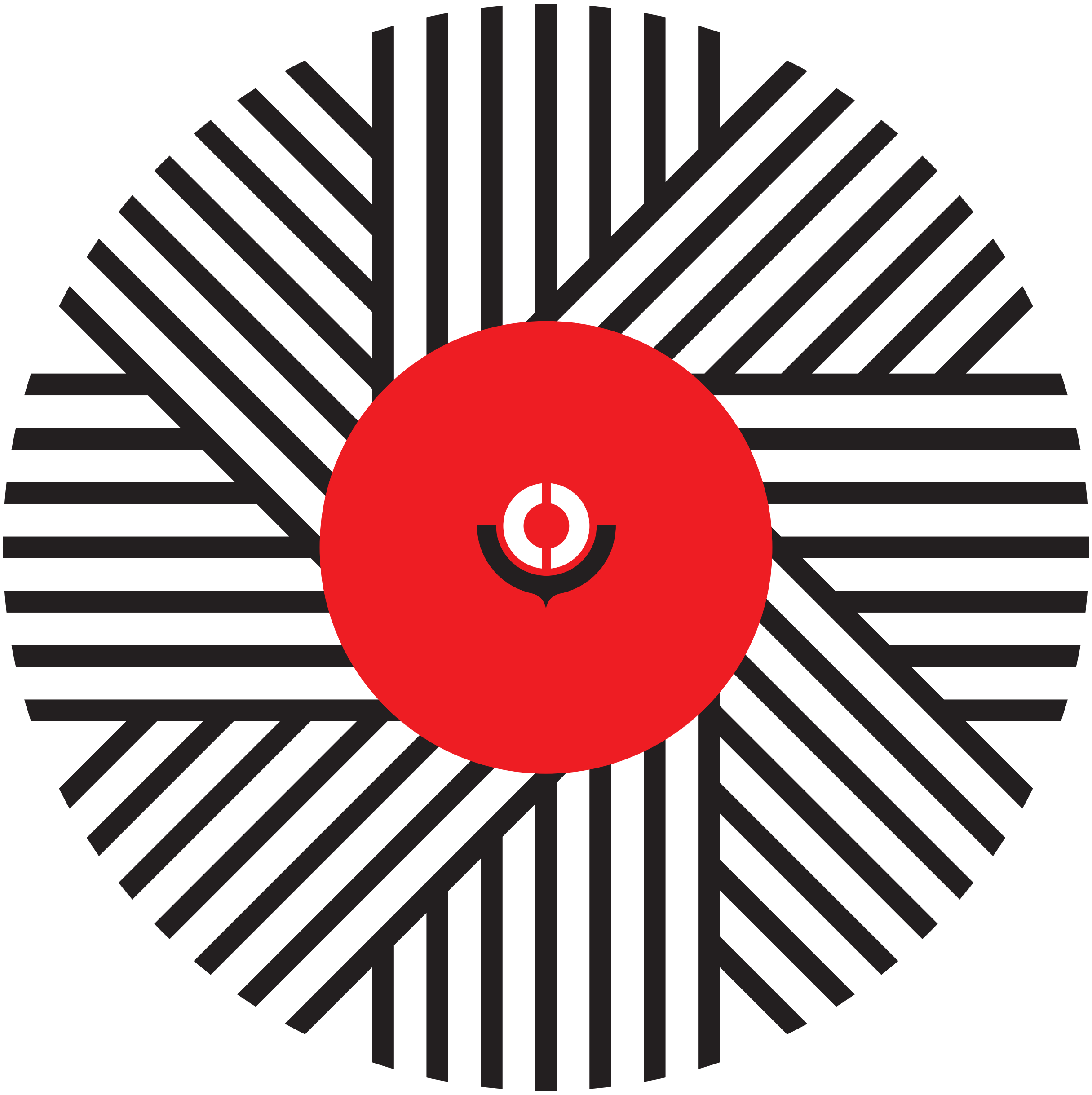
VOLUME 1



1. Risk management in the Customs context

2. Developing an organizational framework for managing risk

3. Embedding risk management as an organizational culture

4. Conclusion

RETREAD
the
THREADS
ble Thread Restorer

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, 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.[1]

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 in a way that reduces the impact of interventionist strategies as much as possible. This implies keeping the amount of intervention to the minimum necessary to achieve a policy outcome and also ensuring that regulatory requirements (red tape) are not unduly onerous or overly prescriptive.[2]

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. This is untrue and it is important to understand that control and facilitation are not mutually exclusive goals. On the contrary they are mutually reinforcing objectives and it is possible to achieve optimal levels of both.

In addition to the widening objectives of Customs, what has changed, and changed dramatically, is the trading environment – the manner in which goods are carried and traded, the speed of such transactions and the sheer volume of goods that are traded around the globe. In the past few decades there have been a number of significant changes in global trading practices, and 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 wide-bodied aircraft, shipping containers and e-commerce, and the increasing complexities of international trade agreements, have all impacted on the way in which Customs fulfills their responsibilities, and Customs administrations worldwide have seen a dramatic increase in workload across all areas of activity.[3]

The introduction of risk management techniques within Customs often comes as a result of the acknowledgement that due to increasing cross-border flows and changing government priorities, the administration is unable to continue to deliver its business operations in the same manner as previously. The realization and acknowledgement that business as usual is no longer sustainable generally means the administration will need to make a fundamental reassessment of its mission, roles and methods of operation. This often leads administrations to recognize that they can no longer interact in a physical manner with 100% of cross-border flows and need to move from traditional gate-keeper style controls towards a risk-based operating model.

To address this challenge most administrations have implemented risk selectivity and targeting[4]. However it is well recognized that a modern risk management strategy, while continuing to embrace these techniques, must go beyond selection and targeting and introduce new ways of working. This will increasingly lead administrations to adopt a holistic, risk-based compliance management approach allowing Customs to allocate its resources more effectively and efficiently on behalf of the government.

[1] Widdowson (2006), p. 2.
[2] Widdowson and Holloway (2010), p. 98.
[3] Widdowson (2006). p. 2 – 3.
[4] Selectivity and targeting will be addressed in Volume 2 of the Compendium.

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.[5]

Risk-based compliance management 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, education and awareness raising, 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 procedures 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[6]. Automation enables vast amounts of information to be processed in practically no time; it allows the effective and efficient screening of information against predetermined risk criteria, and assists with the making of decisions on both high and low risks. In the same way, modern non-intrusive inspection technologies, when used on the basis of risk assessment, can lead to more effective inspection activity and reduced delays.

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.

According to the Customs in the 21st Century strategy, the expanding responsibilities facing Customs require a more sophisticated understanding of the risk continuum and how scarce resources can be better targeted towards the higher end. Therefore, it is useful to think of the risk continuum as a method to achieve client segmentation by risk categorization. Conceptually, Customs clients can be divided into four broad-based categories:

1. those who are voluntarily compliant;
2. those that try to be compliant but do not necessarily always succeed in their endeavours;
3. those who will avoid complying if possible; and
4. those that deliberately do not comply.

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).

The key in relation to risk-based compliance management is to actively "steer" the client population towards the low-risk category. This can be

[5] Widdowson (2005), p. 93 – 94.
[6] Widdowson (2005), p. 94.

achieved both by providing incentives for traders and travellers to comply, and by operating a credible enforcement regime which effectively and efficiently detects and punishes non-compliance. 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.

In the Customs context, control and risk management of goods, conveyances or people commences at the export or departure point and continues with ongoing verification actions at the point of import or arrival and, in post-control audit circumstances, beyond. 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. 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.

At the operational level, a modern risk-based compliance 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. This is the point where intelligence holdings inform decision makers of a recommended

Diagram 1. Compliance management model

	LOW	RISK LEVEL		HIGHT
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 craft	• Advanced cargo/passenger/ craft information (in and out). • Monitoring of physical movement of all people, goods and craft across (in and out) the border	Patterns of non-compliance by: • Industry, product, location, ethnicity, destination or port of origin • Type of non compliance (e.g., incorrect documentation)	• Profile of individual non-compliant traders/travellers • Identification of specific compliance problem (e.g., bad systems, poor data entry etc)	• Profile and ongoing intelligence (on and offshore) about offenders/potential offenders and their associates
Assessment Assessment of the level of risk posed by arriving and departing people, goods and craft	• 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 (e.g., FrontLine, Call Centre) • 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 →

priority order for intervention and assist decisions about where Customs resources should be mobilized and deployed.

The WCO Global Information and Intelligence Strategy (GIIS) contained in Volume 2 sets out what intelligence is, how it is derived, for whom it is being produced, and why it is needed. GIIS also sets out the intelligence cycle and fundamental principles and processes that underpin all intelligence activity. Customs practitioners should be guided by the GIIS when developing their risk management approach.

2. DEVELOPING AN ORGANIZATIONAL FRAMEWORK FOR MANAGING RISK

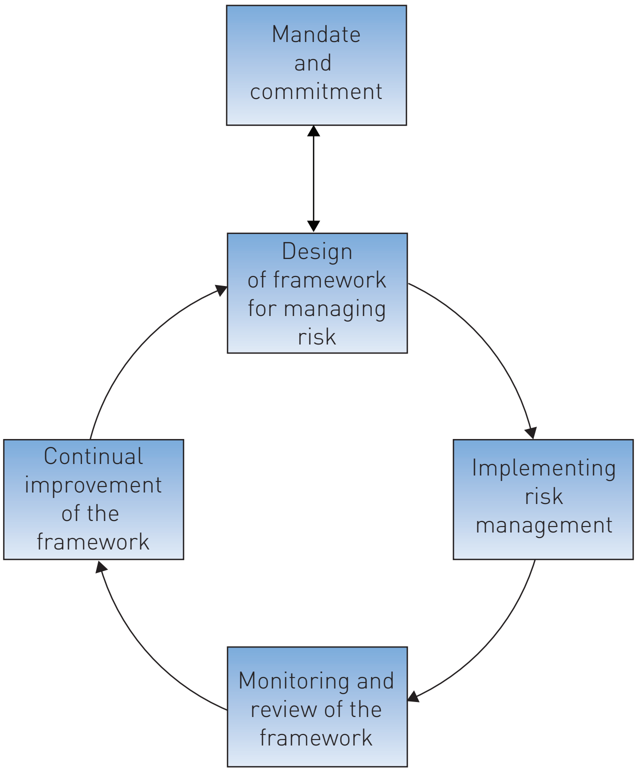
Overview

A risk-based compliance 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 an organization 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 risk[7].

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


Mandate and commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework

Source: ISO 31000:2009 Risk management – Principles and guidelines

Mandate and 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 organization. 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.

To promote understanding of, and adherence to risk management, Customs leaders must:

- adopt a risk management policy that matches organizational strategy and objectives;
- clearly articulate and communicate the risk management policy and accountabilities;
- develop risk management indicators that complement the organization's performance measurement; and

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

- ensure the risk management policy continues to be valid.

