1. RISK MANAGEMENT IN THE CUSTOMS CONTEXT

Changing operating environment

Customs administrations around the world are responsible for implementing a broad range of government policies in areas as diverse as revenue collection, trade and traveller compliance, protection of society including anti-terrorism, cultural heritage, intellectual property, collection of statistics and environmental protection. Some of these responsibilities are often carried out on behalf of other government ministries and agencies, through the implementation of a diverse range of agreed control regimes, with Customs having responsibility for the administration and enforcement of relevant regulatory requirements at the point of importation and exportation.[4]

In addition to their overarching responsibility to maintain control over the cross-border movement of goods, people and conveyances, Customs administrations also have a mandate to provide an appropriate level of facilitation to trade and travel, and consequently need to maintain regulatory control that favours minimum intervention over intrusiveness, including by means of advanced technologies. This implies close monitoring and evaluation of the rate of physical inspection and revamping the targeting process while ensuring that regulatory requirements (red tape) are not unduly onerous or overly prescriptive.[5]

Sometimes the pursuit of achieving a balance between intervention and facilitation has been seen as a “zero-sum” game where an increase in one would necessarily imply a decrease in the other. In reality it is important to understand that control and facilitation are not mutually exclusive goals. In fact, they are mutually reinforcing objectives and it is possible to achieve optimal levels of both. Applying the principles of risk management provides the means to achieve this balance, and allow Customs administrations to move from traditional ‘gate-keeper’ style controls towards a risk-based operating model.

Customs’ role in border control has dramatically changed in the wake of technological advancement, the sheer volume of goods and the manner in which they are traded around the globe and the speed of such transactions, as well as the risk of global pandemic and its influence on risk management. Customs administrations around the world have been required to continually adapt their methods of operation in an effort to maintain their effectiveness and relevance.

For example, the emergence of global value chains, disruptive technologies, trade-based money laundering and terrorism financing, as well as the increasing complexities of international trade agreements have all impacted on the way in which Customs fulfils their responsibilities. An exponential number of small packages represent new challenges for Customs administrations in terms of their border risk management. Customs administrations are faced to check huge quantity of small-packages which also represents a challenge for Customs administrations in the enforcement area. As a result, Customs administrations have seen a worldwide dramatic increase in workload across all areas of activity.[6] It is expected that collaboration of stakeholders and the transmission of more specific E-Commerce data to the Customs administration would facilitate the efficient processing by Customs on the vast number of parcels crossing borders daily.

[1] Widdowson (2006), p. 2.
[2] Widdowson and Holloway (2010), p. 98.
[3] Widdowson (2006). p. 2 – 3.

Digitalization is a top priority to create a paperless customs environment for facilitation of Customs processes: electronic clearance of goods, single window concept, non-intrusive inspections and risk management based on data analysis are pillars for modern Customs administration. Customs may obtain digital data of cross-border goods, exchange electronic data, which is normally timelier than paper-based information, with relevant government agencies as well as with other Customs administrations abroad. Enhancement of use of data for risk management purposes order to move towards the digital future of Customs administrations.

Customs administrations can no longer interact a physical manner with 100% of cross-border flows. According to the Revised Kyoto Convention (RKC) and the SAFE Framework of Standards, risk management should be adopted by all modern Customs administrations. Furthermore, the World Trade Organization (WTO) also recognizes and endorses risk management to be adopted so that Customs administrations concentrate their control and, to the extent possible other relevant border controls, on high-risk consignments and expedite the release of low-risk consignments.[7]

Although the application of risk management in the operational Customs context varies across Customs administrations, many Customs administrations today implement standardized risk assessment, selectivity criteria and targeting. By exploiting a substantial amount of data at their disposal, using predictive analysis and machine learning, Customs enable smarter control of Customs risks and allow Customs administrations achieving their objectives and turning a long-historic public administration into a robust organization. This Risk Management Compendium provides an overview of core aspects of modern Customs risks management practice and assists Customs administration and cooperation among them.

Compliance management approach

Modern risk-based compliance management builds on several key foundations. These can be broadly grouped into four main categories – a country's legislative framework, and the administrative, risk management and technological frameworks adopted by Customs administrations. Collectively these four categories represent the key determinants of the manner in which cross-border flows may be expedited and the way Customs control may be exercised over such flows.[8]

Risk-based compliance management aims to differentiate as much as possible between compliant, low risk trade and higher risk, noncompliant trade. It starts with robust legislation that incorporates areas such as acknowledgement of the respective responsibilities of government and industry, includes regulations for electronic communication, provides sanctions for non-compliance and provisions to break the nexus between physical movements and processing, reporting and revenue liability, and, finally, allows for flexible and tailored business solutions.

This approach also requires administrative arrangements that include initiatives such as the introduction of a client service approach, know your client ('KYC') guidelines, education and awareness campaigns, technical assistance and advice, consultation and cooperation, the publishing of formal rulings, and formal appeal mechanisms.

The adoption of a risk management framework introduces risk-based decision making and proce-

[7] WTO TFA Measure 7.4

5. Widdowson (2005), p. 93 – 94.

dures into the organization that enable a balance between control, facilitation and supply chain security to be maintained. The introduction of risk-based procedures includes activities such as those associated with the early and accurate lodgement of information for risk assessment, intervention as early as possible in the supply chain for high-risk transactions, self-assessment and post-entry verification for lower risk, and investigative capability where non-compliance or fraud is detected.

The available technology represents an enabler that serves to significantly enhance an administration's ability to adopt such an approach[9]. Automation enables screening of vast amounts of information effectively, efficiently and timely against predetermined, intelligence-based risk criteria and assists with the making of decisions on both high and low risks. In the same way, advanced technologies, in particular modern non-intrusive inspection technologies, when used on the basis of risk assessment, can lead to more effective inspection activity and expedite clearance. All the above is consistent with the standards and guidelines of the Revised Kyoto Convention, the SAFE Framework of Standards and the Customs in the 21st Century strategy, which together provide the key building blocks for modern Customs administration.

