Chapter 6.

Strengthening the lines of defence against corruption: Risk management, internal control and audit

Public sector organisations should ensure that their "lines of defence" against fraud and corruption are strong and based on sound risk management, internal controls, and independent assurance (internal audit) activities. This comprehensive approach allows organisations to pre-emptively tackle potential corruption, detect integrity violations when they occur, continually monitor and improve controls over time, and more swiftly adapt to changing contexts and risks. As such, this chapter focuses on these three key elements in Mexico's federal public administration. The first section assesses Mexico's Ministry of Public Administration's risk management process (the Administración de Riesgos Institutional, or ARI). The second section examines the internal control environment and processes put in place by the federal government and line ministries. The third section highlights the importance of an independent internal audit function for consulting senior management and providing assurance over the effectiveness and efficiency of internal control and risk management arrangements within public organisations.

Introduction: Building a system of defence against public sector corruption

A solid internal control framework is the cornerstone of an organisation's defence against corruption, and consists of the policies, structures, procedures, processes, tasks and other tangible and intangible factors that enable an organisation to identify and appropriately respond to internal and external operational, financial, or compliance-related risks. An effective internal control framework should ultimately help the organisation comply with its mandate and any relevant legislation, safeguard an organisation's assets, and facilitate internal and external reporting.

Although senior managers are primarily responsible for implementing internal controls and monitoring their effectiveness, all officials in a public organisation, from the most senior to junior, have a role to play in identifying risks, deficiencies and ensuring that internal controls address and mitigate these in a cost-effective manner. Every staff member should be encouraged to continuously contribute to the development of better systems and procedures that will enhance integrity and improve the organisation's resistance to corruption.

Internal audit is the next pillar of defence against corruption and provides objective assurance that risk management and internal controls are functioning properly. An effective internal audit monitoring and assurance function ensures that internal control deficiencies are identified and communicated in a timely manner to those responsible for taking corrective action. The monitoring process involves establishing a foundation for designing and executing monitoring procedures that are prioritised based on risk, and assessing and reporting the results, including following up on corrective action where necessary.

While risk, control and audit functions are essential in the fight against corruption, they are also necessary ingredients for greater accountability, better management and cost effectiveness. Controls help organisations run more smoothly, reduce costs, and avoid waste. They also help hold officials to account for their actions, and to report to the public and oversight institutions on performance and value-for-money achieved.

Mexico's Ministry of Public Administration (*Secretaría de Función Pública*, SFP) is the federal entity responsible for developing and overseeing policies, standards and tools on internal control, including risk management and internal audit functions in the federal administration. The SFP also establishes policies and frameworks and provides guidance to line ministries in collaboration with the Supreme Audit Institution (*Auditoría Superior de la Federación*, ASF), mainly through the National Auditing System.

Mexico's recent national anti-corruption system (NACS) reforms have placed a strong emphasis on ensuring that a robust internal control system based on solid risk management and internal audit functions is in place across the public sector. As noted in Chapter 2, the inclusion of the SFP and ASF in the NACS Co-ordination Committee demonstrates the high relevance of the control and audit functions in preventing and detecting integrity violations.

This chapter will examine the maturity and integration of internal control functions, as well as the assignment of roles and duties regarding these activities within the three lines of defence model in Mexico's federal public administration, and the extent to which they are based on the principles of risk management, balanced and cost-effective controls, and effective assurance oversight.

Better risk-management: Taking a pre-emptive and cost-effective approach to fighting public sector corruption

The SFP should further emphasise risk management in its internal control policies, ensuring that risk assessments and mitigation activities are more effectively embedded into the strategic and operational activities of public sector organisations through stronger institutional arrangements and capacity-building efforts.

Corruption risk mapping and assessment are key prerequisites towards understanding risk exposure and allowing public organisations to reach informed risk management decisions. This process has to identify risk factors (e.g. why would corruption occur in these specific area of our organisations?), as well as potential corruption schemes (e.g. how would corruption be perpetrated in our organisation?). The evaluation of the probability that the identified corruption risks might occur, and the potential impact of the materialisation of these threats, is essential for prioritising responses and allocating adequate resources.

The assessment of the probability and impact for each corruption risk produces an assessment of inherent corruption risks without taking into consideration existing controls. Therefore, the next methodological step involves mapping existing controls and mitigating strategies for each of these risks. During this step it is very important to assess with the business process owners whether the identified mitigating controls and policies are functioning and having the expected impact on the relevant risks.

The output of this exercise is the identification of the residual risks, which is followed by the decision on the risk treatment action plan. Available options can include reviewing and amending existing controls and introducing new controls. The logical follow up is the development of a corruption risk treatment plan which provides for a detailed implementation plan (allocation of tasks, resource requirements, monitoring and reporting requirements, etc) of the risk mitigation options.

The quest to develop and maintain the right policies and controls to effectively identify and manage corruption risks poses serious challenges. Countries such as the United States, the United Kingdom, Australia, and Colombia have introduced dedicated frameworks for managing corruption risks. Box 6.1 below illustrates some key elements of the Colombian methodological approach to corruption risk management.

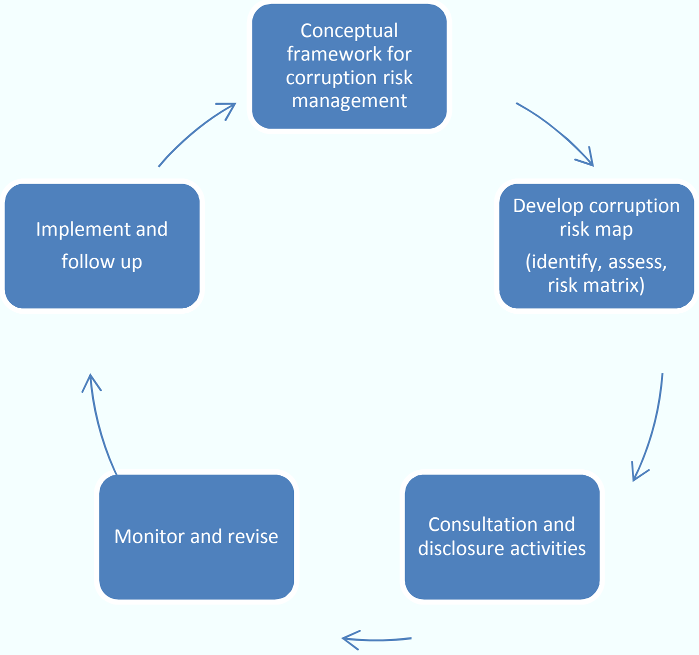
Box 6.1. Corruption risk management: The example of Colombia

The Secretariat of Transparency, together with the Ministry of Public Administration (*Departmento Administrativo de la Funcion Publica*, DAFP), have developed a corruption risk management methodological framework, described in a comprehensive manual updated in 2015.