When adopting risk management, there are some general guiding principles to which the approach at all levels of the administration should adhere. These include, but are not limited to, the following[8]:

- risk management must contribute to better achievement of organizational objectives. Management of risks should improve performance in a demonstrable and measurable way;
- risk management practices are tailored and aligned with the administration's external and internal context and role;
- risk management should be embedded as an integral part of all organizational processes including strategic and business planning as well as all project and change management activities;
- risk management practices will assist decision makers to make informed choices, prioritize actions and distinguish among alternative courses of action to ensure risk treatments will be adequate and effective. It is not a magic formula that will always give the right answers. Risk management is a way of working and thinking that will give better answers to better questions. Managing risk is about acknowledging the fact that when you manage risks there is always a risk that something negative may happen;
- risk management should be systematic, structured and timely. It needs to follow a predetermined methodology that contributes to efficient, consistent, comparable and reliable outcomes;
- risk management shall always be based on best available information derived from intelligence and information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment;
- risk management shall be transparent and inclusive. It needs to take into account appropriate and timely involvement of all relevant stakeholders;
- risk management needs to be dynamic, iterative and responsive to change. As external and internal events occur, context and knowledge change, the monitoring and review of risks take place, new risks emerge, some change, and others disappear;
- risk management facilitates continual improvement of the administration. Strategies and plans should be developed and implemented to improve risk management maturity alongside all other aspects of the organization; and
- risk management should take human and cultural factors into account, recognizing the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of an administration's goals.

Senior managers play a crucial role in ensuring that an administration's organizational culture is aligned with the risk management policy and the principles outlined. Effective and efficient risk management practices can be fully materialized only when management of risks is embedded in the way "we do business around here". Senior managers should make clear to staff that they are expected to follow the risk management policy. Perceived norms and values are important in influencing a risk-sensitive and responsive culture, and senior leaders can influence organizational culture by shaping and moulding the values, basic assumptions and beliefs shared by the administration's personnel.

Once introduced, risk management requires sustained commitment to the policy and plans. The benefits of risk management are often materialized in the medium to long-term. Therefore, it is important that the same level of commitment be maintained over time. Sustained commitment can be maintained through continuously reinforcing high levels of awareness and reminding employees about the importance of managing risk.

Design of framework for managing risk

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

[8] ISO 31000: 2009 Risk management – Principles and guidelines. p. 7 – 8.

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 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:[9]

- the maturity[10], 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.

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 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 business 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);

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

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

- 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 the organization can respond or recover quickly and effectively when risks are realized.

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 organization.

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 organization. They are expected to provide leadership and support*

for risk management, ensuring at the same time that the organization meets stakeholder expectations and requirements.

Senior managers "own" the risks specific to their individual areas and are accountable for individual business unit risk management. Senior managers provide leadership and support to enable risk management objectives and principles in their business units. They also make sure that priority areas of their business 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 business.

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 business 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.

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. 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 organization at all levels with good risk management products that identify organizational risks and recommend necessary treatments.

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.

While each administration will find its own way to integrate risk management into existing decision-making structures, the following are some of the factors that may be considered:

- aligning risk management with objectives at all levels of the organization;
- introducing risk management into existing strategic planning and operational processes;
- communicating organizational directives on acceptable levels of risk; and
- improving control and accountability systems and processes to take into account risk management and its results.

The integration of risk management into decision making is supported by an organizational philosophy and culture that encourages the management of risk. This can be achieved in numerous ways, such as:

- seeking excellence in management practices, including risk management;
- encouraging managers and staff to develop skills in risk management;
- including risk management as part of performance measurement at all levels of the organization;
- introducing incentives and rewards;
- recruiting risk management expertise and capability; and
- encouraging innovation, while providing guidance and support in situations where something goes wrong.

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 organization. Good internal communication and reporting should ensure that:

- all staff know and understand what risk management is, and what their role in the process is;
- modifications to the risk governance arrangements and framework are communicated to everyone;
- outcomes of risk management are properly communicated;
- relevant information on risk management practices is available at appropriate levels in a timely manner; and
- internal consultation and feedback mechanisms exist between different levels and functions of the organization (field operations, risk analysts, investigators, regional staff, post-clearance auditors, etc.).

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:

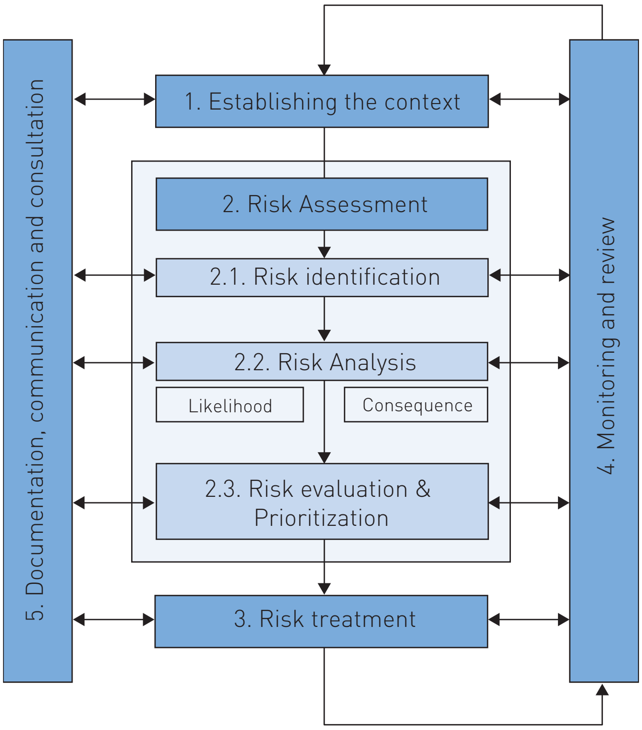
- how to involve and engage appropriate external stakeholders and give effect to their expectations and requirements, and how they are taken into account in the approach;
- how to ensure that external risk reporting will comply with national legal, regulatory and governance requirements;
- how to use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

Implementing risk management

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



Source: adapted from Revised Kyoto Convention General Annex Guideline 6 and ISO Standard 31000:2009 Risk management – Principles and guidelines

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[11]. 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.

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 organization 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.

Example

In a hypothetical example the Director General of Country X Customs service calls the heads of his administration's four organizational divisions (Head of Revenue Collection and International Trade Head of Community Protection and Security Head of Operations and Head of Administration) and their deputies to a risk management workshop. The aim of the workshop is to conduct a strategic review and identify risks that may prevent the service from achieving its goals. The main objectives of the organization relate to revenue collection ensuring community protection and security and ensuring compliance with the laws and regulations administered by Customs in a way that guarantees facilitation of trade.

Prior to the meeting the Heads of the three operational divisions were required to circulate relevant

[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.

reports from their divisions. Thus the Head of Operations was tasked with circulating a summary report of seizures investigations and court cases. The Head of Revenue Collection and International Trade provided an update on AEO applications and compliance as well as trade statistics. The Head of Community Protection & Security provided a report on examinations and on statistics reported by other border control agencies and the police. The Intelligence Unit assisted with the preparation of all summary reports by the Head of Administration.

After setting the parameters and context for the process the group uses historical data and awareness of the various programmes to identify the major organizational risks utilizing brainstorming techniques.

The major risks are divided into "Risk Areas" and the key risks under each area are identified as follows:

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

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 4 suggests possible descriptions and indicators for estimating the likelihood of a risk occurring.

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

Repeating this exercise on a regular basis (annually in the organizational and business 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,

Diagram 4. Example description and indicators for determining likelihood

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

Diagram 5. Example description and indicators for determining significance of consequences

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 organization
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

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

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

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 6 represents an example of a simple 3x3 risk significance matrix[12].

The evaluation enables Customs to better understand the risks. The process consists of deciding

Diagram 6. An example of a Risk Significance Matrix (3x3)

High	Medium	High	High
Consequence	Low	Medium	High
Low	Low	Low	Medium
	Low	Likelihood	High

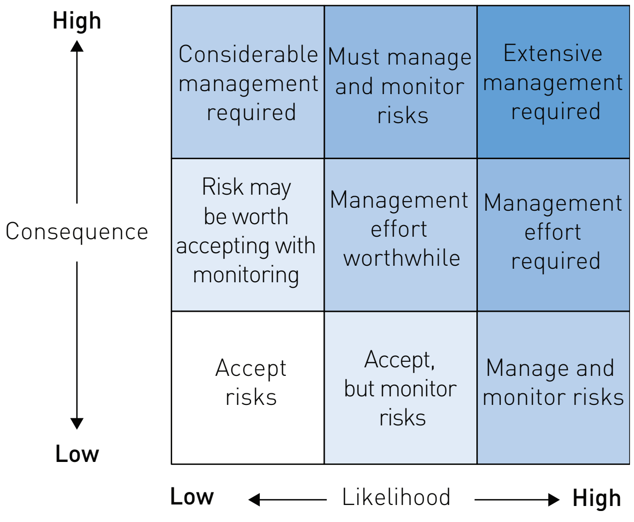
[12] Some Members may decide that there is a need for more detailed tolerance estimation beyond "high, medium or low". There are examples in the Capacity Building Compendium of a 4x4 matrix and a 5x5 matrix. In the case of a 5x5 matrix the tolerances may be expressed as minor, acceptable, tolerable, 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.

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 6 it may be necessary to group a tolerability result and add specific response criteria for different categories.

Diagram 7. 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.

Example

This stage would see the Workshop participants evaluating and prioritizing the identified and analyzed risks for response. The process is recorded in a prioritized risk register which links the risks to the respective risk owners. The register would form part of the organizational risk management plan and serve as a guide for an administration's risk management activities. The prioritized risk register would allow senior managers to convene meetings with their relevant managers and supervisors to consider control strategies.

	Objective	Risks	Likelihood	Consequence	Significance	Risk Owner
1	Effective and efficient collection of revenue	1.1 Fraud	H	H	High	Head of Operations
		1.2 Lack of staff competence	M	M	Medium	Head of Revenue Collection and International Trade
		1.3 Integrity	L	L	Low	Head of Administration
2	Community protection and security	2.1 Narcotics	H	M	High	Head of Community Protection and Security
		2.2 Illegal importation of weapons and ammunition	L	M	Low	Head of Community Protection and Security
		2.3 IPR	M	L	Low	Head of Community Protection and Security
3	Trade facilitation	3.1 Ineffective procedures	L	H	Medium	Head of Revenue Collection and International Trade
		3.2 Lack of coordination with other agencies	H	H	High	Head of Operations
		3.3 IT failure	L	H	Medium	Head of Administration

Risk treatment

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

- tolerate;
- treat;
- transfer; or
- terminate.

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[13].

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 subcontractors 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.

Termination means avoiding a risk by deciding to discontinue or no longer pursue an activity that may cause the risk to be realized.

Example

Based on evaluation and prioritization, the risks would be further analyzed and seconded for response decisions. Once different response options have been considered, the identified risk owners are responsible for creating more detailed treatment plans to mitigate the risks.

	Objective	Risks	Likelihood	Consequence	Significance	Risk Owner	Treatment
1	Effective and efficient collection of revenue	1.1 Fraud	H	H	High	Head of Operations	Treat: A thorough mitigation strategy and plan needed
		1.2 Lack of staff competence	M	M	Medium	Head of Revenue Collection and International Trade	Tolerate once additional training to the staff is provided. Monitor continuously.
		1.3 Integrity	L	L	Low	Head of Administration	Tolerate: Monitor through SOPs

[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.