An effective risk-based compliance management strategy acknowledges that the client categories outlined require different responses. Incentives and simplified procedures should be applied to those who are voluntarily compliant (low risk), assisted compliance to those who try to be compliant but do not necessarily always succeed, directed compliance to those who try to avoid following the letter of law, and enforced compliance to those who are deliberately non-compliant (high risk).. Affecting client behaviour and actively steering the population towards low risk will allow Customs to concentrate its control resources on high risks. Diagram 1 illustrates an example of a compliance management model.

Diagram 1. Compliance management model

	LOW	**RISK LEVEL**		**HIGH**
Client Categories	Voluntary compliance People who want to comply	Assisted compliance People who try to comply, but don't always succeed	Directed compliance People who will avoid complying if they can	Enforced compliance People who deliberately do not comply
Client Behaviours	•Voluntary compliance •Informed clients	• Attempting to comply • Uninformed clients	• Resistance to compliance • Will avoid if possible	• Criminal intent • Illegal activity
Customs' Competencies		**Interventions**		
Information High quality,timely, and accurate information about the arrivaland departure of all persons, goods and conveyance	• Screening of regular information flows Advanced cargo/passenger/ conveyance information (in and out). • Monitoring information of physical movement of all	Patterns of non-compliance by: • Industry, product, location, destination or port of origin • Type of non compliance (e.g.,	• Profile of individual non-compliant traders/travellers •Identification of specific compliance problem (e.g., bad systems, poor data	• Profile and ongoing intelligence (on and offshore) about offenders/potential offenders and their associates

[6] Widdowson (2005), p. 94.

	people, goods and conveyanceacross (in and out) the border • Information from customs declarations	incorrect documentation)	entry etc)	
Assessment Assessment of the level of risk posed by arriving and departing people, goods and conveyance	• FrontLine Pax/Goods staff intuition • Intelligence profiles • Statistically valid random checks	• Complie information on client behaviours • Identify and monitor compliance trends/patterns	• Problem solving approach to specific compliance problems • Investigation	• Assess risk and information needs in relation to seriousness of offence • Investigation
Action Actions required to mitigate identified risk(s) without unduly disrupting legitimate trade and travel	• Compliance programmes • Education and advice • Visible deterrence • Cargo and baggage screening	• Targeted compliance guidance • Punitive sanctions • Rolling audit programme • Increased attention	• Deter by detection and surveillance • Comprehensive audits • Prosecution	• Pre and post clearance interventions • Comprehensive audits • Passenger/cargo searches • Prosecution
	Direction that Customs wants to move travellers and traders			
	Increasing levels of intervention by Customs			

In the Customs context, control and risk management of goods, conveyances or people commences at the export or departure point , continues with ongoing controls at the point of import or arrival and, beyond with post-control audit. A modern compliance management approach recognizes that risk mitigation strategies can and should be applied throughout the supply chain. It also recognizes that a combination of multiple measures often leads to better results and more effective use of resources. Where appropriate legal, technological and operational arrangements are in place, a multi-layered approach can also facilitate risk identification, response coordination and collaboration across and between governments. The term multi-layered is used to encapsulate the entire decision-making and other activities that may be carried out by Customs along this supply chain continuum.

2. DEVELOPING AN ORGANIZATIONAL FRAMEWORK FOR MANAGING RISK

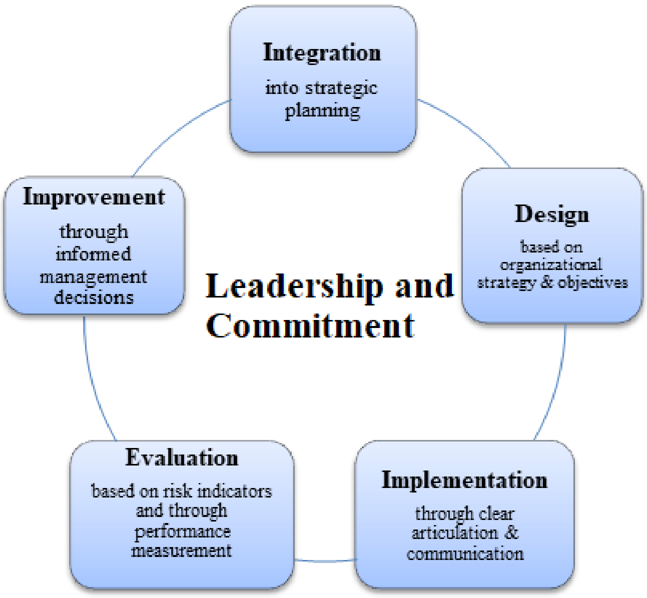
1. Overview

Organizational risk management approach demands a more holistic approach to risk management, spanning everyone from the Director General to the front line. It is no longer sufficient to manage risk at the individual activity level or in functional silos. A holistic approach to risk management requires an ongoing assessment of potential risks for an administration at every level, and then aggregation of the results at the organizational level to facilitate priority setting and improved decision making. The identification, assessment and management of risk across customs administration helps reveal the importance of the whole, the sum of the risks and the interdependence of the parts.

Holistic management of risk requires a solid and robust organizational risk management framework empowering officers at all levels of the administration to make risk-based decisions in a structured and systematic manner. The framework allows risk management activities to be aligned with an administration's overall objectives, corporate focus, strategic direction, operating practices and internal culture. In order to ensure risk management is a consideration in priority setting and resource allocation, it needs to be integrated into existing governance and decision-making structures at both operational and strategic levels. When this is achieved, everyone in the administration becomes involved in the management of risk10.

There are various ways of going about establishing an organizational risk management framework. In general the framework consists of five key elements. These are mandate and commitment, the organizational risk governance arrangements (designing the framework), implementing and practising risk management, monitoring and review, and, finally, continuous development. Diagram 2 illustrates these elements and their interlinkages.

Diagram 2. Risk management framework


Integration
into strategic planning
Design
based on organizational strategy & objectives
Implementation
through clear articulation & communication
Evaluation
based on risk indicators and through performance measurement
Improvement
through informed management decisions
Leadership and Commitment

Source: ISO 31000:2018 Risk management – Principles and guidelines

2. Development of Risk Management Framework

2.1 High-level and sustained commitment

High-level mandate and commitment are crucial for effective risk management. Risk management will rarely be effective if it is not supported by the highest level of the administration. The Director General and the senior managers must set the policy, objectives and authorization to plan, deploy resources and make decisions based on risk management and risk assessment.

