WORLD CUSTOMS ORGANIZATION

GUIDE TO CORRUPTION RISK MAPPING

Table of contents

* * *

INTRODUCTION

Most Customs administrations have attempted to address corruption but, by and large, related initiatives appear not to have given the expected results for a range of reasons. One of the reasons is that anti-corruption projects have not been envisaged holistically and bad practices have remained. Different approaches have been adopted by WCO Members to address corruption and enhance integrity, such as performance measurement, changes in human resources policies, increases in salaries, and automation, to name a few. One approach identified by a number of Customs administrations has been to identify where potential corruption risks lie and establish a map to better understand where they can appear and be able to remedy the situation.

Risk mapping enables senior management to have an overview of the vulnerabilities of Customs processes and specific Customs units in order to make informed decisions to prevent and address the issue of corruption. Senior management can then focus its anti-corruption and integrity efforts on areas that are considered as high risk, and therefore prioritize their actions to guarantee better results.

Risk mapping is not a new concept, but one which several international organizations have looked into and where they have advocated a series of approaches in different sectors (health, education, etc.). Similarly, in the Customs sector, a number of WCO Members have engaged in risk mapping to identify corruption risks. In response to interest in this approach, the WCO Secretariat presented a document entitled “Risk mapping and risk analysis for better governance” at the 13th Session of the Integrity Sub-Committee in February 2014. This document introduced the approach of risk mapping based on the experience of international organizations and WCO Members, who were invited to share their methodology.

To produce this Guide, the WCO Secretariat collated information provided by Members who have responded to the WCO invitation to share their own practices in relation to risk mapping with a view to fighting corruption. The aim of this Guide is to assist Members that wish to engage in this activity in understanding the importance of knowing where corruption risks are, and to propose a methodology that will need to be adapted to the national context.

The Guide to Corruption Risk Mapping starts by explaining the notion of risk mapping, in particular in the Customs context and in relation to corruption. It then explores the benefits of using such an approach and describes elements of a methodology to obtain information and identify those who will carry out such an exercise, providing detailed explanations of key steps. It concludes by describing in detail the different steps of the risk mapping process.

1. Corruption risk mapping in the Customs context

There are various definitions of corruption, depending on the context (criminal law or policy). Transparency International proposes a general definition: “Corruption involves behaviour on the part of officials in the public sector, whether politicians or civil servants, in which they improperly and unlawfully enrich themselves, or those close to them, by the misuse of the public power entrusted to them”.

Most useful definitions, however, focus on three key concepts to effectively describe corruption, namely: (1) the departure from, or contravention of, public duty; (2) the provision or receipt of some form of improper inducement, and (3) an element of secrecy (WCO, 2014).

The risk of corruption within Customs administrations is prevalent due to the very nature of Customs work, which is directly linked to money, goods and people. Corruption in Customs has negative consequences such as loss of revenue, waste of resources, and a reduction in social

trust, and also presents security challenges[1]. Such security challenges can be purely related to physical security, but also to health and economic security. Risk mapping can help a Customs administration determine the areas in which potential risks of corruption lie, and develop plans to prevent them. The objective is to develop targeted and preventative measures against corruption to ensure that the image of Customs is improved and that it enjoys the trust and confidence of Customs staff, stakeholders and the entire community by acting with integrity.

2. Risk mapping in a nutshell

2.1. Visualization

A risk map is a data visualization tool for communicating specific risks an organization faces. The goal of a risk map is to improve an administration's understanding of its risk profile, and seek clarification of the nature and the impact of the risks. Risk maps can be a useful tool for explaining and communicating various risks to senior management and employees.

There are a variety of representations of risk maps. They can, for example, be presented as a matrix. For example, the likelihood a risk will occur may be plotted on the x-axis, while the impact of the same risk is plotted on the y-axis.

The graph below depicts the likelihood or frequency on the vertical axis, and impact or significance on the horizontal axis. In this configuration, likelihood increases as you move up the vertical axis, and impact increases from left to right. The points on the profile represent risks that have been categorized into four impact categories and six likelihood categories. The categories simplify the prioritization process by forcing placement of each risk into a particular box showing its position relative to the others. Risks that fall above the "stepped" line are considered intolerable and require immediate attention, while risks below the boundary do not require immediate attention. The threat below and to the left of the boundary is currently considered tolerable. The level of tolerance has to be determined beforehand.

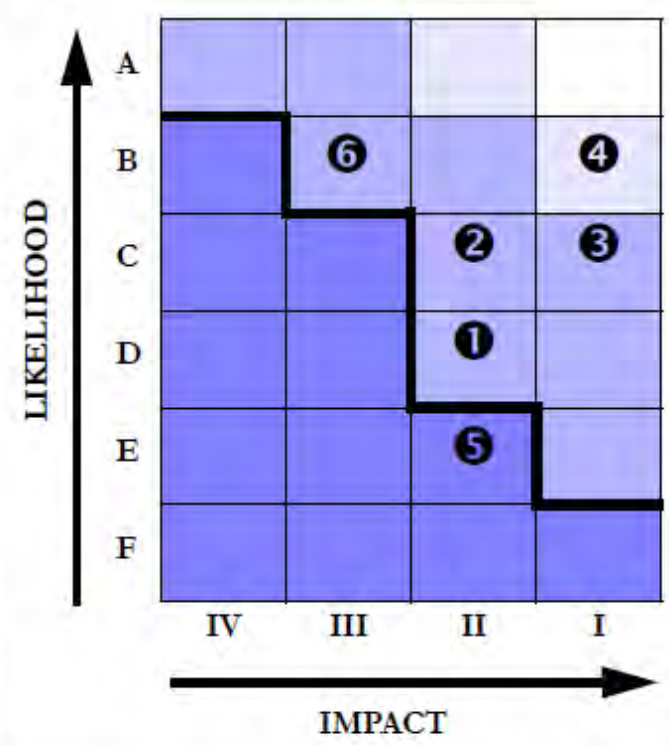


Fig. 1. Likelihood and impact graph (Williams T. and Saporito S., 2001)

[1]For reference purposes, the reader is invited to consult the WCO Integrity Development Guide, which provides details on the different types of corruption in Customs and why it is a serious issue.

Risk maps can also be illustrated by a heat map, using colours to illustrate the level of risks individual branch offices are exposed to (see Annex III).

Other representations can help visualize how risks are clustered and understand the relationship that exists between risks. For example, the risks are displayed on a severity and frequency grid after each risk is assessed. This chart would be used to prioritize risk across the organization. Another map might show the risk reduction after risk management action is adopted.

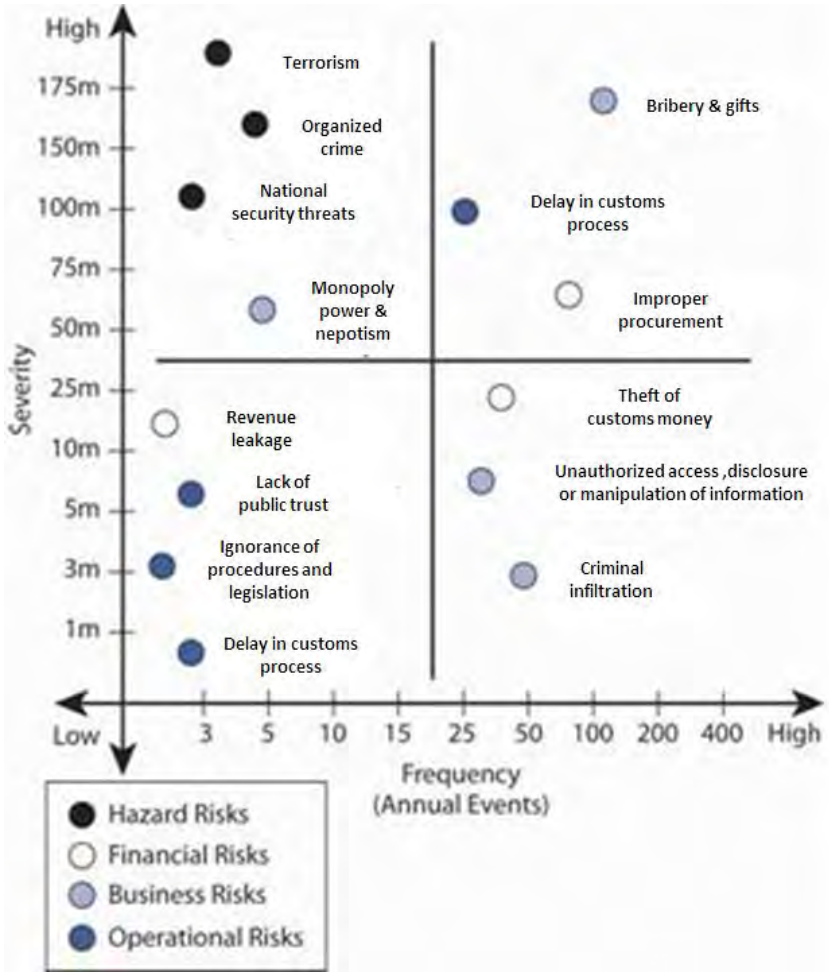


Fig. 2.