	Objective	Risks	Likelihood	Consequence	Significance	Risk Owner	Treatment
2	Community protection and security	2.1 Narcotics	H	M	High	Head of Community Protection and Security	Treat: A thorough mitigation strategy and plan needed
		2.2 Illegal importation of weapons and ammunition	L	M	Low	Head of Community Protection and Security	Tolerate: Monitor continuously through SOPs.
		2.3 IPR	M	L	Low	Head of Community Protection and Security	Tolerate after raising awareness among public. Monitor through SOPs
3	Trade facilitation	3.1 Ineffective procedures	L	H	Medium	Head of Revenue Collection and International Trade	Tolerate after a thorough review and alignment against international best practices.
		3.2 Lack of coordination with other agencies	H	H	High	Head of Operations	Treat: A thorough coordination and stakeholder engagement strategy and plan needed
		3.3 IT failure	L	H	Medium	Head of Administration	Transfer to a third party service provider. Create a contingency plan.

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:

- 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[14] 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.

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

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

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.

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 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[15]; and
- communicating feedback throughout the organization and to external stakeholders, if appropriate, on progress, benefits and results of risk management.

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.

Summary

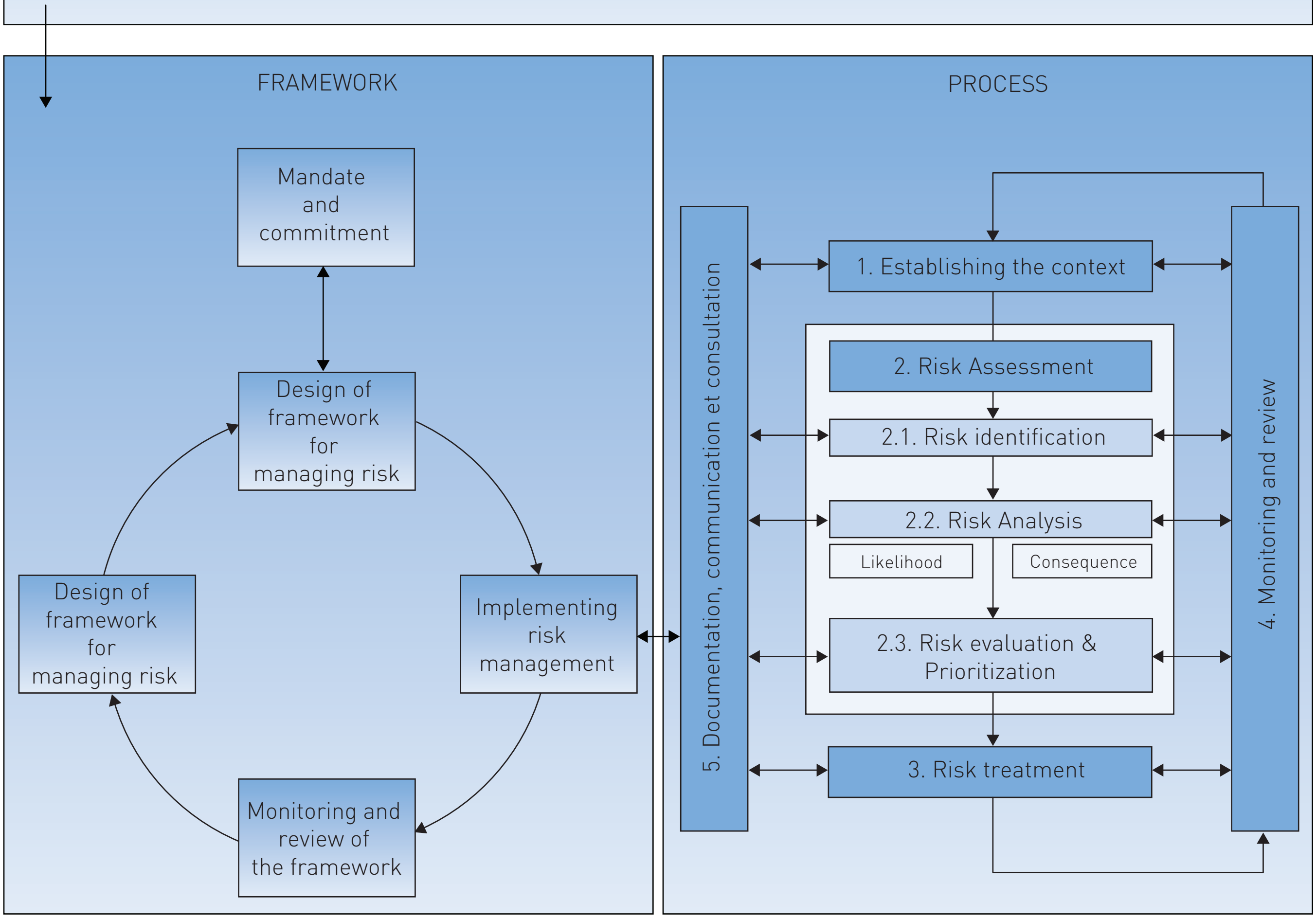
This chapter introduced the different components of an organizational risk management framework and outlined a common methodology and process for managing risk. Diagram 8 summarizes the aspects outlined in this chapter and illustrates the relationship between the components of the framework.

[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.

Diagram 8. Risk management “architecture”

PRINCIPLES

- Contribute to the achievement of objectives and improve performance;
- Be tailored and aligned with the administration’s external and internal context and role;
- Be an integral part of all organizational processes;
- Be part of all the decision-making processes;
- Be systematic, structured and timely;
- Based on best available information;
- Be transparent and inclusive;
- Be dynamic, iterative and responsive to change;
- Facilitate continual improvement; and
- Take into account human and cultural factors recognizing capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of authority’s goals.


FRAMEWORK
Mandate and commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Design of framework for managing risk
PROCESS
5. Documentation, communication et consultation
1. Establishing the context
2. Risk Assessment
2.1. Risk identification
2.2. Risk Analysis
Likelihood
Consequence
2.3. Risk evaluation & Prioritization
3. Risk treatment
4. Monitoring and review

Source: ISO Standard 31000:2009 Risk management – Principles and guidelines

3. EMBEDDING RISK MANAGEMENT AS AN ORGANIZATIONAL CULTURE

Risk management maturity

Embedding risk management as an organizational culture is not always straightforward. Anecdotal experience provided by Members indicates that it may take several years, and requires strong ongoing commitment from managers and staff at all levels. 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 and Annex 3 incorporates another template for this purpose (APEC risk management process self-assessment 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. 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.

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 (naïve, aware, defined, managed, enabled) and measures maturity on several key attributes (culture, process, infrastructure). The following sub-sections briefly explain the different maturity stages[16] and describe some of the actions needed when developing organizational risk management capacity.

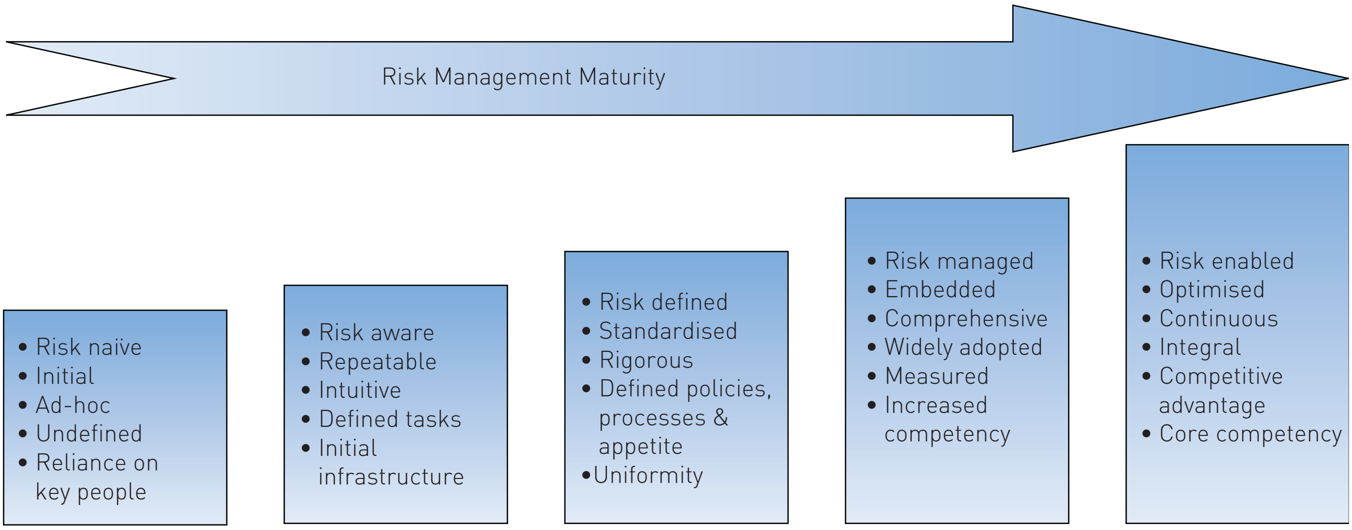
"Naïve"

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 in a systematic way.

In order to move to the next level of risk management maturity, a number of actions must take place. Some of these actions may include the following:

- obtaining highest organizational mandate and commitment to risk management;
- objectives of risk management implementation need to be established, to enable the risk process to be tailored and scoped accordingly;
- defining key accountabilities and risk ownership;
- adequate training and support for the key risk owners;
- undertaking awareness briefings to sell the vision of risk management and its potential benefits to the entire organization, from senior management to front-line employees. These awareness briefings should also include key stakeholders;
- nominate pilot applications for risk management, carefully selected to maximize the chances of early success;
- communication of successes. Seek to develop momentum in the risk process and to encourage other projects and individuals to apply risk management to their areas as they see that clear benefits have been articulated clearly;
- planning for the long term, recognizing that effective implementation of risk management

Diagram 9. An example of a risk management maturity model



Source: Netherlands Customs 2010

[16] The interpretation of the model has been performed by the Secretariat.

will not be achieved overnight. Count the cost of the implementation project, and ensure commitment of the necessary resources before starting;

- building effective controls into the process from the outset, with breakpoints to enable progress to be monitored and reviewed at key intervals. Collect and trend appropriate metrics; and
- consider producing draft risk procedures with templates for key inputs and outputs.

"Aware"

At this second maturity level, the organization is aware of its mission, objectives and related risks. 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 all levels of the organization. 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.

The actions for moving to the next level of risk maturity may include some of the following:

- reinforcing and strengthening corporate backing for the implementation of the risk management process. Strong and visible commitment from senior management is essential to give the necessary credibility;
- developing and promulgating an organizational policy on the use of risk management;
- formalizing the risk management process, with clear definition of the scope and objectives of risk management, as well as agreed upon procedures and properly selected tools;
- providing formal risk training to managers and staff and encouraging them to attend ongoing risk management training courses, conferences and seminars, workshops, etc;
- allocating adequate resources to the risk management implementation process, with assignment or recruitment of sufficient staff, and assigned budgets for risk management training, risk assessment tools and other required risk management activities;
- selecting key projects to demonstrate the benefits of risk management in all areas of the organization's business;
- communicating success and encouraging wider application of risk management in other areas as benefits become clear;
- ensuring managers use risk management as part of their routine management of projects and business processes. Include regular risk reporting as an important part of management reviews;
- assembling metrics from the risk process; identification of generic risks, effective responses, the cost of risk reduction, etc; and
- creating checklists to facilitate risk identification and assessment processes, based on actual experience of risk management within the organization.

