Journal of Risk Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rjrr20

A new perspective for the integration of intelligence and risk management in a customs and border control context

Marja Ylönen & Terje Aven

To cite this article: Marja Ylönen & Terje Aven (2023) A new perspective for the integration of intelligence and risk management in a customs and border control context, Journal of Risk Research, 26:4, 433-449, DOI: 10.1080/13669877.2023.2176912

To link to this article: https://doi.org/10.1080/13669877.2023.2176912

Published online: 13 Feb 2023.

JOURNAL OF RISK RESEARCH
2023, VOL. 26, NO. 4, 433–449
https://doi.org/10.1080/13669877.2023.2176912

Routledge
Taylor & Francis Group

A new perspective for the integration of intelligence and risk management in a customs and border control context

Marja Ylönen and Terje Aven

University of Stavanger, Stavanger, Norway

ABSTRACT

This paper concerns intelligence and risk management in a customs and border control context. Intelligence here refers to the collection, sharing, processing, analysis and dissemination of information on threats, related to cross-border movements of goods, travellers, illegal activities, and serious organized crime. The main aim of the paper is to present a new perspective for the integration of intelligence and risk management for this context. The perspective, which builds on contemporary risk and safety science knowledge, as well as studies on intelligence, organizations, management, and social mechanisms, provides concepts, principles, and a unified framework for this integration. The paper gives customs and border control management new insights and instruments on how to organize and handle risk and intelligence issues and studies.

ARTICLE HISTORY
Received 16 June 2022
Accepted 22 January 2023

KEYWORDS
Risk management; intelligence; integrated framework; customs and border control

1. Introduction

Customs and border control are currently undergoing considerable changes due to geopolitical developments, the increasing flow of goods and the development of new technologies, such as digitalization and artificial intelligence (AI) tools. These changes give rise to both new risk sources, for example in the form of cybercrimes, and new possibilities for more efficient intelligence and risk analysis, particularly in relation to the identification and detection of risk sources. Intelligence has been described by the World Customs Organization's (WCO) Customs Co-operational Council (WCO 1992) as a crucial weapon in terms of fighting against illegal activities, such as commercial fraud or drug smuggling.

Intelligence is an ambiguous concept with various connotations (Marrin 2012; Omand 2020; Lohse 2020; Lowenthal 2020; Scott and Jackson 2004, Buckley 2014). In this paper, it refers to the collection, sharing, processing, analysis and dissemination of information about threats, related to cross-border movements of goods, illegal activities, and serious organized crime. The intelligence supports related decision-making at different levels and in different forms, including strategical, tactical, and operational decisions. Our focus is on intelligence in relation to activities that are relevant to customs and border control, to fulfil their responsibilities, such as gathering information about illegal activities, including organized crimes, the smuggling of narcotics and safety and security threats regarding cross-border movements of goods.

As intelligence is related to data and information about threats, there is an obvious link between intelligence and risk. Intelligence work concerns statements and beliefs about 'an

CONTACT Marja Ylönen marja.k.ylonen@uis.no University of Stavanger, Stavanger, Norway

uncertain future, based on an incomplete image of the present, with the aim of directing future police and crime prevention action' (Ratcliffe 2010). As such, intelligence can be viewed as a risk assessment aiming at identifying and understanding the threats, what can happen, and reflecting the uncertainties. However, intelligence analysis books commonly do not refer to the risk concept or provide a thorough discussion of risk assessment & management (e.g. Clark 2020; Buckley 2014; Fischhoff and Chauvin 2011). In many respects, intelligence and risk assessment & management are two schools or fields with different traditions and focuses, on education, science and practice. The WCO has developed guidelines for 'intelligence-led Risk Management', but large parts of the document with recommended methods are not publicly available and hence cannot be used as a source for scientific discussions. However, the WCO has addressed the topic on their website, and volume 1 of the document referred to on risk management is available (WCO 2021a, 2021b). Work by WCO as well as articles in the World Customs Journal (e.g. Widdowson 2020, Komarov 2016) indicate that there is an increased focus on risk management systems for the improvement of customs and border control performance. However, the degree to which such systems have been developed within customs and border control agencies, varies considerably. Buckley (2014, p. 339) points to an underlying explanation factor for this, that many people working in law enforcement agencies, such as in customs, have poor understanding of risk management. He also points to the fact that there is a lack of understanding of intelligence, and often inadequate management of intelligence, in the agencies.

The customs and border control field is characterized by rather inconsistent terminology, in relation to terms such as risk, threat assessment, risk assessment and risk analysis (Buckley 2014). Different types of risk definitions are referred to, as in nearly all types of applications of risk science. Most commonly, we see definitions based on probability, as in Widdowson and Holloway (2011), Laporte (2011) and Komarov (2016): risk is the chance of something happening that will have an impact on organizational objectives, and risk is the probability of infractions. Definitions commonly seen in security contexts are also referred to, covering threats, vulnerabilities and consequences. Many customs organizations follow standardized risk assessment procedures (WCO 2021b), and it is common to refer to the ISO 31000 (ISO 2018), with its guidance on risk assessment and management principles and its definition of risk, which states that risk is the effect of uncertainties on objectives (Buckley 2014; WCO 2021a).

Paté-Cornell (2015) highlights the role of intelligence as a tool supporting risk management, particularly in relation to warning mechanisms and systems. As for risk assessments of events that are developing (emerging risk assessments), the intelligence provides warnings about potential threats, despite large uncertainties (Paté-Cornell 2015; Byman 2016). As stated by Paté-Cornell (2015), the intelligence supports risk management by providing information that can be used to construct adequate warning systems, which constitute a crucial part of risk management strategies. Typically, the intelligence focuses on the possible occurrence of an extreme event, which is commonly referred to in the literature as a 'low probability–high consequence' type of event. However, in the customs and border control context, high-probability events are also studied, such as the smuggling of drugs across borders. Unique tools are developed for intelligence, but there are also examples of the use of some well-established risk assessment methods, such as Bayesian analysis (Paté-Cornell 2002; Clark 2020). The intelligence and the risk assessment provide decision support, preventing and/or mitigating the risks. In line with this, the WCO refers to intelligence-enhanced risk management, which suggests that intelligence contributes to better risk management (WCO 2021a, 2021b).

The present paper aims to contribute to the further integration of the fields of intelligence and risk assessment & management by presenting a new, integrated perspective, covering a set of suitable concepts and principles and a unified framework. The perspective is built on what we refer to as contemporary risk and safety science knowledge, as summarized by documents produced by the Society for Risk Analysis (SRA 2015, 2017) and related scientific works. Risk science has discussed how to conceptualize, describe and communicate risk for several

decades, and the knowledge generated by the research and developments made is also applicable to the customs and border control area. We also add insights by building on studies on organizations, management and social mechanisms (Schein 2010; Scott 2014; Jørgensen, Remmen, and Mellado 2006; Stacey 2012; Hedström and Swedberg 1998). The setting for the work is customs and border control, but many aspects of the perspective presented are general and also applicable to other domains.