This Figure represents an example of a holistic risk map for an administration examining the dynamics of frequency and severity as they relate to each risk. By assigning the probability of occurrence against the estimate of future magnitude of possible loss, risk managers can form the basis upon which an administration can focus on risk areas in need of action. The possible actions – including risk avoidance, risk control, and insurance – can therefore be taken. Note that risk maps include plotting intersection points between measures of frequency (on an x-axis) and severity (on a y-axis). Each point represents the relationship between the frequency of the exposure and the severity of the exposure for each risk measured.

Strategies for risk mapping will vary from organization to organization. Organizational objectives arise out of the institutional risk culture. These objectives help determine the organization's risk tolerance level. The first step in mapping risk is to identify the organization's risk exposures, and estimate and forecast the frequency and severity of each potential risk (Baranoff E. et al., 2009).

In the context of anti-corruption, risk mapping seeks to identify weaknesses within a system which may present opportunities for corruption to occur. It differs from many other corruption assessment tools in that it focuses on the potential for – rather than the perception, existence or extent of – corruption.

2.2. Risk mapping and organization planning

Organizational planning and risk assessment are complementary (Beswick K. and Bloodwort J., 2003). It is vital to assess risks, which may affect the organization's ability to meet its key objectives. Corruption risks can clearly impede the organization's objectives and therefore must be taken into account at the time of developing the organizational plan.

A risk mapping strategy builds on the organization's vision to provide the organization with a well-defined pathway for the future. This strategy helps move away from the focus on individual risk analysis component missions to a much broader and integrated goal structure. This is intended to show that to be successful, risk mapping efforts must be combined, and resources used efficiently towards a common strategic direction (FEMA, 2008).

2.3. Risk mapping objectives

The objectives of risk mapping are as follows:

- Identify risks and how they are interconnected;
- Provide a mechanism to develop a robust risk management strategy;
- Compare and evaluate current risk handling and aid in selecting appropriate strategies;
- Show the remainders of risks after all risk mitigation strategies have been put in place; and
- Communicate risk management strategy to both management and employees.

3. Benefits of corruption risk mapping

Because "a picture tells a thousand words", risk mapping enables a visualization of how risks are prioritized through their position, and reveals which threats require senior management's attention and organizational resources. This may entail reallocation of time and resources from controlled threats to those that require immediate attention (Williams T. and Saporito S., 2001). In addition:

- It allows the identification of risks that could slow down Customs performance and give a negative image of Customs.
- It optimizes the decision-making process by avoiding unnecessary levels in that process, thus creating gains in time and efficiency. If risk profiling is part of an organizational risk management process, the benefits increase significantly. By way of example, a decision made by one department may seem to be appropriate when considered in isolation, but when considered in the context of the organization as a whole, that decision may not be optimal.
- It supplements evidence of actual or perceived corruption in a given context in order to inform anti-corruption strategies and policies, or for advocacy purposes.
- It enables senior management to have a more complete vision of areas and positions that are more vulnerable to corruption, and to focus its anti-corruption efforts on those particular areas.
- It makes senior management more accountable as it has officially been made aware of the risks and the solutions to mitigate those risks.

4. Risk assessment approaches

Based on the information provided by WCO Members and the research carried out to develop this Guide, it is clear that the conceptualization of risk varies depending on the tool or the approach used. For example:

- Corruption risk may correspond to a set of institutional vulnerabilities within a system or process which might favour or facilitate corrupt practices;

- Measures of institutional vulnerability can be combined with data on perceptions and/or experience of corruption;
- Risk can be expressed as a factor of the likelihood of corruption multiplied by the impact of corruption;
- Objective risks (weak institutions and regulations) are sometimes differentiated from subjective risks (tolerance to corruption, personal motivation, weighing up of costs/benefits, past experiences);
- Corruption risk may be understood as a factor of the level of transparency and level of fairness in a process;
- Corruption risk may be understood as the difference between the current system and an ideal system.

Thus, the sophistication of risk mapping/assessment ranges from the identification of corruption and/or institutional weaknesses/gaps as an indicator of risk of corruption, to an analysis of the impact and estimation of the likelihood of corrupt practices. Additional steps of the risk assessment may include prioritization of risks, identification of tools to address the identified risks, and guidance on the development of anti-corruption strategies. In many cases, the first stage of the process consists of identifying broad risk areas (usually through secondary sources), which are then analysed in more detail in the second stage. In some cases, intermediate steps in the analysis are left out, such as impact assessment and the likelihood of corrupt practices. In other cases, the analysis stops at the risk identification stage, or even at the point of identifying 'institutional weaknesses' (McDevitt A., 2011).

5. Risk mapping methodology

The risk mapping process is part of a systematic, comprehensive methodology to identify, prioritize and quantify risks to gather all relevant data. Other methods that can be used for capturing information include structured interviews, surveys (written and electronic)[2], or a combination of these. In gathering information, it is important to consult Customs stakeholders so that they can participate in relevant stages of the risk mapping process.

5.1. Definitions

"Risk" is defined as the "effect of uncertainty on the achievement of objectives" (WCO, 2011). Risk is the probability that objectives are not achieved. For any given risk, it is important to consider the likelihood of it occurring, the vulnerability of the organization to it, and the consequences of it occurring, given the effectiveness of existing or planned controls in mitigating it.

Interestingly, a severe threat may pose little risk if controls are effective and there is nothing else that can reasonably be done.

"Risk management" is the ongoing process for establishing the context, including identifying objectives, measuring and evaluating risk, designing counter-measures, implementing these measures and assessing their performance.

A "consequence" is the outcome of an event. In some instances, it may be more practical to manage the consequences of a risk than to reduce its likelihood (e.g. a motor vehicle driver insuring against accident).

Once it is decided which risks require further treatment, there is a need to decide on the way to treat them. Approaches to risk treatment include:

- Tolerating the risk;
- Terminating the activity that creates the risk;

[2]See Annex I.

- Mitigating the risk (in the case of a threat) to reduce the likelihood and/or consequence, or (in the case of an opportunity) to enhance the likelihood and/or consequence;
- Increasing the risk;
- Sharing or transferring the risk to another work area.

A "control strategy"/ "risk treatment" is a plan to reduce the severity of the organization's exposure to a risk. A control strategy may include removing risk drivers, reducing the likelihood of events, or reducing the severity of the consequences.

5.2. Who should carry out risk mapping?

Although it is possible to outsource the assessment to an external consultant, the responsibility and oversight should be allocated to a senior officer within the Customs administration. This is particularly important given that, to build a solid anti-corruption policy, the risks and effects of the measures that will follow need to be continuously assessed and progress measured. This is only possible when applying a standardized methodology which can be better ensured by the same organizational unit. It goes without saying that this unit also needs to be given the necessary support, resources and powers/independence to pursue its objectives. Some administrations have described and assigned these positions, as well as their roles and responsibilities, in an overall policy document. This policy describes in detail the methodology of an ongoing risk assessment exercise, and the involvement of operational and governance units has also been stressed as important (Ahmed M. and Biskup R., 2013).

5.3. Sources of information

First-hand risk-related information can be obtained from individual officers. This contributes to raising awareness of the problem and can generate a sense of ownership for future policies.

Most corruption risk mapping and assessment uses a combination of secondary sources (legal analysis and research) and primary sources (surveys and questionnaires, focus groups, key informant interviews, checklists, benchmarking). Secondary sources are often used in the preliminary stages to give a picture of the overall governance environment in a country, institution and sector, or to identify priority risk areas. Primary sources are used for deeper analysis of the more critical corruption risks (or perceived risks). In addition, some form of expert analysis is usually required to assess the level of risk (e.g. likelihood and probability of corruption).

A corruption risk mapping exercise does not need to be too resource-intensive. In contrast with tools which aim at establishing the incidence, scope and forms of corruption, much of the data required for risk assessment can be collected from existing sources, although some additional primary sources may be needed for the specific system/process under analysis. A careful selection of stakeholders who are consulted as part of the assessment will have an important bearing on which risks are identified and prioritized (McDevitt A., 2011).

5.3.1. Risk assessment standards

As already mentioned, it would be advisable to develop specific guidelines outlining the objectives, the methodology, and the roles and responsibilities of all the stakeholders in each and every step of the whole risk mapping progression[3]. Some administrations use International Organization for Standardization (ISO) standards for their risk assessment (ISO 31000:2009) to guarantee the efficiency of all procedures and steps.

[3] See Annex III.

5.3.2. Interviews and cross-functional workshops

Assessments can be conducted through interviews or facilitated meetings with Customs officers who work in areas related to anti-corruption and integrity, as well as with Customs stakeholders. Cross-functional workshops are preferable to interviews or surveys for assessment and risk identification purposes as they facilitate consideration of risk interactions and breakdown. Setting up working groups at various organizational levels to elaborate the questionnaire will help reduce biased answers and, in turn, increase ownership, which is particularly useful in the context of anti-corruption. It is essential that all relevant stakeholders are represented to get an overview of possible risk areas. Stakeholders include the Customs administration staff, external audit representative, internal audit representative and representatives of the private sector.