"Defined"

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.

The actions that assist an administration to progress from the third maturity level to the fourth may include some of the following:

- ensuring effective learning from experience. Undertaking regular reviews of the risk management process, with value engineering of the process to ensure that it remains fully effective;
- amending and strengthening the risk management process where necessary, including investment in new tools, new methods, personnel training, etc;

- investigating novel applications of the risk management process beyond those already covered. Seeking to modify and apply risk management to every activity within the organization;
- using every means possible to develop a true risk management culture, encouraging all personnel to think risk, be aware of uncertainty and use risk techniques to assess and manage potential threats;
- ensuring that risk is included as a routine criterion in all decision making;
- identifying and countering incidences of risk fatigue, where staff are losing interest in the process or there is a potential loss of momentum. Using regular re-launch promotions to renew the process, celebrating successes, publicizing improvement metrics, and rewarding effective risk management; and
- organizing regular risk management training to ensure that skills remain current.

"Managed"

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.

Moving from the fourth maturity level to the fifth requires:

- ensuring continued commitment of senior management;
- using audit and review techniques to keep the application of risk management techniques at the required quality and standard;
- taking full advantage of the competitive edge that results from proactive management of uncertainty (including both risks and opportunities);
- extending risk management beyond the usual applications, pioneering its use in all areas of the business;
- continually investing in improving the risk process, tools, techniques, personnel skills, etc; and
- continuing involvement and consultation with stakeholders of the risk management process.

"Enabled"

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 organization.

CUSTOMS

4. CONCLUSION

The changing operating environment has affected the way Customs administrations go about their business. The sheer volume of cross-border transactions, together with the new functions that Customs administrations all over the world have been assuming, have made old operating models largely redundant and required a new approach. As a result Customs administrations are required to achieve a reasonable and equitable balance between ensuring compliance and minimizing disruption and cost to legitimate trade and the public. This can be achieved increasingly through the adoption of a holistic risk-based compliance management approach.

Intelligence-enabled risk management is a crucial building block for an effective risk-based compliance management approach. Traditionally Customs risk management has been seen through operational selectivity/targeting practices. However, this Compendium proposes a more holistic compliance management approach going beyond selectivity and aiming at actively managing and improving compliance (affecting client behaviour) through a bundle of different strategies mixing incentivized voluntary and enforced measures. Through this approach administrations are better able to achieve sustainable compliance outcomes that enable them to facilitate low risks and target the bulk of their scarce control resources towards high risks or unknown areas.

The adoption of a risk-based compliance management approach requires the creation of a robust organizational risk management framework which provides the foundation and organizational arrangements allowing individual risks to be identified, assessed and managed across the organization and empowers officers at all levels to make risk-based decisions in a structured and systematic manner. This Volume of the Compendium has outlined the key aspects of such a framework.

For risk management to be effective, it needs to be aligned with an administration's overall objectives, corporate focus, strategic direction, operating practices and internal culture. In order to ensure that risk management is a consideration in priority setting and resource allocation, it has to be part of existing governance and decision-making structures at both the operational and strategic levels.

The ultimate success of risk management activities often comes down to the question of how well risk management can be embedded as an organizational culture. Effective organizational risk management practices often will not be established overnight, and in fact may require several years and strong ongoing commitment from managers and staff at all levels of the administration.

Many of the skills and resources needed to manage risk effectively already exist within Customs. Sometimes these resources may need to be better organized in order to deliver a more structured approach to managing risks. Customs administrations are encouraged to monitor, review and assess their risk management practices and continuously develop their risk management capacity based on the guidance outlined in this Volume.

The annexes to this Volume introduce a number of practical tools that can be used to facilitate the implementation of risk management. One of the annexes (Annex 5) also includes case studies by Members, providing useful information on different aspects of risk management.

RESANDE FRÅN LAND UTANFÖR EU
UTAN VAROR ATT DEKLARERA
NON INTRA-COMMUNITY TRAVELLERS
NOTHING TO DECLARE
HM King Carl XVI Gustaf
HM Queen Silvia

5. BIBLIOGRAPHY

AS/NZS 4360:2004. "Risk management" Standards Australia/Standards New Zealand.

International Convention on the Simplification and Harmonization of Customs Procedures (Revised Kyoto Convention), WCO, Brussels.

ISO/IEC Standard 73:2009 *Vocabulary*

ISO/IEC Standard 31000:2009 *Risk management – Principles and guidelines*

ISO/IEC Standard 31010:2009 *Risk management – Risk assessment techniques*

Widdowson, David and Holloway, Stephen (2010) 'Core border management disciplines: risk based compliance management' pp.95-113 in: McLinden, Gerard; Fanta, Enrique; Widdowson, David and Doyle, Tom Border Management Modernization, The World Bank, Washington, DC.

Widdowson, D. (2006). "Raising the Portcullis." Paper presented at the WCO Conference on developing the Relationship between WCO, Universities and Research Establishments, Brussels.

Widdowson, D. (2005). "Managing risk in the Customs context" in De Wulf, L. and Sokol, J.B. (2005), Customs Modernization Handbook, The World Bank, Washington D.C.

World Customs Organization (2008) Customs in the 21st Century: Enhancing Growth and Development through Trade Facilitation and Border Security, WCO, Brussels

World Customs Organization (2005) The SAFE Framework of Standards to secure and facilitate global trade, WCO, Brussels.

SEABOARD SPIRIT
SEABOARD
392759
U.S. Customs and Border Protection

ANNEXES

ANNEX 1: RISK MANAGEMENT TECHNIQUES AND TOOLS

There are many different tools and techniques to assist the various steps of the risk assessment process. More detailed information on these tools can be found in ISO Standard 31010:2009 "Risk management – Risk assessment techniques".

Risk identification

Techniques

The above-mentioned ISO Standard 31010:2009 lists the following techniques that can be used in the identification of risks[17]:

- Brainstorming;
- The Delphi technique;
- Structured or semi-structured interviews;
- Use of check-lists;
- Primary hazard analysis;
- Hazard and Operability Studies (HAZOP);
- Hazard Analysis and Critical Control (HACCP);
- Environmental risk assessment;
- Scenario analysis;
- Structure "What if?" (SWIFT);
- Failure mode effect analysis;
- Cause-and-effect analysis;
- Human reliability analysis;
- Reliability centred maintenance;
- Consequence/probability matrix; and
- Fault tree analysis.

Instead of using only one technique, a combination of different tools should be used where appropriate. It is also important to combine aspects of qualitative and quantitative analysis in order to reach the best outcomes.

Tools

As previously shown, a risk register is an essential documentation tool for risk management. The risk register is like an "index" of an administration's risks, from which each functional area can develop its respective risk plans. The register should be tailored to meet the requirements of the organization and may be set out in many different ways. Three examples of risk registers appear below.

Example #1 of 3 RISK MANAGEMENT REGISTER: ORGANIZATIONAL ELEMENTS

	The Risk	*Likelihood* Rating	*Consequence* Rating	Tolerance	Risk Priority	Risk Treatment
1	Strategic Management					
2	Resources					
3	Legal Framework					
4	Customs Systems and Procedures					
5	Information Technology and Communication					
6	External Cooperation, Communication and Partnership					
7	Good Governance					

[17] ISO Standard 31010:2009 "Risk management – Risk assessment techniques" includes additional details on the above-mentioned techniques.

Example #2of 3 RISK MANAGEMENT REGISTER: ORGANIZATIONAL PRIORITY

	The Risk	*Likelihood* Rating	*Consequence* Rating	Tolerance	Risk Priority	Risk Treatment
1	Revenue Collection					
1.1	e.g. Duty					
1.2	e.g. Excise					
2	National Security					
3	Community Protection					
3.1	e.g. Narcotics					
3.2	e.g. IPR					
4	Trade Facilitation					
5	Collecting Trade Data					

Example #3 of 3 -RISK MANAGEMENT REGISTER: ORGANIZATIONAL STRUCTURE

	The Risk	*Likelihood* Rating	*Consequence* Rating	Tolerance	Risk Priority	Risk Treatment
1	Head Office / Corporate					
	e.g. Personnel					
	e.g. Legislation					
	e.g. Finance					
2	Maritime					
	e.g. Wharf / Port offices					
	e.g. Sea Cargo					
	e.g. Sea Passengers / Crew					
	e.g. Vessels					
3	Aviation					
	e.g. Airports					
	e.g. Air Cargo					
	e.g. Air Passengers / Crew					
	e.g. Aircraft					
4	Land					
	e.g. Border control points					
	e.g. Conveyances					

Risk analysis

Techniques

Various techniques and tools for the risk analysis process are recognized by ISO Standard 31010:2009 "Risk management – Risk assessment techniques". These tools can be categorized with reference to their usability for analyzing consequences, likelihood or the level of risk.

Box 2: Risk analysis techniques

Technique	Consequence	Likelihood	Level of risk
Bayesian statistics and Bayes nets	✓		
Bow tie analysis		✓	✓
Cause-and-consequence analysis	✓	✓	
Cause-and-effect analysis	✓		
Consequence/probability matrix	✓	✓	✓
Cost/benefit analysis	✓		
Decision tree	✓	✓	
Environmental risk assessment	✓	✓	✓
Event tree analysis	✓		
Failure mode effect analysis	✓	✓	✓
Fault tree analysis		✓	
FN curves	✓	✓	
Hazard Analysis and Critical Control (HACCP)	✓		
Hazard and Operability Studies (HAZOP)	✓		
Human reliability analysis	✓	✓	✓
Layer protection analysis	✓		
Markov analysis	✓		
Multi-criteria decision analysis	✓		✓
Reliability centered maintenance		✓	✓
Risk Indices	✓	✓	
Root cause analysis		✓	✓
Scenario analysis	✓		
Structure "What if?" (SWIFT)	✓	✓	✓

Tools

The previous chapter presented some simple 3x3 examples of consequence and likelihood matrices. The following tables provide additional examples of 5x5 scales and their attributes.