The methodological approach is based on the risk management process described in the Colombian internal control framework (*Modelo Estandar de Contro Interno*, MECI), but highlights the inherent characteristic of corruption risks versus the institutional risks of public organisations. This means that Colombian public organisations have to develop two different risk maps following predetermined and standardised steps and templates. There are positives and negatives to having two separate risk management exercises based on the same methodological model. On one hand, it may be seen as burdensome and bureaucratic, duplicating efforts and wasting valuable resources. On the other hand, it can be argued that it raises awareness among senior management and staff of the importance of having a sound anti-corruption policy with distinct activities from the mainstream managerial and financial control and risk activities.

Box 6.1. Corruption risk management: The example of Colombia *(cont.)*

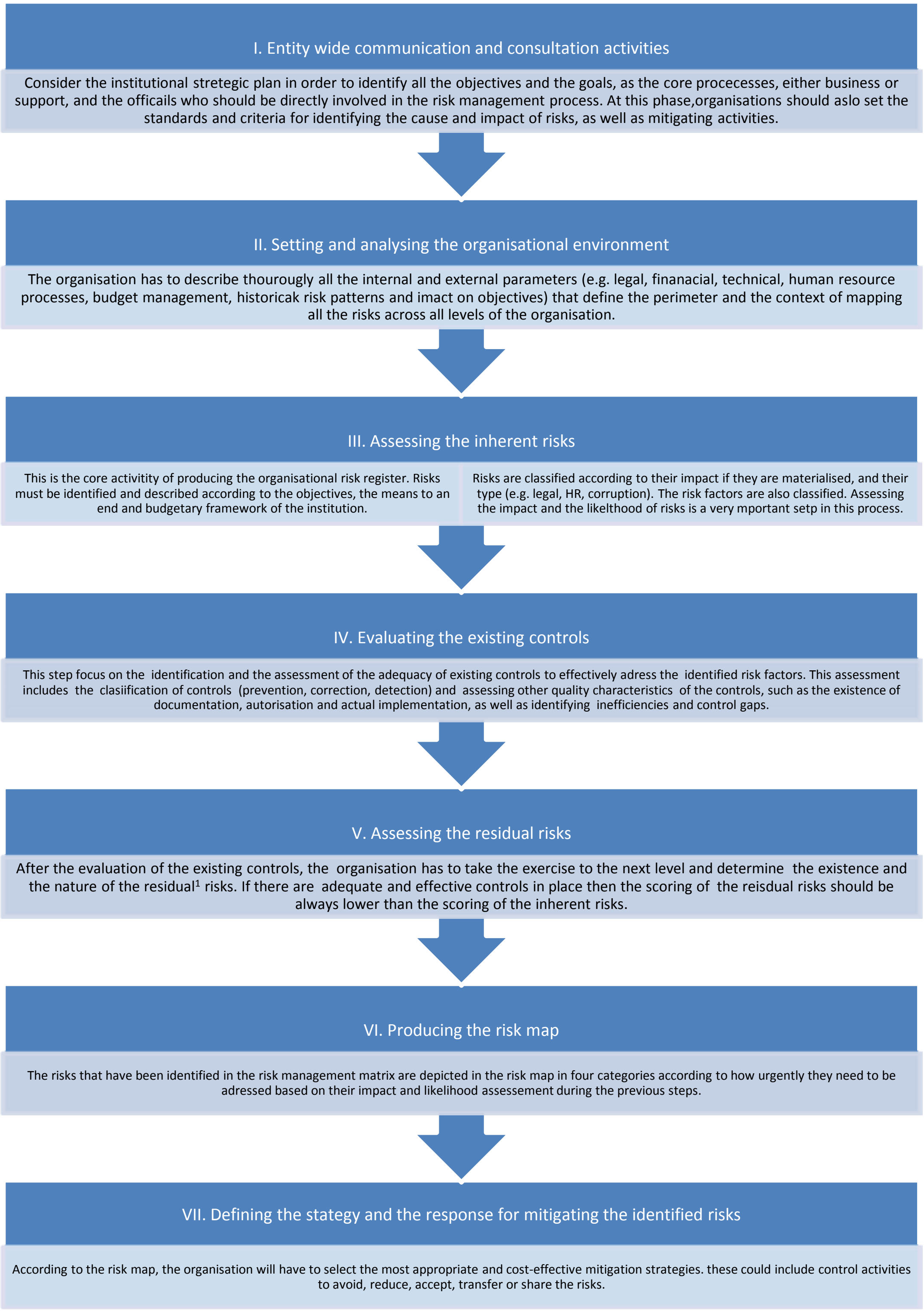
The following graphic depicts the Colombian methodology for corruption risk management:


Conceptual framework for corruption risk management
Develop corruption risk map
(identify, assess, risk matrix)
Consultation and disclosure activities
Monitor and revise
Implement and follow up

Source: Corruption Risk Management Manual, Colombia's Presidency of the Republic, Bogota 2015 https://www.unicauca.edu.co/versionP/sites/default/files/files/guia-gestion-riesgo-corrupcion-2015.pdf.