The paper is organized as follows. Section 2 presents the aforementioned perspective – with its concepts, principles and framework – and its rationale. The section provides guidance on how customs-related risk can be conceptualized and described, following the SRA ideas and terminology. The perspective is applied in Section 3 and discussed in Section 4. Finally, Section 5 provides some conclusions and ideas for further research.

The present work can be seen as a contribution to applied risk and intelligence science, where the aim is to improve current knowledge on understanding, assessing, characterizing, communicating and handling risk in the customs and border control context – with respect to concepts, principles, approaches and methods. The paper is mainly a conceptual work as discussed in Aven (2018), addressing concepts, principles, approaches, methods and models for understanding, assessing, communicating and handling risk. This type of research is founded on elements such as: identification (for example, identifying what are the key challenges), revision (for example, changing or modifying a perspective by using alternative ideas and methods), delineation (for example, to focus the study on some aspects or dimensions and leave others out), summarization (for example, to underline the key points of a theory), differentiation (for example, to distinguish between alternative approaches and methods), integration (for example, to build the study on an integrated perspective on risk and intelligence), by advocating (for example, to argue for a given perspective or statement), and refuting (for example, to rebut a given perspective or statement) (MacInnis 2011). The research is based on different types of reasoning, such as comparative, integrative and divergent thinking.

The SRA documents (2015,2017) and related research provide the reference when referring to risk science and risk science knowledge. The subjective element in concluding what this knowledge covers is recognized. However, building on the extensive work by the SRA, the foundation for the analysis is considered broad and strong. It is hoped that the conclusions made, as well as the analysis and argumentation provided, will stimulate a discussion on how the risk and intelligence fields can be better integrated.

2. A Perspective and framework for integrated risk and intelligence management (IRIM)

This section presents the aforementioned perspective and framework for integrated intelligence and risk management (IRIM). We first define integration. Then, we present the overall structure and the main concepts of the framework, as well as the core IRIM principles.

2.1. The concept of integration

There are different ways to approach integration. What we mean by integration in this context refers to three different ways to link intelligence and risk management. *Structural integration* refers to the increased compatibility of systems elements, such as using the similarities of different standards or creating company-level policies that integrate intelligence and risk management. *Functional integration* refers to the integration of core functions or the coordination of generic processes, such as intelligence and risk management systems, or risk analysis and intelligence analysis. The deepest level of integration is *cultural integration*, which refers to the embeddedness of IRIM in a culture of learning and continuous improvements (Jørgensen,

Remmen, and Mellado 2006). In addition, we added a social dimension in the analytical framework, as described in the next section.

2.2. The overall structure

The framework for supporting the IRIM consists of four organizational dimensions, as shown in Figure 1: structural, functional, cultural and social. There are two layers associated with each dimension. The upper explains how that dimension supports the IRIM. The lower layer provides a more detailed explanation of the IRIM for each of these dimensions, covering i) organizational aspects and ii) core principles supporting the IRIM. In this section we explain the organizational part. The core principles we will discuss in Section 2.3. The framework is inspired by organizational theories, and in particular how internal organizational structures and cultures influence organizational performance (Fischhoff and Chauvin 2011; Pfeffer 1997; Schein 2010).

Structural aspects include management systems, roles and responsibilities, hierarchies and the ways activities are organized (Fischhoff and Chauvin 2011; Pfeffer 1997; Scott 2014). They constrain or enable actions and learning in organizations, and provide important conditions for integration, in terms of the organization's priorities, strategies, policies, management systems,

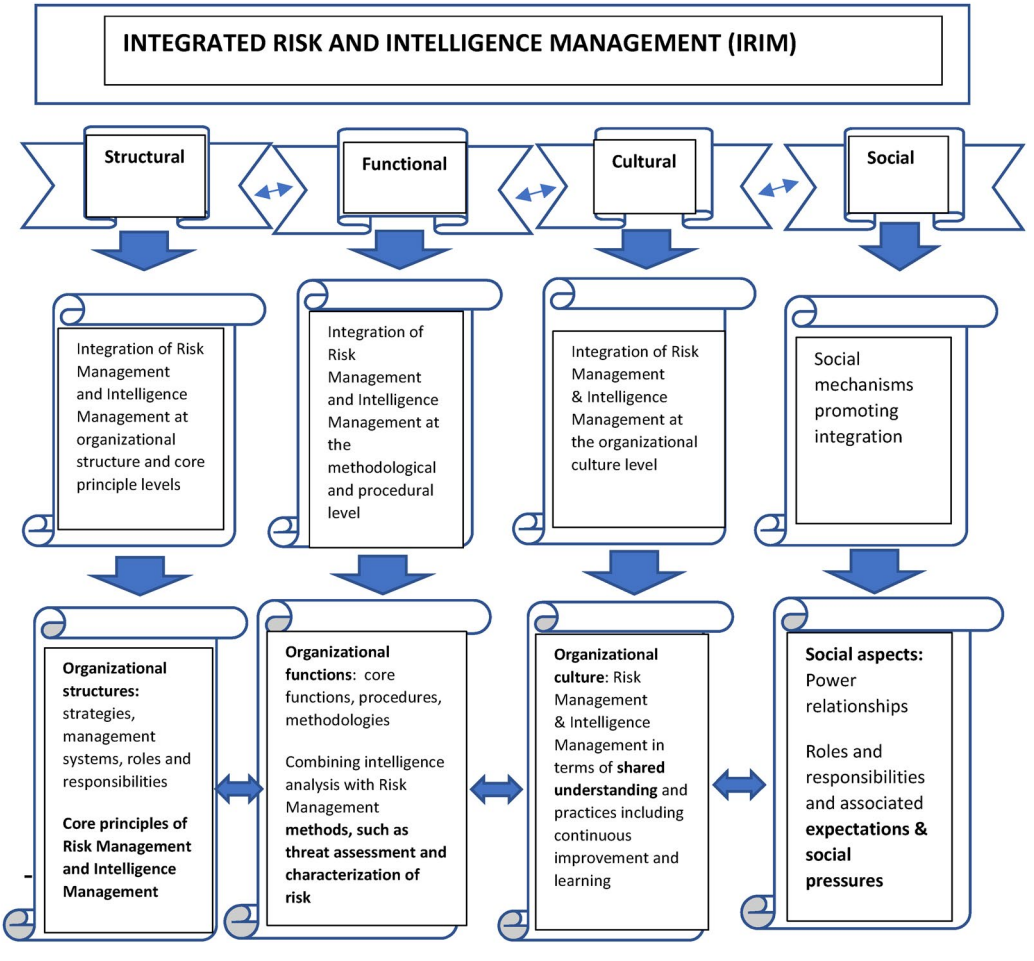

Figure 1. The framework for integrating risk management and intelligence management.

resources and competences (Jørgensen, Remmen, and Mellado 2006). The structures enable the integration, but they do not stand alone, they need to be implemented through the organization's main functions, such as border management, intelligence, risk management and related procedures, as well as methods of threat & risk assessment and intelligence analysis. The organization's functional level is the most visible dimension in organizations. It is at this procedural, methodological and practical analytical level – the most concrete level – where functional integration of risk management and intelligence management can be obtained (cf. Giddens 1986; Campbell 1998; Aven and Ylönen 2021).