EXAMPLE OF A 5x5 LIKELIHOOD SCALE

	Example of Qualitative Measure	Examples of Quantitative Measures				Other Measures
Almost Certain	The event is expected to occur in most circumstances	Once per week or more frequently	10 chances a year	> 1 in 10	9 to 10 times out of 10 occurrences	If these scales do not match your circumstance, then you should develop your own scale
Likely	The event will probably occur in most circumstances	On average once per month	Once a year or more	1 in 10-100	7 to 8 times out of 10 occurrences	
Possible	The event might occur at some time	On average once per year	Once in ten chances a year	1 in 100 – 1,000	4 to 6 times out of 10 occurrences	
Unlikely	The event is not expected to occur in most circumstances	Typically once every ten years	One in 100 chances a year	1 in 1,000 – 10,000	2 to 3 times out of 10 occurrences	
Rare	The event may occur only in exceptional circumstances	Typically once every hundred years	One in 1,000 chances a year	1 in 10,000 – 100,000	0 to 1 times out of 10 occurrences	

New Zealand Customs Service Example of A 5x5 LIKELIHOOD scale

Rating	How likely	Description / Example *
5	Almost Certain	• **Definite probability, or** • **No Controls, or** • **Has happened** in the past and **no compensating controls** have been **implemented**, or Without additional controls the event is **expected to occur in most circumstances, or** • Has happened **within the last 3 months**
4	Likely	• The event will **probably occur** in **most circumstances**, or • **Weak Controls** e.g. Limited QAPs, no internal audits performed**,** or • **With existing controls** in place this event will probably **still occur with some certainty, or** • Has **happened in the last 6 months**
3	Possible	• The event **should occur in some circumstances**, or • **Minimal controls**, e.g. Some QAPs, some internal audits performed, or • The event **has occurred in other customs agencies** with similar levels of controls in place, i.e. substandard control assurance, or • Has **happened in the last 12 months**
2	Unlikely	• The event **could occur** in some circumstances, however more **likely through human error** for not following the control environment, or • **Effective Controls** in place, e.g. Timely QAPs, internal & external audits, or • The event **hasn't occurred in Customs** recently but it could occur in some circumstances, or • Has **happened in the last 2 years**
1	Rare	• The event **may occur in some exceptional circumstances**, i.e. deliberate fraud / attack outside of existing deterrents, or from activity beyond the control of Customs actions, or • **Strong Controls.** Despite effective controls an external event or **uncontrollable event** could occur, or • **Improbable:** A very small chance of an event occurring that would be caused by stressed economic, market and operating conditions or events **not previously seen in similar agencies**, or • Has **not happened in the last 3 years**

EXAMPLE OF A 5x5 CONSEQUENCE SCALE

	SEVERITY OF RISK				
Risk*	**Insignificant**	**Minor**	**Moderate**	**Major**	**Severe**
Cargo/ Passengers	Rare for passenger clearance targets not to be met. Few clients are affected by delays. Air and sea cargo delays are causing insignificant financial and community impact.	Passenger clearance targets sometimes not met. Air and sea cargo delays are causing minor financial and community impact.	Passenger clearance delays are occurring, causing moderate disruption to the client. Air and sea cargo delays are causing moderate financial and community impact.	Passenger clearance delays are occurring, causing major disruption to the client. Air and sea cargo delays are causing major financial and community impact.	Passenger clearance delays are occurring, causing severe disruption to the client. Air and sea cargo delays are causing severe financial and community impact.
Border Enforcement	Rare for non-compliers to avoid detection and action. This applies particularly for serious offences under Customs Act and other agency's legislation enforced by Customs.	Unlikely that non-compliers will avoid detection and action. This applies particularly for serious offences under Customs Act and other agency's legislation enforced by Customs.	Possible that non-compliers will avoid detection and action. This applies particularly for serious offences under Customs Act and other agency's legislation enforced by Customs.	Highly likely that non-compliers will avoid detection and action. This applies particularly for serious offences under Customs Act and other agency's legislation enforced by Customs.	Almost certain that non-compliers will avoid detection and action. This applies particularly for serious offences under Customs Act and other agency's legislation enforced by Customs.
Revenue collection	Collections against revenue forecast are under target and it could be justified by statistical error.	Collections against revenue forecast are under target but only by a small amount.	Collections against revenue forecast are under target, and the shortfall is not linked to general economic conditions.	Collections against revenue forecast are unexpectedly and/or significantly under target. The shortfall cannot be linked to general economic conditions. An explanation may be required for Parliament and Government.	Collections against revenue forecast are unexpectedly and/or significantly under target. The shortfall cannot be linked to general economic conditions. It is possible that Parliament and/or Government will initiate an enquiry into the shortfall.

Risk evaluation and prioritization

Techniques

There are a number of risk analysis models in business literature for use when evaluating and prioritizing tolerance for risk. These include:

- Threat analysis;
- SWOT analysis (Strengths, Weaknesses, Opportunities, Threats);
- Fault tree analysis;
- FMEA (Failure Mode & Effect Analysis);
- BPEST (Business, Political, Economic, Social, Technological) analysis;
- PESTLE (Political Economic Social Technical Legal Environmental);
- Dependency modeling and Real Option Modeling; and
- Statistical Modelling.

Tools

Risk criteria are terms of reference against which the significance of a risk is evaluated. They are defined when establishing the context for the risk management process, and before risk identification takes place. Risk criteria often take the form of a risk significance or tolerance matrix. It is important to note here that risk criteria must be based on organizational objectives, and the external and internal context. They can be derived from standards, laws, policies and other requirements. The following diagram presents a potential example of a 5x5 risk tolerance/significance matrix.

EXAMPLES OF A 5x5 RISK TOLERANCE MATRIX

	Minimal 1	Minor 2	Moderate 3	Major 4	Severe 5
Almost Certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

	Minimal	Minor	Moderate	Major	Severe
Almost Certain	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
Likely	LOW	MEDIUM	HIGH	EXTREME	EXTREME
Possible	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Unlikely	LOW	LOW	MEDIUM	MEDIUM	HIGH
Rare	LOW	LOW	LOW	LOW	MEDIUM

MAN EXPRESS CARGO
JES MUDANZAS ALMACENAJES
CapMax 6099
DIRECT INJECTION DIESEL
800★KRT

ANNEX 2: COMPLIANCE MEASUREMENT

Overview

For any risk management process to be successful and effective, it will have to be constantly monitored and evaluated. One method for this is the use of compliance measurement. "Compliance measurement" is a phrase used when statistically valid random sampling techniques are employed to determine the degree to which traders, carriers, imported goods, etc. conform to Customs rules and procedures. When designed in a systematic and appropriate manner, compliance measurement methodologies provide objective and statistically valid results. Compliance measurement can be used as a diagnostic tool to identify areas of non-compliance.

Compliance measurement as a diagnostic tool for Customs administrations should be used in conjunction with risk assessment, profiling and other targeting procedures. Used strategically, compliance measurement and targeting can provide the necessary balance to help focus resources effectively in areas of concern to Customs. In addition, the results of initial compliance measurements can provide important information to enhance risk assessment methodologies.

A compliance management programme also provides a basis for Customs to assess its own performance in revenue protection and enforcement of laws, improve its efficiency and effectiveness, and develop strategies to improve compliance.

Compliance Measurement Areas

One approach to compliance measurement is to consider that in some countries or economic unions, as few as 10% of traders account for over 80% of imports and exports. By focusing on the top 5-10% of these highest volume manufacturers, importers, exporters and commodities, Customs can ensure that those which have the most significant impact on the national economy are being reviewed more effectively.

Compliance measurement areas may include:

Documentary issues:

- proper tariff classification by traders;
- proper valuation by traders; and
- country of origin.

Procedural issues:

- importation and exportation (from the goods declaration through revenue collection);
- transit operations; and
- warehousing, free trade zones, processing.

Revenue issues:

- timely and accurate revenue payments; and
- proper posting of securities.

Transport issues:

- accurate reporting of the quantity of goods;
- accurate description of goods on the manifest and/or transport document;
- accuracy of container quantities and identification numbers; and
- transporter compliance.

Specific concerns:

- compliance by tariff number or range of tariff numbers;
- public health and safety issues;
- Intellectual property rights and copyright issues;
- compliance with trade agreements;
- proper country of origin marking on goods;
- high revenue commodities; and
- selected traders.

Measurement Process

Customs gathers data from a variety of sources, both internal and external, and by both manual and automated means. With the data (import and export records), the tools (statistical analysis) and the methodology (systematic analysis of large traders or commodities), Customs can arrive at reasonable, informed conclusions about the compliance rates of many entities. These rates can be determined for each step of a transaction process, e.g. for imports, from the manifest to the goods declaration to the collection of duty and taxes. The automated systems that Customs uses to evaluate high-risk shipments can support the compliance review requirements for a scientific approach to accurate data collection and analysis and projections, although compliance rates can also be measured effectively without automation.

Customs should determine a designated universe of transactions and, using a statistically valid sampling methodology, select specific transactions or entities from this universe for review or verification. Depending upon the results, the universe may be modified in many ways.

Customs must also determine what level of compliance is acceptable. For example, a compliance rate of 95% of the transactions or entities reviewed in a given area may be the acceptable level for an administration. This may also be called the level of tolerance.

Some of the transaction processes for compliance verifications would be :

- goods declaration compliance;
- trader compliance;
- transit compliance;
- free trade zone or warehouse compliance;
- manifest and transport document compliance ; and
- transporter compliance.

Below are a few factors that should be considered during a verification review for a selected example of these processes.

Goods Declaration Compliance

a) Is there evidence of documentation to support an accurate goods declaration?

b) Do the quantities declared match what is contained in the consignment?

c) Does the declared country of origin match the country of origin marking on the goods?

d) Does the declared description of the goods match the actual goods?

Thus, a typical compliance measurement review relating to intellectual property rights for a selected commodity, at a tolerance level of 95%, might progress as follows :

a) Conduct a statistically valid random sampling of goods declarations for the selected HS number.

b) If the resulting compliance rate is less than 95%, conduct another measurement of the same HS number, but stratified by selected countries of origin.

c) For countries of origin found to have a compliance rate of less than 95%, conduct a measurement for each of the major importers.

d) For importers found to have a compliance rate of less than 95%, Customs should seek to:

- inform the importer ("informed compliance");
- establish profiles/targets for the identified areas of non-compliance;
- conduct subsequent measurements to ensure that the importer has corrected the problem;
- conduct more reviews and/or examinations; and
- issue fines or penalties, if appropriate, in cases of continued non-compliance.

Use of Compliance Measurement Results within the Control Programme

Statistically valid compliance measurement procedures can be used in various ways, e.g. to:

- define any revenue gap;
- prevent widespread commercial fraud;
- assess performance by major key industries;
- assess performance by major importers and exporters;
- increase commercial compliance; and
- accurately measure international trade.

The results of these measurements can help direct resources effectively. In determining compliance rates for individual importers, those found to have high compliance rates may have their goods examined less frequently, while those having low compliance rates may have their goods examined more frequently.

The findings of compliance reviews for commodities, traders and industries provide information for updating existing selectivity criteria used to target high-risk transactions, as well as for the overall effectiveness of an administration's risk management programme. In addition, they contribute significantly towards determining trends and issues relating to specific industry sectors and should result in focused, up-to-the-minute analytical information being available to assist Customs officers in their daily activities.

ANNEX 3: APEC RISK MANAGEMENT PROCESS SELF-ASSESSMENT

Box 3 outlines and explains the APEC Risk Management Process Self-Assessment model.