The SFP's methodological and implementation Manual of Internal Control System (*Acuerdo por el que se emiten las Disposiciones y el manual Administrativo de Aplicacion General en material de Control Interno*, MAAG-CI), which was published in the Official Gazette on 2 November 2016, details the risk management methodology and related activities that aim to identify, assess and mitigate corruption risks. Federal public entities have to apply concrete methodological steps in order to produce: 1) the annual risk management matrix (*Matriz de Administración de Riesgos*), which gives a detailed picture of each of the risks; 2) the risk map, which is the graphic illustration of the risk matrix and; 3) the Working Programme of Risk Management (*Programa de Trabajo de Administracion de Riesgos*, or PTAR), which is the implementation action plan. Figure 6.1 depicts the basic steps of the overall risk management exercise:

Figure 6.1. Phasing in the risk management model (ARI) of the SFP



I. Entity wide communication and consultation activities

Consider the institutional stretegic plan in order to identify all the objectives and the goals, as the core procecesses, either business or support, and the officails who should be directly involved in the risk management process. At this phase,organisations should aslo set the standards and criteria for identifying the cause and impact of risks, as well as mitigating activities.

II. Setting and analysing the organisational environment

The organisation has to describe thourougly all the internal and external parameters (e.g. legal, finanacial, technical, human resource processes, budget management, historicak risk patterns and imact on objectives) that define the perimeter and the context of mapping all the risks across all levels of the organisation.

III. Assessing the inherent risks

This is the core activitity of producing the organisational risk register. Risks must be identified and described according to the objectives, the means to an end and budgetary framework of the institution.

Risks are classified according to their impact if they are materialised, and their type (e.g. legal, HR, corruption). The risk factors are also classified. Assessing the impact and the likelthood of risks is a very mportant setp in this process.

IV. Evaluating the existing controls

This step focus on the identification and the assessment of the adequacy of existing controls to effectively adress the identified risk factors. This assessment includes the clasiification of controls (prevention, correction, detection) and assessing other quality characteristics of the controls, such as the existence of documentation, autorisation and actual implementation, as well as identifying inefficiencies and control gaps.

V. Assessing the residual risks

After the evaluation of the existing controls, the organisation has to take the exercise to the next level and determine the existence and the nature of the residual[1] risks. If there are adequate and effective controls in place then the scoring of the reisdual risks should be always lower than the scoring of the inherent risks.

VI. Producing the risk map

The risks that have been identified in the risk management matrix are depicted in the risk map in four categories according to how urgently they need to be adressed based on their impact and likelihood assessement during the previous steps.

VII. Defining the stategy and the response for mitigating the identified risks

According to the risk map, the organisation will have to select the most appropriate and cost-effective mitigation strategies. these could include control activities to avoid, reduce, accept, transfer or share the risks.

Source: OECD Secretariat based on the Ministry of Public Administration's "Acuerdo por el que se emiten las Disposiciones u el manual Administrativo de Aplicacion General en material de Control Interno", November 2016 www.gob.mx/cms/uploads/attachment/file/174036/acuerdo-disposiciones-manual-CI.pdf.

The recently updated manual has several elements that address the weaknesses of the previous manual. Both its structure and content are more aligned with leading international standards (Committee of Sponsoring Organizations [COSO] Internal Control and Enterprise Risk Management Frameworks, ISO 31000, The International Organisation of Supreme Audit Institutions [INTOSAI] guidelines on internal control, etc). For the first time, the policy explicitly recognises how risk management methodology applies to corruption risks. Overall, the approach to corruption risks is the same as for all other types of risks, with some differences, such as:

- In relation to the first methodological step, "entity-wide communication and consultation activities", the manual states that organisations should focus on processes that are vulnerable to corruption, such as financial and budgetary issues, public procurement, investigations and sanctions.
- Regarding step two on "defining the organisational environment", the manual states that the focus should be directed to the identification of the root causes for corruption and fraud risks by identifying the weaknesses (internal factors) and threats (external factors) that can affect processes and procedures more prone to corruption schemes.
- "Assessing the residual corruption risks" is a procedural step that details the full range of risks and their degree of probable impact described in the risk assessment exercise. In the case of corruption risks, assessment of the materialisation can only be classified as unacceptable and intolerable because of the impact on reputation, public trust and credibility, and transparency of the institution, while it always results in damaging public financial resources.
- During the process of "selecting the right mitigation strategy", in the case of corruption risks, the manual underscores that there can only be control activities to avoid or reduce the risk.

As described earlier, the risk matrix forms the basis for the risk map and for developing the programme of work for risk management (*Programa de Trabajo de Administracion de Riesgos*, PTAR), which is endorsed by the head of the entity, the co-ordinator of internal control and the liaison for risk management. The PTAR is one of the main tools developed by the SFP to complement and assist public organisations in mainstreaming risk management related activities. The PTAR's primary objective is to monitor and assess the execution of the mitigating strategies and controls, with the aim of addressing the risks. To this end, it includes all the necessary elements describing the risks, the mitigating strategies and the resources needed to implement these activities, as well as implementation monitoring requirements. The progress of the PTAR must be thoroughly documented and communicated to relevant stakeholders within the entity every three months.

According to the relevant provisions of the conceptual framework and the implementation guidelines, all officials in the organisation are responsible for communicating and reporting risks related to the processes in which they are involved. It is important that controls are owned by someone responsible for their operation. The control owner or operator would normally be the person who executes the control on a day-to-day basis, and can be someone other than the risk owner, who remains accountable for the design, application, monitoring and evaluation of controls according to the risk evolution.

The "*Oficialias Mayores*", or chief administration officers who report directly to ministers, take the lead in the process within federal public entities. There are also specific duties assigned to the head and the senior administration of the organisation that focus on monitoring, reviewing, assessing and approving the proper implementation of the risk management methodology and its outcomes. The internal control co-ordinator (usually the *Oficialia Mayor*) of each ministry and organisation has an important role in the risk management function as they are responsible for:

- Agreeing with the head of the institution the methodological approach, the objectives and the processes to be part of the risk mapping exercise, and communicating these across all entity levels.
- Convening the heads of all administrative units of the institution, the head of the internal control unit (the OIC) and the liaison for risk management to form the working group that will produce the matrix, the map and the PTAR.
- Review the quarterly progress reports of the PTAR and the annual report on risk management, disseminate the matrix, the map and the PTAR across the entity, and provide guidance to those responsible for specific control activities.

