FORUM ON TAX ADMINISTRATION

Communities of Interest Series

Enhancing Reputational Risk Management

OECD

BETTER POLICIES FOR BETTER LIVES

Please cite this publication as:
OECD (2020), *Forum on Tax Administration: Enhancing Reputational Risk Management*, OECD, Paris.
www.oecd.org/tax/forum-on-tax-administration/publications-and-products/coi/enhancing-reputational-risk-management.htm

Photo credits: © optimarc – Shutterstock.com

Communities of Interest Series

Enhancing Reputational Risk Management

Preface

I am pleased to share with my colleagues in the Organisation for Economic Co-operation and Development's Forum on Tax Administration (OECD FTA) the Canada Revenue Agency (CRA)'s research paper on reputational risk management for tax administrations.

We at the CRA have worked closely with our partners in the OECD FTA Enterprise Risk Management Community of Interest (COI) to develop a set of strong tools and resources that can help tax administrations strengthen their capacity to manage reputational risk.

As our economies develop and our tax landscape evolves, tax administrations more than ever have to ensure that they have the trust and respect of their taxpayer and stakeholder populations. For this reason, it is crucial that all tax administrations actively protect their reputations. When the reputation of a tax administration is put into question, taxpayers may have less incentive to voluntarily comply with their tax obligations.

The paper describes a reputational risk management maturity model. Tax administrations can use this model to gain insight into the maturity of their reputational risk management practices. The paper also presents two tools developed by the CRA that help tax administrations actively protect against significant sources of reputational risk.

This topic is also very timely as we continue to deal with the impacts – present and future – of the COVID-19 crisis. A tax administration's reputation can be an important factor in providing confidence and trust during such an extraordinary event. This is true not only as the crisis unfolds but also as we, hopefully, move past the crisis and into the recovery period.

There are strong, naturally reinforcing linkages between a tax administration's reputation and its employees. While we rely on our employees to deliver the results and services to our stakeholders that strengthen our reputation, a strong reputation acts as a source of pride and motivation for those employees to keep delivering at their best. I have seen countless examples of CRA employees going far, far beyond the call of duty since the current crisis began. These incredibly dedicated and talented individuals, who number in the thousands, do so in part because they believe that it is their duty to protect and support our citizens – and they are proud to do so.

The CRA consciously undertook a service transformation in the past couple of years, driven the by the desire to adopt an organisational culture that puts "People first". This encompasses not only our employees, but also the citizens of Canada, whom we serve. In mobilising our employees to contribute to the Government of Canada's response to the economic impacts of the pandemic on the Canadian population, our recently adopted vision of being *Trusted, fair and helpful by putting people first* became ever more meaningful. I know my colleagues in other

tax administrations have their own perspectives on how their reputations played a role during this crisis.

Tax and benefit administrations have long been one of the most crucial pillars of governments in support of their citizens not just in times of prosperity and stability, but also in time of crisis. The global economic impacts of the coronavirus pandemic have been sudden, and they will be felt for some time to come. As governments around the world work to address these impacts, there is a heightened awareness and importance of tax administrations as they play a significant part in the recovery solution. This is a platform to build on as we go into the recovery phase in thinking about how to measure the impact of this experience on our respective organisations' reputational risks. This is something that not only helps in recovery but could be a notable shift in the relationship between tax administrations and taxpayers for a long period.

Bob Hamilton

Commissioner

Canada Revenue Agency

Acknowledgments

This successful creation of a comprehensive reputational risk management maturity model for tax administrations rests on the shoulders of a number of members and friends of the CRA family.

The partnership of Brian Philbin, Assistant Commissioner and Chief Audit Executive of the Audit, Evaluation and Risk Branch at the CRA and Jane Hazel, Vice President, Public Affairs and Communications at the Canadian Food Inspection Agency (formerly the Director General of Communications of the Public Affairs Branch at the CRA) provided leadership, energy and direction to the initiative. The CRA's Enterprise Risk Management Division and the CRA's Public Affairs Branch as well as other members of the Audit, Evaluation, and Risk Branch at the CRA brought inspiration and expertise to give shape and substance to the project.

The CRA's Enterprise Risk Management team and the OECD FTA Enterprise Risk Management COI Steering Committee members built a supportive, global community through their efforts to survey tax administrators, solicit their feedback, develop summary assessments of responses and raise community consciousness through their presentations highlighting the value of the CRA approach and mechanisms to gauge and manage reputational risk.

Members of the OECD FTA Enterprise Risk Management COI have been instrumental in the development, acceptance and adoption of the model and their tremendous contributions were paramount in the realisation of this project.

Table of contents

Executive summary

> "It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."
>
> - Warren Buffett

The Canada Revenue Agency (CRA) defines **Reputational Risk** as any event that could damage stakeholders' trust in and respect towards an organisation. Managing this risk suggests that an organisation proactively protects against reputation damaging events, and effectively deals with those events should they occur.

In November 2018, the CRA initiated the development and delivery of a survey of the Organisation for Economic Co-operation and Development (OECD) Forum on Tax Administration (FTA) Enterprise Risk Management Community of Interest (COI) with the aim of developing and improving reputational risk management practices within tax administrations. As many tax administrations in the world are dependent on the willingness of their taxpayers to participate and voluntarily comply with their obligations, the reputation of tax administrations should therefore be actively and concretely measured and managed.

Using the survey information received from participating countries, the CRA developed an approach to protecting and improving reputation that focuses on gauging public perception with priority given to mitigating risk through a combination of operations monitoring and transparency of communications. This paper[1] includes a maturity model, developed in consultation with the OECD FTA Enterprise Risk Management COI, including the active collaboration of 19 member countries. This maturity model allows organisations to assess where they are and where they would like to be along the various components of the reputational risk management continuum.

A reputational risk maturity model highlighting such gaps provides a mechanism that promotes a positive culture of learning and continuous improvement through recognition and adoption of good practice to better align perception and behaviour. The CRA also developed two tools, further explained in the paper, to help identify potential reputation damaging vulnerabilities at the operational level – the Error Prevention Self-Assessment Tool (EPSAT) and the Internal Fraud Risk Self-Assessment Tool (IFR-SAT).

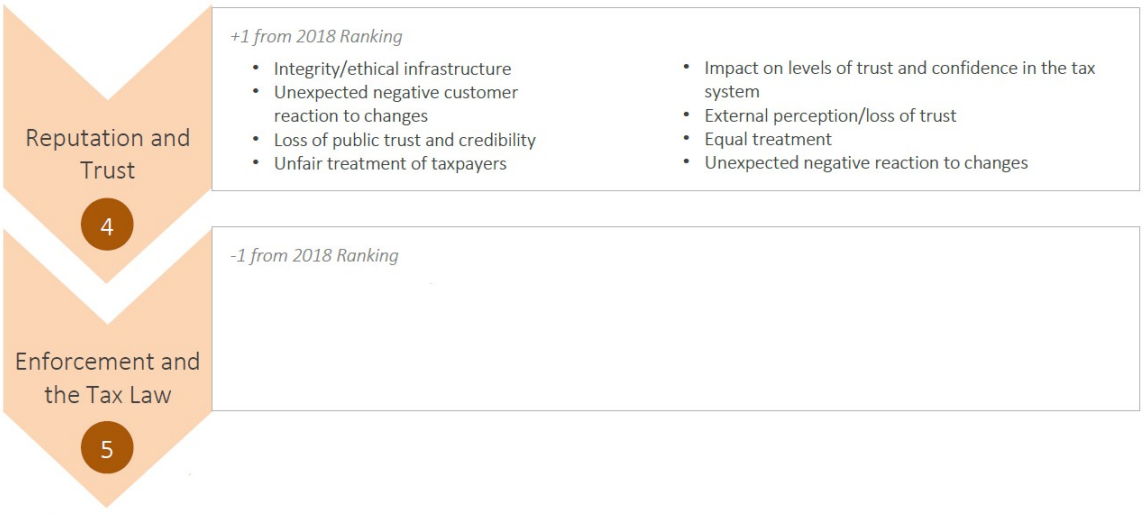
[1] This document was approved by the Committee on Fiscal Affairs on 26 June 2020 and prepared for publication by the OECD Secretariat.

1 Introduction

The concept of reputational risk was first discussed with members present at the 2019 OECD FTA Enterprise Risk Management COI risk workshop in Paris, France. At this workshop, member countries re-ranked the top 11 risks facing tax administrations that were identified in the first FTA Risk Management COI workshop held in January 2018. One notable change that resulted from this re-ranking was that the risk theme "Reputation and Trust" was ranked fourth overall, up one position from 2018 and taking the rank of the risk theme of "Enforcement & the Tax Law".

During the workshop discussions, members noted key drivers of reputational risk for tax administrations as listed in Figure 1.

Figure 1. Excerpt from OECD FTA Enterprise Risk Management COI 2019 top risk ranking



In analysing these drivers, two key principles of reputation come to light: the first, trust of the organisation and its members; and the second, respect towards the organisation. When tax administrations demonstrate their integrity and ethical infrastructure, they position themselves in line (at least) with existing standards and expectations, and this helps to gain respect from their taxpayers. When those organisations consistently abide by their ethical duties, they establish trust in the eyes of their taxpayers and other stakeholders. When they fail to meet their own standards and the expectations of their stakeholders, especially with respect to the fair and equal treatment of taxpayers, public trust and credibility can be quickly eroded.

Reaction to changes made by tax administrations may also indicate the level of trust and respect towards an organisation. The extent to which taxpayers and tax professionals respect the authority of their tax administration will contribute to their confidence in, and acceptance of, changes proposed to the system. In the event that taxpayers do not trust or respect their tax

administration, changes may be met with suspicion, hostility, or dismissal, all of which may lead to non-compliant behaviour.

The CRA has therefore defined Reputational Risk not only as any event that could result in damaging stakeholder trust, but also any event that could damage respect towards an organisation. The importance of managing this risk is related to the impact that reputation has on taxpayer behaviour.

Given the impacts of reputation damage, **reputational risk management** is a critical organisational function both to proactively protect against (prevent) and effectively deal with events (detect and respond) that may cause damage to its reputation.

2 The case for managing reputational risk

The importance of reputation has been understood and studied by many organisations in both the public and private sectors. Executives in the private sector know the importance of their companies' reputation. Firms with strong positive reputations attract better people. Customers are more loyal and buy a broader range of products and services. Likewise, lawmakers and tax administrators also know the importance of the reputation of the public institutions that underpin our system of government. In particular, public policy and meeting the needs of society depends to a large extent upon revenues collected through taxation.

The associated costs of a taxation function in government are greatly influenced by the degree to which taxpayers comply with the rules, requirements and procedures spelled out by those responsible for the collection of business and individual taxes. While these rules themselves are not voluntary, the CRA effectively operates in a largely voluntary compliance tax system. Under this system, when taxpayer are faced with choices as to whether or not to comply (such as whether to report all income or taxable events), they are generally relied on to do so voluntarily. Such a voluntary compliance system can only work if taxpayers have trust in the process and respect towards the agents of their tax administration. Trust is built on a positive reputation for good governance, organisational competence and fair and transparent processes. Respect towards a tax administration stems from perceptions of the administration's competence, effectiveness, credibility, authority, and professionalism. A positive reputation rests upon continued demonstration that perception reflects reality in these two components.