Workshops improve understanding of a risk by bringing together diverse perspectives. For example, when considering a risk such as an information security breach, workshop participants from Information Technology, Legal and Compliance, Public Relations, Customer Services, Strategic Planning, and Operations Management may each bring different information regarding causes, consequences, likelihoods, and risk interactions. Interviews may be more appropriate for senior management, board members, and senior line managers due to their time constraints.

5.3.3. Questionnaires and surveys

Standardized questionnaires, such as Guttman scale questionnaires, can be used[4]. In statistical surveys conducted by means of structured interviews or questionnaires, you can have a subset of the survey items with binary answers (Yes or No). In other words, on a Guttman scale, items are arranged in an order so that an individual who agrees with a particular item also agrees with items of lower rank-order[5]. This type of questionnaire will make it easier to quantify risks and to compare answers with future assessments. For the sake of consistency, the questionnaire should remain more or less identical over a period of time, and so questions would need to be carefully formulated to make sure that answers can provide appropriate information.

Surveys are useful for large, complex, and geographically distributed organizations, or where the culture may not allow for open communication. Survey results can be downloaded into analytical tools allowing risks and opportunities to be viewed by level (board members, executives, managers), by business unit, by geography, or by risk category. Surveys have their limitations in that response rates may be low and, when the survey is anonymous, it may be difficult to identify information gaps. The quality of responses can be low if respondents give survey questions superficial attention or if they do not fully understand the questions. Therefore, surveys should be combined with cross-functional discussions in the context of a workshop or working group or other methods.

5.3.4. Benchmarking

Benchmarking is a collaborative process among a group of entities. Benchmarking focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. Data on events, processes, and measures are developed to compare performance. Some administrations may use benchmarking to assess the likelihood and impact of potential events across the different locations and regions. Benchmarking data are available from research organizations, stakeholders, government agencies, and regulatory and supervisory bodies.

[4] Annex IV b).
[5] http://en.wikipedia.org/wiki/Guttman_scale.

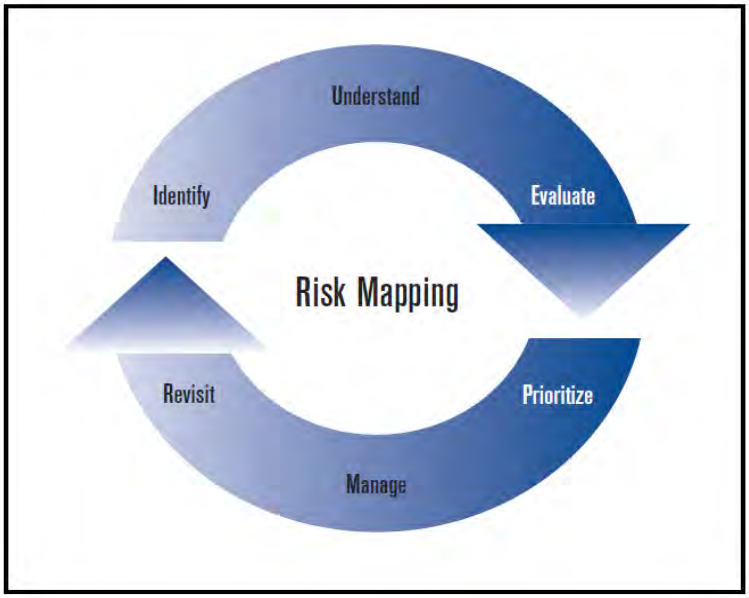
6. The risk mapping process

Risk mapping is a tool used for the identification, control, and management of risks. It can be the first step of an organizational risk management process, or it can stand alone as the primary risk management process.

Organizations considering the risk mapping approach in the area of anti-corruption should be reminded that it is one amongst many other measures. It is also an iterative process that refines senior management's understanding of the risks the organization is exposed to in terms of corruption risks, and measures the effect of the mitigation strategies used to control risks.

The scope of the risk mapping process is determined at the beginning of the analysis to specify the areas considered. The scope provides the parameters necessary to the analysis. The scope is often defined as identifying, prioritizing, and understanding risks and impediments to achieving organizational strategic objectives. The scope can be as broad or as narrow as desired; however, a balance exists between the breadth of scope and the value of information derived from the risk mapping process.

Fig. 3. Scope of risk mapping[6]



The risk mapping process is made up of six key steps:

6.1. Identify risk areas

Risks must be identified in order to:

- Ensure that the full range of significant risks is encompassed within the risk management process;
- Develop processes to measure exposure to those risks; and
- Begin to develop a common language for risk management within the organization.

Starting with a comprehensive but generic list of risks, the administration should aim to select its own list by considering the following criteria:

[6] Williams T., Saporito S., 2001.

- Relevance to the organization's activities;
- Impact on the organization's financial condition;
- Ability to manage separately from other risks.

This step is often undertaken in the context of a brainstorming exercise involving key team members from across the organization (IT, Strategic Planning, Operations, Legal Department, HR and Security). This not only leads to a comprehensive list being compiled, but also aids in building support for the exercise. The final "risk list" should then be checked for consistency with the organization's business plans and intended risk management processes.

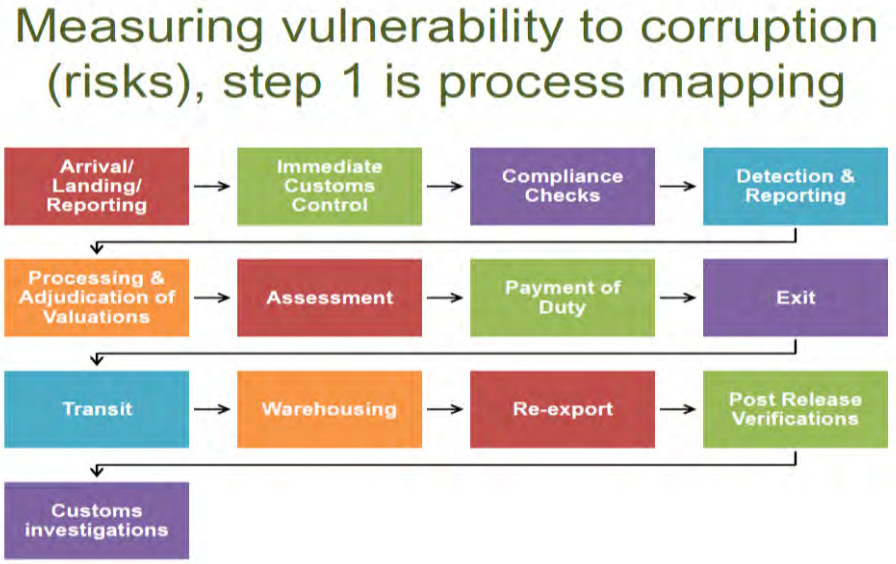


Fig. 4. Source – World Bank

The experiences of all stakeholders can be very helpful in identifying which actions/omissions can be considered as unethical or corrupt, and in determining the vulnerability level of the organization for each level.

6.2. Understand risks

For each of the selected risks from Step 1, it is necessary to determine whether the risk is driven by internal or external events. In some situations, it may prove helpful to plot the exact sequence of events leading to a risk. This could result in the identification of intermediate intervention points where risks can be prevented or limited. Existing risk measurement and control processes should be documented, and if the risk sequence has been plotted, the location of the control process in the sequence can be identified[7].

Sources of risks	Internally driven	Externally driven
Financial	• Fraud • Historical liabilities • Revenue targets • Liquidity and cash flow • Licensing	• Taxpayer non-registration • Return non-filing • Payment non-remittance • Credit risks • Liquidity risks • Market risk • Fraud • Globalization

[7] Ingram D., 2014.

Sources of risks	Internally driven	Externally driven
Operational	• Documentation • Internal control • Bureaucracy • Contracts • Environmental	• Economic environment • Technology developments • Legal and legislative • Customer/taxpayer demand regulatory requirements
Infrastructural	• HR • Recruitment • People skills • Health and safety • Premises • IT systems	• Communications • Transport links • Supply chain • Terrorism • Natural disasters • Pandemic
Reputational	• Board composition control • Environment • Revenue performance • Taxpayer services • Corruption	• Public perception • Regulator enforcement • Taxpayer behaviour • Social responsibility

Table 1. Source – Kenya Revenue Authority

Fig. 5. Source – World Bank

6.3. Evaluate risks

The next step in risk mapping is to evaluate the risks stemming from various situations. This involves:

- Estimating the frequency of risks;
- Estimating the potential severity of risks, e.g. low, medium and high; and
- Considering counterbalancing factors to limit frequency or severity of risks and understand potential control processes.

Not all of the various scenarios that are developed are equally risky. Therefore, it is important to assign relative risk values to each scenario and see which scenario is more risky than others. This helps make clear which risk areas should be under close scrutiny. Risk can be divided into total risk and the risk level after mechanisms are in place (resilient risk)[8].