Another important actor is the liaison officer for risk management (*Enlace de Administracion de Riesgos*), who links the internal control co-ordinator with all of the administrative and operational areas of the organisation, supports managers and staff throughout the different steps of the process, and reviews and documents input from the areas in order to finalise the expected deliverables and communicate the results to all stakeholders. The head of the internal control unit supports entity staff in the implementation of the recommendations stemming from the risk management process; ensures that the activities included in the PTAR are designed for avoiding, reducing, accepting or transferring the risks; and provides non-binding opinions to the working groups and staff responsible for carrying out the whole exercise.

In this sense, the role of the Committee of Control and Institutional Performance (*Comité de Control y Desempeño Institutional*, COCODI) in effective corruption risk management could be decisive. The head of public organisations have to establish COCODIs, which are organisation-wide committees with a broad scope of competencies. Their mandate entails contributing to institutional risk management, including analysis and monitoring of strategies and control measures identified in the PTAR, as well as prioritising the institutional risks that call for immediate attention with a special focus on corruption risks. COCODIs also have to promote the application of preventive measures to avoid the occurrence of risks. They may work towards treating risk management as an integral part of the management systems since they can link the risk assessment with improvements in organisational performance, which is also one of their core tasks.

Committing adequate and qualified personnel, while taking care of the necessary institutional arrangements, is a crucial issue for the success of anti-corruption policies. The new manual puts the spotlight on corruption risk management, and the SFP should identify a "champion" to highlight the importance of this function. Box 6.3 illustrates the approach of the Australian Crime and Misconduct Commission of Queensland. As such, Mexico could consider introducing a dedicated risk management committee, other than COCODI, in large public organisations. Alternatively a committee could be established that focuses only on fraud and corruption control, while COCODI would focus on business risk management and governance issues. Such an option could be better examined and first piloted in the framework of evaluating the impact and the challenges related to the new role of the COCODIs, as described in the new manual. The institutional and operational models for audit and risk boards/committees are further elaborated in the section focusing on strengthening independence and the assurance role of the internal audit function. Smaller organisations could appoint a fraud and corruption control co-ordinator/manager with the right training, skills and expertise to undertake this specific task.

Box 6.2. Establishing fraud and corruption risk management "champions"

Depending on the size of the organisation, the fraud and corruption control programme may warrant different levels of response. These may involve establishing one or more of the following:

- risk management committee
- fraud and corruption control committee
- fraud and corruption control co-ordinator and/or manager

The risk management committee

- ensures that the agency maintains effective risk management practices across all its activities
- oversees the development of a systematic and co-ordinated risk-management framework
- monitors the external risk environment
- assesses the impact of any changes on the agency's risk profile

Fraud and corruption control committee

A larger agency may also establish a fraud and corruption control committee to deal specifically with fraud and corruption issues. This committee should have a broadly based (cross-functional) membership to ensure that it can cover all areas at risk. It should carry a clearly defined responsibility for overseeing the effective implementation of fraud and corruption control measures.

Fraud and corruption control co-ordinator or manager

Change management is more likely to be successful where there is accountability for the commitment of human and financial resources and for the outcomes. Nominating a responsible person, position or small taskforce as a "champion" to drive the programme and bring about change is one of the best ways to ensure success.

Source: Fraud and Corruption Control - Guidelines for best practice, of the Crime and Misconduct Commission of Queensland, Australia, 2005, www.ccc.qld.gov.au/research-and-publications/publications/prevention/fraud-and-corruption/fraud-and-corruption-control-guidelines-for-best-practice-1.pdf/download.

Mexico needs to address its compliance mentality, as risk management has become simply a "tick box" exercise without genuine reflection and action on behalf of organisations. Interviews suggested that the exercises had become a formalistic administrative or bureaucratic requirement that cover superficial risks such as formal roles and responsibilities and compliance with laws and regulations, but that neglect preventing and detecting actual risks (including fraud and corruption risks). Moreover, exercises were sometimes seen as the responsibility of a specific group of people working in a "silo" approach, detached from the operational units where real risks are present, thus failing to identify the whole range of institutional and corruption risks threatening the achievement of the entity's objectives.

Therefore, in addition to piloting risk management committees, it would be important for the SFP to accompany its new policy reforms and institutional arrangements with an effective awareness and capacity-building programme around risk management generally, and with a specific module on risk management for fraud and corruption. Such a programme should look beyond the idea of one-off training sessions, the SFP should instead leverage a variety of existing programmes that span an official's time with the federal public administration. For example, training should be provided as part of induction or orientation programmes, and as part of code of conduct and ethical decision-making training. Furthermore, specialist and specific training for high-risk functions and for different staff groups, such as those responsible for audit, financial functions or investigations, should be provided.

While the manual, and corresponding PTAR, risk map and matrix tools demonstrate progress and more advanced risk management strategies, limitations remain in their full implementation. As such, the SFP could explore ways to closely monitor, assess, and even review if needed, the quality and impact of these tools on the management and operations of the entity to ensure that this exercise has real added value concerning the improvement of service delivery to citizens and the achievement of the entity's mission and objectives. To this end, the SFP could consider creating an online observatory of organisations' PTAR exercises, along with the corresponding risk matrices and maps. This online observatory could allow entities to share good practice, learn from the most advanced organisations, and motivate officials to improve their respective risk management activities and tools.

The SFP and line ministries should consider leveraging data analytics to better identify and address integrity risks, and thereby improve the quality of their institutional risk maps and mitigation strategies.

As already highlighted, risk management in the Mexican federal public administration frequently operates as a standalone exercise. This approach does not allow the organisation to fully identify all institutional risks and use structured and unstructured data to better understand the potential impact of a range of risks. By incorporating data analytic practices into the risk management function, organisations can monitor performance through risk sensitivity analysis, model key risk event scenarios, and become more risk intelligent in developing intervention and mitigation strategies. Data analytics is an analytical process by which insights are extracted from operational, financial, and other forms of electronic data internal or external to the organisation. These insights can be historical, real-time, or predictive, and can also be risk focused (e.g. controls effectiveness, fraud, waste, abuse, policy/regulatory noncompliance). Data analytics combines analytic technology and techniques with human interaction to help detect operational risks, improper transactions and integrity breaches such as corruption events, either before they are manifested or after they occur.