When adopting risk management, there are some general guiding principles to which the approach at all levels of the administration should adhere. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and

7. AS/NZS 4360/2004, Risk Management, p. v.

processes. These principles should enable customs administration to manage the effects of uncertainty on its objectives.

2.2 Understanding the organization and its context

A clear understanding of the operating environment is an important step in developing the organizational risk management framework. Through an environmental scan, an administration can identify various external and internal factors and risks that influence the way it may achieve its objectives. External factors to be considered may include various political, economic, social, environmental and technological considerations. When outlining the internal risk management context, thought should be given to: the overall management framework; existing governance and accountability structures; stakeholders; values and ethics; operational work environment; individual and organizational risk management culture and tolerances; existing risk management expertise and practices; types of information flows and systems used; and local and organizational policies, procedures and processes.

A thorough environmental scan increases an administration's awareness of the key characteristics and attributes of the risks it faces, including the type and source of risk, what is at risk, and the level of ability to control the risk. The scan will assist the administration to establish a strategic direction for managing risk and reinforce existing management practices supporting the attainment of overall management excellence.

In many administrations, existing management practices and processes include elements of risk management. Before starting to develop the framework, the administration should critically review and assess those elements that are already in place. In assessing internal risk management capacity, it is important to review the mandate, the governance and decision-making structures, the planning processes, the infrastructure, and human and financial resources. The review should deliver a structured appreciation of:[11]

- the maturity[12], characteristics and effectiveness of existing business and risk management culture and systems;
- the degree of integration and consistency of risk management across the administration and across different types of risk;
- the processes and systems that should be modified or extended;
- constraints that might limit the introduction of systematic risk management; and
- resource constraints.

As part of understanding the organization and its context for managing risk, it is important to consider the concept of risk tolerance. The environmental scan will identify stakeholders affected by the organization's decisions and actions, and their degree of comfort with various levels of risk. Understanding the current state of risk tolerance of the government, other agencies, citizens, parliamentarians, interest groups, etc., will assist in making decisions on what risks must be managed, how, and to what extent.

2.3 Risk management policy

Each Customs administration will need to establish its unique risk management policy, which will take into account its strategic goals and objectives with commensurate plans. The risk management

[9] AS/NZS 4360:2004, Risk management, p. 25.

[10] Risk management maturity will be further discussed in Chapter 4.

policy statement should clearly outline the administration's overall intentions and direction regarding risk management. Together, the risk management policy and an organizational risk management plan which specifies the approach, management components and resources to be applied to the management of risk, should include at least the following elements:

- linking organizational goals and objectives with risks;
- rationale and commitment for managing risks (risk strategy);
- linking risk management to strategic and planning processes;
- level and nature of risk that is acceptable (risk appetite/tolerance);
- risk management organization and arrangements;
- information on risk identification and evaluation techniques;
- list of documentation for analyzing and reporting risk;
- risk mitigation requirements and control mechanisms;
- specific accountabilities and responsibilities for managing risk (i.e. risk owners);
- criteria for measuring risk management performance;
- assigning dedicated resources to managing the implementation of risk management;
- internal and external communication and reporting plans and systems; and
- the timeframe for periodic review of the risk management policy and associated plans.

An effective risk management policy will contribute to:

- a sustained and transparent risk management environment;
- an environment where all employees take responsibility for managing risk and make decisions based on sound risk assessment;
- effective and efficient resource deployment;
- a continuous monitoring and evaluation culture that leads to better operational capability; and
- assurance that customs administration can respond or recover quickly and effectively when risks are realized.

2. 4 Accountability for managing risk

An administration needs to make sure that clearly defined responsibilities, authority and competence for managing risk exist. Allocating responsibility and authority to deal with risks is a key aspect of embedding risk management into an organizational culture.

Defining accountabilities includes identifying and allocating accountability at the organizational level for the development, implementation and maintenance of the risk management framework as well as defining risk owners for different key risks across the customs administration.

When considering risk ownership in general, in principle everyone in an administration is responsible for identifying and managing risks. When considering the formal roles in an organization, the following responsibilities can be defined:

The Director General or organizational head and senior management team have overall accountability for the risk management policy and practices of the customs administration. They are expected to provide leadership and support for risk management.

Senior managers "own" the risks specific to their individual areas and are accountable for individual unit risk management. Senior managers provide leadership and support to enable risk management objectives and principles in their units. They also make sure that priority areas are resourced according to organizational priorities, and that risk identification, assessment and treatment plans are incorporated in objective-setting and planning processes. Senior managers are also responsible for making sure that sufficient intelligence capability to effectively assess both strategic and operational risks is maintained, and that managers and staff have the tools to manage risks.

Managers are accountable for managing risks in their respective areas of responsibility. They must guarantee that priority areas within their span of control are resourced, and that operational systems and procedures are efficient and operating effectively. Managers and staff are expected to record key risks and develop a risk picture within their areas, by identifying and documenting assessment and treatment details to provide an audit trail. They must also guarantee that reporting systems are contributed to and ensure risk documentation is relevant and up-to-date. Managers also have to ensure that staff are continuously trained, guided and supported and have the tools to manage risks arising in their area of responsibility.

Front-line staff are largely responsible for intervention. Therefore, all staff are expected to

> *know and understand the legislation, delegated authorities and powers they have. They are also expected to follow instructions, policies and procedures and to identify risks and opportunities in their area of activity, including assessing the likely consequences and taking appropriate actions to mitigate risks. The feedback from staff and front-line interventions is a critical aspect of keeping the risk management framework continually up-to-date with the operating and risk environment.*

Depending on organizational structures and arrangements, there may be some specific entities that have collective risk management responsibilities. These may include a risk management committee, a central risk management unit, and/or a risk assessment/targeting centre.

A risk management committee is generally established and responsible for ensuring oversight and reporting to the senior management team and the Director General. The committee reports on whether the risk management framework is effective and is being followed by the organization in accordance with its policy. Typically, the functions of the risk management committee should include:

- preparation and advice on risk appetite, tolerance and strategy for the senior management team and the Director General;
- review of risk management reports for high-level risks, in particular those strategic risks which inform long-term decision making;
- analysis of the risk management process and its effectiveness; and
- review of organizational internal controls and their effectiveness.