This is why the CRA has made significant efforts in improving both taxpayers' trust, by taking on a client centric approach toward how they interact with taxpayers, as well as in maintaining their reputation as a competent and effective tax authority, by reminding taxpayers of the organisation's deterrence initiatives and capacities. This mixture of techniques has allowed the CRA to maintain levels of high compliance.

3 The threat of negative events

Reputational risk events can stem from either external threats, such as system hacks, or internal threats such as poor client service or fraud. When speaking about reputational risk management, focus is placed on how well tax organisations set internal controls that protect against the threat of negative events. Internal risks to reputation can be categorised under the umbrella of errors or intentional malicious behaviour.

Two different sources of internal risks to reputation

By their very definition, errors are unintentional acts that, if understood as mistakes, should have little bearing on perceptions of trust towards an organisation. However, they have significant negative implications for feelings of respect towards that organisation, as they diminish perceptions of credibility, competence and capacity.

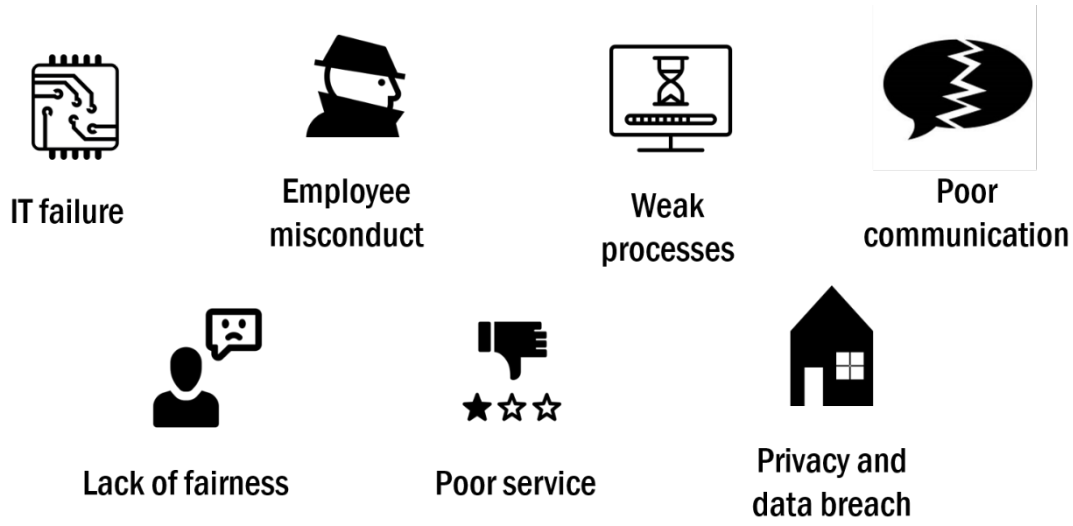
Intentional, malicious behaviour, such as misconduct and fraud as well as negligence will conversely affect trust, because they speak not only to the character of the actors, but also to the seriousness with which the tax administration looks after and cares about protecting its taxpayer's information, privacy, and tax dollars.

While overlap is possible, looking at these two categories separately can help tax administrations tailor their responses and explanation to their clients, and will have implications for how the sources of risks are monitored. Both types of risks will bring up the question of organisational culture, its credibility, competence, capacity, corporate character, and duty of care.

The range of negative possibilities

When considering the nature of events and situations that can impact the reputation of the enterprise, the CRA reached out to members of the OECD FTA Enterprise Risk Management COI to provide hypothetical events and scenarios that could negatively impact a tax administration's reputation should they occur. The CRA gathered over 50 hypothetical situations from the survey. These situations were then grouped into seven categories, shown in Figure 2.

Figure 2. The seven categories of hypothetical situations



Source: Canada Revenue Agency.

Each of the seven themes has an associated list of potential, related events that could cause significant damage to a tax administration's reputation should they occur. Some examples include:

- System/equipment failure that affects operational activities, such as a system outage or hack;
- A lack of fairness stemming from inconsistent decisions or a perception of bias;
- Privacy/data breach leading to a loss or release of sensitive information;
- Weak processes that contribute to system and human errors;
- Poor service to taxpayers or tax preparers;
- Poor communication reflected in the misuse of social media, or incomplete or misleading compliance guidelines; and
- Misconduct or intentional, malicious behaviour of an employee.

If not detected, prevented or mitigated, these events have the potential to negatively impact taxpayers' trust and respect towards their tax administration. For example, they can give rise to a perception of weak client-centred service, incompetence, a sense that the tax authorities are "going after the little guy" instead of aggressively targeting tax evasion and avoidance, that they are secretive in their operations and decision-making or do not exercise an adequate duty of care.

4 Existing approaches to risk management fall short

Following documentary research and consultation with other tax administrations, the CRA found that there does not appear to be a conventional, universally accepted standard for the management of reputational risk in the public sector.

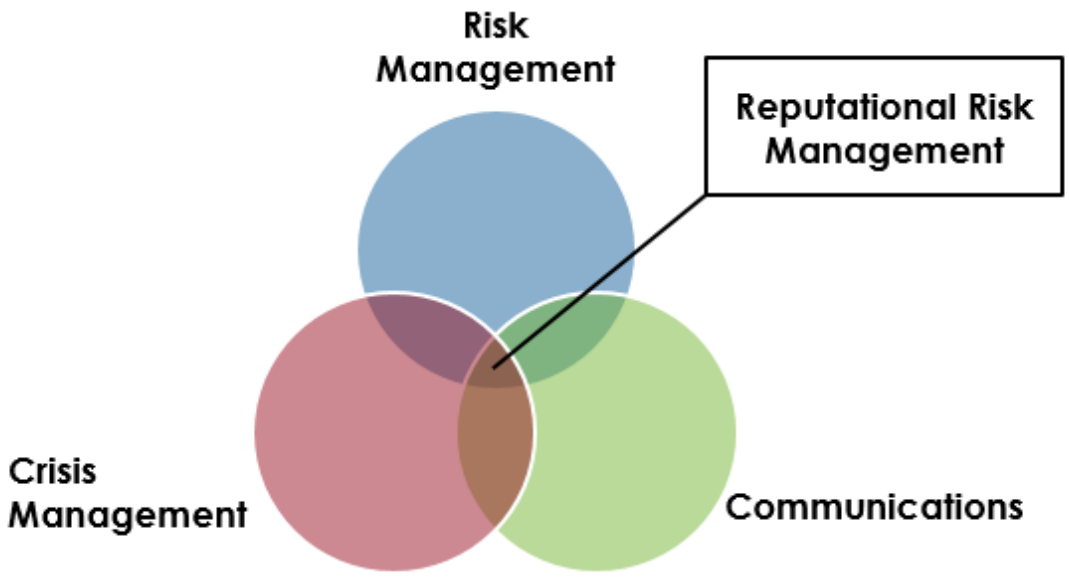
When looking at frameworks of reputational risk management that did exist, the CRA found that tax administrations primarily focused on crisis management rather than proactive prevention and protection. Managing a crisis seeks only to limit damage of an event after it occurs rather than assessing not only existing but also potential threats to reputation and deciding whether to address them by proactively accepting, or mitigating the risks.

Furthermore, there are enterprise risk management systems to be found in practice for managing operational and financial risks (risk management) as well as managing the hazards from external events such as natural disasters (business continuity and disaster recovery plans as well as crisis management processes). There may be embedded in such risk management frameworks potential elements that could affect reputation, including weak compliance or regulatory processes that can lead to errors or weak controls for detecting management fraud. Underlying these two risk perspectives, a robust communications strategy featuring a variety of media, platforms and channels contributes fundamentally to the shaping of an organisation's reputational risk management framework.

Integrating three functions to address the breadth of reputational risk

When considering the existing reputational risk management frameworks and their identified gaps, the CRA identified three components - risk management, crisis management, and communications as the underlying theory of its reputational risk management framework (see Figure 3).

Figure 3. The Components of Reputational Risk Management



Source: Canada Revenue Agency.

Proactive *risk management* enables tax administrators to anticipate and prevent or minimise threats that can damage reputation. Augmenting such capability is the active participation of communications. An effective *communications* function can engage stakeholders, provide assurances, and enable the entity to "get ahead of the story" in all matters that shape public perception of the organisation. The impact of good communications through shaping the narrative and influencing public opinion and sentiment is to preserve trust and respect towards an organisation. Crisis management is the tax organisations' capacity to quickly respond and mitigate a crisis that could impact reputation should it materialise. Identifying potential, or hypothetical events will not only help organisations to implement actions that may prevent risk events from occurring, but they also allow proactive preparation for crisis management that includes rapid response strategies should an event occur. It is an essential element as large and complex bodies such as a national tax administration will inevitably face real crisis situations from time to time, as indeed is the case with the COVID-19 pandemic. When these three elements are pieced together and managed well, tax organisations will be able to better manage risks to their reputation.

5 Building an approach to reputational risk management

"The way to gain a good reputation is to endeavour to be what you desire to appear."

- Socrates

In November 2018, the CRA developed a reputational risk management survey that was sent to all the FTA Enterprise Risk Management Community of Interest (COI) members. The results were then used to develop applicable and relevant tools to help tax administrations gauge their level of maturity in protecting their organisations from reputational risk, and proactively identifying vulnerabilities that can increase the likelihood of that risk materialising.

Developing a reputational risk management maturity model

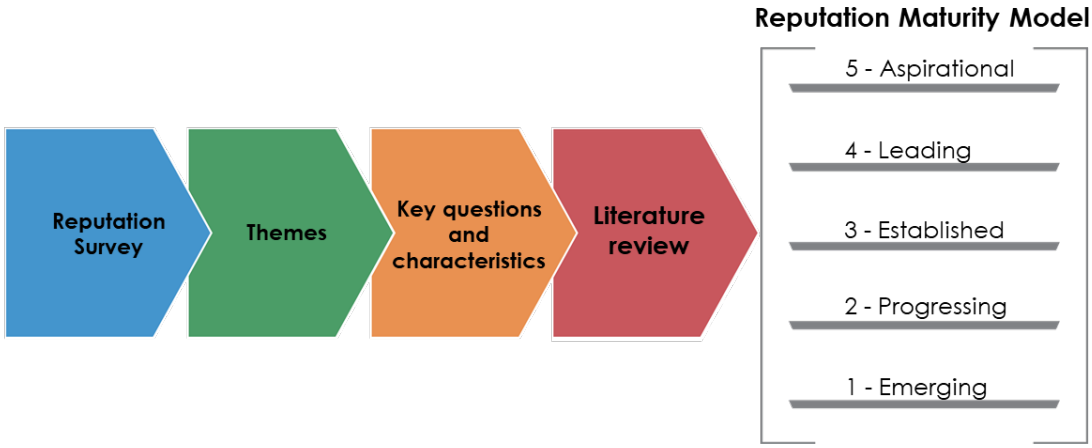
To determine how best to fill the gaps found in proactive and consistent reputational risk management, the reputational risk management survey sent to COI members asked questions that captured the three previously identified elements of risk management, communication strategies, and crisis management. The survey also allowed participants to provide information on additional reputational risk management practices, where they existed. These survey questions would later become embedded into the maturity model.

Nearly half of the COI members who received the survey provided detailed responses. The CRA analysed the results and sought to design a way to help tax administrations identify where they stand along the wide spectrum of reputational risk management practices. The result was the development of a reputational risk management maturity model. In addition to helping tax organisations see where they stand amongst different levels and elements of maturity, it also provides an indication of the main actions they would need to be taken in order to reach a higher level of maturity. To do this, the model is structured in a way that allows users to pass through the levels in sequence as they become more mature.