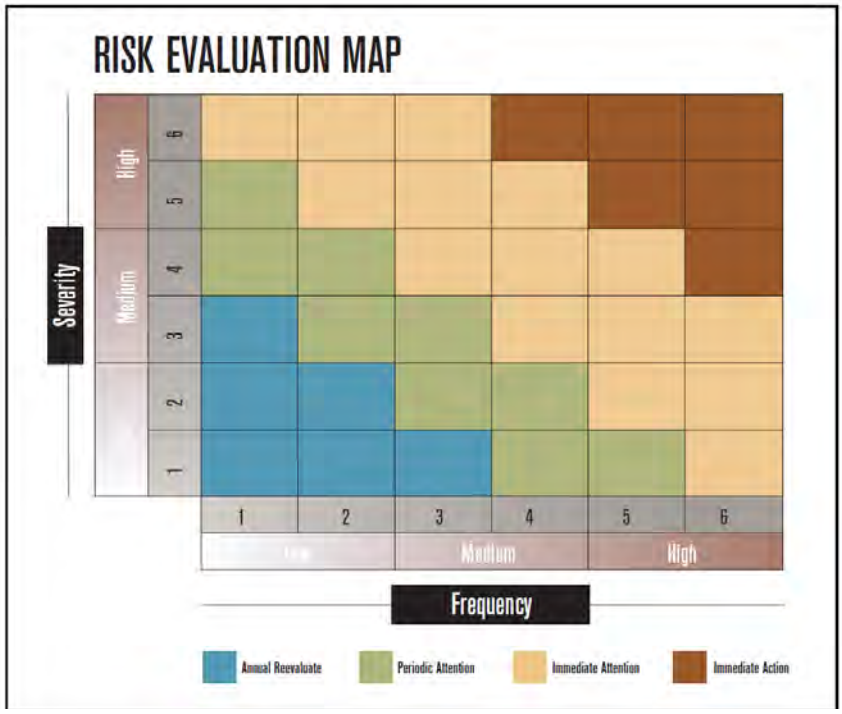


Fig. 6. Ingram D. et al., 2004

6.4. Prioritize risks

The evaluation of risk frequency, severity, and controls described under Step 3 can be consolidated into a single report where risks are ranked according to a combined score incorporating all three assessments. The ranking starts with the risk presenting the worst combination of frequency, severity and control scores.

After the risk areas are ranked, evaluated and all possible scenarios are outlined, it is advised to propose recommendations and remedial measures to prevent, or at least limit, the risk of corruption.

[8] See Annex III.

6.5. Manage risks

The consolidated evaluations can be presented in the form of an action plan that will guide senior managers to take appropriate measures. The action plan should clearly indicate the action required, the party responsible for its implementation and a timeframe. Such an action plan usually increases commitment and leads to more productive results.

Measuring the effect of the measures taken is essential, and the results should be presented through a regular reporting mechanism, particularly in the case of serious risks, so that senior management can regularly be kept aware of the situation and make timely decisions. Ongoing monitoring and measurement is the key to successful risk management.

This critical stage involves deciding how to manage the most important and largest risks, considering the risk-return relationship, correlation with other risks, consistency with the administration's strategy, and the administration's risk tolerance level. It is important to achieve the right balance between the application of the risk management techniques and monitoring the key risk indicators in the administration. This should include, wherever possible, the use of information already generated by the organization.

6.6. Revisit risks

Risk areas can change in intensity and new risk areas can occur. Hence, it is key to keep the risk map up-to-date and to monitor the implementation of the action plan. Because risks are not static, the process of identifying, understanding, evaluating and prioritizing risks must be repeated regularly in order to ensure that the key risks are being appropriately managed. Senior management will periodically review what has happened in the recent past and assess whether risk management efforts produced the expected results.

A risk mapping exercise should be carried out regularly so that progress can be registered and new threats taken into account. In between risk mapping exercises, the use of performance measurement enables an administration to measure progress in real terms to see if the measures taken have had an effect on corrupt behaviour. This kind of performance measurement is done on a monthly basis and enables senior management to make a series of decisions with immediate effect. After a while, in particular if the expected progress has not been registered, it is important to commit to another risk mapping exercise.

This includes monitoring and assessing in order to:

- Ensure that controls are effective;
- Obtain further information to improve risk assessment;
- Analyse and learn lessons from risk events (changes, trends, successes and failures);
- Detect changes in the external and internal context, including changes to the risk criteria and to the risks, which may require revision of risk treatments and priorities; and
- Identify emerging risks.

The process of risk management through risk mapping is continuous and requires constant monitoring of the programme to be certain that (1) the decisions implemented were correct and have been implemented appropriately, and that (2) the underlying problems have not changed so much as to require revised plans for their management. When either of these conditions exists, the process returns to the step of identifying the risks and risk management tools, and the cycle repeats. In this way, risk mapping can be considered as a continuous process.

7. CONCLUSION

Overall, risk mapping can be perceived as a first step to combat corruption. It is used to identify high risk areas within Customs and keep these under scrutiny in order to safeguard resources and the integrity of the Customs administration.

Risk areas need to be continuously updated and evaluated to see whether the corruption risk has increased/decreased and what caused this change.

As corrupt officers can quickly find alternatives in order to continue engaging in bad practices once their behaviour has been discovered, the response from the administration must also be quick in order to stop such behaviours. Risk mapping will contribute to identifying the risks, and performing data mining using the database provided by the Customs clearance system will enable senior management to make informed decisions in very little time. Data mining will also enable the administration to see the evolution of the measure taken by senior management.

This Guide to Corruption Risk Mapping is based on information collated from WCO Members, academia and international institutions and is intended to provide WCO Members with the broad guidelines to engage in a risk mapping exercise as a tool to fight corruption. Clearly, there are different approaches to risk mapping and different visualizations of risk maps. A Customs administration should decide which of the options is most appropriate to its needs. However, the general sequences of the risk mapping process can serve as a guide for the exercise, whatever the model used. In terms of the methods used for gathering information, some examples are provided in this document, although the list is not exhaustive and can be expanded.

The WCO hopes that this Guide to Corruption Risk Mapping will become a useful tool to be used in combination with other approaches to fight corruption. Feedback on the use of this Guide from Members would be welcome, with a view to potentially including case studies to illustrate the theory presented in this document.

*

* *

BIBLIOGRAPHY

AHMED M. and BISKUP R. (2013), 'Anti-Corruption Risk Assessment'. Available at, last accessed on 21/12/2014

BARANOFF E., BROCKETT P., PATRICK L. KAHANE, (2009), 'Risk Management for Enterprises and Individuals', Chapter 4 Evolving Risk Management: Fundamental tools, available at:http://www.saylor.org/site/wp-content/uploads/2013/06/Risk-Management-Ch4.pdf, last accessed on 15/1/2015

BESWICK K. and BLOODWORT J. (2003), 'Risk mapping– Dilemmas and solutions' in Risk Management Topic Paper No. 4.Available at http://www.rudnicki.com.pl/pub/Aus_risk_mapping.pdf), last accessed 21/12/2014

INGRAM D. (2014), 'Guide to ERM: Risk identification'. Available at http://blog.willis.com/2014/01/erm-practices-risk-identification, last accessed on 10/04/2015

INGRAM D., HEADEY P. (2004), 'Best Practices for the Risk Mapping Process', Milliman Consultants and Actuaries. Available at http://publications.milliman.com/research/life-rr/archive/pdfs/Best-Practices-Risk-Mapping-RR-07-01-04.pdf, last accessed on 5/2/2015

FEDERAL EMERGENGY MANAGEMENT AGENCY (2008), 'Risk Map Strategy – Integrating Mapping, Assessment, and Mitigation Planning. Available at http://www.fema.gov/pdf/plan/risk_map_strategy_02202008.pdf, last accessed on 21/12/2014

GOVERNMENT OF THE REPUBLIC OF MOLDOVA (2011), Informative Note to the draft Governmental decision on approval of the methodology of corruption risk assessment in public institutions. Available at: http://www.coe.int/t/dghl/cooperation/economiccrime/moneylaundering/projects/molico/AC/Output1.6/912%20MOLICO%20Nat%20%20Legisl%20_methodology%20of%20corruption%20risk%20assessment.pdf, last accessed on 15/1/2015

McDEVITT, A. (2011), 'Corruption Risk Assessment Topic Guide' in Gateway Corruption Assessment Toolbox, Transparency International. Available athttp://gateway.transparency.org/files/uploads/Corruption_Risk_Assessment_Topic_Guide.pdf, last accessed on 21/12/2014

WCO (2011), WCO Customs Risk Management Compendium

WCO (2014), WCO Integrity Development Guide

WILLIAMS T., SAPORITO S. (2001), 'Risk mapping – a risk management tool with powerful applications in the new economy'. Available at: http://sun.iwu.edu/~jpark/bus200/reading/risk%20mapping.pdf, last accessed on 22/12/2014