Both the organizational structures and the functions are embedded in the organization's culture. It is at the level of culture, i.e. the shared values, norms, beliefs and knowledge, that the understanding of the content of intelligence and risk is clarified, and improvement and learning regarding the integrated risk and intelligence can be achieved (cf., Schein 2010; Scott 2014; cf., Petersen and Rønn 2022; Jørgensen, Remmen, and Mellado 2006). However, cultural aspects in terms of strong beliefs in existing ways of performing intelligence and risk management can also act as internal barriers regarding organizational change (Fischhoff and Chauvin 2011), such as the adoption of new management system.

In addition to the structural, functional and cultural dimensions, we address here the social dimension and the social mechanisms that are important for understanding human action – oriented towards the action of other people – in organizations (Giddens 1986; Campbell 1998; Hedström and Swedberg 1998). Social mechanisms can be seen as mediators, in terms of the integration of risk management and intelligence management. Since theories on organizational culture do not always adequately address social aspects, such as how organizational members relate to each other, power relationships, or loyalties, these often invisible social mechanisms should be examined (e.g. Antonsen 2009; Alvesson 2013; Alvesson and Spicer 2016).

The first set of social mechanisms refers to the roles and responsibilities and associated expectations and the subsequent social pressures that result from a member of the organization internalizing other members' expectations of him/her. An example is front-line custom officers who follow the norms and rules related to their roles and responsibilities. Otherwise, they would be punished either in symbolic ways (moral indignation) or concretely with a notice, or in the extreme case, they would be fired. There are formal or informal social expectations and norms (how to behave) and associated sanctions, such as praise or punishment, that act as a social mechanism to enforce action. Another example is the roles and responsibilities associated with intelligence analysts who are not supposed to deal with risk analysis, or risk analysts who are not supposed to be experts in intelligence. These types of roles, with responsibilities, may create silos, and hamper integration. Sociological and organizational studies have shown the effects of social pressure on people's behaviour (Campbell 1998; Schein 2010; Alvesson and Spicer 2016). It is through various social mechanisms that the organization exerts power over individuals.

The second set of social mechanisms relates to power relationships and hierarchies. Senior management's understanding, favourable attitude and commitment to integration would be necessary. This is because senior managers exercise power in the organization: they participate in deciding organization's priorities, strategies, policies, resources and investments and in defining the competences of people. It is through the senior managers' decisions, commitment and examples in terms of integration that the IRIM can be advanced.

Within this general framework, we can deal with various aspects of general organizational factors as necessary preconditions for the IRIM, as well as aspects of general risk management and intelligence management, as will be further described in the coming sections.

2.3. The core principles of IRIM

The literature refers to many principles for risk management and intelligence management (Aven and Thekdi 2022; Aven, Seif, and Karatzoudi 2022; Aven and Zio 2021; SRA 2017; ISO 2018;

Lowenthal 2020; Buckley 2014). These principles range from meta levels on organizational and management issues to more detailed levels addressing analysis methods. The focus of this article is on the former type of principles. For this paper, we distinguish between two sets of meta-level principles, one set regarding the integration of generic organizational and management topics, covering, e.g. organizations' structures, cultures and functions, and the other set regarding the integration of more specific risk and intelligence management topics, covering, e.g. the use of risk assessments.

2.3.1. IRIM principles covering generic organizational and management topics

Inspired by Aven, Seif, and Karatzoudi (2022), on an overall level, there is one principle that should be mentioned first:

> *The risk and intelligence management is based on current risk and intelligence science knowledge, related to concepts, principles, approaches, models and methods* (P1)

The logic is simple: we should apply the best knowledge on risk and intelligence management available, not just use guidance provided by standards which, to varying degrees, have a scientific foundation. As for all sciences, there is a debate concerning what is the best knowledge, i.e. the state of the art. The scientific literature includes different, to some extent also conflicting, concepts, principles, approaches, models and methods. The present paper is to a large extent based on work conducted by the SRA, as mentioned in the introduction section. The principle P1 expresses a clear stand, stating that science comes first, and the organization should refer to the scientific knowledge as a basis for their risk and intelligence management (Aven, Seif, and Karatzoudi 2022). The importance of this stand is that it triggers continuous striving to adopt the most updated knowledge. In practice, there will always be a need to balance this ideal against simplicity and expediency. There can be practical advantages of using standards in the daily work of an organization, as concepts, approaches, models and methods are then recognized and can be referred to worldwide. Standards are frequently updated to reflect current knowledge, but, as shown by Aven and Ylönen (2019), there can be a serious gap between the standards and contemporary scientific knowledge.

The organization and management literature points to many features of good management that also apply to risk and intelligence management (Stacey 2012; Jørgensen, Remmen, and Mellado 2006; Schein 2010; Scott 2014; Aven and Ylönen 2021). The ISO 31000 standard on risk management (ISO 2018) refers to eight risk management principles: Integrated, Structured and comprehensive, Customized, Inclusive, Dynamic, Best available information, Human and cultural factors, and Continual improvement. All of these have a rationale, but many more principles are relevant, related, e.g. to effectiveness and efficiency, knowledge management, emphasis on processes and system thinking, and ethical conduct (Aven, Seif, and Karatzoudi 2022). The ISO 'best available information' principle stresses the use of *available* information, whereas the knowledge management also highlights the need to strengthen some knowledge, that is, reliance on available information is not sufficient. The 'emphasis on processes' and 'system thinking' are also key principles of quality management and are based on the belief that the desired results are more efficiently obtained when activities and related resources are handled as processes, and there is a holistic focus addressing the total system, rather than seeking to manage separate subsystems and processes (Aven, Seif, and Karatzoudi 2022).

These are just examples of management principles that can be defined, supplementing the ISO 31000 principles. The literature on generic organizational and management topics points to many other formulations. Here are some examples from Paté-Cornell and Cox (2014):

> *Put the right people in the right place with the right knowledge, incentives, and resources; clearly define leadership and responsibilities; share knowledge and experience across organizations.*

These statements overlap with some of the eight ISO 31000 principles but extend beyond these on aspects of leadership, organizational capacity and transfer of knowledge.

Other concepts that need to be highlighted are organizational culture, and risk culture, which express shared beliefs, norms, values, practices and structures, with respect to risk, in the organization (Aven and Ylönen 2021). The culture can strongly affect the management activities; hence, building a good culture for the IRIM should be considered a principle for integrated risk and intelligence management. But what does good culture mean here? Following Aven and Ylönen (2021), one possible formulation of a principle for the present setting is: 'Build a risk and intelligence culture based on risk and intelligence sciences'. The principle P1 states that the integrated risk and intelligence management is founded on risk and intelligence sciences; the risk culture helps it to be implemented. What is highlighted in this section is the importance of developing an organizational *culture that supports IRIM*. That would mean, e.g. creating an adequate understanding of IRIM and a mindset, including openness and trust, that supports collaboration between different IRIM experts (cf. Fischhoff and Chauvin 2011). However, influencing the organizational culture is challenging and requires constant work (Bieder and Bourrier 2013; Schein 2010; Grote 2012; Haukelid 2008).