Depending on the level of risk management maturity, some administrations are reorganizing unit arrangements associated with risk assessment and/or intelligence activities. A central risk management unit and/or a risk assessment/targeting centre is often responsible for information collation and analysis, and for the assessment of raw information. The resulting evaluation in an operational context provides risk indicators and profiles for goods, people, means of transport and economic operators. The functions of risk assessment/targeting centres are further explored in Annex 4.

2.5 Resources

It is important to ensure that sufficient resources are allocated to the management of risk. Administrations should analyze what kinds of people, skills, experience and competencies are required for staffing risk management related functions. Managers and staff should be provided with adequate training to ensure they are competent in all aspects of risk management and supported by customs integrity programmes and training. Automation is an increasingly important component of the collection, collation and analysis of data and information. Administrations need to evaluate their ICT capability and ensure that appropriate tools are available to conduct appropriate risk assessment, in order to provide the customs administration at all levels with good risk management products that identify organizational risks and recommend necessary treatments.

Automation can also increase the level of accountability and provide an audit trail for monitoring and review of administrative decisions and the exercise of official discretion. Where possible, automated systems should be configured in such a way as to minimize the opportunity for the inappropriate exercise of official discretion, face-to-face contact between Customs personnel and clients and the physical handling and transfer of funds.

2.6 Integrating risk management into organizational processes

Effective risk management cannot be practised in isolation, but needs to be built into existing decision-making structures and processes. As risk management is an essential component of good management, integrating it into existing strategic management and operational processes will ensure that risk management is an integral part of the day-to-day activities of the administration.

2.7 Communication and reporting

Good communication is an essential part of good risk management. Effective and efficient communication includes both internal and external aspects. Internal communication lines and reporting mechanisms support and encourage accountability and ownership of risk and enable risk related information to flow within the customs administration. Good internal communication and reporting should ensure that all staff is aware, responsible and accountable to their role in the risk management process. Internal consultation and feedback mechanisms ensure that the outcomes of the strategy are available and reviewed at different levels.

External communication and reporting mechanisms should be established to inform external audiences about the risk management strategy and to engage them in the process. Good external communication and reporting should include the following aspects:

- how to involve and engage appropriate external stakeholders and give effect to their expectations and requirements, and how they are taken into account in the approach;
- how to ensure that external risk reporting will comply with national legal, regulatory and governance requirements;

- how to use communication to build confidence in the customs administration in order to support its risk management approach, including the reporting of results; and
- how to communicate with relevant stakeholders in the event of crisis or contingency.

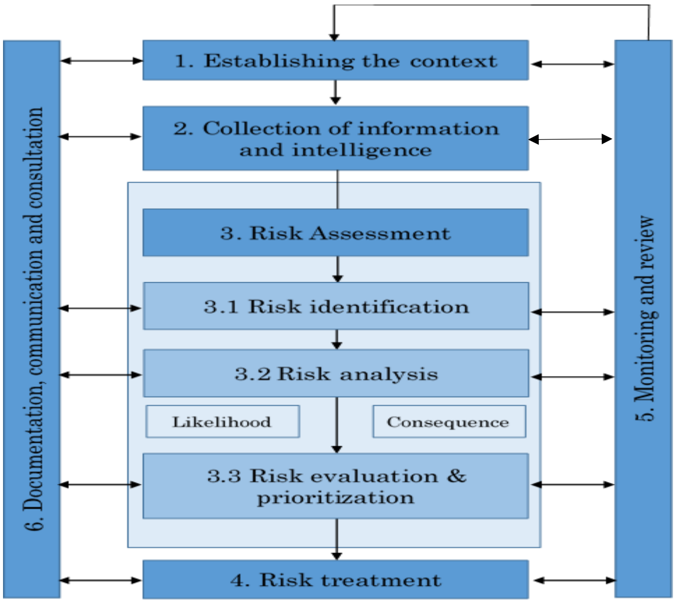
3. Implementing risk management

3.1 Risk management process

When implementing the framework, it is important to have a thorough plan and implementation strategy in place. This plan should describe the implementation of the organizational arrangements and define the timing and strategy for this. Implementation of the framework includes applying the risk management policy to organizational activities.

Adopting a common, continuous and systematic risk management process provides a standard methodology for implementing risk management in practice. The process is a cyclic methodology with well-defined steps that support better decision making by providing insight into risks and their impact, outlining a common foundation for management decisions regarding the allocation of resources and prioritizing treatment actions. It is important that the risk management process be applied at all levels of the administration. The steps of the process are described in Diagram 3.

Diagram 3. Risk management process


6. Documentation, communication and consultation
1. Establishing the context
2. Collection of information and intelligence
3. Risk Assessment
3.1 Risk identification
3.2 Risk analysis
Likelihood
Consequence
3.3 Risk evaluation & prioritization
4. Risk treatment
5. Monitoring and review

3.2 Establishing the context

Any effort to manage risk must begin by first establishing what needs to be managed. This stage defines the context in which risk management will take place, and aims at clearly articulating and clarifying the objectives and what risks are being examined[13]. Determining what needs to be managed helps set the parameters for the rest of the risk management process. The following questions can be used to establish context, outlining both the internal and the external aspects:

- What are the objectives in the context where the risk management process takes place?
- What is the operating environment?
- What capabilities and resources are available for managing risk?
- What criteria are used to assess risks and to determine if additional control is needed?
- What are the scope and limits of risk management?
- What are the expectations of stakeholders such as the government, affected communities, traders and other private sector groups? and
- What other details are known about the process or activity?

An outcome of this phase should be a statement of the environmental operating context which includes a clear indication of the objectives ("risk to what") and the risk areas, and defines the criteria and parameters for the risk assessment phase.

3.3 Collection of information and intelligence

Customs administrations need to collect information which will be used to implement their risk management processes. Possible information sources for Customs' risk management include other Customs administrations, relevant border agencies, private sectors and neighbouring states.

Customs administrations are encouraged to develop cooperative relationship with them. Regarding the information exchange among Customs administrations, Customs administration may consider establishing arrangements such as memoranda of understanding or conclude bilateral or regional agreements on customs cooperation or mutual administrative assistance. The latter formal frameworks may provide enhanced legal assurance, which may often be required to exchange sensitive information.