Box 6.3. Leveraging data analytics for managing corruption risks

The 2016 Global Fraud Study of the Association of Fraud Examiners (ACFE) report identifies proactive data monitoring/analysis as the most effective tool for anti-corruption control in helping to reduce corruption losses and corruption scheme duration. More specifically, the 36.7% of victim organisations that were using proactive data monitoring and analysis techniques as part of their anti-fraud programme suffered fraud losses that were 54% lower, and detected the fraud in half the time, compared to organisations that did not use this technique.

Furthermore, according to the Institute of Internal Auditor's (IIA) Global Technology Audit Guide (IPPF-Practice Guide), data analysis can help internal auditors meet their auditing objectives relating to the efficiency of risk management arrangements. Analysing data within key organisational processes enables internal audit to:

- Identify instances of fraud, errors, inefficiencies, or noncompliance, with data driven from 100% of relevant transactions and diverse sources.
- Detect changes, vulnerabilities and weaknesses that could expose the organisation to undue or unplanned risk.
- Identify changes in organisational processes and ensure that it is auditing today's risks — not yesterday's.

A number of specific analytical techniques have been proven highly effective in analysing data for wrongdoing and anti-fraud auditing purposes:

- Calculation of statistical parameters (e.g. averages, standard deviations, highest and lowest values) to identify outlying transactions.
- Classification to find patterns and associations among groups of data elements.
- Stratification of numeric values to identify unusual (i.e., excessively high or low) values.
- Digital analysis using Benford's Law to identify statistically unlikely occurrences of specific digits in naturally occurring data sets.
- Joining different data sources to identify inappropriately matching values such as names, addresses, and account numbers in disparate systems.
- Duplicate testing to identify simple and/or complex duplications of organisational transactions such as payments, payroll, claims, or expense report line items.
- Gap testing to identify missing numbers in sequential data.
- Summing of numeric values to check control totals that may have errors.
- Validating data entry dates to identify postings or data entry times that are inappropriate or suspicious.

Sources: ACFE (2016), *Report to the Nations on Occupational Fraud And Abuse: 2016 Global Fraud Study*, Association of Certified Fraud Examiners, Austin, TX.

IIA (2009), *Global Technology Audit Guide, Fraud Prevention and Detection in an Automated World*, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, www.iia.org.uk/media/54541/gtag13_fraud_prevention_and_detection_in_an_automated_world.pdf.

When applied to detecting fraud corruption, data analytics processes involve gathering and storing relevant data and mining it for patterns, discrepancies, and anomalies. The findings are then translated into insights that can allow a public organisation to mitigate potential threats before they occur, as well as develop a proactive corruption detection environment. In an era of digitisation and e-government, almost every corrupted act leaves behind a trail of digital fingerprints. Data analytics can enhance traditional rule-based methods to detect wrongdoing. It can also provide evidence to assess the performance of existing controls for constant improvement, since potential perpetrators and corruption schemes are constantly evolving. To this end, purpose-built data analytics is light years ahead of manual sampling. The use of data analytics can allow an organisation to find root issues, identify trends, and provide detailed results.

One of the most commonly used data analytics tools is data mining. Data mining as an analytic process is designed to explore data and to extract information from data sets in order to discover patterns and relations. It can be defined as "the nontrivial extraction of implicit, previously unknown, and potentially useful information from data" (Frawley et al., 1992; Bresfelean et al., 2007), or "the science of extracting useful information from large data sets or databases" (Hand and Mannila, 2001).

Organisations that wish to use data mining tools can purchase mining programmes designed for existing software and hardware platforms, or they can build their own custom mining solution. Risk management practitioners need to be aware of the different kinds of data mining tools available and recommend the purchase of a tool that matches the organisation's needs. This should be considered as early as possible in the project's lifecycle, perhaps even during the feasibility study.

Most data mining tools can be classified into one of three categories:

- **Traditional data mining tools:** Traditional data mining programmes help organisations establish data patterns and trends by using a number of complex algorithms and techniques. Some of these tools are installed on the desktop to monitor the data and highlight trends, while others capture information residing outside of a database. While some may concentrate on one database type, most will be able to handle any data using online analytical processing, or a similar technology.

- **Dashboards:** Installed in computers to monitor information in a database, dashboards reflect data changes and updates onscreen, often in the form of a chart or table. Historical data also can be referenced, enabling the user to see where things have changed (e.g. increase in pharmaceutical expenses from the same period last year). These could be considered asred flags for further analysis/investigation.

- **Text-mining tools:** The third type of data mining tool is sometimes called a text-mining tool because of its ability to mine data from different kinds of text, such as Microsoft Word, Acrobat PDF documents or simple text files. These tools scan content and convert the selected data into a format that is compatible with the tool's database, thus providing users with an easy and convenient way of accessing data without the need to open different applications. Capturing these inputs can provide organisations with a wealth of information that can be mined to discover trends, concepts, and attitudes.

Several OECD countries are moving towards a more advanced use of data analytics for managing corruption risks. Box 6.4 below gives some examples of the United Kingdom's and the United States' use of data analytics for effectively addressing internal and external fraud and corruption risks.

Box 6.4. Data analytics and data sharing for managing fraud and corruption risks in the United Kingdom and United States

The UK example

With the growing sophistication of corruption, many public sector organisations in the United Kingdom are looking to take a more proactive approach to verifying and validating transactions, or to uncovering potential and actual corruption. Common approaches have included: real-time credit reference and other data checks; online verification techniques; data matching with data held by other public and private sector organisations; and predictive/innovative analytics, which involves developing a model to score data for potential fraud and error that can forecast probabilities of fraud and error to an acceptable level of reliability.