To summarize this discussion, an overall principle is suggested, formulated as (Aven, Seif, and Karatzoudi 2022):

> *The integrated risk and intelligence management is based on principles derived from contemporary management science and its practice, including those of ISO 31000 and others referred to above in this section* (P2)

The principle P2 provides a foundation for developing a suitable risk and intelligence management framework, which structures and specifies the main types of risk and intelligence management functions and activities, as well as the risk and intelligence assessment/management process, which covers activities related to the planning, execution and use of risk and intelligence assessments.

The IRIM framework will include objectives and scope for the risk and intelligence management, principles, strategies, a POLC (Planning, Organizing, Leading and Controlling) type of framework, the risk and intelligence management process, documentation, responsibilities, and activities. There are different ways of formulating the POLC concept, the idea that, for all forms of work, there is a need for proper planning of the activities; specification of the objectives to be achieved; organization of the work to use the resources efficiently; leadership by inspiring, influencing and guiding others to take part in efforts to meet the organizational objectives; and control, by checking that the performance is in line with the standards and objectives established (Aven, Seif, and Karatzoudi 2022). In quality management, the term PDCA (Plan, Do, Check, Act) is also used, based on similar ideas. ISO 31000 recommends a similar framework, based on the elements, Integration, Design, Implementation, Evaluation and Improvement, with Leadership and Commitment influencing all the other elements (ISO 2018). This ISO 31000 framework can be seen as a suggestion for how to follow up and implement the POLC framework in a risk management context. In addition, the structural, functional, cultural aspects and social mechanisms explained in Section 2.2. are key pillars of the IRIM.

The present paper does not provide recommendations on what framework to adopt, as the choice is more of an implementation issue than one concerning basic principles.

Many versions of the assessment/management process also exist. An integrated process can be formulated as follows:

a. Establishing context with objectives and requirements, frame conditions
b. The collection of data and information
c. Analysis
d. Use of the analysis

More specific principles related to risk and intelligence management are discussed in the following.

2.3.2. IRIM principles covering more specific risk and intelligence management topics

The two first principles relate to how risk is defined and described, which provides essential input to how to understand and assess risk.

> *The threat and risk conceptualization is sufficiently broad to capture all relevant threats and risks, including potential surprises* (PA 1)

> *The magnitude of the threat/risk reflects judgments about the severity of the threat/risk, likelihoods and related knowledge strengths* (PA 2)

Risk is defined and understood in many ways; see Section 2.3.2 and overviews in Aven (2012). Here, we accept the definitions adopted by the SRA (2015), which provides a broad perspective on risk, incorporating nearly all other definitions referred to in the literature and in practice:

Risk is related to an *activity*. Two examples in the customs case at different levels are i) cross-border movement of goods, passengers and transport means in a period of time and ii) a control of a specific unit (e.g. goods) at a given point in time. Related to this activity, we can define some values or goals, e.g. compliance with customs laws and regulations. Risk is conceptually understood as the potential for undesirable consequences of the activity seen in relation to these values and goals, e.g. events not in line with the customs laws and regulations. More formalized risk can be seen as the combination of the consequences C of the activity and associated uncertainty U, for short written (C, U). It is common to rewrite (C, U), without loss of generality, as (A, C, U), where A is an event (or events, hazards/threats) and C the consequences given the occurrence of A. In this case, A could represent a smuggling event and C the health effects in the country as a result of this event. Looking into the future, A and C are unknown, subject to uncertainties. The focus in a risk context is on undesirable consequences, but the conceptualization is general and allows for both positive and negative consequences. Vulnerability refers to the combination of the consequences C and associated uncertainties, given the occurrence of an event A. Hence, risk can be seen as a threat contribution (A, U) and vulnerability (C, U, |A).

A main aim of the risk assessment is to understand the activity risks to support decision-making on, e.g. the choice of alternatives or measures. To understand the risk, events A need to be identified and the consequences specified. We refer to them as A′ and C′, respectively. A and C are the actual events and consequences occurring, whereas A′ and C′ are those identified and specified in the risk assessment. There could be cases where a surprise occurs, in the sense that an event A happens which was not identified in the risk assessment, i.e. A′ does not cover A.

The uncertainties are assessed using probability, precise (stating that the probability is, e.g. 0.10) or imprecise (e.g. expressing that the probability is at least 10%). The interpretation is this: The uncertainty about the event occurring and the degree of belief in the event occurring is the same as randomly drawing a red ball out of an urn containing 10 balls, of which 1 is red (maximum 1 in the imprecise case). In addition, the strength of the knowledge (SoK) supporting the probabilities needs to be assessed, e.g. using categories like strong, medium strong and weak. The basis for the SoK judgments is assessments of factors like amount of reliable and relevant data/information, justification of assumptions made, agreement among experts, understanding of the phenomena involved, and the degree to which the knowledge has been examined (Aven and Reniers 2013; Flage et al. 2014; Askeland, Flage, and Aven 2017; Aven 2020; Aven and Thekdi 2022). The justified beliefs forming K, with its basis in data, information, analysis, assumptions, etc., supporting the probabilities and SoK judgments, should always be documented.

A customs officer could make a judgment that it is likely (at least 75%, say) that some goods are not in compliance with customs laws and regulations, but this assignment should be

supported by a SoK judgment, as the probability alone is not sufficient to express the uncertainties.

Bayesian analysis is a useful tool for the probabilistic analysis. Starting with some prior probabilities about A′ and C′, updated posterior probabilities are generated using Bayes' formula when new information becomes available.

Specific risk and intelligence assessments of the importance of assumptions are conducted (PA 3)

Specific risk and intelligence assessments to identify potential surprises are conducted (PA 4)

A main purpose of a risk assessment is to improve the understanding of risk. This understanding is to a large extent based on the risk description (A′, C′, Q, K), where Q is the measure or description of uncertainty used. The knowledge K is an important element of this risk description and includes, in particular, assumptions. The characterization (A′, C′, Q) is conditional on K. The strength of this knowledge can vary, and the knowledge can also be wrong. This creates a potential for surprises, e.g. as a result of the assessors not having knowledge about a type of event or an event being ignored, as a result of probability being judged to be low and associated knowledge considerations, given some plausible assumptions. Decision-makers need to see beyond the conditional risk given some knowledge – they also need to be informed about the quality – and particularly the strength of this knowledge – to be able to make good decisions.

The principles PA 3 and PA 4 state that the risk and intelligence assessments need to specifically address risks related to such potential surprises, particularly as a result of poor assumptions. The risk science and intelligence literature provides considerable work on how to conduct assessments. Examples include assessments highlighting assumptions (e.g. Aven 2014; Berner and Flage 2016), knowledge and black swan type of analysis (e.g. Paté-Cornell 2012; Aven 2014, Bjerga and Aven 2016) and red teaming (Masys 2012).