Figure 4 depicts the development process of CRA's maturity model. First, responses were analysed to identify common themes, strategies and/or policies. Patterns were identified that were indicative of tax administrations with positive and negative reputations in order to identify which criteria seemed to correspond with higher and lower levels of effective reputational risk management. Using this information together with additional supplementary research, a reputational risk management maturity model was defined that determined elements set along four levels of maturity: 1-Emerging, 2-Progressing, 3-Established, and 4-Leading. Further

literature review was done to identify a fifth level of maturity, 5-Aspirational, which captures criteria for visionary or aspirational reputational risk management practices.

Figure 4. Developmental Sequence for the Reputational Maturity Model



Source: Canada Revenue Agency.

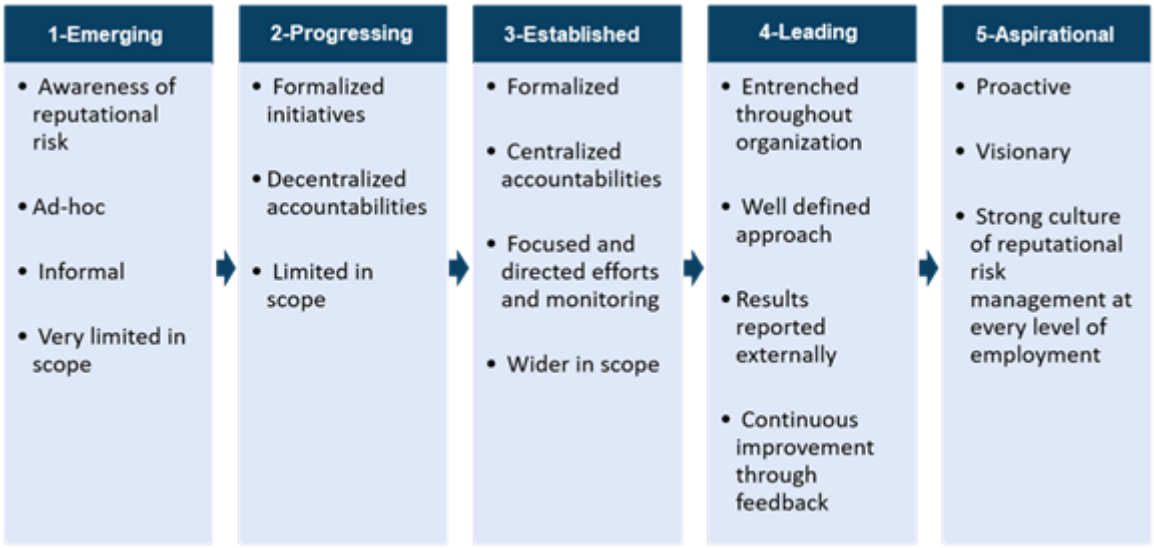
The preliminary findings of this process were presented and discussed with OECD FTA Enterprise Risk Management COI members at the 2019 risk workshop in Paris. A final step in the process was to continue analysing the unstructured data.

Using the maturity model

Working with a maturity model begins with an assessment to determine at which level the organisation is currently performing. Once the assessment establishes which level the organisation has achieved, the next level prescribes what capabilities are required for continued improvement. This prioritisation of learning is a substantial benefit of using a maturity model. It is founded on the notion that if you are at level 2 in something, it is much more important to understand the capabilities required at level 3 than level 4. The model therefore acts as a guide to what to learn, putting some structure on what otherwise would be a more complex process.

A reputational risk management maturity model establishes the stages of maturity of factors which contribute to reputational risk management and provides a comprehensive snapshot of how well the tax administration is managing the various potential risks to its reputation. This perspective is at the enterprise level and is self-assessed. Assessment is ideally carried out at the senior leadership level capitalising on the unique perspectives of executives at both the operational and enterprise level. The stages of maturity for each theme along the horizontal axis are summarised in Figure 5. More detail on what can be included in each level is provided in Annex A.

Figure 5. Reputational Risk Maturity Model Levels

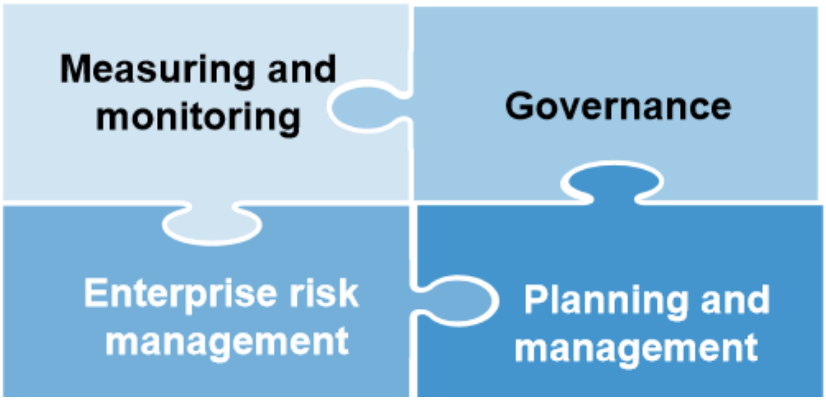


The maturity model works in four steps:

1. Users identify where they are on the model according to the criteria that define each level of maturity.
2. Users identify where they want to be based on their priorities and strategic visions.
3. Users assess the gaps and weigh the costs and benefits of achieving their goals for where they want to be on the model.
4. Users create strategies to get them to the level they aspire to be at before circling back to step one at regular intervals.

The maturity model pinpoints how mature an organisation is across each of four thematic elements and their component practices, as shown in Figure 6:

Figure 6. Reputational risk management maturity model themes



Each quadrant spells out states of practice in progressive levels of maturity. The organisation, through a self-assessment process, can identify where they are situated in each of the quadrants and look forward to where learning and progress is warranted. If widely adopted by other jurisdictions, it allows for comparison and identification of best practices to help learning.

These four elements are measured through a series of questions. Users of the model are encouraged to respond to each question under each thematic element in order to determine which level of maturity they fall into for that theme. A series of criteria were identified for each level of maturity, and validated by respondents who reviewed and tested the model.

To illustrate, Table 1 shows an example of the Measuring and Monitoring element (thematic element 1). Users of the maturity model were asked to respond to the following question: *How does your organisation measure, monitor and report on its reputation?*

The criteria applied to this question relate to the scope of factors that relate to reputational risk and the extent to which they are monitored and measured. Organisations that identify only external factors, for example, and do minimal measurement or analysis of them with no internal reporting of their trends, are at the "1-Emerging" level of maturity.

Table 1. Reputational Risk Management Maturity Model – Thematic Element 1: Measurement and Monitoring - Emerging Level

Reputational Risk Management Maturity Model	
Theme	1 - Emerging
1. Measuring and Monitoring	
How does your organisation measure, monitor and report on its reputation?	☐ Organisation informally identifies external factors that influence the health of its reputation. There is little measurement and monitoring of these factors and what exists is ad hoc. ☐ Organisation does not report either internally to senior management or externally to the public on the health of its reputation.

As the organisation makes its way up the levels of maturity, it must have increasingly formalised measurement analysis and monitoring structures of an increasingly wider scope of factors that affect reputation. Those in the "5-Aspirational" level of maturity go as far as having measurement analysis and monitoring strategies that effectively anticipate trends related to reputational risk and would thereby act proactively, as opposed to reactively. This is illustrated in Table 2.

Table 2. Reputational Risk Management Maturity Model – Thematic Element 1: Measurement and Monitoring - Established and Aspirational Levels

Reputational Risk Management Maturity Model		
Theme	3 - Established	5 - Aspirational
1. Measuring and Monitoring		
How does your organisation measure, monitor and report on its reputation?	☐ Organisation formally identifies, measures and monitors internal and external factors that influence the health of its reputation at both the strategic and operational level. ☐ Organisation reports on its reputation internally on a consistent basis for senior management. Employees contribute to the reporting of the organisation's reputation. ☐ Organisation incorporates available data horizontally, and leverages technology to gather additional data to assess the health of its reputation. Horizontality is limited due to poor communications.	☐ Organisation scans the external environment on an ongoing basis to identify, assess, and forecast emerging factors that influence their reputation. ☐ Results from reputation measurement and monitoring inform the organisation's enterprise risk management framework, corporate strategy and operational plans including but not limited to communications plans. ☐ Organisation shares leading practices of reporting on reputation with other interested parties.

Criteria for higher levels of maturity relate to the scope, embeddedness, and application of reputational management tools and practices. It may not make sense for an organisation to be leading or aspirational in every dimension as it can be a factor of cost, effort, experience, culture and even the willingness to make it a priority. The detailed reputational risk management maturity model and criteria for each element can be seen in Annex B.

Validating and applying the maturity model with the tax administration context – the improvement of world maturity in governance

To validate the model, CRA further invited the COI member countries to conduct and undertake an optional self-assessment using the reputational risk management maturity model and share the results along with any feedback on the model with the CRA to further the analysis. The self-assessments were then measured against CRA's objective assessments of those same tax administrations based on the information they shared as part of the initial reputational risk management survey from the previous year.

The majority of respondent's self-assessments were aligned with the CRA's objective assessments using their initial responses to match against the maturity model. This alignment served to validate the maturity model as a tool that adequately depicts their existing levels of maturity in reputational risk management. The average and median levels of the assessments are mapped out along the model in Figure 7.

There was, however, one area of discrepancy between CRA's initial, objective assessment of the maturity model, and tax administrations' self-assessment the following year. This was in the

Governance theme. Respondents self-assessed their organisations at a higher level of maturity than the CRA had assessed them in the previous year. An analysis of the rationale and discussions with various countries found that respondents added new initiatives that improved the governance of reputational risk management practices, compared to their initial submissions from the reputational survey that they completed in the previous year. Although these new initiatives came as a result of their initial review of the maturity model and discussions led by the CRA, their responses were still seen as validating the model with more updated information. The existence of the reputational risk management maturity model and the collective focus of all countries on the importance of reflecting on their reputational risk management culture in itself, contributed to an overall improved world maturity in Governance.