ZARNOWIECKI M. DURANI A. and HUSSAIN Y. (2010), 'Governance Analysis Toolkit for Customs and Border Management', World Bank

x

x x

ANNEXES

Annex I **Example of risk identification and risk description form**

Organization/ department:	**Sheet : of**

Scope :	**Date: by:**

#	Vulnerability	Trigger	Consequences	Severity	Probability

Source: Williams T. and Saporito S., 2001

x

x x

Annex II **Examples of risks specific to Customs**

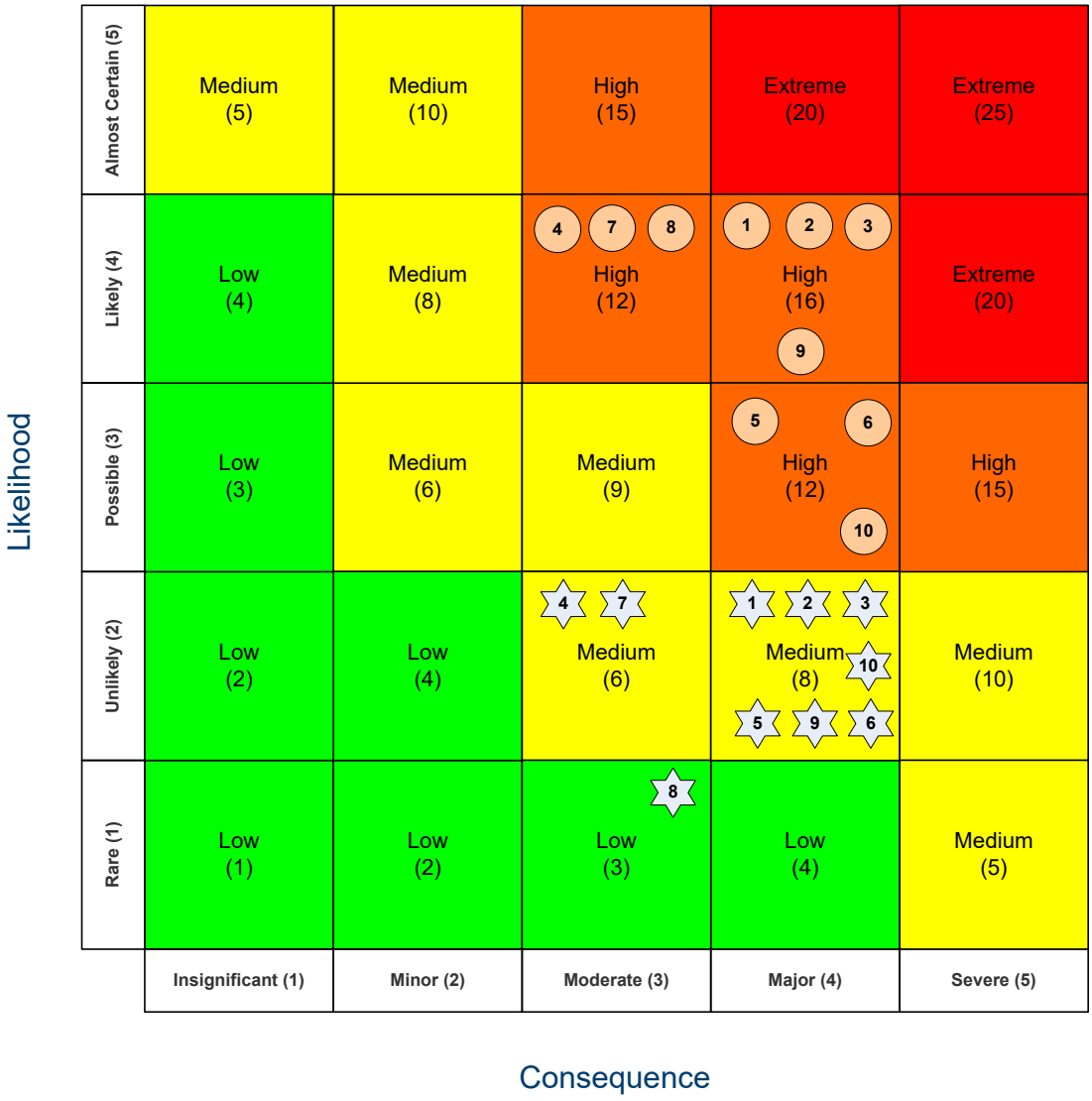
Risk number	Risk Title
1	Misuse of information
2	Criminal Infiltration
3	Organizational culture undermined
4	Theft
5	Abuse of office
6	Criminally motivated persons go unchecked
7	Improper procurement
8	Inappropriate use of resources and/or property
9	Drug use and/or possession
10	Dishonest disclosure

Source: New Zealand Customs Service

x

x x

Annex III **Risk Heat Map**



Absolute risk Residual risk

Source: New Zealand Customs Service

x

x x

Annex IV **Consequences and likelihood of risks**

Likelihood Scales

Category	*Example of Qualitative Measures*
Almost Certain	The event is expected to occur in most circumstances / has occurred in portfolio in the last year
Likely	The event will probably occur in most circumstances / has occurred in portfolio in the past
Possible	The event might occur at some time / has occurred at least once in portfolio
Unlikely	The event is not expected to occur in most circumstances / has not occurred in portfolio but has occurred in other government entities
Rare	The event will only occur in exceptional circumstances / is possible, but is not known to have occurred in the past

Consequence Scales

SEVERE	***Reputation / Compliance***	• Royal commission • Complete loss of stakeholder confidence • Intense public, political and media scrutiny/criticism evidenced by front-page headlines, adverse international media and reports and/or sustained television coverage • Ministerial/secretary resignation • Breach of Constitution
	Safety and security of Australians	• Safety and security of Australia and/or Australians at risk with severe consequences due to failure to adequately protect the border • Large scale serious offences under Customs Act and other agency's legislation enforced by Customs and Border Protection
	Supporting legitimate trade and travel	• Clearance delays causing severe disruption to clients • Air and sea cargo delay are causing severe financial and community impact
	Economic (including Commercial interest of Australians and Collection of border revenue)	• Collections against revenue forecast are unexpectedly and/or significantly under target. The shortfall cannot be linked to general economic conditions. It is likely that Parliament and/or Government will initiate an enquiry into the shortfall
	Resources	• Greater than 5% impact on budget • Death or serious permanent disablement of staff or clients
	Business continuity	• Loss of service capacity for more than four hours • Destruction or disastrous long term damage to most assets • Epidemic causes long term, large scale staff absences, death or disablement
	Environment	• A Customs and Border Protection action will accidentally cause very serious, long term environmental impairment of world listed ecosystem functions. Damage will occur beyond Australian

		waters. Damage will be economic, social and environmental
MAJOR	***Reputation / Compliance***	• Parliamentary enquiry • Serious loss of stakeholder confidence • Adverse national media reports on failings, inefficiency or inadequacy • Serious embarrassment to Minister and government • Breach of Commonwealth law and regulations (including standards)
	Safety and security of Australians	• Safety and security of Australia and/or Australians at risk with major consequences due to failure adequately protect the border • Serious offences under Customs Act and other agency's legislation enforced by Customs and Border Protection
	Supporting legitimate trade and travel	• Clearance delays causing major disruption to clients • Air and sea cargo delays are causing major financial and community impact
	Economic (including Commercial interest of Australians and Collection of border revenue)	• 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 Parliamentary and Government • Fraud – theft of (external) revenue collected greater than $500,000 • Error in revenue collection – undetected long term of high value
	Resources	• Up to 5% impact on budget • Unable to attract any skilled staff • Political decision to cut program • Work accident leads to extensive or serious staff/client injury or temporary disablement
	Business continuity	• Loss of service capacity for over one hour • Loss of large number of staff • Destruction or serious damage to key physical or information assets • Change of government leads to unsupported program changes
	Environment	• A Customs and Border Protection action will accidentally cause very serious, long term environmental impairment of nationally critical ecosystem functions. Damage will have economic consequences for Customs and Border Protection
MODERATE	***Reputation / Compliance***	• Scrutiny/criticism by external committees, ministerial questions or ANAO • Substantial adverse publicity or loss of some stakeholder confidence • Risk event requires Ministerial response • Breach of CEI's and other CEO instructions / reportable breach of legislation
	Safety and security of Australians	• Safety and security of Australia and/or Australians at risk with moderate consequences due to failure to adequately protect the border • Moderately serious offences under Customs Act and other agency's legislation enforced by Customs and Border Protection
	Supporting legitimate trade and travel	• Clearance delays causing moderate disruption to clients • Air and sea cargo delays are causing moderate financial and community impact
	Economic (including Commercial interest of	• Collections against revenue forecast are under target, and the shortfall is not linked to general economic conditions • Fraud – theft of internal funds greater than $1000