The Audit Commission's National Fraud Initiative was launched as the United Kingdom's largest data matching exercise in relation to fraud. The Serious Crime Act of 2007 enabled bodies, other than those with a mandatory requirement to provide data for the National Fraud Initiative, to volunteer to participate by providing data to the Commission. The following list shows how the Department for Work and Pensions, the Driver and Vehicle Licensing Agency and HM Revenue & Customs use data matching to detect evasion acts, and how the British Broadcasting Corporation (BBC) and the National Health Service (NHS) Counter Fraud Service have used data mining for the same purpose:

- The Department for Work and Pensions has a dedicated database and matching service to identify possible fraud and error. It matches data: across benefit systems, between other government departments and Department for Work and Pensions data, for other government departments, for local authorities on housing and council tax benefits, and to tackle internal fraud.
- The Driver and Vehicle Licensing Agency uses data matching to detect vehicle excise duty evasion.
- The HM Revenue & Customs application of data matching has identified people who may have received income from property but have not disclosed this income.
- The BBC uses data mining software tools to match details of licensable places with external commercially available data to identify specific places or segments of the population for targeted enforcement activity.
- The NHS Counter Fraud Service uses data mining and analysis software to examine pharmaceutical and dental data. The software is capable of advanced data analysis that establishes data profiles and highlights anomalies. These can indicate potential fraud for further investigation.

The US example

The US Bureau of Fiscal service has created the Do Not Pay (DNP) Business Centre, which is a multi-functional analytics tool and one-stop data shop.

DNP's mission is to protect the integrity of the government's payment process by assisting agencies in mitigating and eliminating improper payments in a cost-effective manner, while safeguarding the privacy of individuals.

Box 6.4. Data analytics and data sharing for managing fraud and corruption risks in the United Kingdom and United States *(cont.)*

DNP allows government agencies to check various data sources for pre-award and pre-payment eligibility verification, at the time of payment and any time in the payment lifecycle. It allows them to verify eligibility of a vendor, grantee, loan recipient, or beneficiary. This will help prevent, reduce, and stop improper payments, as well as prevent fraud, waste, and abuse.

- DNP offers a centralised system (the DNP portal) that agencies can use at no cost to isolate and identify the potential for improper payments.
- DNP will benefit the federal agency that enters into a financial transaction with a person or entity.
- DNP is NOT a list of entities or people that should not be paid.
- DNP provides many data sources - in one place - that agencies can use to verify eligibility.
- DNP is committed to providing: quality data, more data sources, continuous system development, cutting edge data analytics, customised agency outreach.

Overview of data source functions:

Data sources	Function
Credit Alert System (CAIVRS) inputs from Department of Justice, Department of Education, Small Business Administration, Department of Housing and Urban Develoment, Department of Agriculture & Veterans Affairs	Verify whether an individual is a delinquent federal borrower.
Dept. of Health and Human Services' (HHS) List of Excluded Individuals & Entities (LEIE	Verify whether payments are to entities excluded from participating in federal health care programmes.
General Services Administration's (GSA) System for Award Management (SAM) Entity Registration Records	Verify that a vendor seeking to do business with the federal government has registered, in accordance with the Federal Acquisitions Regulation (FAR).
GSA SAM Exclusion Records	Verify whether payments are to debarred individuals.
Treasury's Office of Foreign Assets Control (OFAC)	Verify whether an individual or entity is prohibited from entering into financial transactions with US financial institutions and the US government.
Social Security Administration's (SSA) Death Master File (DMF)	Verify whether a payee is deceased.
Treasury Offset Programme (TOP) Debt Check	Verify whether payee owes delinquent non-tax debts to federal government (and participating states).

Sources: NAO/HM Treasury (2008), *Good Practice Guide: Tackling External Fraud*, National Audit Office, London.

HM Treasury (2011), *Tackling Internal Fraud*, HM Treasury, London, http://webarchive.nationalarchives.gov.uk/20130129110402/http:/www.hm-treasury.gov.uk/d/managing_the_risk_fraud_guide_for_managers.pdf.

US Bureau of the Fiscal Service (2017), Website of Do Not Pay, http://donotpay.treas.gov/ (accessed March 2017).

Mexico has identified the added value of using information and communication tools to strengthen integrity in the public sector by introducing effective measures to prevent, detect, investigate and reduce corruption events. In this framework, information and communications technology are indispensable for promoting timely access to information and tightening interagency co-operation.

The federal government, in the context of the National Digital Strategy, has engaged in various projects and initiatives related to the use of open data and technology to combat corruption:

- Labora is a platform for civic entrepreneurs that offers cutting-edge tools and connects with a network of world-class companies, mentors and investors to accelerate the impact of their ideas through innovation data.
- Datalab is a federal programme, in collaboration with the National Laboratory of Public Policy to boost the capabilities of use and data analysis for the development, implementation and evaluation of public policy based on evidence.
- Based on a series of surveys, workshops and focus groups with users, the portal Open Government Data of the Republic, datos.gob.mx, was updated to provide a better user experience. Updates include mechanisms for interacting with users to receive notifications of new publications, and reports from citizens so that they can improve the quality and availability of government open data. As part of the new release, the database of who's who in the prices PROFECO was published. This is a database that contains information on the prices of more than 3 000 products of the basic basket in more than 2 000 establishments in 32 states, since 2006 to date.
- The instruction of the President, Enrique Peña Nieto, during the Global Summit of the Alliance for Open Data focused on the implementation of the Open Data Standard for Procurement in the larger project of the government, the new airport of the City of Mexico.
- The implementation of the Open Data Standard Procurement in the shared telecommunications network.
- The announcement of the SFP regarding seven amendments to regulations, including boosting open contracts through amendments to the regulations of the Law of Acquisitions, Leases and Public Sector Services, and the Law on Public Works and Related Services, to incorporate the stages of planning and execution of contracts in Compranet, the public procurement platform.
- The Mexico Open Network is a mechanism of co-operation between the three levels of government to support states and municipalities in the publication and use of open data.
- The creation of a Commission on Transparency and Open Government Anti-Corruption within the National Confederation of Governors (CONAGO), and the signing of the collaboration Network Mexico Open on state-wide data.

As a result of these projects and initiatives, Mexico has positioned itself as a regional leader in the use of open data and technologies as key tools in the fight against corruption, spearheading efforts for the development and adoption of the Principles of Open Data for Anti-Corruption in the G20.