The data and information are evaluated with respect to trustworthiness, reliability and validity (PA 5)

The sources and information are evaluated with respect to truthfulness and reliability (PA 6)

Evaluation of the quality of the data and information is critical in the risk and intelligence assessment. For a source, we need to question the truthfulness (the degree to which the source tells the truth), as well as its reliability (the degree to which the source is trustworthy and produces consistent answers). Validity is another key concept, reflecting solidness in argumentation and logic, as well as the degree to which one is able to 'measure' what one sets out to 'measure'. For example, if an analysis is to be conducted aiming to convey a specific risk associated with an activity, and the analysts describe risk using the probability times loss interpretation of risk, risk science would consider the analysis to have a low level of validity, as it does not adequately describe or measure the risk.

There is a logic explaining the interrelationships between uncertainty, knowledge and evidence (PA 7)

The reporting and communication are clear on meaning and interpretation of key concepts, highlighting limitations and assumptions (PA 8)

The results of a risk and intelligence assessment cover aspects of (A′, C′, Q, K), particularly judgments about probabilities (precise or imprecise) P of undesirable events A′, with associated knowledge strength judgments (SoK). A and C, as well as A′ and C′, are uncertain. We do not know, e.g. if a specific person is involved in a smuggling operation. We may have some data or information (evidence) that the person could be involved, which is reflected in K and through P and SoK. This provides a logic for understanding and describing the interrelationship between unknown quantities, uncertainty, uncertainty description, probability, knowledge and evidence. See Figure 2.

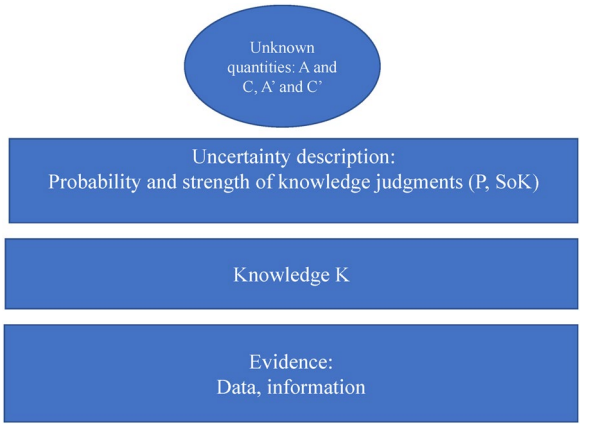

Figure 2. Key concepts and their links in risk and uncertainty assessments.

Assumptions are key elements of K and need to be reported together with P and SoK. Specific assessments should be conducted on the risks related to deviations from the assumptions, as mentioned in relation to the principles PA 3 and PA 4. All concepts in the assessments need to be defined and interpreted in the reports, to allow efficient and precise communication of insights and findings.

> *'Management review and judgements' are needed for making appropriate risk and intelligence management decisions* (PA 9)

This principle acknowledges the importance of 'management review and judgements' (MRJ) in risk and intelligence management (Hertz and Thomas 1983; Aven 2020). The basic idea is that there is a gap between the risk and intelligence assessments and the decision-making. An assessment does not specify or prescribe what decision to make, as it always has limitations and there are concerns that are not fully reflected by the assessment which could be important for the decision-making. The concept of risk-informed decision-making is in line with this idea (Apostolakis 2004).

3. Case

This section presents a case, with a focus on the smuggling of weapons, to illustrate the framework and the principles of Section 2 for an integrated risk and intelligence management and analysis (IRIM). The case follows the structure of the intelligence cycle, with an additional stage covering the organization's priorities, follow-up and decision-making. Many frameworks, approaches and methods exist for describing and conducting intelligence and related activities (see e.g. Fischhoff and Chauvin 2011; Clark 2020; Lowenthal 2020; Buckley 2014). One example is the intelligence cycle, which is presented in most textbooks on intelligence. The cycle typically covers the following four steps: i) identifying requirements, i.e. defining the questions which intelligence should answer; ii) the collection of data and information; iii) processing, exploitation, and analysis of data and information; and iv) the dissemination of results (Buckley 2014; Ratcliffe 2016). The intelligence cycle – with a linear application – has been criticized for not describing how intelligence processes work in practice and how they should work, yet it is commonly referred to (Buckley 2014; Clark 2020). When allowing for some flexibility in the way the stages are conducted, the cycle is considered to provide a useful model for describing and understanding key features of the intelligence processes.

In the customs and border control context, the requirements in i) should be based on agency priorities, e.g. focus on cross-border smuggling of narcotics or weapons. In relation to step ii), it is essential to clarify when information becomes intelligence, to be able to effectively allocate responsibilities and resources. In addition, it is important to link law enforcement data (e.g. police reports) and other types of records with the intelligence process, as the former can contain some parts that are valuable for the intelligence focusing on threats (Buckley 2014, 155-170).

First we look at the Customs and Border Control Agency from the organizational point of view. The Agency identified structural factors that constrain the implementation of the integrated management system. These constraining factors include existing policies, the way risk management and intelligence management are currently organised, as well as roles and responsibilities that hinder the implementation of the integrated management system.

Structural level integration is implemented through changes in the organization structure, for example i) drafting a new company level policy in line with the key ideas of the integration, ii) a reorganization of the Agency's activities ensuring that intelligence management and risk management are located in the same organizational unit, iii) resources are provided to support the IRIM in terms of competence building, and iv) (re)definition of roles and responsibilities so that they support the collaboration between risk and intelligence experts.

Functional integration in the Agency is carried out by i) integrating intelligence and risk management systems as well as risk analysis and intelligence analysis regarding smuggling of weapons. In the following subsections 3.2–3.5 the functional integration is discussed from an intelligence cycle perspective.

Cultural integration in the Agency is shown by the establishment of common norms that emphasize the integration, and the creation of a shared understanding of the benefits and needs of the IRIM.

Social aspects such as power relationships, roles and responsibilities and associated expectations regarding appropriate performance, have been considered by the Agency in its implementation of the IRIM. The Agency's senior managers have provided extensive resources to ensure successful implementation of the IRIM.

The Agency is aware of interrelationships between structures, functions, cultures and social aspects, which contribute to ensuring an effective adoption and implementation of the IRIM. An example is culturally favourable attitudes towards integration which contribute to senior management's decision to provide resources to IRIM and reorganise the activities in a way that support the IRIM at the organizational structure level.

3.1. Identifying requirements (i)

The Customs and Border Control Agency has prioritized risks and control areas at the organizational level. However, these priorities have not been based on a risk assessment and risk science approach. It is decided to adopt the IRIM, which means that the Agency's priority list is reconsidered, to allow for the inclusion of all types of threats, including those earlier found to be extremely unlikely and ignored. Drug smuggling is on the priority list, but the smuggling of weapons has not been up until now, as this type of threat has been considered unlikely. The threats are to be classified according to the risk set-up described in Section 2.3.2 and explained below.

3.2. The collection of data and information (ii)

The Customs and Border Control Agency has received clues from its intelligence department about the possible smuggling of weapons. The data on smuggling are based on weak signals

that emerged in another context when data on drug smuggling were collected. The concern is that criminals may smuggle weapons into the country and use them to commit serious crimes. It is unclear who would engage in the smuggling and how, when, and where this smuggling could take place, as well as how the weapons are planned to be used. The consequences of the smuggling are thus highly uncertain.