Wider and closer information sharing among border agencies increases recognition of existing risks at border. Customs administrations should further enhance cooperation with other border agencies in central, regional and local levels. External stakeholders provide valuable information for Customs risk management as well. The data and information communication from the private sector may contribute to enhancing risk management and risk mitigation as early as possible in the supply chain, whilst minimizing unnecessary disruption of normal trading practices.

Such information may complement data that is required as part of different types of declarations or procedures according to the legal frameworks in place, e.g. advance information on postal items, Pre-loading sea/air cargo security data or Passenger Name Record in relation to travellers and other information readily available in an electronic format for use by Customs administrations and other government agencies involved in the control of goods and people crossing the border.

[11] The context can be, for example, the whole organization, one of its key functions, a process, a project, a specific location, a group of border transactions, etc.

Information collected through various channels will be processed and stored in Customs data-base or in databases accessible to Customs. The stored information will be used or accessed in the risk management process. WCO Data Model and other international standards such as UN/CEFACT standards are key instruments to build a reliable, harmonized and standardized digital collaboration. Harmonization is an important step forward in terms of trade facilitation, the use of modern communication and information technologies, and the implementation of a Single Window environment. It also opens up new perspectives for networking on coordinated border management.

At the operational level, a modern Customs risk management approach is increasingly enabled by intelligence support. Intelligence enabled risk management brings together information and knowledge learned by Customs with a systematic approach for identifying and treating risks of greatest consequence. This is a critical process, as high risks identified through the risk management process will often be greater in number than Customs' resources and ability to respond. Risk Assessment reports support the top management in prioritizing risk treatment, thereby deciding the strategy for mobilization and deployment of customs resources"

International Conventions and the WCO tools also play an important role in global enforcement cooperation. In particular, WCO Customs Enforcement Network (CEN) is the global enforcement information and intelligence tool available for customs services, the WCO Regional Intelligence Liaison Offices (RILOs) had been established as a global network for information and intelligence exchange for collecting, analysing and supplementing data as well as disseminating information on trends, modus operandi, routes and significant cases of fraud.

International cooperation between WCO and other international organizations, such as, Interpol, Europol, International Chamber of Commerce (ICC), International Air Transport Association (IATA) and International Maritime Organisation (IMO) enables international and regional bodies to fulfil their international role and work in a more efficient and effective manner with a view to the further development exchange of information and intelligence.

3.4 Risk identification

Risks cannot be analyzed or managed until they are identified and described in an understandable way. The risk identification phase identifies and records all potential risks by using a systematic process to identify what risks could arise, why, and how, thus forming the basis for further analysis. Some of the questions asked in this phase could include:

- What are the sources of risk?
- What risks could occur, why, and how?
- What controls may detect or prevent risks?
- What accountability mechanisms and controls—internal and external—are in place?
- What, and how much, research is needed about specific risks?
- How reliable is the information?

Risk identification activities at various levels of the customs administration must be closely linked to each other. Once an administration's strategic risks have been identified they are handed down to managers, who then further refine the broad strategic risks and determine priority areas for action within their areas of influence. Once these decisions have been taken and priorities assigned, operational line management can begin the process of identifying specific cases from within their areas of influence for further action. At each step in the process, the extent of the risk being managed is progressively reduced and the risk is managed at an appropriate level within the organization.

The outcome of the risk identification process is a register of risks, which documents the risks and ensures that the entire risk spectrum is considered. There are many different ways to construct a risk register. Annex 1 outlines examples of risk register templates.

3.5 Risk analysis

Risk analysis is principally about quantifying risk, and requires consideration of the sources of identified risks, an assessment of their potential consequences in terms of achieving objectives, and judgment as to the likelihood that the consequences will occur (in the absence of any specific treatment with the existing controls in place). It relies upon the use of data and information to substantiate the consequences that are likely to be incurred if the risk occurs and/or remains unaddressed. Even though risk analysis should be evidence-based to the extent possible, it needs to be remembered that it is not an exact science. Knowledge about the business environment, expert judgment and common sense should never be overlooked when analyzing risks.

In short, the analysis considers:

- how *likely* is an event to happen; and
- what are the potential *consequences* and their magnitude.

Combining these elements produces an estimated level of risk. Risk estimation can be quantitative or qualitative, or a combination of the two.

Based on tolerance judgments using a 3x3 matrix (high, medium, low), Diagram 5 suggests possible descriptions and indicators for estimating the likelihood of a risk occurring.

Diagram 4. Example 3-tier risk management model (for illustration purposes only)

Risk level	Possible measures of influence
High risk level (or «red risk level»)	Application of control measures
Medium risk level (or «yellow risk level»)	Conducting work to obtain additional information for the possibility of assigning it to either a high or low level of risk.
Low risk level (or «green risk level»)	Continuing risk monitoring

Diagram 5. Example description and indicators for determining likelihood (for illustration purposes only)

Likelihood	Description	Indicators

High (Probable)	Likely to occur or more than a 20% chance of occurring	Has occurred in the last 12 months
Medium (Possible)	Could occur, but less than 20% chance of occurring	Has occurred between 1 year and 3 years ago Has occurred in another country within the last 2 years
Low (Remote)	Not likely to occur and less than 5% chance of occurring	Has not occurred in the last 3 years or more Has not occurred in another Member country in the last 2 years

Based on tolerance judgments using a 3x3 matrix (high, medium, low), Diagram 6 suggests possible descriptions and indicators for estimating the consequences of a risk occurring.

Diagram 6. Example description and indicators for determining significance of consequences (for illustration purposes only)

Consequence / Impact	Description	Indicators
High (Serious)	If adverse risk occurs then there could be a severe community, economic or political crisis	Long-term ramifications for government or administration
Medium (Manageable)	An adverse risk occurring would obstruct workflows and harm community or business	Damage to ability to meet organizational goals and commitments to government, community and business
Low (Treatment within existing workflows)	An adverse risk would cause minor delays to service delivery	Adverse risk event can be absorbed within existing standard operating procedures

Repeating this exercise on a regular basis (annually in the organizational and unit context) is required, and normally results in changes to the estimated level of risk. These changes occur because of the treatments and preventative measures put in place. For example, the amendment of ambiguous legislation would leave less room for interpretation and therefore decrease the likelihood of an adverse event occurring. This in turn would lead to a lower risk level compared to the time before the preventative measure was implemented, etc.