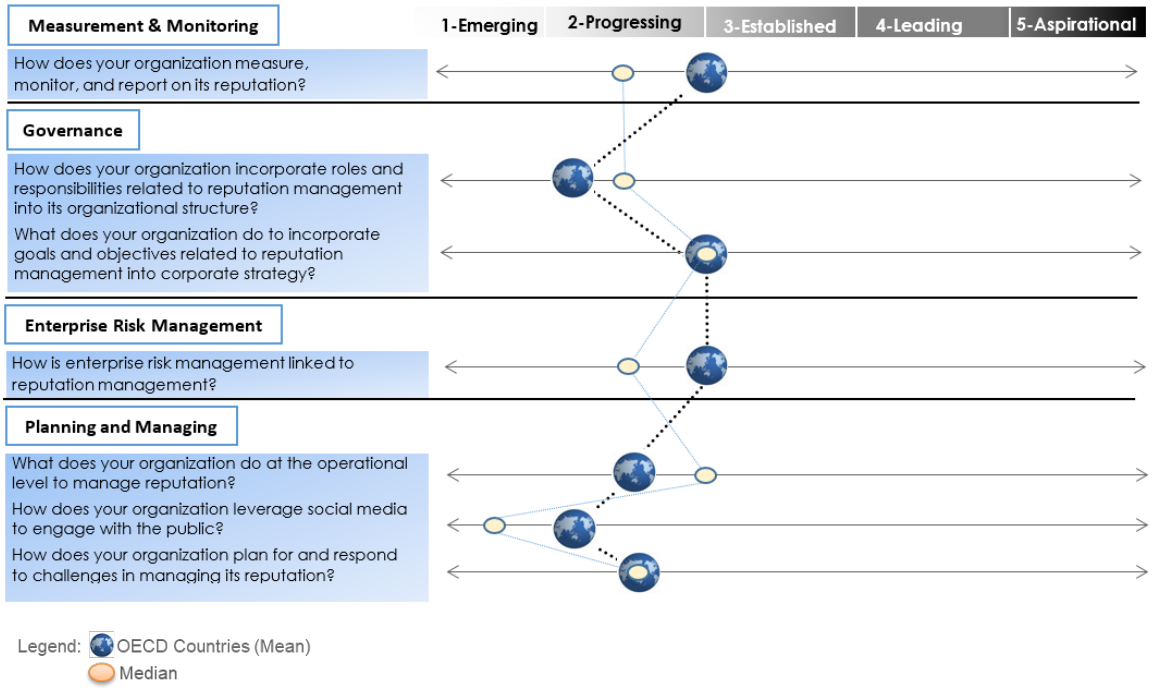
Benefits of using the reputational risk management maturity model

The model can be used by tax administrations productively in several ways. For example, a unique insight that is integrated into the model is recognition of the state of maturity of the organisation and the matching of appropriate practice to level. This lays the groundwork for recommended actions to move to the next step rather than an ideal end state.

As another example, the CRA formally identified positive and negative influences on its reputation using the maturity model as a validation measure for the criteria depicting each level of maturity. The CRA uses a Public Perception Index to measure and monitor reputation health, which is then reported to senior management and the Board of Management. The index is also published on the CRA external website. These are characteristics of the “3-Established” level of maturity in terms of measuring and monitoring. In looking at the maturity model, the CRA could move to “4-Leading” by using the results of monitoring exercises to inform both operational and strategic decision making, or report on reputation health to the public. The detailed reputational risk management maturity model and criteria for each element can be seen in Annex A.

The model also signals where corrective adjustment or improvement would strengthen reputational risk management by comparing the tax administration’s self-assessment with the mean scores of the participating OECD countries. As seen in **Figure 7**, users of the model can position themselves on the world stage and decide what levels they want to strive for based on international trends and standards.

Figure 7. Average and Median OECD Reputational Risk Maturity Model



6 Evaluating reality and closing gaps

When reviewing the responses from the reputational risk management survey, the CRA found that 83% of organisations who experienced a recent reputational crisis managed their reputation only at the strategic level, not at the operational level.

In this regard, it is worth recalling that the primary categories of reputational risk sources are errors and malicious events. Human error is often the source and in many cases is manageable through elevated staff awareness, training, correction, continuous improvement and good process design. Therefore, while these categories can and need to be mitigated at the strategic level through establishment of policies and corporate plans, they are fundamentally sourced at the operational levels by the employees of the tax administration—those who have direct contact with and impact on taxpayers and their representatives.

The CRA sought to develop an operationalisation strategy that would mix compliance-driven and value-driven motivations. Compliance-driven motivations work by obligating employees to follow certain behaviour using a rigid hierarchy and deterrence structure. It works through regular monitoring and reporting and is primarily top-down in its approach to encouraging behaviours. Alternatively, a values-based approach is less hierarchical and calls on all participants to self-monitor and promote the desired behaviour. For the latter to work, employees need to believe in the common objective.

Two additional tools were developed by the CRA that merged elements of compliance and values-based approaches to behavioural change. The tools act as compliance-based motivations in that they provide a reporting structure in which managers self-assess their area of responsibility in terms of vulnerabilities to errors and fraud or misconduct. The values-based approach comes in the presentation of the tools and related training, in which managers and their employees are informed that they all have a role to play in protecting their organisation's reputation. The tools are intended to be preventative and to encourage improved capacity to identify vulnerabilities and prevent reputation damaging events.

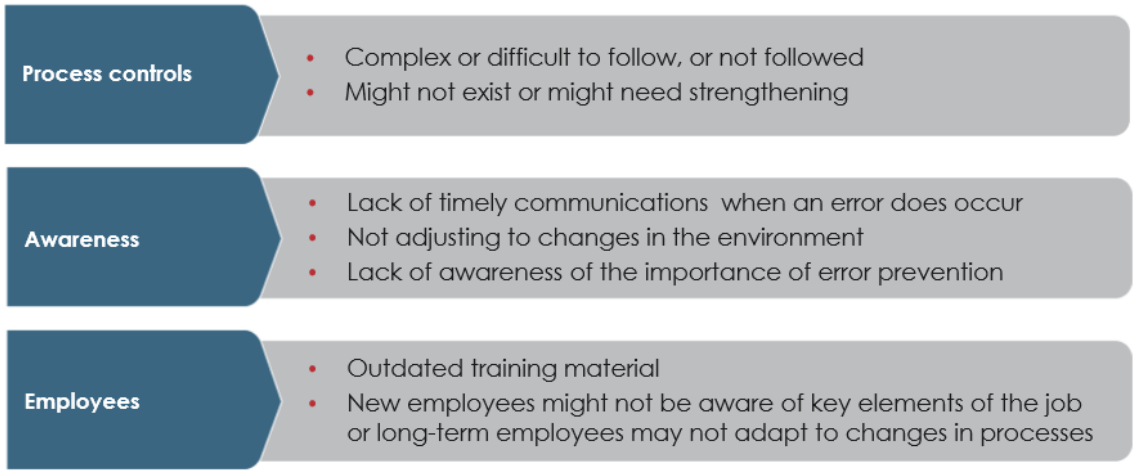
The two tools incorporate hypothetical situations to help managers understand the connection between specific vulnerabilities and the impact that they may have on the reputation of the CRA. The tools reflect the balance of compliance-based and values-based approaches in that they provide a way to monitor and control risks but also act as reminders to employees of how each of them has an impact on the wellbeing and reputation of the CRA as a whole.

Error Prevention Self-Assessment Tool (EPSAT)

The Error Prevention Self-Assessment Tool (EPSAT) is available for use by managers to flag where their operations may be vulnerable, and is intended to prompt identification and adoption of appropriate controls. The tool covers three broad areas of vulnerabilities related to process controls, awareness, and employees (see Figure 8). Specific corrective responses are largely left in the hands of managers in order to facilitate reputational risk management at the operational level. By using this tool, managers not only monitor and report vulnerabilities to

reputational risk up to senior management, but they can also use the tool to have conversations with their teams that increase their awareness of the role they play in managing the CRA's reputation.

Figure 8. Vulnerabilities to be assessed by managers using EPSAT



Source: Canada Revenue Agency.

As seen in Figure 9, the tool consists of a checklist of questions for consideration by a manager.

Figure 9. Excerpt of EPSAT questionnaire

#	INTERNAL PROCESS QUESTIONS TO CONSIDER	YES, THIS APPLIES TO MY AREA
1	In the past 12 months, has your team experienced a high[1] rate of, or continuous, staff turnover?	☐
2	Do employees miss opportunities for training on key processes, procedures and refresher courses?	☐
3	In the past 12 months, has your team experienced a significant change in how you do business (e.g. business transformation or realignment)?	☐
4	Does your team communicate with external stakeholders such as: a) Taxpayers, tax preparers b) Other (e.g. other government departments, tax professional organizations, media)	☐
5	Does your team work with large volumes of sensitive information? • Verify the types of sensitive information by consulting the Protecting and Handling Information Pamphlet.	☐

Source: Canada Revenue Agency

Once users complete the tool, they are then guided to the list of hypothetical situations according to a table that matches each vulnerability to one of the seven hypothetical situation themes. Users are then instructed to review the list of hypothetical situations and apply the "5 Rights" analysis to ensure the hypothetical situations do not become a reality. The "5 Rights" of the tool are:

> **Guideline 1:** The RIGHT controls: Are the right controls in place to reduce the risk of errors?
>
> **Guideline 2:** The RIGHT knowledge: Do employees have the right job training and receive it in a timely manner?
>
> **Guideline 3:** The RIGHT communication: Is there open and constant communication with employees at all levels (front line employees and above) about error prevention?
>
> **Guideline 4:** The RIGHT contingencies: Are the appropriate plans in place at all levels of the organisation in case an error occurs?
>
> **Guideline 5:** The RIGHT planning: Are there plans in place for future continuous improvement for error prevention?

Management can make sure that specific areas are sufficiently covering the "5 Rights" to reduce the risk of hypothetical events that relate to their vulnerabilities from occurring. The full EPSAT tool can be found in Annex C. Administrations may wish to consider using this tool, with any appropriate adjustments.

Internal Fraud Risk Self-Assessment Tool (IFR-SAT)

In addition to the EPSAT, the CRA also developed a self-assessment tool that managers can use to assess their area's vulnerability to internal fraud, called the Internal Fraud Risk Self-Assessment Tool (IFR-SAT).

The IFR-SAT is intended to proactively identify risks of internal fraud before it occurs and highlights the controls that are presently in place to assure that vulnerabilities are not exploited. Similar to EPSAT, it is designed to be a self-assessment process undertaken by managers to encourage continuous improvement.

There are four steps to completing the IFR-SAT:

> **STEP 1:** Managers are asked to consider their risk drivers by selecting from a series of potential drivers of fraud, or suggesting their own.
>
> **STEP 2:** Managers are asked to consider the risks should fraud occur.
>
> **STEP 3:** Managers to determine the controls they already have in place for the risks they identified in step 2.
>
> **STEP 4:** Managers are guided to consider and develop their own mitigation strategies they could apply to their area's vulnerabilities.

The objective of the tool is to gain a comprehensive understanding of the program area's vulnerability to the risk of internal fraud, and of the effectiveness of existing internal controls designed to mitigate risks of fraud. The IFR-SAT tool can be found in Annex D. Both tools are designed for managers to be able to complete the questionnaires in less than one hour. Managers are encouraged to review the questionnaire annually, or if there is a major change in their organisation. Administrations may wish to consider using this tool, with any appropriate adjustments.

7 Monitoring, measurement and communication

The tools that have been presented above show the risk management side of reputational risk management. As set out in Figure 3, communications is also a critical part of the approach to shaping and managing image, reputation, and perception. For tax administrations in a voluntary compliance system to do their job effectively, citizens must trust the organisation, believe that others are paying their fair share, understand what is required of them, understand the materials provided by the tax administration and receive adequate service when they need it.

Risk management and communication functions are typically at the extreme ends of reputational management. Trust is fundamental and communications shape perceptions about the organisation and the events associated with the organisation responsible for tax administration. The CRA has attempted to bridge the divide through a conscious and concerted effort by both functions working with other areas of the Agency to develop a holistic view of reputational risk management. By combining the reputational risk maturity model and the CRA's communications and operational orientation, it becomes possible to narrow the gap between perception and reality. In this way, the communications function works as both a barometer to measure how well the tax administration is doing in managing its reputational risk, and also a tool to help mitigate the impact of public affairs incidents with the potential to harm the organisation's reputation.

Reported incidents in today's news feeds could pose a risk to a tax administration's reputation if not managed appropriately and in a timely manner. To communicate effectively with the public, communications must be well coordinated, integrated, consistent, and transparent in messaging and information sharing. The communications function features three components – monitor and measure, maintain and protect, and build.