The intelligence plans for additional work to obtain supplementary data and information by reviewing and checking criminal environments and specific groups with respect to their capacities, motives, networks, strengths and weaknesses, etc., in relation to a potential smuggling of weapons event. The work is conducted in parallel with the analysis stage (iii), as it builds on knowledge obtained through the threat and risk analysis and particularly the identification of threats and risk sources.

In the data collection phase, the IRIM supports collaboration between intelligence collectors, intelligence analysts and risk assessors. These experts work as a team in the same department. At the functional level of the organization, IRIM promotes procedures for formal and informal communication and cooperation, and, at the cultural level of the organization, IRIM promotes respect for different competences and an attitude of openness, to stimulate the sharing of data and information.

The smuggling of weapons is connected to the smuggling of drugs and even to cybercrimes, as smugglers could use cyberattacks on the customs and border control management's database and electronic systems as a way of facilitating the smuggling. This indicates the complexity of analysing and understanding the risks related to the smuggling threat and the need to conduct the collection of data and information in an extensive way, capturing relevant risk sources and influencing factors.

3.3. Analysis of data, information, threats and risks (iii)

The analysis is based on a list of identified events (threats) A'_1, A'_2, …. The events particularly include events related to drug smuggling, the smuggling of weapons and cyberattacks. Different methods and techniques are used to identify these events, building on both intelligence and risk literature (see overviews in, e.g. Clark 2020; Fischhoff and Chauvin 2011; Buckley 2014; Aven 2014). In the following, the main focus is on the smuggling of weapons event; we just refer it to as A′. Initially, a crude threat risk assessment is conducted, to assess the magnitude of the risk related to the smuggling of weapons. The main results are outlined in Table 1. To simplify the analysis, it is understood that A′ is severe, suitably defined by the Agency. In practice, there would be a need to split A′ into different subevents to reflect different degrees of severity of the smuggling.

Table 1 shows that the risk is considered high when basing the conclusion on the intelligence report. The risk is also judged moderately high without this report, as the knowledge supporting the rather low probability is weak. Earlier judgment basically ignored the risk related to the smuggling of weapons, with reference to the low probability; however, risk science and the IRIM framework stress the importance of also considering the knowledge supporting the probability judgments. The knowledge strength judgments are based on criteria, as listed in Section

Table 1. Crude risk assessment of identified events (threats), before and after the initial intelligence report about the smuggling of weapons.

Risk judgment Threat	Probability	Knowledge strength	Data, information Evidence	Conclusions. Risk ranking
A′ (before initial intelligence report)	<0.01	Rather weak	Not much data and information available	Moderate high
A′ (after initial intelligence report)	>0.10	Moderately strong	Intelligence report	High

2.3.2, covering factors like amount of reliable and relevant data/information, justification of assumptions made, agreement among experts, understanding of the phenomena involved and the degree to which the knowledge has been examined. A key element of the fourth criterion is the degree to which the capacity and the intention of the risk sources (i.e. criminal groups) are considered well understood.

The above analysis is supported by different types of studies, to identify factors, events and scenarios that can lead to or cause A' to occur. These studies use methods like anticipatory analysis and modelling, scenario analysis, event trees and network models (Clark 2020).

To strengthen the analysis, further intelligence work is conducted, and the analysis is updated.

The Agency also conducts a longer term (5-10-year horizon) integrated intelligence and risk analysis. The focus is on factors, events and scenarios that could lead to considerable likelihood and risk changes related to the smuggling of weapons. In this case, three factors were identified as having the potential to significantly increase the likelihood and risk:

1. Dramatic changes in the geopolitical situation due to war in neighbouring countries (the current situation is characterized by some tensions)
2. Increasing number of cyberattacks
3. Increased level of corruption in neighbouring countries

Each of these scenarios is assessed with respect to plausibility, reflecting likelihood and supporting knowledge (Glette-Iversen, Aven, and Flage 2022). We judged scenarios 1) and 2) to be plausible, but not 3).

3.4. Dissemination of results

The results of the analysis are presented using formats like that in Table 1, with explanations of key concepts and terms. IRIM emphasizes the use of risk assessment and the evaluation of strength of knowledge related to assumptions and beliefs in all phases of the intelligence cycle, including the dissemination phase. When designing the dissemination, care must be shown concerning potential exploitation of the intelligence results. IRIM highlights all risks related to sharing the intelligence product with other stakeholders. If, e.g. the information about the route and place of the weapon smuggling is received by several partners, and this information is leaked or hacked and received by another criminal group, the smuggler could be warned and use an alternative plan to accomplish the smuggling.

Timely dissemination of results is ensured via authorized access to the intelligence product. IRIM supports timely and targeted dissemination of results, as it is important that customs officers working on the front line, e.g. receive information and warnings about the smuggling of weapons, as it may have an impact on their personal safety and that of their colleagues.

IRIM includes identification of risks that may affect customs officers at certain border crossing points, or when inspecting certain consignments or vehicles.

In addition, IRIM helps proper protection of the sources of the intelligence information, so that the sources are not revealed when intelligence is disseminated.

There is often a tension regarding whether the intelligence should be used for short-term tactical purposes, such as stopping correct consignments or cars at the border, or whether it should be used in relation to strategic, long-term goals such as creating strategies to deal with organized crimes related to smuggling weapons. The priorities need to be made at the top level of the organization. IRIM can identify risks related to the achievement of the short-term and longer-term goals and provide support for the decision-making.

3.5. Priorities, follow-up and decisions

Based on the IRIM analyses, the Agency prioritizes the smuggling of weapons. This again influences the intelligence requirements and intelligence targets in the future. The Agency defines two intelligence targets for the smuggling of weapons. At the strategic level, the Agency needs a broad and in-depth analysis of weapon smuggling. There is a need for better understanding of the risks related to the smuggling of weapons, particularly the factors influencing these risks, in relation to, e.g. type of weapons, networks, countries and the geopolitical situation. Updating of scenarios helps the Agency to prepare for the smuggling in the long term.

At the tactical level, the Agency's intelligence target is to support ongoing border management activities. This includes producing adequate intelligence information to be able to more rationally – using the integrated threat and risk assessments – identify which consignments, cars, trucks, containers or persons to select for further investigation.

The intelligence and risk analysis loop also highlights a review of the process and particularly how well the requirements were met. Feedback loops are crucial for the improvement of the intelligence management and the intelligence products.

The loop returns to the first stage: the requirements.

4. Discussion

Today, intelligence and risk assessment are both crucial activities in customs and border control operations and a prerequisite for the Customs and Border Control Agencies' successful performance. However, these activities are often conducted separately, despite many functions overlapping. Both areas deal with severe threats and risks and deploy many similar analytical approaches. There are differences between intelligence and risk assessment in terms of traditions, education, science, and practice. We know that intelligence collectors and analysts are often unfamiliar with risk assessment and management theories and, vice versa, risk analysts and experts typically have no or very little competence in intelligence (Clark 2020; Buckley 2014). However, the problems at hand require not only diversity in thinking and methods but also coordination and effective use of resources, and these can only be obtained if intelligence and risk assessment are more strongly integrated than is currently seen.