However, despite this progress, the use of data analytics has not been widely introduced in the internal control system, especially the risk management function. The introduction of innovative ICT systems should not be confused with the use of data analysis techniques. As already highlighted, data analytics can be described as the process of inspecting, cleaning, transforming, and modelling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making. In this sense, innovative oversight tools, such as continuous auditing, is any method used by auditors to perform audit related activities on a more continuous or continual basis. It is the continuum of activities ranging from continuous control assessment to continuous risk assessment. For example, the use of the information system for the Institutional Development and Control Committee (*Comité de Control y Desempeño Institucional,* COCODIs, and *Sistema Informatico del COCODIs*, SICOCODIS) for the purposes of the annual evaluation of the effectiveness of the organisation's internal control system, and the relevant evaluation report of the Offices of Internal Control (*Órganos Interno de Control*, OIC), does not mean that COCODI and/or the OIC are using data analysis tools for their tasks in relation to the risk management function.

The SFP should consider developing a concrete action plan to promote the use of data analytics tools for effective risk management. The interoperability of existing information systems, and the training of risk management practitioners, are considered key priorities for integrating data analytics within risk assessment and mitigating policies.

Internal control: A tool for continual organisational improvement

The SFP's new Standard Model for Internal Control is a positive step forward in strengthening and harmonising internal control frameworks in the federal administration. However, the priority at this point should be to address the implementation gaps of the past by fostering greater ownership for internal control with operational units, and aggressively scaling-up capacity-building efforts.

Integrity, ethical values and competence of the entity's people are crucial elements of a healthy internal control environment, which also includes how management assigns authority and responsibility, and organises and develops its employees. The internal control environment consists of formal structural and "soft" behavioural aspects. Formal rules and procedures, such as a code of ethics, human resource processes, accountability arrangements and delegation of duties, are mostly well documented.

The SFP's System of Institutional Internal Control (SCII), is composed of three basic components:

1. The Standard Model of Internal Control (Modelo Estándar de Control Interno, or MECI).
2. The Institutional Risk Management (Administración de Riesgos Institucionales, ARI).
3. The Institutional Development and Control Committee (Comité de Control y Desempeño Institucional, COCODI).

The SFP is responsible for developing guidance and assistance for OICs, which are located in line ministries and other public sector organisations and are the responsible units for conducting audits and monitoring the implementation of the internal control framework in government entities. The new MECI, *Modelo Estándar de Control Interno,* introduced by the new "*Acuerdo por el que se emiten las Disposiciones y el Manual Administrativo de Aplicacion General en Material de Control Interno*, MAAG-CI" is aligned with the *Marco Integrado de Control Interno en el Sector Público*, known as MICI, developed by Mexico's Supreme Audit Institution, (*Auditoría Superior de la Federación*, ASF). MECI ensures harmonisation between the criteria of external audit and internal audit. Box 6.5 highlights the main attributes of the new MECI.

Box 6.5. Mexico's new MECI for federal public sector organisations: Key elements

Internal control is a process affected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. These objectives and related risks can be broadly classified into one or more of the following four categories:

- Operations: Effectiveness and efficiency of operations
- Reporting: Reliability of reporting for internal and external use
- Compliance: Compliance with applicable laws and regulations
- Safeguarding: Protection of public resources and prevention of corruption acts

The new MECI is structured around five components and 17 principles depicted in the following table:

Control environment	1. The organisation demonstrates a commitment to integrity and ethical values 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives 4. The organisation demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. 5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives
Risk assessment	6. The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. 7. The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed. 8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives. 9. The organisation identifies and assesses changes that could significantly impact the system of internal control.
Control activities	10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. 11. The organisation selects and develops general control activities over technology to support the achievement of objectives. 12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

Box 6.5. Mexico's new MECI for federal public sector organisations: Key elements *(cont.)*

Information and communication	13. The organisation obtains or generates and uses relevant, quality information to support the functioning of internal control. 14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. 15. The organisation communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring activities	16. The organisation selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. 17. The organisation evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: SFP, Acuerdo por el que se emiten las Disposiciones y el Manual Administrativo de Aplicacion General en Material de Control Interno, MAAG-CI, November 2016, http://dof.gob.mx/nota_detalle.php?codigo=5459569&fecha=03/11/2016.

The new MECI introduces two important changes:

- Codifies 17 principles (with associated points of focus) that support the five components of internal control.
- Introduces for the first time a principle dedicated to managing corruption risks

These 17 principles aim to define the fundamental concepts underpinning each of the five components. They can be seen as guidance towards achieving an effective internal control system and helping practitioners apply informed judgement when evaluating the maturity and degree of implementation of each component. There are inherent interdependencies and linkages among components and the fact that they all have to be present, functioning and operating together with the 17 principles. The evaluation of the system of internal control considers how the principles, and the associated points of focus, are being applied. However, it should be noted that the principles are not meant to be used as a checklist. The points of focus represent important characteristics that are linked to the principles. For example, the first principle linked to the control environments component is: "The organisation demonstrates a commitment to integrity and ethical values". The four associated points of focus aim to better frame and indicate the core substance of this principle:

- **Sets the tone at the top**: The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behaviour the importance of integrity and ethical values to support the functioning of the system of internal control.
- **Establishes standards of conduct**: The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organisation and by outsourced service providers and business partners.

- **Evaluates adherence to standards of conduct**: Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
- **Addresses deviations in a timely manner**: Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

The principles should enable the effective operation of the five internal control components and the overall system of internal control. To integrate these principles into the management system, the organisation must understand the intent of the principle and identify practical steps to apply it consistently across the entity. The actual integration and functioning of the principles should be considered during the evaluation of internal control. The new MECI does not prescribe specific controls, as under a principles-based approach it is the manager's responsibility to develop the proper controls that impact or influence the principles through their design and execution across the organisation.