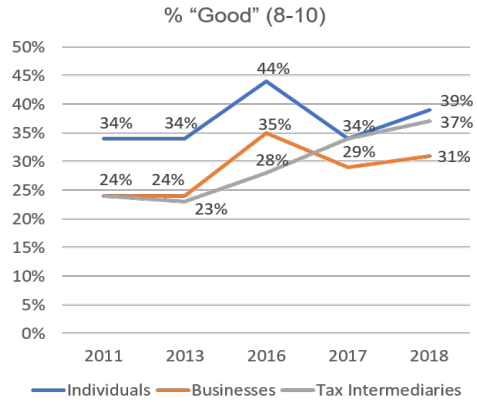
Monitor and measure

The CRA uses a number of different methods to measure Canadians' perceptions of its performance over time. One such tool is the Public Perception Index, which is calculated on an annual basis based on responses provided in public opinion research. It allows the CRA to track changes to key indicators that influence reputation, such as satisfaction levels, perceptions of overall performance, and effectiveness of deterrence strategies. As seen in Figure 10, the index is a blended average score across four indicators and three target audiences - individuals, small and medium businesses, and tax intermediaries. This annual index was established for the purpose of departmental reporting to the Treasury Board of Canada Secretariat and includes 12 distinct elements.

Using a more direct approach, the CRA also conducts surveys on taxpayer views regarding attributes such as treating taxpayers with respect, doing what is right, treating taxpayers fairly,

being efficient in operations, providing information that is easy to understand, working hard to help Canadians, and the CRA's overall performance.

Figure 10. CRA Public Perception Index



Public Perception Index Indicators
CRA Overall Performance
Overall Satisfaction with Service
Information is Easy to Understand
Got What was Needed

Source: Canada Revenue Agency.

Supplementing this broad view, and like most public sector organisations, the CRA also tracks and measures the volume of media coverage pertaining to its activities. It also measures the extent to which media coverage (including articles from traditional media, blog posts and some social media content) casts the CRA's activities in a positive or negative light. This data is another valuable indicator of the evolution of the reputational risk to the CRA over time, and helps the CRA to better anticipate potential negative situations and develop communications to proactively address them.

Reputational risk management also protects and encourages positive perceptions of respect towards an organisation. Respect towards a tax administration depends on perceptions of authority and competence, and the CRA team recognises the need to showcase its very real ability to crack down on non-compliance and bring fairness to the tax system. Still, the fundamental interest of the CRA is to maintain the trust of taxpayers in an effort to encourage continued voluntary compliance. Internal analyses have demonstrated that there are tangible benefits in adopting a more proactive stance from a media relations perspective in an effort to showcase some of the CRA's positive activities.

Maintain and protect

As well as monitoring and measuring perceptions of the CRA, there is also a communications quick response capability that features close collaboration with a number of communications related internal functions and external stakeholders. Efforts in this area are guided by two protocols that shape both media relations and social media engagement. The first, the Media Relations Protocol, considers the potential impact of a news item on existing level of public trust in the CRA, and assigns values that help to prioritise response plans for each media request. The development of this tool was a collaborative endeavour between the communications and risk management units of the CRA, illustrating the critical importance of merging the two channels of operations in order to achieve effective reputational risk management.

A second, more recent Social Media Engagement Protocol defines the process of engaging on social media with taxpayers ranging from if or how to respond, to connecting with the right people within the Agency to provide a response. This protocol is continually monitored for improvements using feedback from taxpayer interactions and posts on social media, and fits under the “4-Leading” level of the maturity model.

Build

Communications also builds a positive CRA reputation through a proactive communications plan which includes efforts to optimise its Web content, rewriting its correspondence to make it more understandable, utilising social media to reach Canadians where they are, using multiple media channels and leveraging advertising.

The CRA is making tangible and measurable progress on reputation management through the adoption of a research driven, evidence based, and risk management focused approach. Disciplined application of this approach assures that communications provides positive contributions to building the CRA’s reputation by providing a seamless service experience, strengthening trust, transparency and accountability, enabling innovation and maintaining fairness in Canada’s tax and benefits administration.

8 Managing reputational risk in the context of international crisis: Impact of the current COVID-19 crisis

The COVID-19 crisis has created an unprecedented climate of change, fear, and uncertainty. In the midst of the economic and social upheaval, tax administrations have found themselves the unlikely and unexpected protagonists, providing not only much needed relief in the form of tax deferrals and regular benefit payments, but also, in many countries, becoming the most important conduit to rolling out government subsidies and relief packages directly to the people and organisations who need it most.

Tax administrations are likely to have up-to-date and fulsome data of the citizens of any country, and so provide potential avenues for the government to issue much needed financial aid to its population. The current crisis provides a chance for this benefit and positive relationship to be visible to the general population. Tax administrations should be mindful of measuring the potential impact that their role in the response to the pandemic has had on their reputation, and the ways in which this role can influence their relationship with taxpayers.

This report on reputational risk management provides tax administrations with timely access to resources that can help them look ahead to understand and protect their reputation in the eyes of their taxpayers and other stakeholders as the world moves from crisis to recovery. During the crisis phase, tax administrations have been leaning on the “crisis management” and “communication” elements of Figure 3 of the report, which illustrates the components of reputational risk management. During this phase, tax administrations can emphasise that their ability to provide relief in times of crisis relies on taxpayers voluntarily complying and providing their most accurate and up-to-date information to their tax authorities in times of stability. This practice may have the added benefit of identifying and further discouraging non-compliant taxpayers such as those in the underground economy and those that are engaged in offshore tax evasion schemes. On the one hand, taxpayers who were engaged in these practices may find less incentive to do so if they change their perspective of tax administrations (i.e., being “registered” with tax authorities allows access to benefits and subsidies). On the other hand, established positive taxpayer sentiment will free up resources for tax administrations so they may spend less time and effort administrating the majority of taxes, and can instead focus on greater and more targeted deterrence for persistent non-compliers.

The crisis phase is also a good time for tax administrations to begin or improve on their capacity to monitor and measure their reputation. The reputational risk maturity model (see Annex B) sets out criteria for different levels of maturity under the *Measurement and Monitoring* theme that tax administrations can aim for. For example, to reach an Established level of maturity in

this theme, tax administrations can create public perception indices, such as the one presented in this paper, to establish a baseline or peak point for positive reputation and measure their evolution over time. Tax administrations should aim to measure taxpayer sentiment as soon as possible so that the benefit and relief provided to taxpayers—such as deferred filing and payment deadlines, easier access to debt payment options, suspended debt collection measures, and rolling out government aid and subsidies—will still be at the forefront of taxpayers' perceptions. To reach the Aspiration level of maturity, tax administrations can analyse the results of these surveys to identify ways to improve or maintain a positive reputation among taxpayers, such as becoming more service and people oriented, more agile, improving communications and reducing taxpayer burden. Further, tax administrations that carefully manage the crisis and communicate effectively the role they are playing and the benefits to society can build reputational equity, or a "reputation bank", that may help them navigate some of the inevitable challenges that will come with the recovery and post-recovery phase. By managing their reputational capital, tax administrations will be better equipped and positioned to continue helping their populations in the event of another crisis.

Tax administrations can continue to use the reputational risk management maturity model to determine their ability to manage the risks towards their current reputation in the eyes of taxpayers. The *Planning and Managing* theme, in particular, lays out criteria that can be particularly useful in guiding tax administrations on how to leverage and nurture positive shifts in reputation. Users of the model must then consider whether they want to move forward in their placement on the maturity model or remain at their current level during these unprecedented times, where so many competing priorities are the order of the day. This is a very important step because as countries move into recovery and post-recovery, tax administrations will have to shift back to their primary mandate of tax collection, and this is where careful planning and communication is needed to maintain the positive reputation gained during the crisis phase.

This is also the point where the third component of Figure 3, *Enterprise risk management*, comes into play. Tax administrations can use the two tools presented in this paper, which can be found in Annexes C and D of this document, to proactively identify risks to re-establishing business operations in the recovery phase. These tools include hypothetical situations (categorised in Figure 2 of the paper) that will remain relevant after this crisis is over. Tax administrations are also encouraged to update this list to help prepare and mitigate risks that they foresee will emerge as a result of the crisis.

For example, in the recovery and post-recovery phase, tax administrations will likely face situations in the categories of lack of fairness or service that does not align with taxpayer needs, as taxpayers may feel overwhelmed in respecting their obligations. The correct balance of tax collection, service and maintaining a positive reputation must be struck. In anticipating these risks, and identifying their sources using the concepts, methodologies and tools included in this paper, tax administrations can proactively plan, and communicate, in a way that leverages their positive reputation to help achieve their mandates effectively while remaining sympathetic to the needs of their taxpayer base.

Tax administrations may also want to consider the risks to reputation that may emerge out of the new and rapidly introduced measures taken during the crisis. For example, while tax administrations are being pressured to provide relief programs to populations rapidly, they must also continue to protect taxpayer information, privacy, and mitigate the threats of fraud and cybersecurity in their tax and refund systems. To mitigate this risk, communication practices can be used during times of crisis to explain to populations that tax administrations are working to balance the timeliness of providing the relief with the equally important need to protect taxpayers' identities, personal information, and entitlements.

Taxation is a fundamental component of strong, stable governments and economies – and in the eyes of citizens, can be viewed as a proxy for the reputations of their governments. This fact has become very apparent during the COVID-19 pandemic. Taxpayers now more than ever can see the benefit of efficient and effective tax administration, and this reputation—if properly considered—has the potential to encourage voluntary compliance of their obligations during times of stability, as well as to highlight the quality of government generally. In keeping reputation top of mind, and consistently and proactively scanning for risks to that reputation, tax administrations can leverage a more positive shift in their relationship with taxpayers to focus on improving their operations and services, and continue to achieve their mandate of supporting their governments and benefiting their societies.

Annex A. Overview of the Reputational Risk Maturity Model

Although it is a continuously evolving effort, through the development of a reputational risk maturity model, the CRA has endeavoured to create a comprehensive mechanism to identify potential risks and vulnerabilities to the CRA's reputation and has effectively tied together crisis management, risk management and communications to formulate proactive and, if necessary, reactive responses. It is a blend of compliance and values-based approaches that depends on senior leadership awareness, oversight and direction augmented by staff sensitivity and a sense of personal responsibility. If managed well, it will contribute in a very productive way forward to influence the values and culture of the CRA.