In this paper, we outline a framework for how such an integration can be facilitated. We argue that combining these two areas along the lines described will strengthen the risk and safety work in relation to customs and border control. The proposed framework for integrating risk and intelligence management – IRIM – builds on risk science and intelligence knowledge, as well as organizational theories. It is not considered a final solution for how to integrate intelligence and risk assessment. Rather, it provides initial ideas and an outline of structures for how to develop such a framework. Further testing of the framework is needed.

Earlier studies and the WCO documents have suggested a one-way relationship between intelligence and risk assessment/management: intelligence enhances risk assessment/management (Paté-Cornell 2015; WCO 2021a, 2021b; Widdowson 2020). We see the relationship as reciprocal: risk assessment/management contributes to several phases of the intelligence cycle and is needed to support prudent intelligence work; refer to Section 4. The intelligence literature supports this thinking (Clark 2020; Buckley 2014), but it also points to some challenges, particularly lack of risk assessment/management competences (Clark 2020; Buckley 2014).

The IRIM focuses on the Customs and Border Control Agency level, i.e. the organizational level. The IRIM makes use of the intelligence cycle, but with flexibility, to be able to meet some of the criticism raised against the cycle. The cycle is considered a general discussion platform for intelligence work (Buckley 2014). From risk science, the IRIM draws on some core principles, in line with the latest risk science knowledge. Standards like ISO 31000 standard on risk

management are not considered sufficient for building the framework, as they are not based on risk science.

IRIM emphasizes the co-construction of intelligence and risk assessment, which requires support at the structural, functional (operational) and cultural levels of the Customs and Border Control Agency. Integration can be achieved at these three levels – and ideally in each of them. Structural aspects refer to integrated management systems, strategies, resources, defined roles, responsibilities, and competencies which support IRIM. A cultural precondition of IRIM is an adequate understanding of the key concepts, principles, approaches and methods of intelligence and risk management, as well as the subsequent motivations for applying IRIM. At the organization's functional level, IRIM would mean integrating intelligence collectors, intelligence analysts and risk analysts in the same multidisciplinary team.

The case of weapon smuggling shows how IRIM can be applied. The smuggling of weapons was initially not considered, based on a judgment of it being unlikely. The Agency had not conducted a prudent risk assessment, opening up to all types of events. To meet this type of challenge, the IRIM emphasizes broad risk judgments, highlighting not only likelihoods but also knowledge and its strength, particularly assumptions and potential surprises. Traditional risk assessment lacks this focus on knowledge but is today an essential component of a prudent risk assessment.

Often, intelligence information is considered secret so that it cannot be shared. However, sharing data and information is critical for the effective intelligence and risk assessment work. For end users, such as customs officers who are working on the front line, information about all risks is needed to adequately guide their inspections. At the same time, one needs to consider the risks related to sharing intelligence products, in case information is misused.

The use of IRIM would promote the establishment of organizations' priorities, and intelligence targets, as well as better warning systems, monitoring, prevention and mitigating the risks, supporting relevant decision-making.

5. Conclusion

In the rapidly changing operational environment, the success of the Customs and Border Control Agencies in performing their main duties – enhancing the smooth flow of goods and travellers crossing borders and controlling illegal cross-border movements of goods and travellers – increasingly depends on a better combination of intelligence and risk management.

The IRIM framework presented and discussed in this paper is an endeavour to integrate these two fields, for better and more efficient performance of customs and border control. IRIM provides a framework for prudent risk and intelligence management. It is based on core risk science and intelligence concepts, principles and methods. It outlines the basic idea, and considerable testing is needed to check both the theoretical and practical suitability of the framework.

The use of IRIM poses some challenges. These include the lack of competencies in risk management and risk science, in the intelligence field, and the lack of intelligence expertise, in the risk management field. Efforts to draw on ISO 31000 are not sufficient for applying risk management at the IRIM level.

Successful IRIM implementation requires both strong motivation for integration and strong and improved understanding of both fields, as well as adequate resources and the competence to perform IRIM.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Marja Ylönen http://orcid.org/0000-0001-9944-9673
Terje Aven http://orcid.org/0000-0001-8309-7861

References

Alvesson, M. 2013. *Communication, Power and Organization*. Berlin: Walter De Gruyter.
Alvesson, M., and A. Spicer. 2016. *The Stupidity Paradox. The Power and Pitfalls of Functional Stupidity at Work*. London: Profile Books.
Antonsen, S. 2009. "Safety Culture and the Issue of Power." *Safety Science* 47 (2): 183–191.
Apostolakis, G. E. 2004. "How Useful is Quantitative Risk Assessment?" *Risk Analysis: An Official Publication of the Society for Risk Analysis* 24 (3): 515–520. doi:10.1111/j.0272-4332.2004.00455.x.
Askeland, T., R. Flage, and T. Aven. 2017. "Moving beyond Probabilities – Strength of Knowledge Characterisations Applied to Security." *Reliability Engineering and System Safety* 159: 196–205.
Aven, T. 2012. "The Risk Concept – Historical and Recent Development Trends." *Reliability Engineering and System Safety* 99: 33–44.
Aven, T. 2014. *Risk, Surprises and Black Swans*. New York: Routledge.
Aven, T. 2018. "Reflections on the Use of Conceptual Research in Risk Analysis." *Risk Analysis* 38 (11): 2415–2423.
Aven, T. 2020. *The Science of Risk Analysis*. New York: Routledge.
Aven, T., and G. Reniers. 2013. "How to Define and Interpret a Probability in a Risk and Safety Setting." *Discussion Paper, Safety Science* 51: 223–231.
Aven, T., A. Seif, and K. Karatzoudi. 2022. What are the Core Principles of Risk Management? ESREL 2022 Conference Proceedings.
Aven, T., and S. Thekdi. 2022. *Risk Science: An Introduction*. New York: Routledge.
Aven, T., and M. Ylönen. 2019. "The Strong Power of Standards in the Safety and Risk Fields: A Threat to Proper Developments of These Fields?" *Reliability Engineering and System Safety* 189: 279–286.
Aven, T., and M. Ylönen. 2021. "How the Risk Science Can Help Us Establish a Good Safety Culture." *Journal of Risk Research* 24 (11): 1349–1367.
Aven, T., and E. Zio. 2021. "Globalization and Global Risk: How Risk Analysis Needs to Be Enhanced to Be Effective in Confronting Current Threats." *Reliability Engineering & System Safety* 205: 107270. doi:10.1016/j.ress.2020.107270.
Berner, C. L., and R. Flage. 2016. "Strengthening Quantitative Risk Assessments by Systematic Treatment of Uncertain Assumptions." *Reliability Engineering and System Safety* 151: 46–59.
Bieder, C., and M. Bourrier. 2013. *Trapping Safety into Rules: How Desirable or Avoidable is Proceduralization?* Boca Raton, Florida: CRC Press, Taylor and Francis Group.
Bjerga, T., and T. Aven. 2016. "Some Perspectives on Risk Management – A Security Case Study from the Oil and Gas Industry." *Journal of Risk and Reliability* 230 (5): 512–520.
Buckley, J. 2014. *Managing Intelligence. A Guide for Law Enforcement Professionals*. Boca Raton, Florida: CRC Press, Taylor & Francis Group.
Byman, D. 2016. "Intelligence and Its Critics." *Studies in Conflicts & Terrorism* 39 (3): 260–280. doi:10.1080/1057610X.2015.1108086. Accessed January 14, 2022.
Campbell, C. 1998. *The Myth of Social Action*. UK: Cambridge University Press.
Clark, R. M. 2020. *Intelligence Analysis. A Targe-Centric Approach*. 6th ed. California: Sage Publications.
Fischhoff, B., and C. Chauvin. 2011. *Intelligence Analysis. Behavioral and Social Scientific Foundations*. Washington DC: The National Academies Press.
Flage, R., T. Aven, E. Zio, and P. Baraldi. 2014. "Concerns, Challenges and Directions of Development for the Issue of Representing Uncertainty in Risk Assessment." *Risk Analysis: An Official Publication of the Society for Risk Analysis* 34 (7): 1196–1207. doi:10.1111/risa.12247.
Giddens, A. 1986. "The Constitution of Society." In *Outline of the Theory of Structuration*. Berkeley and Los Angeles: University of California Press.
Glette-Iversen, I., T. Aven, and R. Flage. 2022. "The Concept of Plausibility in a Risk Analysis Context: Review and Clarifications of Defining Ideas and Interpretations." *Safety Science* 147: 105635.
Grote, G. 2012. Safety Management in Different High-Risk Domains – All the Same? *Safety Science* 50: 1983–1992. doi:10.1016/j.ssci.2007.05.014.
Haukelid, K. 2008. "Theories of (safety) Culture Revisited—An Anthropological Approach." *Safety Science* 46: 413–426.
Hedström, P., and R. Swedberg. 1998. "Social Mechanisms: An Introductory Essay." In *Social Mechanisms. An Analytical Approach to Social Theory*, edited by Hedström, P. and Swedberg, R. UK: Cambridge University Press.
Hertz, D. B., and H. Thomas. 1983. *Risk Analysis and Its Applications*. Chichester: Wiley.
ISO. 2018. ISO 31000 Risk Management. Accessed March 12, 2021. https://www.iso.org/iso-31000-risk-management.html.