	Australians and Collection of border revenue)	• Fraud – theft of (external) revenue collected of less than $500,000 • Error in revenue collection – systematic and/or of significant value
	Resources	• Up to 2% impact on budget • Skilled staff shortages lead to significant additional costs or delays • Work accident leads to staff/client hospitalisation
	Business continuity	• Loss of service capacity for up to one hour • Permanent loss of key staff • Damage to physical and information assets including back-ups
	Environment	• A Customs and Border Protection action will accidentally cause serious medium term environmental effects to important ecosystems. Scrutiny by Federal and State governments may occur
MINOR	***Reputation / Compliance***	• Some adverse publicity • Internal review of existing policies and practices instigated • Minor loss of stakeholder confidence • Breach of guidelines
	Safety and security of Australians	• Safety and security of Australia and/or Australians at risk with minor consequences due to failure to adequately protect the border •
	Supporting legitimate trade and travel	• Clearance delays causing minor disruption to clients • Air and sea cargo delays are causing minor financial and community impact
	Economic (including Commercial interest of Australians and Collection of border revenue)	• Collections against revenue forecast are under target but only by a small amount • Fraud – theft of internal funds between $100 - $1000 • Error in revenue collection – minor value
	Resources	• Up to 1% impact on budget • Staff members sustains minor injury requiring medical attention • Staff absence increase significantly to cause delay
	Business continuity	• Loss of service capacity for up to 30 mins • Temporary loss of key staff
	Environment	• A Customs and Border Protection action will accidentally cause moderate, short term effects but not effecting ecosystem functions. It will be manage by an environmental plan
INSIGNIFICANT	***Reputation / Compliance***	• Internal impact only • No adverse publicity or ministerial involvement • No stakeholder conflict • Managed by Customs and Border Protection staff
	Safety and security of Australians	• Safety and security of Australia and/or Australians potentially impaired in an insignificant manner
	Supporting legitimate trade and travel	• Clearance delays cause insignificant disruption to clients • Air and sea cargo delays are causing insignificant financial and community impact
	Economic	• Collections against revenue forecast are under target and could be

	(including Commercial interest of Australians and Collection of border revenue)	justified by statistical error • Fraud – theft of internal funds less than $100 • Error in revenue collection – isolated and/or insignificant value
	Resources	• No impact on budget or targets • Staff member sustains minor cuts or abrasions requiring first aid treatment
	Business continuity	• Loss of service capacity for up to 10 mins
	Environment	• A Customs and Border Protection action will accidentally cause minor effects on biological or physical environment but will be managed by an environmental plan

Source: Australian Customs and Border Protection Service (ACBPS)

x

x x

Annex V **Effectiveness of control evaluation tool**

	• Current controls are robust and effective and significantly reduce the risk level • The likelihood of the risk occurring is very low • The controls in place practically eliminate the consequences of a risk should it occur.
	• Current controls are very good and reduce the risk level • The likelihood of the risk occurring is low but some improvement to current controls could be made • The controls in place significantly alleviate the consequences of a risk should it occur.
	• Current controls are reasonable but not considered effective enough to reduce the risk to an acceptable level • The likelihood of the risk occurring is moderate • The controls in place moderately alleviate the consequences of a risk should it occur but there is potential for the controls to fail. Further controls or redesign of controls necessary.
	• Current controls manage only some of the risk • The likelihood of the risk occurring is high • The controls in place slightly alleviate the consequences of a risk should it occur. Further work and redesign of controls necessary.
	• Current controls are weak and do not control the risk • The likelihood of a risk occurring is extremely high • The controls in place are largely ineffective and unlikely to lessen the consequences of a risk should it occur. Urgent attention is required to develop and implement effective controls.

Source: ACBPS

x x x

Annex VI

Levels of risk matrix

	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Low (5)	Medium (10)	High (20)	Extreme (40)	Extreme (80)
Likely	Low (4)	Medium (8)	High (16)	High (32)	Extreme (64)
Possible	Low (3)	Low (6)	Medium (12)	High (24)	Extreme (48)
Unlikely	Very Low (2)	Low (4)	Medium (8)	High (16)	High (32)
Rare	Very Low (1)	Very Low (2)	Low (4)	Medium (8)	High (16)

Risk Rating	Tolerance
Extreme	Zero or very limited for risk
High	Low tolerance for risk
Medium	Medium to low tolerance for risk
Low	Medium to high tolerance for risk
Very Low	High tolerance for risk

Source: ACBPS

x

x x

Annex VII **Corruption Prevention Plan and Evaluation Status**

Corruption Prone Area	Current Status	Risk Ranking	Desired Status	Strategies To Achieve Desired Status	Time Frame				Implementation Status	Responsibility	Remarks
					0	3	9	12			

Corruption Prevention Plan (CPP) & Evaluation Status:

1. Identify and document the majority of operational risks that exist in each business unit
2. identify the current status
3. Rank the risk - high risk, medium risk or low risk
4. State where we would like to be i.e. desired status
5. Indicate strategies that will enable the section achieve their desired status
6. Indicate a time frame in achieving the desired status – immediately (0), 3, 6, 9 or 12 months.
7. Each unit/section will on a monthly basis indicate implementation status of the strategies
8. Responsibility- indicates the office responsible for the implementation of strategies

Source: Kenya Revenue Authority

x

x x

Annex VIII **Glossary of terms related to risks**

Term	Explanation
Consequence	Calculation of the outcome of an event affecting objectives. One event can lead to a range of consequences; these can be positive (opportunity) or negative (threat). Consequence is rated on a scale of 1 (insignificant) to 5 (severe).
Control	An action, process, policy or device intended to modify a risk. Controls reduce uncertainty and should avoid, mitigate or leverage the risk.
Control Strategy / Risk Treatment	A plan to reduce the severity of our exposure to a risk. A control strategy may include removing risk drivers, reducing the likelihood of events or the severity of the consequences. They may occur over time (e.g. reducing organized crime) and may include a combination of routinely administered controls (e.g. profiles, site visits) and ad hoc interventions (e.g. investigations, campaigns).
Corruption	Behavior on the part of officials in the public or private sector in which they improperly and unlawfully enrich themselves or those close to them, or induce others to do so, by misusing the position in which they are placed
Current risk	A risk that has existing control(s) in place that is working to control the risk.
Emerging risk	Newly developing or changing risk which may be difficult to quantify and which may have a major impact on the organization.
Employee	All persons employed by the New Zealand Customs Service, within New Zealand and offshore. It applies to persons engaged by Customs in a contractor and consultant arrangements
Fraud	Fraud – Dishonest activity causing actual or potential financial loss to any person or entity, including theft of money or other property, by employees or persons external to the entity; and where deception is used at the time, immediately before or immediately following the activity.
Gross risk	The risk with no controls in place. Also known as absolute or inherent risk.
Harm	The negative consequence that is caused by an untreated risk or by the residual of a risk.
Infiltration	Enter or gain access to an organization or place surreptitiously and gradually, in order to acquire secret information.
Inherent Risk	The raw or untreated risk. Inherent risk is the risk exposure if no attempt is made to reduce or control the exposure. (The risk with no controls in place. Also called absolute risk.)
likelihood	The word likelihood used in Risk management to refer to the chance of something happening ,whether defined , measured or determined objectively and subjectively , qualitatively or quantitatively and described using general terms or mathematically (A measure of how likely it is that a certain consequence will eventuate, ranging from rare to almost certain.)
Misconduct	Behavior that is inconsistent with the Code of Conduct.

Term	Explanation
Organized crime	A structured group of three or more persons, existing for a period of time and acting together with the aim of committing one or more serious crimes in order to obtain, directly or indirectly, a financial or other material benefit
Residual Risk	The risk remaining after controls are taken into account. The residual risk may require further treatment. The exposure to risk after the application of controls. In the absence of controls, residual risk equals inherent risk.
Risk	The effect of uncertainty on objectives Note 1 An effect is a deviation from the expected – positive or negative Note 2 Objectives can have different aspects such as financial, health and safety etc. and can apply at different levels such as strategic, organizational, project, product and process. Note 3 Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives. Note 4 Risk is often expressed in terms of a combination of the consequence of an event or a change in circumstances, and the associated likelihood of occurrence. Note 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, and event, its consequence, or likelihood.
Risk appetite	The amount or type of risk that an Administration is willing to pursue or retain.
Risk Assessment	Overall process of risk identification, risk analysis, risk evaluation and prioritization.
Risk Criteria	The standards by which the significance of a risk is judged including values and evidence given the internal (agency) and external (social, economic, political) contexts in which the risk occurs.
Risk Drivers	The factors that increase uncertainty or cause an exposure to a risk (e.g. patterns of drug use and demand or changes in production and supply).
Risk Evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk responses can include: Tolerate Terminate Treat Pursue (increase risk) Transfer
Risk Events	The evidence of the presence of a risk. Events have consequences. It is these we are trying to manage.
Risk Exposure / Vulnerability	The degree that the consequences of a risk threaten strategic objectives. It is our relative exposure to a risk vis-à-vis our exposure to other risks.
Risk Treatment	The decision or action taken in response to an identified risk. Approaches to risk treatment include: • Tolerate – accepting the risk

Term	Explanation
	• Terminate – ceasing the activity that creates the risk • Treat – mitigating the risk (in the case of a threat) to reduce the likelihood and/or consequence or (in the case of an opportunity) to enhance the likelihood and/or consequence. • Pursue (increase risk) • Transfer – share or transfer the risk to another work area, Division, Group or Agency.
Serious misconduct	Behavior that is inconsistent with the Code of Conduct and breaches the employee's duty to the employer to such an extent that the employment relationship may not be able to continue due to a breakdown in trust and confidence.
Threat	For the purposes of the Risk Management Framework 'threat' and 'risk' have the same meaning - "The effect of uncertainty on objectives" [AS/NZS ISO 31000] Staff may refer to threat(s) in detailed reports where 'opportunity, capability and intent' has been established. The likelihood that an adverse risk event or events will occur.
Tolerance and Acceptance	The exposure to a risk that we are prepared to accept for a set of benefits (e.g. between cargo supervision and trade facilitation). 'Tolerable' means additional risk reduction effort exists, but it is accepted, given the benefits. As resources are limited, tolerance will frequently be a relative judgment given the importance of other risks. 'Acceptable risk' is where remaining risks are evaluated to be low, making additional reduction efforts unnecessary.