Box 3: APEC Risk Management Process Self-Assessment

	Purpose/ Context/Scope	Risk Management Concept	Data	Analysis	Employee Investment
INTEGRATION	Our stakeholders are advocates of our service	Risk management effectively contributes to organisational outcomes	High quality data is available for decision making	Decisions are based on comprehensive understanding of the risk	Risk management is integral to daily work
	Continuous communication with stakeholders is maintained and the organisation expresses a willingness to consider change	Results are measured and reviewed to promote continuous improvement and informed decision making	Best practices are shared and incorporated	Best practices of analysis are shared and incorporated	Review and update role and competencies of employees against work Identify gaps in skill sets and address
ADAPTATION	We constantly review changes to our context and adapt our processes to our stakeholders requirements where appropriate	Risk management is a theme in other management activities and processes	Data reflects changing requirements	Analysis methods adapt to meet changing requirements	Updated skill sets reflect changing organisational needs
	Communication with stakeholders Monitor context Continuously review current processes	Review other management activities and processes to ensure risk management is integrated i.e., project management strategic and corporate planning, resource allocation	Review data requirements in response to changes in context	Review analytical effectiveness and make adjustments as appropriate	Monitor context Continuously review processes Consider process revisions Train employees as appropriate

	Purpose/ Context/Scope	Risk Management Concept	Data	Analysis	Employee Investment
FOCUS	We determine the processes that could be changed and the consequential risk to the mission and goals of Customs	Specific elements of the risk management infrastructure are refocused	Data is aligned with specific needs	Mechanisms to determine likelihood, severity and consequences of risk are in place	Operational activities are supported by employees with appropriate skill sets
	Set service delivery standards and publicise Gap analysis of stakeholders needs and Customs internal processes Performance perception analysed and documented	Evaluate and improve the effectiveness of policies, procedures and training Risk management is a theme in operational planning	Identify gaps and additional data required Modify data requirements	Procure training and tools Consider what support requirements are needed i.e., reporting, dissemination, lines of communication, etc. Place staff as appropriate	Build employee skills as appropriate i.e., training Assign employees to suitable works
REALISATION	Stakeholder perception expectations of our performance is evaluated against Customs current missions and goals	The risk management infrastructure is established i.e., policy procedures and training	The worth of the data in therms of relevance timeliness and integrity is known	Tools and skills required for analysis are identified	Employee skill levels against competencies and gaps are known
	Stakeholders are surveyed Focus groups are formed Feedback consultations are sought	Policy and procedures are developed and disseminated Training and promotional strategies are developed Operational plans that should incorporate risk management are identified	Collect analyse and evaluate data	Assessment of current internal tools skills, elements and abilities is conducted Identify competencies for analysts Undertake gap analysis	Develop competencies Conduct employee skills audit Identify gaps and create solutions to address

	Purpose/ Context/Scope	Risk Management Concept	Data	Analysis	Employee Investment
AWARENESS	Stakeholders are known and their needs are explored We understand Customs current missions an goals	Risk management process is understood	Data needs and sources are known	An analytical process is understood	Employees are aware of the concepts, methodology, principies and benefits of the risk management Employees are aware that change will occur, is necessary and the extent of that change
	Brainstorming of group of managers to identify stakeholders Identify what their might be Customs missions and goals identified and stated	Research and adopt risk management methodology Risk management process is promoted	Brain storming to indentify data needs and sources within the context, goals objectives and measures	Research an adopt an analytical process	Awareness training and communication strategy is developed and delivered High level commitment is demonstred
Starting Point	We recognize we have an internal and external stakeholders and have an assumption of theis needs	The need for risk management concept is recognized	Need for information is recognised	The need o assess of evaluate data/ information and the benefits are recognized	The need to raise employee awareness is recognised

Instructions for Use

The purpose of this matrix is to assist an economy to determine through self-assessment, the current status of their organization in terms of risk management. By charting the current position of your economy, the matrix will assist in helping to identify the next steps to refining or building your risk management process. The subject areas of Purpose/Context/Scope, Risk Management Concept, Data, Analysis, and Employee Investment are individually assessed based on the following stages: Starting Point, Awareness, Realization, Focus, Adaptation and Integration. Your economy will investigate the subject areas and after gathering data, will determine at what stage in that subject area you are. While dependent on each other in practice, the subject areas should be assessed independently and not against each other. It is therefore realistic to be in a Focus stage in reference to your Data subject area, and be at the Starting Point in your Employee Investment subject area. There is no right or wrong answer to this assessment. The purpose is to help your economy see where it currently is, and assist you in advancing your current position.

To properly use this tool, look at the definition in the Starting Point stage for the first subject area Purpose/Context/Scope, and assess whether you have reached this point based on the definition. If you have, then review the definition in the Awareness Stage. If you have reached this stage, look at the definition in the Realization stage and assess your organization. If you have reached this stage, then review the definition against your current position in the Focus stage. Continue reviewing the definitions in relation to the current status of your organization until you reach the Integration stage. If at any point before reaching the Integration stage, you find the definition that best describes your organization, you have determined your current position. Make a notation indicating the stage where your organization fits. It is highly unlikely (although possible) that organizations may be at the Integration stage when first conducting this exercise. Once you have determined and recorded where your organization is relative to all subject areas, you are ready to determine and review what it will take to get to the next level, and the feasibility of that venture.

The grey shaded areas may provide your economy with examples of the actions or activities and tools that may assist in progressing through the matrix. This is not to say that other actions, activities or tools specific to your economy cannot be used or developed, as it is only intended to provide some useful options that you can consider. The actions and activities that are identified as appropriate to help the organization to move to the next level in the matrix will form the basis of your risk management implementation plan.

It would be helpful to review this matrix and conduct this same assessment at various intervals of time to reassess progress, refocus goals, and improve your Risk Management Process.

2.7M
4.6m
WAN HAI
WAN HAI
A0
WHLU 226682 9
22G1
MGW
TARE
NET
CU.CAP.
24,000 KG
52,910 LBS
2,370 KG
5,225 LBS
21,630 KG
47,685 LBS
33.2 CU.M.
1,172 CU.FT.
LONG VEHICLE 長車
43827 T
KN 1967

ANNEX 4: RISK ASSESSMENT/TARGETING CENTRES

There is an increasing trend towards the establishment of specific risk management functions that focus on building a closer interface between the traditional roles of intelligence and front-line operations. In some countries, this function has taken the form of a national risk assessment/targeting centre.

There are different organizational models for operating a risk assessment/targeting centre. Models depend on organizational roles, structures, activities and functions. They may be centralized, decentralized or a mixture of the two. Often this is also influenced by the ICT capabilities of the organization. There is no "one size fits all" organizational model for establishing such a centre. The following activities seem to be typical of the centres currently in existence:

- manage selectivity and targeting criteria;
- manage risk analysis related IT systems and assist with their development;
- provide 24/7/365 tactical analysis and coordination capacity to front-line operations;
- assist with planning & resource deployment;
- act as a hub for risk related information exchange; and
- provide a platform for stakeholder and Coordinated Border Management (CBM) cooperation.

Selectivity and targeting

Risk assessment and targeting centres carry out analytical functions and develop selectivity and targeting criteria relating to activities such as vetting commercial transactions, revenue assurance, fraud and other illegal activities, profiling of travellers, enforcing prohibitions and restrictions, and cultural heritage protection. In some cases these centres serve as a nexus for gathering information from a wide variety of sources (public domain and law enforcement), both internal and external to Customs. Most often they use automated analysis and trade-based research tools (importation trends, common traits, profiles, past violations, passenger data, etc.) to conduct these activities in conjunction with existing Intelligence products. The outcome of the analysis leads to the development of risk profiles and examination criteria, enabling Customs to identify those transactions most likely to be non-compliant in a dynamic manner, thus enabling more effective resource planning and deployment responses to situations presenting the highest risks.

The centres contribute to the management of the selectivity system and can enter criteria into electronic and/or manual systems. While most often managed centrally, this function will generally include selectivity and targeting criteria derived from national systems and regional or local experience. This ensures that national risk management goals and objectives are met and that local knowledge and experience enrich the process. The centres analyze the resultant "hits", collect, and store information from front-line interventions, which in turn enables the continuous refinement and development of the selection and targeting criteria in conjunction with intelligence units.

Information systems and their development

As mentioned above, risk assessment and targeting centres often have a role in managing electronic risk analysis systems and inserting the risk rules, profiles and statistically valid random selection criteria. Their tasks can also include keeping the system and its content relevant.

Operational support

Centres tend to operate on a 24/7/365 basis and support front-line operational activity by providing additional tactical analysis capacity. They bring added value to the front line by providing analysis capacity to operational inquiries originating in realtime from business operations such as goods inspection, passenger inspection, transport and vessel search and investigations activities. The centres can also provide support to resource planning and deployment, particularly in dynamic situations where mobile units may be dispatched to address risks or to bolster static resources where they are deemed insufficient to deal with a high-risk situation.

Information coordination and exchange hubs

Risk assessment and targeting centres often facilitate information exchange on risk related issues, both nationally and internationally. Operating as a central hub they can be used to coordinate information exchange on risk related issues between Customs and other governmental agencies, between Customs and the private sector, and between Customs administrations internationally where the legal authority exists for this.

Stakeholder cooperation and a vehicle for better coordinated border management

These centres cooperate closely with both internal and external stakeholders. They have also provided Customs administrations with an excellent vehicle for strengthening inter-agency cooperation on managing cross-border risks. In many cases Customs have invited other border agencies (national and/or international) to join in, and work in the centres. This has enabled better planning, coordination and response actions, contributing towards more efficient and cost-effective delivery of whole-of-government border management goals. A major feature of such an approach is the fact that even though Customs administrations physically host these centres, each participating organization retains its agency-specific mission, role and identity. This encourages wider buy-in to the concept and enables governments to achieve a "many parts, one view" approach without destabilization of wider institutional and agency arrangements.

ANNEX 5: CASE STUDIES BY MEMBERS

Argentina

"Risk management in the Argentina Customs"

Background

In order to control the foreign trade transactions, the National Executive Power, through Decree No. 898/2005, decided to create the General Sub-Directorate of Customs Control, inside the CUSTOMS GENERAL DIRECTORATE.

The Argentina Customs, through Regulation AFIP No. 36/06, dated on January 18, 2006, included on its organizational structure the Risk Management Directorate, which depends on the General Sub-Directorate of Customs Control.

To comply with the tasks assigned to the Customs General Directorate and to control the international movement of goods, the powers of the different areas were adapted, thus favoring the centralization of the strategic information and the decentralization of the strategic control operation.

According to the new methods of international trade and to the national security risks that suppose the smuggling, the trade mark fraud, the international terrorism and the drug trafficking, the Customs control outline was redesigned, thus centralizing the strategic definitions and the intelligence applicable to said control through the creation of risk profiles for the different foreign trade operators.

Aspects of the Risk Management in the Argentina Customs

The techniques used for the risk management are useful for the fight against the counterfeiting and to secure and facilitate the exchanges of information and good practices.

The risk analysis processes, the use of computerized procedures that permit the analysis of a large amount of information and the use of harmonized criteria to control the goods and the economic operators, are the basis of an effective control that does not affect the legitimate international trade and that minimizes the risks for the citizens.

The main responsibility of the Risk Management Directorate is to create strategic politics for the Customs control, to collect and analyze the information to define the risk profiles and to coordinate the activities in which the Customs General Directorate has to act with other organizations.

The Directorate is formed by two Departments: Selectivity and Strategic Management of Valuation. Their tasks area the following:

- to plan and propose criteria to define the risk profiles of the operations, destinations, operators and foreign trade auxiliaries and to evaluate the results; and
- to create control and analysis criteria for the valuation of the goods. Said criteria will be used on the selectivity procedure.