Jørgensen, T. H., A. Remmen, and M. D. Mellado. 2006. "Integrated Management Systems – Three Different Levels of Integration." *Journal of Cleaner Production* 14 (8): 713–722. doi:https://doi.org/10.1016/j.jclepro.2005.04.005.
Komarov, O. J. 2016. "Risk Management Systems in Customs: The Ukrainian Context." *World Customs Journal* 10 (1): 35–44.
Laporte, B. 2011. "Risk Management System: Using Data Mining in Developing Countries' Customs Administrations." *World Customs Journal* 5 (1): 17–27.
Lohse, M. 2020. "Sharing National Security Information in Finland." *Information & Communications Technology Law* 29 (3): 279–290.
Lowenthal, M. 2020. *Intelligence. From Secrets to Policy*. 8th ed. Los Angeles: SAGE Publications.
MacInnis, D. J. 2011. "A Framework for Conceptual Contributions in Marketing." *Journal of Marketing* 75 (4): 136–154.
Marrin, S. 2012. "Is Intelligence Analysis an Art or a Science?" *International Journal of Intelligence and Counterintelligence* 25: 529–545.
Masys, A. J. 2012. "Black Swans to Grey Swans: revealing the Uncertainty." *Disaster Prevention and Management* 21 (3): 320–335.
Omand, D. 2020. *How Spies Think: Ten Lessons from Intelligence*. UK: Penguin.
Paté-Cornell, E., and A. Cox. Jr, 2014. "Improving Risk Management: From Lame Excuses to Principles Practice." *Risk Analysis: An Official Publication of the Society for Risk Analysis* 34 (7): 1228–1239. doi:10.1111/risa.12241.
Paté-Cornell, M. E. 2002. "Fusion of Intelligence Information: A Bayesian Approach." *Risk Analysis: An Official Publication of the Society for Risk Analysis* 22 (3): 445–454.
Paté-Cornell, M. E. 2012. "On Black Swans and Perfect Storms: risk Analysis and Management When Statistics Are Not Enough." *Risk Analysis* 32 (11): 1823–1833.
Paté-Cornell, M. E. 2015. "Uncertainties, Intelligence and Risk Management: A Few Observations and Recommendations on Measuring and Managing Risk." *Stanford Journal of International Law* 51 (1): 55–67.
Petersen, K. L., and K. V. Rønn. 2022. The Authority of Teaching Intelligence. What kind of future is the Scandinavian intelligence community prepared for? Article manuscript.
Pfeffer, J. 1997. *New Directions for Organization Theory. Problems and Prospects*. New York: Oxford University Press.
Ratcliffe, J. 2010. "Intelligence-led Policing: Anticipating Risk and Influencing Action." The IALEIA Publication. Accessed April 3, 2022. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.6795&rep=rep1&type=pdf.
Ratcliffe, J. H. 2016. *Intelligence-Led Policing*. 2nd ed. London: Routledge. Accesed April 1, 2022. doi:10.4324/9781315717579.
Schein, E. H. 2010. *Organizational Culture and Leadership*. 4th ed. San Francisco: Jossey-Bass.
Scott, L., and P. Jackson. 2004. "The Study of Intelligence in Theory and Practice." *Intelligence and National Security* 19 (2): 139–169.
Scott, W. R. 2014. *Institutions and Organizations. Ideas, Interests, and Identities*. 4th ed. California: Sage Publications.
SRA. 2015. "Glossary Society for Risk Aven Analysis." Accessed March 12, 2022. https://www.sra.org/resources.
SRA. 2017. "Risk Analysis: Fundamental Principles." Accessed March 12, 2022. https://www.sra.org/resources.
Stacey, R. 2012. *Tools and Techniques of Leadership and Management. Meeting the Challenge of Complexity*. London: Routledge. doi:10.4324/9780203115893.
WCO. 1992. "Resolution of The Customs Co-Operation Council Concerning the Importance of Intelligence in Supporting Customs Enforcement Activity." Accessed January 5, 2022. http://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/resolutions/importance_of_intelligence.pdf?la=en.
WCO. 2021a. "Risk Management and Intelligence Programme." Accessed January 24, 2022. http://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/intelligence-and-risk-management-programme.aspx.
WCO. 2021b. "Risk Management in the Customs Context." Annex I to Doc. EC0631E. Accessed January 24, 2022. http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/risk-management-and-intelligence/risk-management-compendium-volume-1.pdf?la=en http://www.wcoomd.org/en/search.aspx?keyword=risk.
Widdowson, D. 2020. "Managing Customs Risk and Compliance: An Integrated Approach." *World Customs Journal* 14 (2): 63–80.
Widdowson, D., and S. Holloway. 2011. "Core Border Management Disciplines: risk-Based Compliance Management." In *Border Management Modernization*, edited by McLinden, G., Fanta, E., Widdowson, D. and Doyle, T. Washington DC: World Bank.