Example (for illustration purposes only)

In the context of the previous example, Workshop participants analyze (using a suitable technique, see Annex 1) each of the individual risks under the risk categories in terms of their likelihood and consequence, using a high (H), medium (M), and low (L) scale. They jointly come up with the following ratings:

	Objective	Risks	Likelihood	Consequence

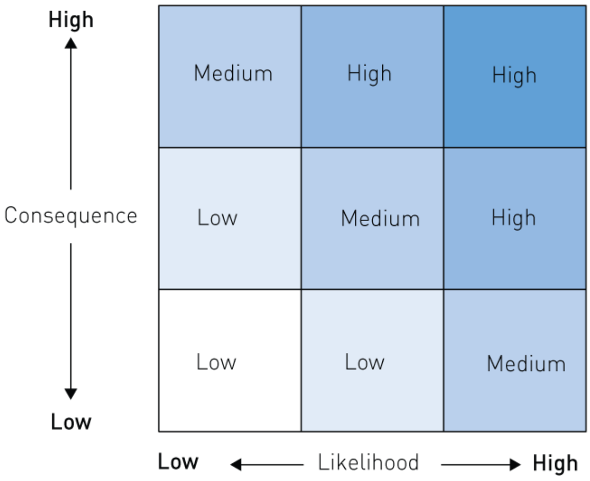
1	Effective and efficient collection of revenue	1.1 Fraud	H	H
		1.2 Lack of staff competence	L	M
		1.3 Integrity	L	L
2	Community protection and security	2.1 Narcotics	H	M
		2.2 WMDs	L	H
		2.3 IPR	M	L
3	Trade facilitation	3.1 Ineffective procedures	L	H
		3.2 Lack of coordination with other agencies	H	H
		3.3 IT failure	L	H

3.6 Risk evaluation and prioritization

This step entails comparing the assessed risks against a pre-determined significance criterion. By considering the risk level of each of the risks as described by the relevant management team in the matrix, it is possible to evaluate and prioritize the key risks that need to be analyzed in more detail. This will then lead to the deployment of proportionate resources in order to prepare for, prevent or respond to the risk.

For illustrative purposes, Diagram 7 represents an example of a simple 3x3 risk significance matrix[14].

Diagram 7. An example of a Risk Significance Matrix (3x3)



Medium	High	High
Low	Medium	High
Low	Low	Medium

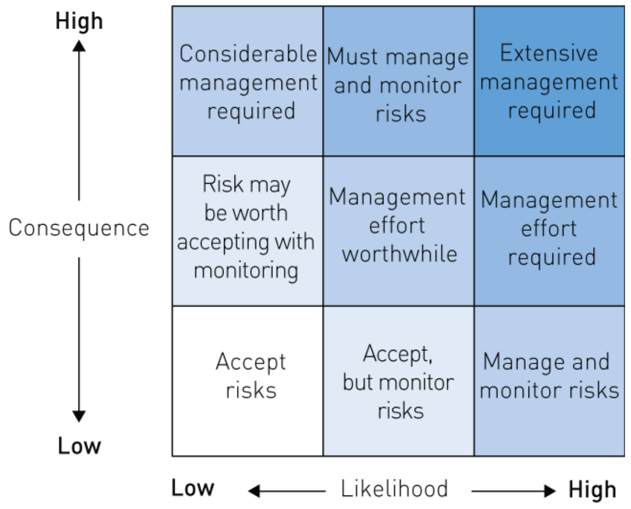
[12] Some Members may decide that there is a need for more detailed tolerance estimation beyond "high, medium or low". There are examples in the Capacity Building Compendium of a 4x4 matrix and a 5x5 matrix. In the case of a 5x5 matrix the tolerances may be expressed as minor, acceptable, tolerable, major and unacceptable. Another method of expressing risks is to use 'traffic-lights', i.e. red for high, amber for medium and green for low. An IT based system may apply a numeric value, such as a range from 1 to 100.

The evaluation enables Customs to better understand the risks. The process consists of deciding whether the risk is tolerable (acceptable), and assists in determining how imminently the risk event may occur. Decisions about which risks to respond to and which to monitor will potentially be impacted by many different issues, including:

- internal capability;
- internal capacity;
- is there an effective capability to implement the treatment;
- risk rating/level;
- return of treatment;
- effects to reputation; and
- the cost/benefits of proposed treatments (this is a feedback loop from the next step).

These issues form the basis on which the effectiveness of treatment strategies will ultimately be evaluated. Note that in the example at Diagram 7 it may be necessary to group a tolerability result and add specific response criteria for different categories.

Diagram 8. An example of a Risk Significance Matrix with response criteria



Considerable management required	Must manage and monitor risks	Extensive management required
Risk may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Accept risks	Accept, but monitor risks	Manage and monitor risks

The outcome of the risk evaluation and prioritization process should be a risk register that has been quantified and prioritized according to the risk level, linking risks with the risk owners responsible for their mitigation and monitoring.

While respecting confidentiality, privacy, data protection and due process requirements, advanced technologies such as Artificial Intelligence (AI) may help Customs administration to process vast amounts of data very quickly and increase the accuracy of data analysis. AI potentially increases efficiency of all steps of risk management. It is expected that AI may also automatically collect valuable information for risk identification from open-source information. AI can take over simple and labor-intensive tasks in risk analysis such as data organization and data cleansing. In addition, AI *may calculate potential patterns of smuggling or other violation of Customs laws from the Customs' database of past cases and other existing data.*

3.7 Risk treatment

Risk treatment refers to the decisions or actions taken in response to identified risk. In the customs context, there are three generic types of responses that can be applied. These are the so-called "three t's":

- tolerate;
- treat;
- transfer.

Tolerating risk would be acceptable in many instances, for example where resources are scarce or the risk is considered to be as well managed as possible with existing controls in place, or without expending too much in terms of money or resources to reduce the impact or consequence only marginally. Tolerating or accepting a risk does not mean that the risk would not be controlled and monitored. Monitoring is often done through standard operating procedures to see whether there are any changes to the level of risk[15].

