Carrier Name**	**Destination**	Region of Origin
3rd Party History	3rd Party History	**Carrier Address**	Insurance	**Country of Destination**
Typical Cargo Classification	Typical Cargo Classification	System Transaction History	**Receiver Name**	System Transaction History
KS and D&B Scores	**IAC and D&B* Scores**	Carrier Profile	**Receiver Address**	Region of Destination
Inspection Results/ Vulnerabilities	**Inspection Results/ Vulnerabilities**	D&B Score	**Shipper Name**	**Airport of Departure**
System Transaction History	System Transaction History	Aircraft Type	**Shipper Address**	**Airport of Destination**
Shipper Profile	IAC Profile		**Value**	Flight Date
			Content Verification (through inspection)	Flight Time
			Multi-mode Travel Route	
			Number of Handlers	
			Classification Codes	
			Date	
			Hazmat Data	
			Trucking Company and Driver Data	
			Piece Count	

Data used in Pilot Risk Model

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

IAC = Indirect Air Carrier

Revisiting EU ISS, Objective 4

Action 4: Improve interagency cooperation at national level

Member States should by the end of 2011 start developing **common risk analyses**. This should involve all relevant authorities with a security role, including police, border guards and customs authorities who identify hot spots and multiple and cross-cutting threats at external borders, for example repeated smuggling of people and drugs from the same region at the same border crossing points. These analyses should complement the yearly report by the Commission on cross-border crimes with joint contributions from Frontex and Europol. By the end of 2010 the Commission will finalise a study to identify best practices on cooperation between border guards and customs administrations working at EU external borders and consider the best way to disseminate them. In 2012, the Commission will make suggestions on how to **improve coordination of border checks** carried out by different national authorities (police, border guards, and customs). Further to that, by 2014 the Commission will develop, together with Frontex, Europol and the European Asylum Support Office, minimum standards and best practices for interagency cooperation. These shall particularly be applied to joint risk analysis, joint investigations, joint operations and exchanging intelligence.

Recommendations

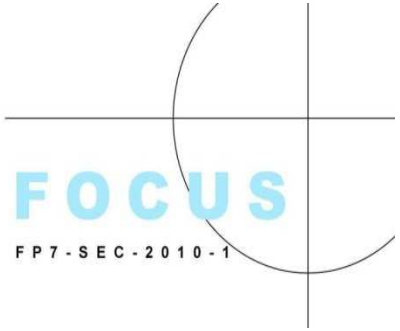
1. Specify which additional ”risk related information and data sharing” would have tangible benefits:
   - Public to private, e.g. organized crime threats and MOs
   - Private to public, e.g. internal risk management practices and outcomes

2. Analyze the costs and risks of enhanced ”risk related information sharing” between public and private, including:
   - Risk that enhanced sharing leads into educating the bad guys (government concern)
   - Risk that enhanced sharing reveals some ”additional issues” (business concern)
3. Based on the outcomes of step 1 and 2 above, take tangible next steps towards enhanced ”public-private risk related information and data sharing ” in the supply chain.
4. Look at also possibilities to improve ”multi-agency common risk analyses”, as explained in EU ISS

More information: email cbra@cross-border.org ; tel. +41-22-548 1956

Related on-going research – please pick a brochure!

- FP7-FOCUS



- FP7-CASSANDRA

- CBRA 30 Customs Case Studies

More information: email cbra@cross-border.org ; tel. +41-22-548 1956