These actions are conducted within the framework of the World Customs Organization, which establishes the rules for the system for risk analysis: "The Customs Administrations must apply a computerized system to analyze the risks and to identify the goods that can be of high risk".

Even though the adoption of the Revised Kyoto Convention is still pending at the Parliament, the Customs perform the tasks according to the Guidelines on Customs Control, as set forth in the General Annex of Chapter VI of the RKC.

Finally, the agency also takes into account what is set forth in the ISO Standard 31000:2009 for the successful risk management. The Standard is a practical document that is intended to help the public and private organizations, advising them to develop, apply and improve a risk management framework as a fundamental part of their management system.

Tasks

This system includes a mechanism to validate the risk analysis, to adopt strategic decisions and to identify "good practices" to produce a change in the way in which the selectivity is managed.

This change is based on the following pillars:

- definition of the general and uniform criteria;
- measurement of the results;
- increase of the risk perception; and
- joint work of the operational areas and other control agencies.

Advantages

- to guarantee a better use of resources;
- to increase incomes;
- to improve compliance;
- to increase the risk perception in relation to operations and operators;
- to reduce clearance times;
- to decrease logistics costs; and
- to enhance cooperation among operators, control agencies and Customs.

Jamaica

"From traditional to risk-based control approach"

The Jamaica Customs Department is implementing proactive risk management. The table below compares the Department's previous Customs controls with its current approach and includes some lessons learned.

Previous approach	Risk-based approach
100% examinations conducted	Focus on high-risk areas, with minimal intervention in low-risk areas Increased focus on post-transaction compliance assessment Balance between regulatory control and trade facilitation
Lack of coordination and structure within operating environment – "fragmented"	Strategic and holistic approach Centralised risk management coordination
Focus on identifying non-compliance	Focus on identifying both compliance and non-compliance Focus on assessing the integrity of trader systems and procedures
Lack of formal feedback mechanism, limited incentives for compliance	Consultative, cooperative approach Rewards for recognized compliant traders Dual enforcement/client service focus
Unilateral approach & inflexible procedures	Simplification of procedures with appeal mechanisms
Limited automation & IT integration	Information management focus Pre-arrival import clearance Greater integration of systems Intelligence driven

Lessons learned throughout the implementation experience were:

- risk management requires a structured communication network for the exchange of information both within Jamaica Customs Department and with stakeholders and clients;
- staff awareness about risk management and change in organizational culture is vital;
- a formal process for evaluating and monitoring risk management solutions is paramount; and
- there are direct and indirect impacts on trade, such as reduced processing times and lower transaction costs.

Future work will include:

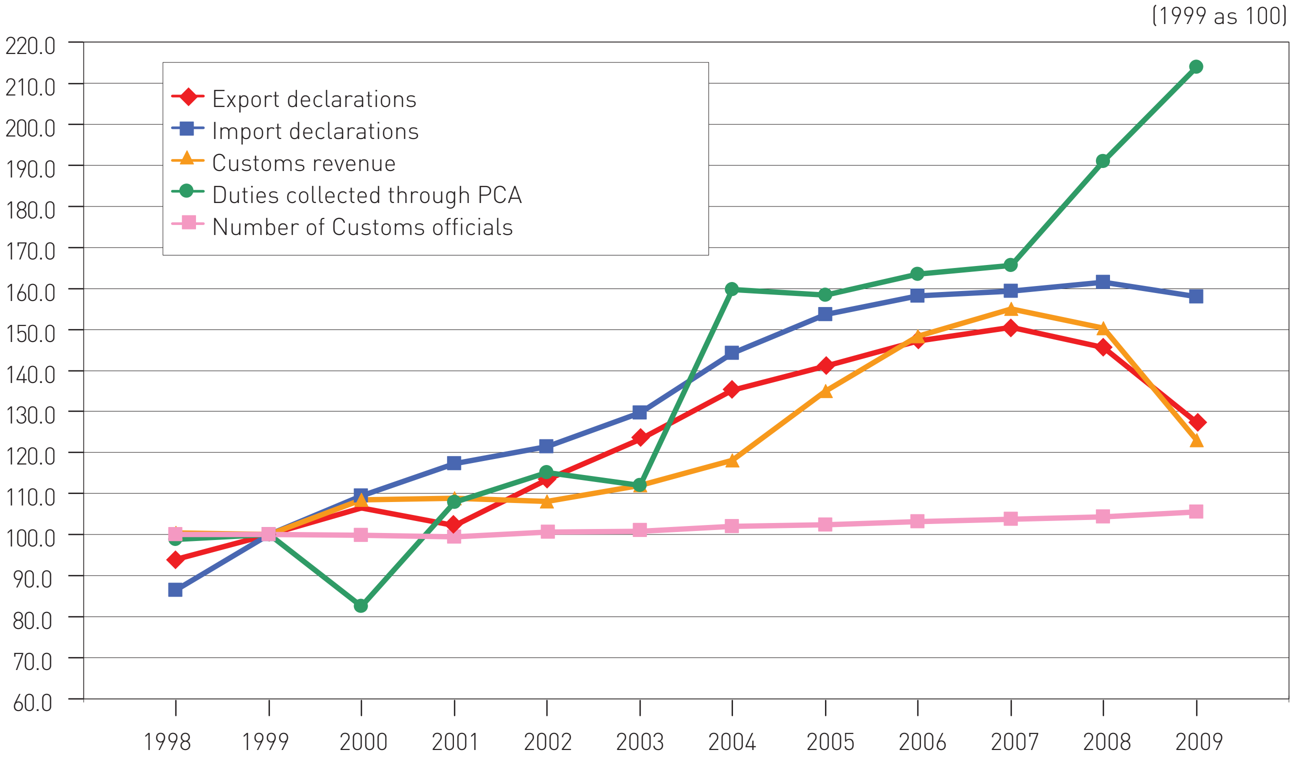
- client education;
- legislative amendments;
- operational changes;
- resource re-allocation; and
- technology and technical support.

Japan

"Example of benefits of risk management"

The following graph shows the transition in the volume of main services and the number of officials in Japan Customs. While the workload has been increasing, the number of officials has remained at the same level, which shows that operational efficiency has been improved. Better resource allocation through the enhancement of the risk management approach greatly contributes to this achievement.

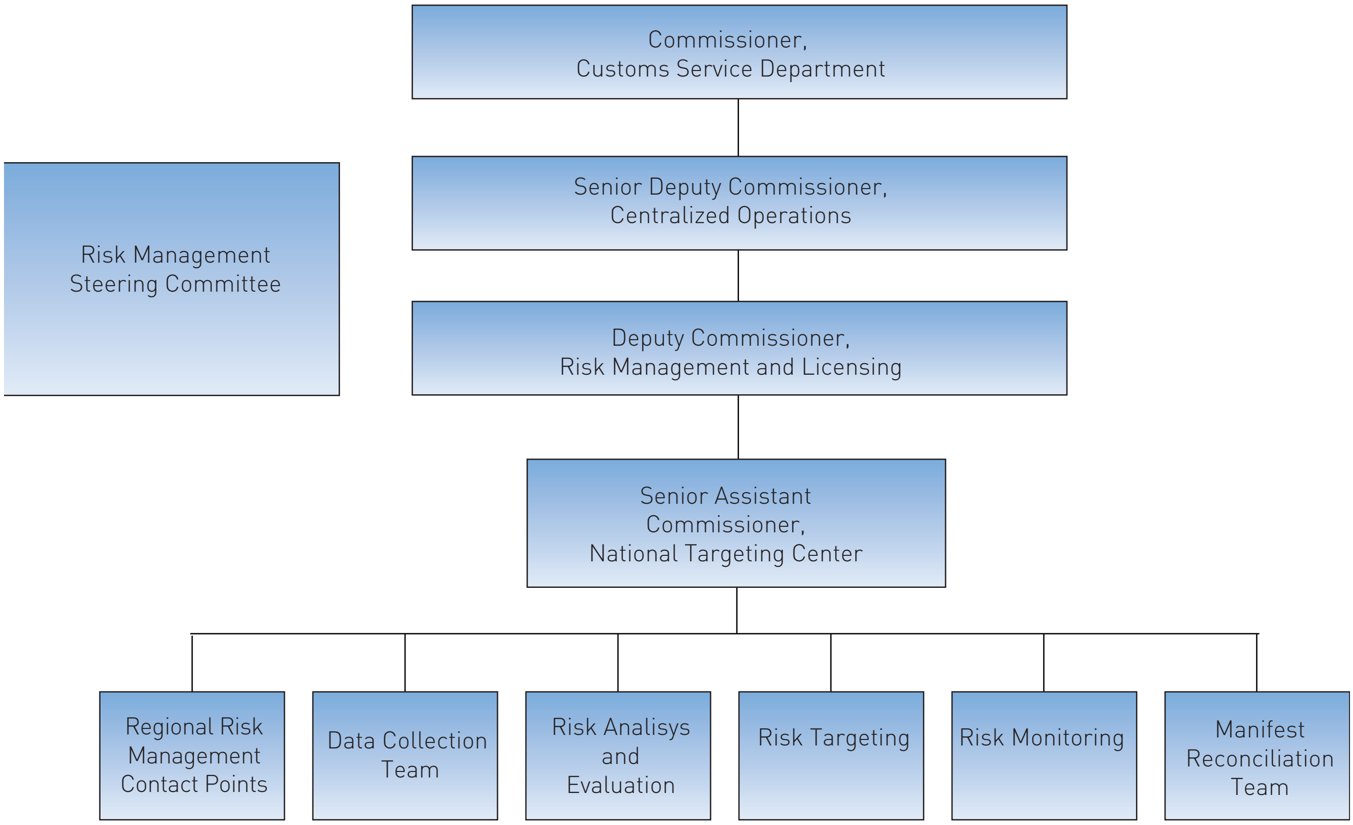
Transition in main Customs services and the number of Customs personnel



Kenya

"Organization of the risk management function"

The following diagram shows the organization of risk management functions in the Kenya Customs Department. A Risk Management Steering Committee deals with organizational risks and priorities, whereas a National Targeting Centre has been established to support operational risk assessment, profiling and targeting practices.