Treating risks is often the most used option by Customs in terms of managing the risks it faces in its operations. This means reducing the likelihood or consequence of risks occurring by putting in place control measures and actions that are intended to modify the level of risk to fit the organizational tolerance. Depending on the type of risk, there are often many available treatments including preventive, detective and enforcement measures. When deciding on treatments, it is important to understand the causes of risks instead of concentrating only on the symptoms. A better understanding of the risks and the causes behind them enables more informed decisions to be made about the best treatment strategy or mix of strategies to mitigate them.

Risk transfer means transferring a risk to a third party for mitigation. Risks can be transferred internally or externally. For example within a Customs administration, a risk could be transferred from Operations to IT or from human resources to operations, etc. External transfer of risks may occur in operational and non-operational environments and even at strategic levels. Operationally, risks may be transferred to another law enforcement agency, or to a sub-contractor – where sub-contractors are involved the risk transfer often entails having a legal contract or agreement in place for the work. It is important to remember that transferring risk does not necessarily mean transferring responsibility. In the first example above, if the risk is realized the senior manager in operations may still be held responsible for the risk even though IT are dealing with it.

3.8 Monitoring and review

Monitoring and review should include all aspects of the risk management process, including the performance of the risk management system, the changes that might affect it and whether the original risks remain static. Some of the questions asked at this stage could include:

[13] Sometimes risks which may have an extreme consequence, but have a very low probability may also be tolerated after proper contingency and business resumption planning is in place. This can be due to the fact that there may be no control measures for these types of risks. A risk of a natural disaster could qualify as an example of this type of risk.

- Are assumptions about risks still valid?
- Are there any new or emerging risks?
- Are treatments for minimizing risks effective and efficient?
- Are the treatments cost-effective?
- Are management and accounting controls adequate?
- Do the treatments comply with legal requirements and government and organizational policies?
- How can the system be improved?

To monitor and review the results and progress with the treatments implemented, a robust evaluation framework is needed, with criteria against which the outcomes are compared. The framework may include various measures aimed at outlining the direct and related results and effects of the chosen actions, enabling comparison of the pre- and post-treatment results. Different compliance measurement[16] activities such as campaigns, random checks or other types of statistically valid analysis methods or surveys can all be potential tools for measurement in the operational context.

3.9 Documentation, communication and consultation

Communication and consultation with internal and external stakeholders should be conducted as appropriate at each stage of the risk management process, and for the process as a whole. Communication and consultation should be planned and ongoing activities addressing not just the process, but any issues that may arise.

Good governance requires decision making that is accountable and transparent. To ensure accountability it is important that the documentation indicate why decisions were made and actions were taken. Therefore, risk management activities at all different stages of the process need to be well recorded and stored in a way that enables their retrieval:

- assumptions;
- methods used;
- data sources;
- logic and analysis;
- results; and
- decisions made and the reasoning behind them.

4. Monitoring and review of the framework

The development of evaluation and reporting mechanisms provides feedback to management and other interested parties in the administration and government-wide. Making sure that risk management activities are monitored and reviewed and that results are fed back to the policy level assists in ensuring that risk management remains effective in the long term.

Some of the monitoring and review functions could fall to functional groups in the administration

[14] More detailed information on compliance measurement can be found in Annex 2.

responsible for review and audit. Responsibility may also be assigned to managers and staff to ensure that information affecting risk is collected and effectively reported. Reporting could take place through regular management procedures and channels (performance reporting, ongoing monitoring, etc.) as part of the advisory functions associated with risk management (e.g. risk management committee).

Reporting facilitates learning and improved decision making by assessing both successes and failures, monitoring the use of resources, and disseminating information on best practices and lessons learned. When monitoring and reviewing the risk management framework, attention should be paid to:

- risk management performance against identified indicators;
- continuing confidence in risk ratings and indicators;
- suitability of the accountabilities assigned to risk owners;
- reviewing the risk management framework, policy and plan against current contexts;
- reporting on treatment of risks and subsequent utilization of plans;
- assessing the ongoing relevance of risk treatments[17]; and
- communicating feedback throughout the customs administration and to external stakeholders, if appropriate, on progress, benefits and results of risk management.

5. Continual improvement of the framework

Continual learning is fundamental to more informed and proactive decision making. It contributes to better risk management, strengthens an administration's capacity to manage risks and facilitates the integration of risk management into organizational structures and culture. Customs administrations should continually develop their risk management maturity (see Chapter 4) and ensure that information accumulated through risk mitigation activities and from the front line is utilized to keep the framework up-to-date. Based on the findings through the monitoring and review processes, decisions should be taken on how to improve the framework, risk management policy, and the strategic and operational level risk management plans.

3. EMBEDDING RISK MANAGEMENT AS AN ORGANIZATIONAL CULTURE

3.1. Introduction

Embedding risk management as an organizational culture is not always straightforward. Anecdotal

[15] This is important since if treatments are effective, they could well have an impact on the pattern of risk and become less important or even redundant. For example, if a risk treatment involves recruiting experienced auditors into the organization to combat a particular type of fraud, it can be expected that ongoing recruitment would not be necessary but an alternate method of maintaining competence levels (e.g. supplementary training or on-the-job mentoring for less experienced employees) may be more relevant.

experience provided by Members indicates that it may take several years, and requires strong ongoing commitment from managers and staff at all levels.

In the process of developing efficient risk management in the customs context a number of challenges may arise both in the internal and external framework of the Customs administrations. The importance of their understanding, recognition and quick reaction capability of the customs authorities' management directly affects the possibility of implementing a highly effective risk management system.

As indicated in Chapter 2 (Developing an organizational framework for managing risk), a holistic approach to risk management requires an ongoing assessment of potential risks for an administration at every level, and then aggregation of the results at the organizational level to facilitate priority setting and improved decision making. The identification, assessment and management of risk across customs administration helps reveal the importance of the whole, the sum of the risks and the interdependence of the parts.

Holistic management of risk requires a solid and robust organizational risk management framework empowering officers at all levels of the administration to make risk-based decisions in a structured and systematic manner. The framework allows risk management activities to be aligned with an administration’s overall objectives, corporate policies, strategic direction, operating practices and internal culture.

Therefore, developing a risk management framework and updating it regularly will support efforts of the administrations for embedding risk management as an organizational culture.