1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
• Establishing and enforcing a code of conduct for tax administration employees • Soliciting ad hoc informal and formal feedback from taxpayers • Investigating and mitigating any instances of perceived wrongdoing • Delivery of employee training in the areas of: ▪ Conflict of interest ▪ Privacy of information ▪ Values and ethics	• Cooperation with partner tax administrations • Establishing a charter that sets out expectations for the tax administration's engagement with the public • Public environment analysis • Ad hoc surveys delivered to select clients or communities • Delivery of employee training in the areas of: ▪ Issue management ▪ Cyber security ▪ Media engagement ▪ Leveraging social media ▪ Client interactions ▪ Developing spokespeople	• Ongoing measurement of public opinion using one or more of the following tools: ▪ Public opinion research ▪ Public perception index ▪ Consumer satisfaction index • Key Performance Indicators related to reputation such as: ▪ customer satisfaction • Regular outreach to the public through one or more of the following methods: ▪ Press conferences ▪ Focus groups ▪ Workshops ▪ Advertising or marketing campaigns ▪ Web or digital communications • Post mortems are conducted after significant changes to reputation	• Ongoing monitoring of public opinion such that year over year performance is tracked and reported on • Multi-dimensional reputation index that considers and engages all functions of the Administration • Implementation of a horizontal strategy • Existence of a social media strategy and protocol leveraging Lithium. • Established crisis management teams • Corporate social responsibility programs	• Reputation is scanned and assessed on an ongoing basis • Use of emerging technology to proactively scan and monitor the external environment including but not limited to: ▪ Blockchain ▪ Artificial Intelligence ▪ Algorithms ▪ Quantum computing • Ongoing analysis of interdependencies between operational performance and reputation • Assesses readiness and ability to respond through regular tests or drills and live scenario planning

Annex B. Full Reputational Risk Management Maturity Model

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
1. Measurement and Monitoring					
How does your organisation measure, monitor and report on its reputation?	☐ Organisation informally identifies external factors that influence the health of its reputation. There is little measurement and monitoring of these factors and what exists is ad hoc. ☐ Organisation does not report either internally to senior management or externally to the public on the health of its reputation.	☐ Organisation formally identifies, measures and monitors a few select factors that influence the health of its reputation at the strategic level (i.e. through the use of customer satisfaction surveys) with limited use of technology and available data. ☐ Management level employees monitor the health of their reputation ☐ Senior management oversight exists, but is not formalised.	☐ Organisation formally identifies, measures and monitors internal and external factors that influence the health of its reputation at both the strategic and operational level. ☐ Organisation reports on its reputation internally on a consistent basis to senior management. Employees contribute to the reporting of the organisation's reputation. ☐ Organisation incorporates available data horizontally, and leverages technology to gather additional data to assess the health of their reputation. Horizontality is limited.	☐ Organisation uses the results of reputation measurement and monitoring to inform and reassess strategic and operational decision making including but not limited to communications plans. ☐ Organisation shares the internal report on the health of its reputation externally with the public on a consistent basis. ☐ Organisation regularly adopts new technologies as well as multiple internal and external data sources (i.e. a multidimensional reputation index) to assess the health of their reputation. Increased and regular communication supports horizontality of efforts. ☐ Public reaction to results is periodically monitored.	☐ Organisation scans the external environment on an ongoing basis to identify, assess, and forecast emerging factors that influence their reputation. ☐ Results from reputation measurement and monitoring inform the organisation's enterprise risk management framework, corporate strategy and operational plans including but not limited to communications plans. ☐ Organisation shares leading practices of reporting on reputation ☐ An organisation-wide data model has been established. Organisation leverages emerging technology such as artificial intelligence to assess its reputation in real time.

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
2. Governance					
How does your organisation incorporate roles and responsibilities related to reputation management into its organisational structure?	☐ Organisation does not include people with designated roles and responsibilities accountable for measuring and monitoring their tax administration's reputation. ☐ Guidance on reputation management is inferred or provided indirectly on an ad hoc basis to employees through mechanisms such as a global code of conduct.	☐ Organisation measures and monitors their tax administration's reputation in a decentralised way (i.e. through their public relations function) and does not include people with clearly defined roles, responsibilities and accountabilities. ☐ Specific guidance on reputation management exists and is provided to select employees such as employees who have interactions with the public or senior management.	☐ Organisation has established a reputation management framework that includes dedicated people with roles and responsibilities who are accountable for measuring and monitoring their tax administration's reputation at the strategic and operational level. ☐ Specific guidance on reputation management exists. There is a proactive approach to delivering the guidance to all employees across the organisation.	☐ Reputation Management framework has a clearly defined approach, that is actively reassessed, towards measuring and monitoring the organisation's reputation including the identification of key performance indicators which have been assigned to responsible persons throughout the organisation. ☐ Mandatory training on the subject of reputation management is delivered to all employees of the organisation and is refreshed periodically.	☐ Organisation has built a culture of reputation management such that every member of the organisation understands their individual responsibility to uphold and maintain the organisation's reputation. ☐ The reputation management framework incorporates emerging technology i.e. artificial intelligence or blockchain, in their approach to measuring and monitoring the organisation's reputation. ☐ The framework is integrated with the rest of the organisation and is embedded in business processes and reputation management findings drives decision making.

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
What does your organisation do to incorporate goals and objectives related to reputation management into corporate strategy?	☐ Goals and objectives related to reputation management exist indirectly and are developed on an ad hoc basis i.e. as an outcome of another goal or objective and may or may not be included in corporate strategy.	☐ Corporate strategy includes sections related to reputation such as service or public relations. ☐ Goals and objectives related to reputation management are discussed and considered by senior management.	☐ Goals and objectives related to reputation are defined at both the strategic and operational level taking into consideration the organisation's appetite and tolerance, and are formally included in corporate strategy. ☐ Goals and objectives related to reputation are recognised and accepted across the organisation.	☐ Goals and objectives related to reputation management are a core component of corporate strategy and are directly linked to goals and objectives set at the operational level including communications plans. ☐ Goals and objectives related to reputation are developed and recognised, accepted by personnel across the organisation.	Reputation management is integrated into a defined corporate strategy and vision that: ☐ Is incorporated into business processes and strategy throughout the organisation, ☐ Includes a communication plan ☐ Includes ongoing monitoring of changes in the external environment, ☐ Assesses readiness and ability to respond through periodic drills and live scenario planning, ☐ Is measured, monitored and reported on regularly to senior management; and, ☐ Is integrated into the enterprise risk management framework.

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
3. Enterprise Risk Management					
How is enterprise risk management linked to reputation management?	☐ Organisation does not formally make a link between reputation management and enterprise risk management. The link is informally made but only at the strategic level.	☐ Organisation understands the links between certain risks in its enterprise risk management framework and its reputation (i.e. risks with public facing impacts are identified). ☐ Specific requirements are placed on management, with senior management oversight, to manage activities aimed at maintaining, and strengthening the link with reputation.	☐ Strategic level documents exist that link reputation management and enterprise risk management. Regular reporting against these documents is done internally. ☐ The link between reputation and enterprise risk is understood horizontally, across the organisation, including at the employee level. ☐ A participatory culture in maintaining reputation exists. ☐ Organisation has specific policies and roles in place to respond to breaches to reputation.	☐ Organisation regularly monitors and analyses indicators reflecting how reputation is affecting enterprise risk. ☐ A collection of activities, roles, and responsibilities, are clearly defined to maintain the link between reputation and enterprise risk management, and these activities are continuously reassessed to meet the challenges and needs identified by the analysis. ☐ Regular reporting of the link between reputation and enterprise risk is presented both internally and externally. ☐ Understanding and consideration of the link between reputation and enterprise risk management is effectively communicated horizontally.	☐ Organisation regularly asses as a component as its enterprise risk management framework its reputational risk and uses the results to make business decisions that enhances their reputation.

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
4. Planning and Managing					
What does your organisation do at the operational level to manage reputation?	☐ Reputation is managed at the strategic, not operational level. ☐ Processes to support reputation management have not been explicitly identified.	☐ Reputation is managed at the strategic, not operational level. ☐ Processes to support reputation management are identified and managed formally within local business units of the organisation. ☐ Senior management oversees management of internal factors of reputation. ☐ Senior management does **not** oversee management of external factors of reputation (i.e. economy, social environment, etc.).	☐ Reputation is managed at both the strategic and operational level. ☐ Processes to support reputation management, including specific roles of employees, are identified, recognised, and managed formally within divisions. ☐ Regular reporting of both internal and external factors of reputation are conducted internally. ☐ Reports of both internal and external factors of reputation are shared horizontally across the organisation. ☐ Employees have an opportunity to contribute to reports, including providing suggested management and solutions, fostering a culture of reputation management.	☐ Reputation is managed at both the strategic and operational level. ☐ Processes to support reputation management are continuously reassessed to ensure improvement. ☐ Roles and responsibilities of reputation management are formally defined, monitored, and assessed at each level of employment within the organisation. ☐ Reporting on reputation management and planning is done both internally and externally.	☐ Reputation is managed at both the strategic and operational level. ☐ The organisation has defined inventory that includes processes related to reputation. The processes are consistently applied across all functions of the organisation.

Theme	1 - Emerging	2 - Progressing	3 - Established	4 - Leading	5 - Aspirational
How does your organisation leverage social media to engage with the public?	☐ Organisation's methodology to assess its reputation does not leverage social media.	☐ Organisation uses select social media platforms in an ad hoc manner to engage with the public.	☐ Organisation has a strategy in place to leverage social media across various platforms to engage with the public.	☐ Organisation uses the results of interactions with the public on various social media platforms to create data which is used to make informed operational and strategic decisions.	☐ Organisation leverages emerging technology such as artificial intelligence to proactively scan social media platforms to assess the health of its reputation.
How does your organisation plan for and respond to challenges in managing its reputation?	☐ Organisation reactively responds to challenges in managing their reputation.	☐ Processes and procedures to plan for and respond to challenges to the organisation's reputation exist but are not consistently applied across the organisation.	☐ Processes and procedures to plan for and respond to challenges to the organisation's reputation are documented, standardised and implemented across the organisation.	☐ Organisation has a distinct response plan in place that outlines its planned response in detail to various scenarios that could impact the reputation of the organisation.	☐ Senior management can articulate the response plan and see it as a value-added contribution to the organisation. ☐ The response plan is periodically tested in the form of live drills.

Annex C. Error prevention self-assessment tool (EPSAT)

Introduction and purpose

The EPSAT was originally introduced in 2016 and was updated to ensure that it would flag vulnerabilities, warning signs and/or enablers of the items included in the list of hypothetical scenarios that threaten tax administrations' reputations. The CRA leveraged its participation in the OECD's FTA Risk Management Community of Interest to initiate a discussion on hypothetical situations which could negatively impact the reputation of a tax administration. The CRA collected and analysed the data from these discussions and rolled up the results into common themes.

How the tool was updated to incorporate hypothetical scenarios

To ensure that the tool captured all scenarios, the hypotheticals were grouped into 7 themes, and then each theme was mapped against the questions. The 7 themes are:

1. Misconduct
2. IT Failure
3. Privacy/Data Breach
4. Lack of Fairness
5. Poor Service
6. Weak Processes
7. Poor Communication

Your role as manager is to go through each of the steps for your area of responsibility. The steps are:

STEP 1: Complete the EPSAT Questionnaire

The EPSAT questions can be found on pages 2-3 where of this document. All 7 themes of the hypothetical situations are covered by the questions.

STEP 2: Consider your controls and identify potential situations that you do not currently have control over. Hypothetical situations that may affect the CRA's reputation are included in pages 5-7 of this document. Use the mapping analysis on page 4 to identify the theme associated with the vulnerabilities you identified in Step 1.

At the end of the exercise you will receive a percentage of vulnerability to errors in your area of responsibility, and the potential situations that may arise from those responsibilities which you do not currently have controls over.

A list of hypothetical situations, grouped by theme, can be found on pages 5-7. Some of the specific situations were adjusted or adapted to ensure applicability to the CRA.

*The tool is intended to be an **evergreen** document that reflects the current operating environment. As such, please feel free to add a new hypothetical situation in the "Other" option on pages 5-7.*

ERROR PREVENTION SELF-ASSESSMENT TOOL: A TOOL FOR AGENCY MANAGERS[1]

While errors can happen anytime, the CRA needs to prevent, as much as possible, errors that can have a **significant impact** on its **reputation** and on the **integrity** of its programs and operations.