Korea

"Integrated Risk Management System"

Overview

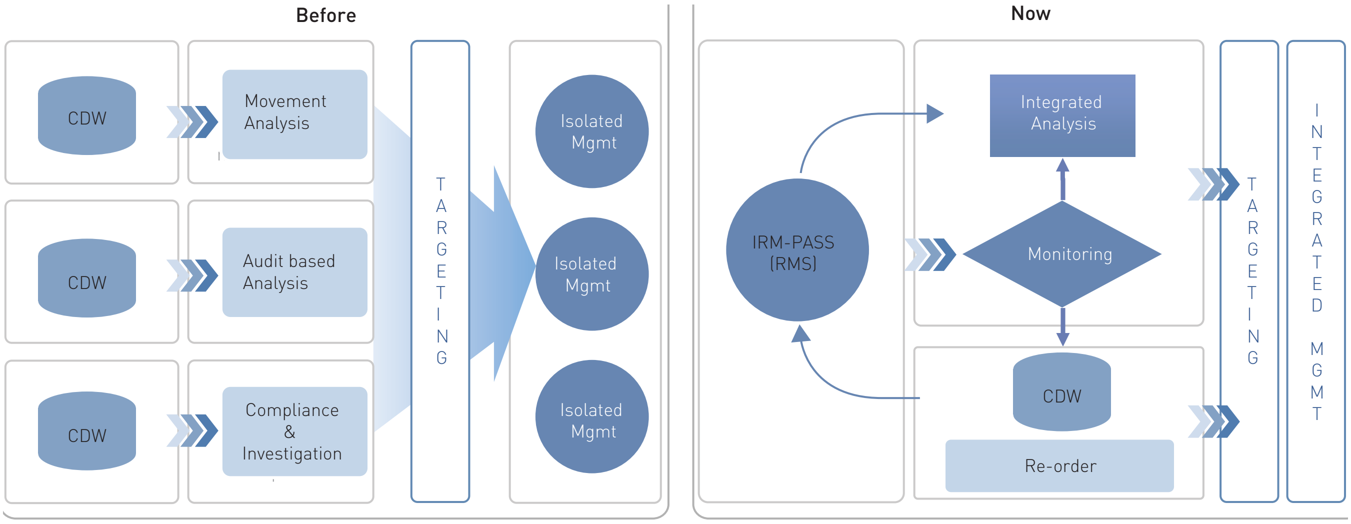
Risk management based on information and communication technology is essential for coping with challenges from cross-border transactions. The Korea Customs Service (KCS) selects and inspects high-risk passengers, goods and transportation based on the results of risk analysis. The KCS has traditionally conducted risk analysis for post- audit on illegal transactions and tax evasion cases, and also established a Customs Data Warehouse (CDW) in 2002.

The CDW collected data not just from Customs divisions but from other government agencies such as the Ministry of Justice, National Tax Service, Ministry of Foreign Affairs & Trade, and Ministry of Land, Transport and Maritime Affairs.

From 2008 the KCS started to establish an Integrated Risk Management System (IRM) with a range of functions:

- automatic integration and segmentation of data;
- providing customized information (e.g. high, mid and field level);
- circulating information and screening criteria; and
- articulating risk factors using complex target selection indicators.

Integrated Risk Management System



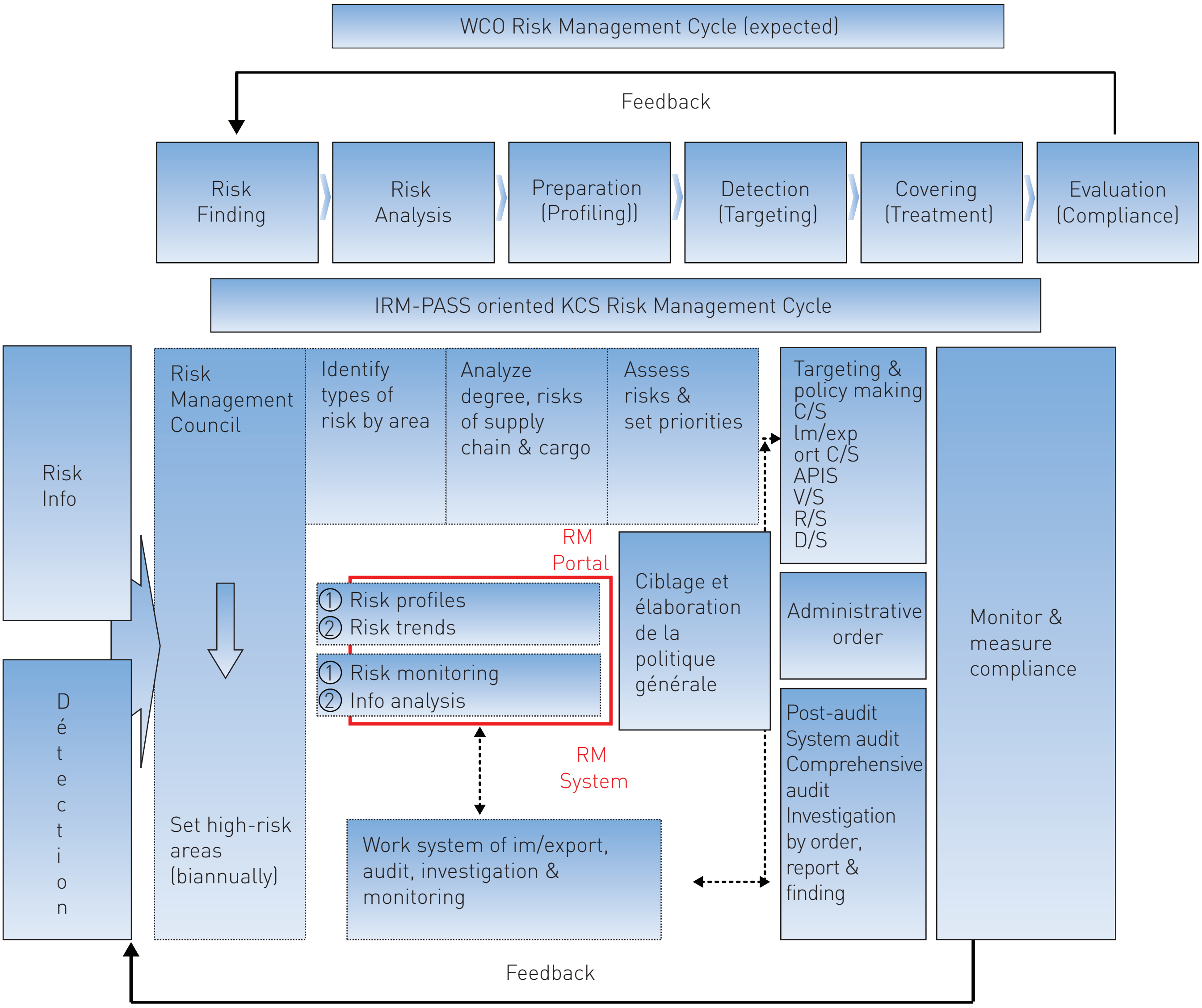
IRM cycle

- step 1: initial screening on prior data & post records;
- step 2: analysis using auto filtering, monitoring;
- step 3: selectivity using simulation and multi-layered factors; and
- step 4: re-evaluate results of risk treatment.

Expected benefits from the IRM system:

- producing comprehensive information with an enhanced reconciliation function;
- real-time data management and reducing time lag;
- focus shifted from correction of mistakes to prevention;
- assisting divisions with their decision making; and
- possible efficiencies in organizational integration.

Risk Management Cycle


WCO Risk Management Cycle (expected)
Feedback
Risk Finding
Risk Analysis
Preparation (Profiling))
Detection (Targeting)
Covering (Treatment)
Evaluation (Compliance)
IRM-PASS oriented KCS Risk Management Cycle
Risk Info
Détection
Risk Management Council
Set high-risk areas (biannually)
Identify types of risk by area
Analyze degree, risks of supply chain & cargo
Assess risks & set priorities
RM Portal
① Risk profiles
② Risk trends
① Risk monitoring
② Info analysis
RM System
Work system of im/export, audit, investigation & monitoring
Ciblage et élaboration de la politique générale
Targeting & policy making C/S
Im/exp ort C/S
APIS
V/S
R/S
D/S
Administrative order
Post-audit System audit Comprehensive audit Investigation by order, report & finding
Monitor & measure compliance
Feedback

A way forward

Developing IRM is a continuing process with a focus on intelligence integration. Building on the successful IRM system, the KCS plans to establish a "National Targeting Council (NTC, tentative name)" for more effective and efficient risk management. Effective risk management requires close cooperation among related entities, including border agencies and other countries. The combination of NTC and technology-intensive information management will improve targeting capability, leading to an increase in revenue collection.

Mauritius

"Using Risk Assessment and profiling to select for examination of textile fabrics having undergone some working such as hemming or formation of necklines."

A consignment declared as fabrics was selected for physical examination. It was observed that this consignment consisted of curtain fabrics with scalloping edges. The fabrics were declared as textile piece goods under HS code 5515.1900.

Fabrics having undergone some workings such as hemming or formation of necklines are classifiable under HS code 6307.9090 according to note 7 to Section X1 of the Harmonized Commodity Coding and Description System.

Fabrics attract 0% duty and 0% VAT at importation under Chapters 50 t0 56 but fabrics having undergone some workings such as hemming or formation of necklines are classifiable under HS code

6307.9090 for which there is no duty but attract VAT at 15% at importation.

An offence report was filed for wrong classification of fabrics with scalloping edges. Feedback was received from the seizing office at Risk Management Section and used as intelligence for targeting.

Data was retrieved from the Customs import database on importers of fabrics. A list of importers of fabrics was compiled and analyzed and it was observed that all consignments were declared as fabrics. The declaration was quite misleading to the extent that the description was not complete to enable the proper classification. A survey was carried out by officers of Risk Management Section to identify/gather information on importers/retailers of curtain fabrics with scalloping edges.

A list of retailers by trading name and selling curtain fabrics was identified and matched against the list of importers registered at Customs. The importers who matched the above list were targeted for physical examination through selectivity. The assistance of the Income Tax and VAT Departments was also sought to identify other importers of curtain fabrics by their trade names and matched against their registration numbers at Customs. An additional list of importers of curtain fabrics was thus obtained and the consignments of these importers were targeted for physical examination through selectivity.

3 cases of wrong classification were observed and Offence Reports filed accordingly. Other importers of these types of fabrics are now being targeted taking into consideration the seasonability of the import of such products.

United States

"Risk-based, layered approach to supply chain security"

The United States Customs and Border Protection (CBP) has adopted a risk-based layered approach to supply chain security. The methodology has evolved over several years into a comprehensive strategy that enhances security across all potential transit vectors that is more efficient and cost effective than alternative approaches that focus exclusively on a single layer of defense. CBP is working to detect, prevent or deter attacks against, or the exploitation of, the supply chain by utilizing technologies where appropriate, but is also relying on layers of non sensor based programmes across air, land and maritime pathways. Some of these additional layers include:

- advanced electronic information under the 24-hour rule – enhanced by the 10+2 importer security filing requirements;
- screening all shipment information by interfacing with import and enforcement systems using the automated targeting system (ATS) and national targeting center;
- authorized economic operator partnerships with industry and the private sector, such as C-TPAT;
- partnerships with foreign governments such as the container security initiative and secure freight initiative;
- partnerships with other U.S. government agencies such as the Transportation Security Administration on air cargo security; and
- use of non-intrusive inspection technology and mandatory exams for all high-risk shipments.

The objective of this layered approach is to integrate these measures into intersecting processes, thereby allowing CBP to receive, process and act upon commercial and security information in a timely manner. This disciplined and highly systemized approach enables the accurate targeting of suspect shipments without hindering the movement of commerce upon arrival in US ports. The discrete layers provide defense in depth for the various segments of the supply chain, ensuring that cargo and associated information is regularly assessed and that security does not rely on any single point that could be compromised.

OOCL
THERMO KING
Hapag-Lloyd
OOCL
THERMO KING
SS