Effective risk management cannot be practised in isolation, but needs to be built into existing decision-making structures and processes. As risk management is an essential component of good management, integrating it into existing strategic management, performance measurement and operational processes will ensure that risk management is an integral part of the day-to-day activities of the administration.

Risk management maturity, on the other hand, is another tool for administrations to embed risk management as an organizational culture and enhance their risk management systems.

3.2. Risk Management Maturity

Risk management maturity, a term often used to describe organizational risk management capacity and agility, can help administrations to continuously develop their risk management practices.

Risk management maturity can be assessed in many different ways. It is suggested that administrations create a tailored measurement framework allowing them to review and develop their maturity in a structured and systematic way. Setting up such a framework involves agreeing a maturity model structure, determining measurement parameters and choosing tools for conducting the measurement.

Establishing a risk maturity model is important as it allows a common baseline to be established against which risk management practices can be benchmarked. Administrations should define and design a model that fits their unique context. Next sub-section provides an example of one potential model.

When selecting a maturity model, administrations should design measurement indicators for the key attributes used in the model. The measurement process itself can be either qualitative or quantitative, or can mix aspects of both. If quantitative measurements are used, it is important to make sure that adequate data is available to support measurement, and that the required analysis tools exist.

Measurement tools depend on the indicators the administration wishes to use and be embedded in the administration's performance measurement. Indicators allowing quantitative measurement can often be supported by data analysis and manipulation, including statistical analysis, etc. For qualitative analysis, tools such as interviews, questionnaires, surveys, audits, etc. can be used.

3.3. Example of a risk management maturity model

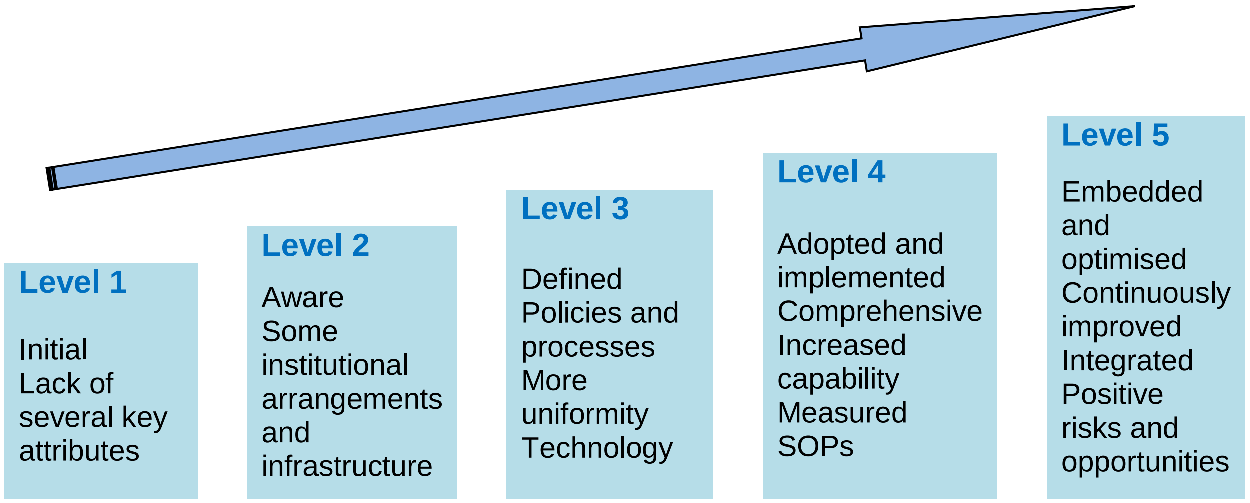
The risk management maturity model displayed in this section (diagram 9) builds on five different levels of risk management maturity (from 1 to 5) and measures maturity on seven key attributes as listed below.

1 - Legislative Framework
2 - Institutional/Organizational Arrangements
3 - Risk Management Implementation
4 - Human Resource, Training and Budget
5 - Cooperation and Information Exchange
6 - Technology Support
7 - Other Programs Supporting RM

On each of these key attributes Customs administrations may face challenges on the way of building a risk management system. Therefore, describing some of the actions needed to overcome challenges are crucial for developing organizational risk management capacity.

The following sub-sections briefly explain the different maturity stages.

Diagram 9 - RISK MANAGEMENT MATURITY LEVELS



Level 1

This is the initial stage of the risk management maturity. At this initial stage, there is growing organizational understanding of a mismatch between available resources and demand. There may not be a clear understanding of a formal risk management process, procedures and techniques even though the language and terminology may be known. At this point, there generally is a lack of a high-level mandate for risk management. This leads to risk being managed on an ad hoc basis where risk management is not applied to organizational programmes and business processes.

Level 2

At this level, the administration is aware of the importance of risk management. It knows its stakeholders and their needs. A high-level mandate for, and commitment to risk management exists. The concept and benefits of risk management are understood at relevant levels of the administration. Accountabilities for risks are defined and an initial organizational infrastructure for risk management is being developed. However, the overall approach to managing risk is still characterized by being somewhat intuitive.

Level 3

At the third level risks are well defined, and the risk management approach is standardized and rigorous. The risk management infrastructure is well established, and includes defined policy, procedures, accountabilities and culture. Operational plans including well identified risks and their management strategies are also defined. The various resources and tools for effective analysis are identified and developed, and training and awareness-raising on risk management take place continually. Operational activities are often supported by a specific risk management function or facilities, which guarantee uniformity in the application of risk management.

Level 4

At the fourth maturity level risks are effectively and efficiently managed. Risk management is embedded in all organizational processes. Risk management practices are comprehensive and a healthy risk management culture exists. Effective two-way communication about managing risk exists, where objectives and resources cascade downwards and effective feedback travels upwards. Risk management practices and outcomes are measured and monitored, and the approach is developed continuously.

Level 5

The fourth and fifth stages are quite similar to each other and represent a very high maturity of risk management. The key difference between these two levels is that at the fifth maturity level, risks are not only managed in terms of mitigating negative outcomes, but also risk management actively seeks to exploit positive risks and opportunities. Risk management practices are optimized and integrated into all organizational processes, effectively contributing to organizational objectives. High-quality intelligence and knowledge exists for decision making and decisions are based on a comprehensive understanding of risk. Risk management is an integral part of the daily work of employees at all levels of the administration.