Source: WCO Customs Risk Management Compendium

x

x x

Annex IX Model personnel questionnaire to assist in the risk mapping exercise

	Question	Answer
1.	Do you carry out vulnerable actions? (If not, go to question 7.)	Yes/No/Don't know
2.	If you do carry out vulnerable actions, could you give (a maximum of) three examples below? Example1: Example 2: Example 3:	Yes/No/Don't know
3.	Are there regulations for the execution of the actions you have mentioned? Example1: Example 2: Example 3:	Yes/No/Don't know
4.	If so, please indicate, for each example, whether you know the content of these regulations. Example1: Example 2: Example 3:	Yes/No/Don't know
5.	Apart from any job-related consultation which normally takes place, do you receive special guidance from your superior in order to execute these actions?	Yes/No/Don't know
6.	Do you execute these actions in co-operation with close colleagues?	Yes/No/Don't know
7.	Are you in possession of your job description?	Yes/No/Don't know
8.	Do you think that, in practice, you have greater powers than you have formally been given? In other words: is there a 'grey area' in this respect?	Yes/No/Don't know
9.	If so, do you consult with your superior *beforehand* regarding decisions in this 'grey area'?	Yes/No/Don't know
10.	Is your superior generally quickly and easily available for consultation?	Yes/No/Don't know
11.	Is there a form of joint consultation about work (work consultation) with your superior and close colleagues?	Yes/No/Don't know
12.	If you have work consultation, can you indicate the average frequency? - Less than once a month - Once a month - More than once a month	Yes/No/Don't know
13.	If you do have work consultation, how often is the topic 'integrity in	Yes/No/Don't know

	Question	Answer
	work situations' discussed? - Never - Less than once a month - Once a month - More than once a month	
14.	Do you have an evaluation by your superior (a minimum of) once a year?	Yes/No/Don't know
15.	If you have an evaluation by your superior, is attention given to the topic of 'integrity in work situations'?	Yes/No/Don't know
16.	Do you have contacts with external parties in your work?	Yes/No/Don't know
17.	Does your superior know which external parties you have contact with in your work?	Yes/No/Don't know
18.	Does your superior know what these contacts are about?	Yes/No/Don't know
19.	How often, on average, do you report to your superior about your work? - Less than once a month - Once a month - More than once a month	Yes/No/Don't know
20.	Does reporting to your superior about your work lead, in practice, to: - A complete report and control of content? - Testing or controlling parts of the work? - Routine approval of the work?	Yes/No/Don't know
21.	In your work, have you ever heard about a colleague's private problems (financial or relationship problems, etc.)?	Yes/No/Don't know
22.	Is it possible to discuss private problems (financial or relationship problems, etc.) in your organization?	Yes/No/Don't know
23.	Have you ever been confronted with matters in which your professional decisions could have consequences for your private life? If so, have you handed over the matter to someone else, or involved a colleague or your superior in the decision?	Yes/No/Don't know
24.	Have you ever heard of attempts by external parties to improperly influence a colleague's professional decisions? If so, do you know if these attempts have been formally reported within your organization?	Yes/No/Don't know
25.	Have you ever heard of cases of fraud, theft or other actions that constitute breaches of integrity?	Yes/No/Don't know
26.	Are there regulations for dealing with such cases?	Yes/No/Don't know
27.	If so, do you know the content of these regulations?	Yes/No/Don't know
28.	Are these regulations applied in practice?	Yes/No/Don't know
29.	Do you deal with confidential information?	Yes/No/Don't know
30.	Are there regulations in your organization or department regarding the dissemination to unauthorized persons of confidential information?	Yes/No/Don't know

	Question	Answer
31.	If so, do these regulations relate to: - The alteration and/or translation of confidential information? - The dissemination of confidential information? - The copying of confidential information? - The administration or documentation of confidential information? - The storage or safekeeping of confidential information (for example, a 'clean desk policy')?	Yes/No/Don't know
32.	Are these regulations applied in practice?	Yes/No/Don't know
33.	Are there regulations in your organization or department for accepting gifts or hospitality? If so, do you know the content of these regulations? Are these regulations applied in practice?	Yes/No/Don't know
34.	Are there regulations in your organization or department for having a second job (moonlighting) or additional income?	Yes/No/Don't know
35.	If so, do you know the content of these regulations? Are these regulations applied in practice?	Yes/No/Don't know
36.	Are there regulations in your organization or department for accepting remuneration from third parties for activities that are a natural part of your function or job (such as giving lectures or courses, consultancy, etc.)? If so, do you know the content of these regulations? Are these regulations applied in practice?	Yes/No/Don't know
37.	Is it common practice for close colleagues to inform each other about work-related actions that will be taken or have already been taken?	Yes/No/Don't know
38.	In the organization or department where you work: Serious mistakes or omissions are generally tolerated. Mistakes made by higher-grade officials are tolerated and covered up much more easily than for lower-grade personnel.	Yes/No/Don't know
39.	It is very important to phrase remarks and comments very carefully if you want to criticize something.	Yes/No/Don't know
40.	Offering criticism seldom leads to adaptations or changes in work procedures.	Yes/No/Don't know
41.	What type of position do you have: Managerial or non-managerial?	Yes/No/Don't know
42.	What is the name of the organization, department, team, bureau, etc. where you work?	Yes/No/Don't know

INTERPRETATION OF ANSWERS FROM THE MODEL PERSONNEL QUESTIONNAIRE

1. Vulnerable actions, Questions 1 to 6:

Possible answers: If the answer is ‘no’ or ‘don’t know’, when it is known for certain that there are vulnerable activities.

Interpretation:

- Insufficient alertness or awareness regarding vulnerable aspects of actions in the role.
- Insufficient clarity about correct execution of vulnerable actions; encouragement to act according to the circumstances (on one’s own accord), with (too much) emphasis on personal concept of integrity.
- Solo actions with insufficient consultation and control.
- Insufficient knowledge and authorization, with the possible result that vulnerable actions are not executed with sufficient care.

2. Grey area, Questions 7 to 9:

Possible answers: If the answer is ‘no’ or ‘sometimes’

Interpretation:

- Insufficient knowledge about formal tasks and powers.
- Complete lack of checks on lawfulness of actions or decisions, resulting in mistaken actions not being noticed or corrected. Arbitrary actions.

3. Consultation, Questions 10 to 15

Possible answers: If the answer is ‘no’ or ‘not once’

Interpretation:

- Encouragement to act according to the circumstances (on one’s own accord), with (too much) emphasis on personal concept of integrity.
- Solo actions and decreasing possibilities for hierarchical and collegiate control.
- Insufficient alertness or awareness concerning the requirement of integrity.
- Insufficient management, coaching, correction and control of actions.
- Insufficient recognition that integrity must play an important part in actions, resulting in less alertness and awareness.

4. External contacts, Questions 16 to 18

Possible answers: If the answer is ‘no’

Interpretation: Insufficient control, resulting in lack of possibilities to recognize risky contacts. Solo actions.

5. Accountability and control, Questions 19 to 20

Possible answers:

- If the frequency given for Question 19 is insufficient, according to the assessment group,

given the nature of the organization and subdivision.

- If the answer to Question 20 is ‘routine approval’

Interpretation:

Insufficient control of vulnerable actions; solo actions and acting according to the circumstances, insufficient depth of control.

6. Interface between work and private life, Questions 21 to 23

Possible answers: The answer ‘yes’ to Question 22 and ‘no’ to Question 23

Interpretation:

- Insufficient recognition of (appearance of) conflict of interest, which
- Possibly results in loss of integrity.

7. Dishonest external parties, Question 24

Possible answers: The answers ‘yes’ to Question 24 part 1, and ‘no’ to part 2

Interpretation:

- Insufficient sense of security of person in question; insufficient level of alertness of supervisor and close colleagues with respect to the external parties concerned.