Ask yourself, if an error occurred in your area, would it impact the following:

- **Taxpayer trust and confidence:** Could it impact the Agency's reputation?
- **Media coverage:** Could it garner media attention at the local, provincial and/or national level?
- **Service delivery:** Could it impact service delivery (e.g. the CRA's ability to deliver its mandate)?

If so, we want you to target and review those areas.

As a CRA manager or supervisor, **you have a key role to play** in reducing the risk of errors. This **two-step** process will help you identify potential vulnerabilities that could lead to errors so that you can **proactively address them**. **This tool is *not* about adding new controls; it is about making sure you have the *right controls* and that they are being followed.**

STEP 1: INSTRUCTIONS - Consider the following questions

#	INTERNAL PROCESS QUESTIONS TO CONSIDER	YES, THIS APPLIES TO MY AREA
1	In the past 12 months, has your team experienced a high[2] rate of, or continuous, staff turnover?	☐
2	Do employees miss opportunities for training on key processes, procedures and refresher courses?	☐
3	In the past 12 months, has your team experienced a significant change in how you do business (e.g. business transformation or realignment)?	☐
4	Does your team communicate with external stakeholders such as: a) Taxpayers, tax preparers b) Other (e.g. other government departments, tax professional organisations, media)	☐
5	Does your team work with large volumes of sensitive information? • Verify the types of sensitive information by consulting the *Protecting and Handling Information Pamphlet.*	☐
6	Does your team use information (e.g. taxpayer information, phone numbers, etc.) that is not always fact checked, in work that is input into Agency documents or correspondence[3]?	☐
7	Does your team work with customised or unique content (e.g. not using pre-existing templates or text)?	☐
8	Is your work unit dependent on the accuracy of information received from or sent to other areas in the Agency?	☐

[1] When using this checklist, please refer to the "Reducing vulnerabilities in Internal Processes" presentation.

[2] Consider what "high" means in your operational context.

[3] Agency documents or correspondence refers to anything that is sent external to the Agency.

9	Do you face challenges in monitoring your team's access to taxpayer information?	☐
10	Do some of the established approval processes get missed, bypassed, or changed?	☐
11	Does your team work with **at least one** of the following: • Quick turnaround times • Legislative deadlines • Service standards • Production targets • Repetitive processes	☐
12	Does your team have a high[2] volume of manual activities (e.g. manipulating data from source systems, data entry)?	☐
13	Do your employees work in one of the following manners: • Independently • In silos • Unsupervised	☐
14	Have there been any complaints from employees related to IT needs not being met (e.g. availability, functionality, security)?	☐
15	Have there been any cyber security issues in the past 12 months (e.g. systems breach, phishing emails)?	☐
16	Are multiple decision points within particular processes made by the same employee?	☐
17	Does your team use judgement in determining taxpayer eligibility (e.g. benefits, audits, appeals)?	☐
18	Have there been any confirmed or suspected cases of taxpayer identity fraud facing your group in the past 12 months?	☐

If you checked **any of the boxes in Step 1**, it is recommended that you **proceed to Step 2** to review your internal processes to address any vulnerability that could lead to an error.

STEP 2: REVIEWING AND/OR ENHANCING YOUR INTERNAL PROCESSES

It is recommended that you review those specific areas where you checked a box in Step 1.

To do this, consider the five enterprise guidelines to designing risk out of the system – the 5 RIGHTs:

Guideline 1: The RIGHT controls

Are the right controls in place to reduce the risk of errors?
Are the processes well defined, communicated, and being followed?

Guideline 2: The RIGHT knowledge

Are employees aware of the impacts and consequences of errors occurring?
Do they have the right job training and receive it in a timely manner?
Is training refreshed or renewed on a regular basis? Are the right courses available?

Guideline 3: The RIGHT communication

Is there open and constant communication with employees at all levels (front line employees and above) about error prevention?
When errors happen, are they communicated up?

Guideline 4: The RIGHT contingencies

Are the appropriate plans in place at all levels of the organisation in case an error occurs?
Leverage best practices and solutions.

Guideline 5: The RIGHT planning
Are there plans in place for future continuous improvement for error prevention?

Consider the 5 RIGHTs as your defense system. By ensuring you have the five RIGHTS in place, the failure of one will have a limited impact given the other four are in place.

As you review your internal processes, the following are key considerations:

1. Talk with your team, colleagues, and similar work areas to discuss best practices and possible solutions on enhancing internal processes.

2. Think about what is and what is not within your control. Communicate up if there are process improvements that are not within your control.

3. Consider the need to have a balance between process improvements and controls (i.e. having the *right balance of the right controls*).

4. Do not increase red tape.

5. Think of *simple* solutions to enhance your processes.

It is recommended that you review this checklist **at least annually** or when changes occur in your operational environment.

Please visit the Enterprise Risk Management Division's website for tools that may be of assistance such as information on conducting a SWOT (strength, weaknesses, opportunities and threats), which is a good idea when looking at bridging gaps in your area, and identifying, assessing and documenting your common work unit risks. Additionally, if you checked any questions marked with an underline, we encourage you to learn more about our Internal Fraud Risk Self-Assessment Tool, which will help you look specifically for internal fraud vulnerabilities in your work area. If you have any questions or if you need support, please send an email to ERMB-Risk-Management@cra-arc.gc.ca.

MAPPING ANALYSIS OF EPSAT QUESTIONS TO HYPOTHETICAL RISK SITUATION THEMES

Questions	Misconduct	IT Failure	Lack of fairness	Privacy/ data breach	Poor service	Weak processes	Poor communication
In the past 12 months, has your team experienced a high rate of, or continuous, staff turnover?				x	x	x	
Do employees miss opportunities for training on key processes, procedures and refresher courses?		x		x	x	x	x
In the past 12 months, has your team experienced a significant change in how you do business (e.g. business transformation or realignment)?		x			x	x	
Does your team communicate with external stakeholders (e.g. taxpayers and tax preparers)?	x		x	x	x		x
Does your team work with large volumes of sensitive information?	x	x		x		x	
Does your team use information (e.g. taxpayer information, phone numbers, etc.) that is not always fact checked, in work that is input into Agency documents or correspondence?	x			x	x	x	x
Does your team work with customised or unique content (e.g. not using pre-existing templates or text)?					x	x	x
Is your work unit dependent on the accuracy of information received from or sent to other areas in the Agency?				x	x	x	x
Do you face challenges in monitoring your team's access to taxpayer information?	x			x		x	
Do some of the established approval processes get missed, bypassed, or changed?	x	x	x	x	x	x	x
Does your team work with at least one of the following; quick turnaround times, production targets, legislative deadlines, repetitive processes, service standards?			x	x	x	x	x
Does your team have a high volume of manual activities (e.g. manipulating data from source systems, data entry)?	x	x		x	x	x	
Do your employees work in one of the following manners: independently, unsupervised or in silos?	x			x	x	x	
Have there been any complaints from employees related to IT needs not being met (e.g. availability, functionality, security)?		x		x	x	x	
Have there been any cyber security issues in the past 12 months (e.g. systems breach, phishing emails)?		x		x			
Are multiple decision points within particular processes made by the same employee?	x					x	

Does your team use judgement in determining taxpayer eligibility (e.g. benefits, audits, appeals)?	x		x		x	x	
Have there been any confirmed or suspected cases of taxpayer identity fraud facing your group in the past 12 months?					x	x	x

HYPOTHETICAL SITUATIONS THAT MAY IMPACT OUR REPUTATION GROUPED BY THEME

IT Failure (6) – situations of system/equipment failure that effect operational activities of the CRA

☐Catastrophic crash of tax filing system during the "filing season"
☐ Hacker or fraud event during launch of a system
☐ Not user friendly IT system
☐ System breach (phishing attempt, ransomware, cyber attack)
☐ System outages
☐ System failure (other)
☐ Other: _____

Lack of fairness (3) – situations of inconsistent decisions, or perceived bias or unfairness

☐ Excessive penalties
☐ Inconsistent and unfair treatment of taxpayers
☐ Incorrect profiling and inability to fight against unfair economy
☐ Other: _____

Misconduct or inappropriate behaviour (15) – wrongful acts committed by CRA employees, officials and/or others

☐ Acceptance of bribes by employees
☐ Corruption (general)
☐ CRA employee asking for bribe
☐ Taxpayer debt fraud and scams
☐ Employee involved in illegal operations (not connected to their work)
☐ Employee misconduct such as harassment and/or discrimination of employees
☐ Employee misconduct or investigations (general)
☐ Fraud committed by employees (general)
☐ Fraud committed by contractors
☐ Identify theft/refund fraud perpetrated by employer

☐ Identify theft/refund fraud perpetrated by contractor
☐ Improper interference by executives in tax audits, enforcement actions, etc.
☐ Arrest or investigations of top level officials for criminal activities
☐ Actions by CRA senior officials that impact perception of their integrity
☐ Procurement fraud
☐ Unprofessional behaviour of employees
☐ Other: _____

Poor communication (3) – situations that delay or spread inaccurate, information

☐ Introduction of new forms of tax administration based on digitalisation, which requires significant investments in the development of taxpayers' information systems (for example, new cash register, mandatory e-invoicing)
☐ Misuse of social media, where inaccurate information can be disclosed or when use of social media is damaging to an organisation's reputation (i.e. negative comments)
☐ Poor communication (general) leads to misunderstanding and affect processes
☐ Other: _____

Privacy/data breach (10) – internal/external situations that contribute to privacy concerns (e.g., CRA employees, hackers, system failures, etc.)

☐ Release of citizen sensitive information
☐ Confidentiality/data breach
☐ "Close to home" data breaches in other organisations
☐ Disclosure of sensitive data
☐ Disclosure of taxpayer data
☐ Disclosure of tax secrecy
☐ Hack into the tax filing system
☐ Leak of politically sensitive tax information by employee
☐ Leak of sensitive information (general)
☐ Loss of taxpayer information
☐ Other: _____

Weak processes (13) – situations and factors CRA's process to respond to system and human errors/misconduct

- ☐ Third party contractors and accountability towards taxpayers
- ☐ Change or cancellation of the decision of the tax authority in court
- ☐ Failure to address a known risk that then manifests and becomes a crisis
- ☐ Identity theft enabling third parties to pass CRA authentication processes
- ☐ Manual work or processes leading to mistakes
- ☐ Mistakes in communication
- ☐ Misunderstanding of proposed changes into Tax Code
- ☐ Poor risk assessment leading to failure to target major risks
- ☐ Risk of not targeting major risks
- ☐ Slow response to crisis
- ☐ Staff skills (e.g. under trained, not enough access to resources or support)
- ☐ Employees that were not replaced after their departure
- ☐ Failure to appropriately support third parties or stakeholders
- ☐ Poor organisational structure
- ☐ Other: _____

Poor service (4) – situations that lead to taxpayer dissatisfaction with the level of service provided by the CRA

- ☐ Failure to deliver services at the quality expected by taxpayers
- ☐ Low capability (both on legal grounds as low competence and also lack of resources)
- ☐ Mistreatment of taxpayers
- ☐ Poor customer service
- ☐ Other: _____

Annex D. Internal fraud risk self-assessment tool: A tool for agency managers

While the vast majority of employees follow their organisation's core values, there are rare times when fraud can happen. However, the CRA needs to prevent, as much as possible, the exposure to potential internal fraud, which can have a **significant impact** on its **reputation** and on the **integrity** of its programs and operations.