8. Dishonest officials, Questions 25 to 28

Possible answers: If the answer is ‘no’ or ‘don’t know’

Interpretation:

- Insufficient safeguarding of consistent approach and correction of actions involving breaches of integrity; insufficient awareness of the consequences of actions involving breaches of integrity; arbitrary actions, acting according to the circumstances.
- Insufficient safeguarding of consistent approach and correction of actions involving breaches of integrity; insufficient awareness of the consequences of actions involving breaches of integrity.
- Arbitrary actions, acting according to the circumstances; insufficient preventive effect of the approach and correction of actions involving breaches of integrity.

9. Confidential information, Questions 29 to 32

Possible answers: The answers ‘no’ or ‘don’t know’

Interpretation: Threshold against information leaks is too low; emphasis on personal alertness and care regarding actions is too great.

10. Gifts and hospitality, Question 33

Possible answers: The answers ‘no’ or ‘don’t know’

Interpretation: Threshold against information leaks is too low; emphasis on personal alertness and care regarding actions is too great.

11. Moonlighting and additional income, Questions 34 to 36

Possible answers: The answers ‘no’ or ‘don’t know’

Interpretation:

- Threshold against conflicts of interest is too low; emphasis on personal alertness and care regarding actions is too great.
- Threshold against conflicts of interest is too low; emphasis on personal alertness and care regarding actions is too great.

12. Communication, loyalty and self-correction mechanisms, Questions 38 to 42

Possible answers: The answers ‘yes’ or ‘no’ to Question 40

Interpretation:

- Insufficient internal communication. Insufficient communication can be particularly risky if, in addition, a negative answer has been recorded for one or more of the following items: ‘grey area’, consultation, external contacts, confidential information, money and budgets, goods and services, gifts and hospitality, or moonlighting and additional income.
- Insufficient mechanisms for self-correction. Insufficient mechanisms for self-correction can be particularly risky if, in addition, a negative answer has been recorded for the item accountability and control.

Source: Government of Moldova

x

x x

Annex X **Model Corruption Risk Report**

Issue	Procedures applied / identified problem	Identified risk	Solutions
Existence of integrity reference (Code of Conduct, for example)	No (or incomplete) regulations.	No uniform procedures; insufficient thresholds against abuses; acting on one's own discretion; establishment of ad-hoc structures; high emphasis on individual interpretation of integrity.	Draw up or improve regulations for all categories of vulnerable activities.
Content of integrity reference	Regulations are insufficiently focused on integrity requirement.	Insufficient provisions to prevent solo actions; insufficient control provisions for supervision.	Discourage solo actions and improve supervision through the formulation of regulations pertaining to teamwork, separation of duties, joint decision-making, accountability (structural reporting), structural supervision, unambiguous criteria for evaluation, written accounts of activities and decisions.
Familiarity of staff with the content	Insufficient familiarity with the regulations.	No uniform procedures; acting on one's own discretion.	Improve familiarity with the regulations by wide distribution and general accessibility.
Application	Inadequate application of the regulations.	Arbitrariness.	Encourage application of the regulations by exemplary conduct of the management, supervision, imposing sanctions in the event of non-application or misapplication.
Specific regulations on management of confidential information	Lack of, unknown and/or unapplied regulations.	Threshold against leaking of information too low; insufficient alertness; reduced personal care.	Prevent viewing by unauthorized persons by drawing up regulations for the handling of information (production, alteration, distribution, duplication, administration, storing, etc.); wide dissemination of the regulations; imposing sanctions for non-compliance; independent audits.

Issue	Procedures applied / identified problem	Identified risk	Solutions
Selection of personnel	Insufficient attention to integrity requirement.	Insufficient insight into integrity of potential personnel; insufficient attention to vulnerable aspects of the new job; arbitrariness.	Selection and appointment via consistent application procedures; requiring extensive CVs; requiring verification of references; enquiries about performance in previous jobs; verification of original diplomas and certificates; requiring a certificate of good behaviour; informing applicants about integrity aspects involved in the position; taking an oath (or solemn affirmation) of office (integrity requirement); induction programme (attention to integrity).
Training of personnel	Omission of an important means of drawing attention to the integrity requirement.	Reduced alertness; reduced awareness; reduced care.	Enhance integrity-related alertness and awareness by drawing specific attention to the integrity requirement in courses, information material.
Job description	None or not updated; incomplete or imprecise job descriptions.	Insufficient clarity about duties and powers; acting on one's own discretion.	Provide clarity on duties and powers through up-to-date, complete and precise job descriptions.
Internal and external positions are combined	Many types of vulnerable activities combined in one position.	Inadequate concentration.	Make the risk controllable through separation of duties.
Existence of 'grey area'	Powers in practice have wider scope than is formally permitted.	Lack of clarity about lawfulness of activities and decisions.	Remove 'grey area' through adequate job descriptions.
Consultation and accountability	No prior consultation or subsequent evaluation; no prior consultation on the conditions for subsequent evaluation.	Lawfulness not checked; mistakes not detected or corrected; correction only possible when mistakes have already been made; occasional prior consultation or subsequent evaluation; arbitrariness.	Guarantee lawfulness of activities in 'grey area' through consistent prior consultation (optimum threshold) or subsequent evaluation (minimum threshold).

Issue	Procedures applied / identified problem	Identified risk	Solutions
Availability of supervision	Supervisor/direct line manager not available for quick consultation.	Solo actions; acting on one's own discretion.	Prevent solo action and improve control by adequate availability of the supervisor; appoint deputy supervisor (if necessary).
Attention to integrity	No or little consultation focused on integrity (less than once a month).	Acting on one's own discretion; insufficient (social) control; insufficient alertness to or awareness of integrity requirement.	Prevent solo actions, encourage (social) control and attention to integrity through regular consultation (at least once a month); integrity as a permanent item on the agenda.
Job performance appraisal interviews	Job appraisal interviews less than once a year and/or no attention to vulnerable aspects.	Inadequate control, guidance, supervision and correction; reduced alertness and awareness.	Encourage control and alertness by periodic job appraisal/evaluation interviews in which attention is paid to integrity aspects.
External contacts	Supervisor/direct line manager is not aware of external contacts of employees.	Inadequate control; reduced opportunity to identify risky contacts; solo action.	Prevent solo actions, encourage control and prevent conflicts of interest through obligatory reports on external contacts; external contacts as a permanent item on the agenda.
Accounting and supervision	Frequency of reporting on vulnerable activities is insufficient; routine checks through supervision.	Inadequate supervision; solo action; acting on one's own discretion; inadequate control.	Encourage the correct and careful performance of vulnerable duties in a preventive sense and, if necessary, correct mistakes by asking employees to provide an account as regularly as possible; overall supervision or representative random checks of work.

Issue	Procedures applied / identified problem	Identified risk	Solutions
Work/private life interface	Private problems affecting the job are not discussed; official decisions with consequences for private life are handled by one person.	Breach of integrity caused by insufficient recognition of tensions and conflict situations; breach of integrity caused by insufficient recognition of conflicts of interest.	Prevent breach of integrity as a result of interface between work and private life through the creation of a working climate in which private problems can be discussed; the appointment of a company social worker; obligation to report to the supervisor decisions with consequences for private life; delegating or sharing such decision-making.
Dishonest external parties	Attempted violations of integrity are not reported.	Undermining of the organization.	Encourage company-wide alertness through obligation to report attempted violations of integrity to the supervisor.
Dishonest employees	Lack of, unknown and/or unapplied guidelines on how to deal with dishonest employees.	Inconsistent approach and correction of violations (arbitrariness); no awareness of the consequences of corrupt behaviour.	Prevent corrupt behaviour by employees by imposing sanctions.
Gifts, additional income	Lack of, unknown and/or unapplied regulations dealing with gifts and additional income.	Conflict of interests; (too much) emphasis on personal perception of integrity.	Prevent conflict of interests by drawing up regulations and distributing them widely. Supervision of compliance and, if necessary, imposition of sanctions for non-compliance.
Lawfulness versus efficiency	Disproportionate attention to efficiency at the expense of lawfulness.	(Excessive) emphasis on personal perception of integrity.	Increase emphasis on lawfulness and decrease emphasis on personal perception of integrity by focusing on proper job descriptions, awareness-raising about vulnerable activity, relevant procedures regarding external contacts, encouraging accountability and supervision.

Issue	Procedures applied / identified problem	Identified risk	Solutions
Loyalty	Insufficient loyalty or exaggerated loyalty to one's own department or colleagues.	(Too) little attention to the common good; defiant behaviour; covering up of mistakes or shortcomings.	Encourage loyalty within the (overall) organization by drawing up a general Code of Conduct. Reduce the risk by focusing on the measures dealing with external contacts, the interface work/private life, gifts/additional income.
Communication	Inadequate internal communication.	Gap between management and employees; no clarity about activities of colleagues; reduced social control.	Reduce the risk by focusing on measures dealing with the job description, supervision, frequency of consultations, focus on integrity, job appraisals, external contacts, regulations covering confidential information, funds and budgets, purchase of goods and hiring services, private use of goods and services, gifts and additional income; encourage internal communication and also lay down agreements in a general Code of Conduct.

Source: Government of Moldova