What is Internal Fraud?

Internal fraud is "any intentional act or omission by an employee for personal enrichment, or for the enrichment of a third party, through the deliberate misuse or misapplication of the CRA's resources, revenues, information, assets or authority" (CRA Internal Fraud Control Policy).

To further illustrate the types of internal fraud that the Agency could fall victim to, hypothetical internal fraud situations have been included in Annex A.

As a CRA manager or supervisor, **you have a key role** to play in reducing your area's exposure to potential internal fraud.

START the Self-Assessment Tool

STEP 1: **DETERMINE YOUR DRIVERS –** Consider the types of internal fraud risk **DRIVERS** in the table below and ask yourself if any are applicable to your area (tick the box.). If your area hires consultants or contract workers, please consider them as employees for the purposes of this assessment.

What are DRIVERS? Drivers are conditions that exist in the environment (internal or external) that introduce or influence exposure to risks. *Recall, you can add your own drivers in the space provided.*

#	DRIVERS	YES, THIS APPLIES TO MY AREA
1	People who work in this area have the ability to access and/or manipulate taxpayer/debtor or benefit recipient information (personal and/or financial).	☐
2	People who work in this area have the ability to provision and de-provision access to Agency servers.	☐
3	People who work in this area have the ability to access and/or manipulate employee information (personal and/or financial, excluding managerial access to employee information).	☐
4	People who work in this area have the ability to generate Protected B/Secret/Confidential CRA business information.	☐
5	People who work in this area require specialised knowledge that makes oversight difficult.	☐

6	The area is responsible for overseeing Agency financial transactions and/or managing financial assets (excluding employee-generated travel claims or employee-level acquisition card use, for example).	☐
7	People who work in this area interact directly and repeatedly with taxpayers, internal/external stakeholders, and/or third party service providers. **If this applies to your area, specify these stakeholders, including other programs/areas within the CRA, that your area directly and repeatedly interacts with (please **do not** include individual taxpayer names)*	☐
Add your own DRIVERS here:		

STEP 2: DETERMINE YOUR RISKS – Consider the types of internal fraud **RISKS** presented in the table below and ask yourself if any are applicable to your area (tick the box.).

What are RISKS? A risk is the uncertainty that surrounds future events and outcomes. *Use the hypothetical situations at the end of the document as prompts or examples to help you think about risks. You can also add your own risks in the space provided.*

#	RISKS	YES, THIS APPLIES TO MY AREA
1	There is potential for misusing insider information for personal gain.	☐
2	There is potential for making inappropriate audit/review/refund related decisions for personal gain.	☐
3	There is potential for stealing taxpayer assets for personal gain.	☐
4	There is potential for inappropriately accessing Agency data and/or taxpayer information for personal gain.	☐
5	There is potential for misuse of authority/position by management for personal gain.	☐
6	There is potential for sharing sensitive information with taxpayers or benefit recipients for personal gain.	☐
Add your own RISKS here:		

STEP 3: DETERMINE YOUR CONTROLS - Consider the types of **CONTROLS** in the table below and ask yourself if any are applicable to your area (tick the box.).

What are CONTROLS? A control is the means by which an organisation reduces the likelihood of a risk occurring or its impact if it does occur. *Recall, you can add your own controls in the space provided.*

#	CONTROLS	YES, THIS APPLIES TO MY AREA
1	The area currently has program-specific internal policies, procedures and directives that could prevent a fraud.	☐
2	The area currently has monitoring of audit trails/system access reviews.	☐

3	The area currently has managerial oversight and approvals of work.	☐
4	The area currently has HQ monitoring of files.	☐
5	The area currently has a secure paper storage system.	☐
6	The area of practice currently has individual professional code of ethics.	☐
7	The area currently has limited access to data (e.g., on a need-to-know basis).	☐
8	The area currently has segregation of duties.	☐
9	The area currently has limited ability to manipulate data.	☐
10	The area currently has secure data storage.	☐
11	The area currently has a quality assurance or review program in place.	☐
Add your own CONTROLS here:		

STEP 4: CONSIDER TAKING ACTION - Ask yourself the following key questions to determine if you need to take steps to reduce your risk exposure to internal fraud.

- Do your controls from STEP 3 sufficiently address your drivers of risk and the potential risks to which your area is exposed? If so, you can choose to **ACCEPT AND MONITOR** these risks.
- Do you think you need to invest in additional measures to reduce your risk exposure from internal fraud? If so, you can choose to **MITIGATE** these risks. The table below provides some potential mitigation strategies that could be applied in your area.

What is risk MITIGATION? Risk mitigation is a set of actions taken to either reduce the likelihood that a risk will occur, or reduce its impact if it occurs.

If you have chosen to mitigate your internal fraud risk(s), consider the mitigation strategies below that might help you reduce your exposure. As well, you can consult with the list of controls in Step 3 for other potential measures that could be implemented.

Keep in mind that not all potential mitigation strategies are included in this list. *In the space provided, add your own mitigation strategies if you feel they could be applicable.*

#	MITIGATION STRATEGIES	YES, THIS APPLIES TO MY AREA	WHO?	WHEN?
1	Implement a Quality Assurance Program, including random file reviews.	☐		
2	Enhance the workload development process, including strengthening the division of responsibilities (segregation of duties).	☐		
3	Enhance the limitation of access, and ability to, manipulate documentation and data.	☐		

4	Enroll employees in existing training courses on ethics and responsibilities.	☐		
5	Strengthen management oversight.	☐		
6	Implement an enhanced electronic data storage system.	☐		
Add your own MITIGATION STRATEGIES here:				

Alright, I have completed the tool. What do I do now?

You are encouraged to review this self-assessment tool periodically, or when there is a major change in the environment. This will ensure that your area continues to reflect on the risks of internal fraud and takes steps to reduce exposure where necessary.

You are encouraged to share the results with your supervisor. You are not asked to disclose the results of your assessment elsewhere within the CRA unless you choose to do so voluntarily.

You are also encouraged to further consider the list of hypothetical scenarios (Annex A) and how they may impact your day-to-day operations.

Please visit the Enterprise Risk Management Division's website for other tools that may be of assistance. You may also consider using our Error Prevention Self-Assessment Tool, which is helpful in determining where gaps exist in your processes.

If you have any questions or if you need support, please email ERMB-Risk-Management@cra-arc.gc.ca

This self-assessment was completed by Insert name of program/area scoped for the exercise **on _____ . Additionally, the program/area consulted:**

1. Program/area external to scoped area that was consulted – delete if not applicable
2. Program/area external to scoped area that was consulted – delete if not applicable
3. Program/area external to scoped area that was consulted – delete if not applicable

Hypothetical Situations in the Internal Fraud Risk Self-Assessment Tool (IFR-SAT)

Introduction and purpose

The CRA leveraged its participation in the Organisation for Economic Co-operation and Development's (OECD) Federal Tax Administration (FTA) Risk Management Community of Interest in a discussion on hypothetical situations which could negatively impact the reputation of a tax administration. The CRA collected and analysed the data from these discussions and rolled up the results into common themes. At a high level, the hypothetical situations can result from errors, or from intentional behaviours, with negative consequences.

The Internal Fraud Risk Self-Assessment tool provides managers with the opportunity to review the existing risks, drivers, controls, and consider action plans, to help mitigate against internal fraud. The hypothetical situations involving intentionally negative behaviours such as misconduct, manipulation, or fraud serve to provide helpful examples of internal fraud for managers to consider in completing the IFR-SAT.

Using hypothetical situations to assess internal fraud vulnerabilities

The hypothetical situations identified by the OECD's FTA that involved intentional, malicious behaviour were grouped into 3 themes. All situations can be used as examples of vulnerabilities to internal fraud. The 3 themes are:

1. Misconduct
2. IT Manipulation
3. Privacy/Data Breach

HYPOTHETICAL SITUATIONS THAT MAY IMPACT OUR REPUTATION, GROUPED BY THEME

The hypothetical situations list is intended to be an **evergreen** document that reflects the current operating environment. As such, suggestions for improvements or updates (i.e. new hypothetical situations) are welcomed.

IT Manipulation (6) – situations of system/equipment manipulated to effect operational activities of the CRA

- ☐ Hacker or fraud event during launch of a system from an internal source
- ☐ Intentional system breach
- ☐ Planned system outages for fraudulent activities
- ☐ Intentional system failure (other)
- ☐ Other:

Misconduct or inappropriate behaviour (15) – wrongful acts committed by CRA employees, officials and/or others

- ☐ Acceptance of bribes by employees
- ☐ Corruption (general)
- ☐ CRA employee asking for bribe
- ☐ Taxpayer debt fraud and scams
- ☐ Employee involved in illegal operations (not connected to their work)

- ☐ Employee misconduct or investigations (general)
- ☐ Fraud committed by employees (general)
- ☐ Fraud committed by contractors
- ☐ Identify theft/refund fraud perpetrated by employer
- ☐ Identify theft/refund fraud perpetrated by contractor
- ☐ Improper interference by executives in tax audits, enforcement actions, etc. for fraudulent purposes
- ☐ Arrest or investigations of top level officials for criminal activities
- ☐ Actions by CRA senior officials that impact perception of their integrity
- ☐ Procurement fraud
- ☐ Access of sensitive information for a fraudulent activity by using the credentials of another employee
- ☐ Misuse of social media, where inaccurate information is purposefully disclosed for personal gain
- ☐ Other:

Privacy/data breach (10) – internal/external situations that contribute to privacy concerns (e.g., CRA employees, hackers, system failures, etc.)

- ☐ Intentional release of citizen sensitive information for fraudulent activities
- ☐ Intentional confidentiality/data breach
- ☐ Deliberate disclosure of sensitive data for fraudulent purposes
- ☐ Deliberate disclosure of taxpayer data for a fraudulent activity
- ☐ Deliberate disclosure of tax secrecy for fraudulent purposes
- ☐ Hack into the tax filing system by an internal actor
- ☐ Intentional leak of politically sensitive tax information by employee
- ☐ Intentional leak of sensitive information (general)
- ☐ Purposeful loss of taxpayer information
- ☐ Employee using organisational information to make a false tax claim
- ☐ Colleague impersonation for a fraudulent activity
- ☐ Other:

FORUM ON TAX ADMINISTRATION

Communities of Interest Series

Enhancing Reputational Risk Management

This report highlights the importance of reputational risk management in modern tax administration and sets out some key considerations as to how to identify and manage reputational risks. It also contains a set of tools to assist tax administrations in developing their capacity in this area, including a maturity model which allows administrations to self-assess their current capacity and to identify areas for possible further development. The report has been produced by the FTA Enterprise Risk Management Community of Interest (COI). It is the first in an intended series of reports by the FTA's Communities of Interest which bring together experts to exchange views and work collaboratively on major themes of modern tax administration. This work was led within the Enterprise Risk Management COI by colleagues from the Canada Revenue Agency.

As noted in the report, managing reputational risk is hugely important in helping to achieve the objectives of tax administration and wider government, something which is particularly true in times of crisis. The key principles driving reputational risk are trust in the administration and its staff and respect towards the organisation. When an administration consistently abides by its ethical duties, it establishes trust in the eyes of taxpayers and other stakeholders. When it fails to meet the standards expected of it, particularly with respect to the fair and equal treatment of taxpayers, public trust and credibility can be quickly eroded.