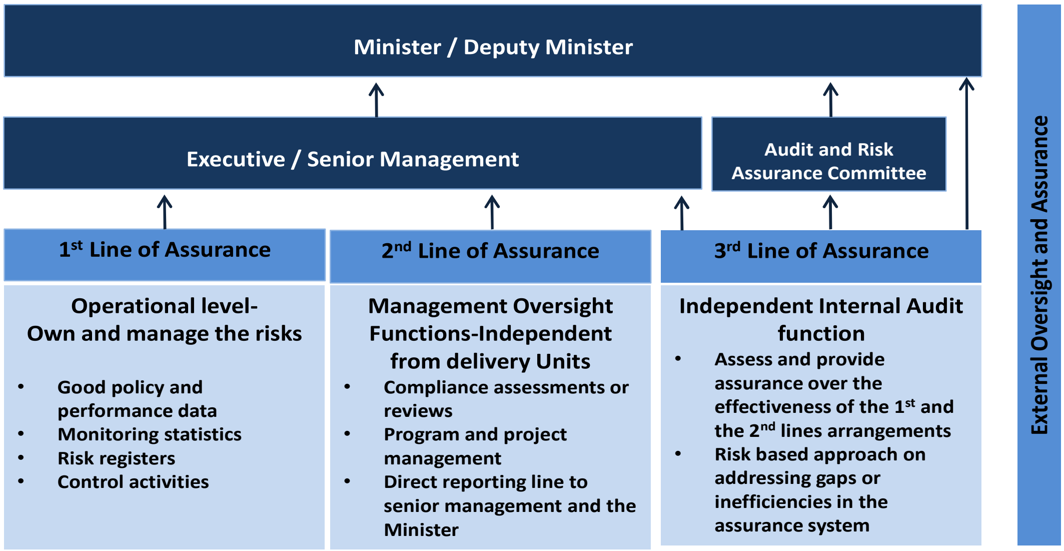
The analysis supported by the answers to the OECD questionnaire, the fact–finding mission in November 2015, and the long-standing co-operation and interaction of the OECD with various public entities in Mexico, underscores the risk of implementing internal control in isolation. In many cases, it seems that internal control and risk management processes are not part of the organisation's overall management system, including the processes for good governance, strategy and planning, monitoring, reporting and strengthening accountability.

More specifically, how an internal control system is implemented appears to remove the main responsibility from where it primarily belongs: line management and staff. One of the main challenges identified in Mexico is that internal control and risk management functions are often seen as an administrative routine, rather than a valuable exercise. The root causes that hinder the mainstreaming of internal control processes and functions may vary widely. As mentioned, the head of the "Oficialia Mayor" is usually appointed as co-ordinator of the internal control system in federal public entities. This option has several advantages, since the head of the Oficialia Mayor reports directly to the head of the organisation (i.e. Minister) and is responsible for overseeing human resources and the financial and equipment resources of the entity. However, in depth implementation requires the input and active involvement of all core business and operational areas to foster greater ownership over controls.

In order to build greater ownership, the role of public organisation managers within the Mexican federal public administration needs to be strengthened in relation to the internal control system. A sound control environment requires correspondence and consistency between authority (empowerment), responsibility and accountability throughout all levels of the public entity. There is no responsibility without authority (authority as a precondition to responsibility), and no responsibility without accountability (accountability as a necessary consequence of responsibility).

Figure 6.2 depicts the allocation of oversight and accountability tasks and functions within public organisations across the three lines of assurance model.

Figure 6.2. The three lines of assurance model


Minister / Deputy Minister
Executive / Senior Management
Audit and Risk Assurance Committee
1st Line of Assurance
2nd Line of Assurance
3rd Line of Assurance
Operational level- Own and manage the risks
• Good policy and performance data
• Monitoring statistics
• Risk registers
• Control activities
Management Oversight Functions-Independent from delivery Units
• Compliance assessments or reviews
• Program and project management
• Direct reporting line to senior management and the Minister
Independent Internal Audit function
• Assess and provide assurance over the effectiveness of the 1st and the 2nd lines arrangements
• Risk based approach on addressing gaps or inefficiencies in the assurance system
External Oversight and Assurance

Source: Adapted with inputs from a. Federation of European Risk Management Associations (FERMA)/European Confederation of Institutes of Internal Auditing (ECIIA) Guidance on the 8th European Company Law Directive on Statutory Audit DIRECTIVE 2006/43/EC – Art. 41-2b, 2010, b. Institute of Internal Auditors (IIA): Three Lines of Defence Model, 2013, and c. Assurance Maps Presentation, PIC EU-28 Conference 2015.

The concept of managerial responsibility and accountability is not developed within the Mexican public administration. This largely stems from a weak management culture dominated by hierarchical decision making and a lack of delegation and segregation of duties. However, it is not easy to find the right incentives to motivate individuals in a set administrative and working environment affected by a range of reasons that further complicate the attempt to improve and integrate internal control and risk management into the Mexican administration (e.g. heterogeneous recruitment, employment and compensations regimes; high turnover; limited performance monitoring and evaluation capacity; weak interoperability of ICT systems).

Public managers have key responsibilities in relation to establishing and maintaining sound internal control processes and activities. How the US Office of Management and Budget (OMB) frames the context of managerial responsibility is described in Box 6.6.

Box 6.6. US Office of Management and Budget circular A-123: Management's responsibility for internal control

The circular states the office policy as:

- Management is responsible for establishing and maintaining internal control to achieve the objectives of effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations.
- Management shall consistently apply the internal control standards to meet each of the internal control objectives and to assess internal control effectiveness.
- When assessing the effectiveness of internal control over financial reporting and compliance with financial-related laws and regulations, management must follow the OMB's outlined assessment process.
- Annually, management must provide assurances on internal control in its Performance and Accountability Report, including a separate assurance on internal control over financial reporting, along with a report on identified material weaknesses and corrective actions.

Actions required by the circular indicate agencies and individual federal managers must take systematic and proactive measures to:

- Develop and implement appropriate, cost-effective internal control for results-oriented management.
- Assess the adequacy of internal control in federal programmes and operations.
- Separately assess and document internal control over financial reporting consistent with the process.
- Identify needed improvements.
- Take corresponding corrective action.
- Report annually on internal control through management assurance statements.

Source: United States Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (Revised 07/15/2016).

Fountain, L. (2012), *Manager's Responsibility for Internal Control*, www.kscpa.org/writable/files/Self-Study/FGE/updated_managers_responsibility_for_internal_control-_article.pdf.

Mexico could consider focusing on policies to create awareness and involvement amongst senior and middle management, as well as general staff. Public servants must be involved in turning the organisation's vision and mission into concrete sub-objectives that are further disseminated across all structural organisational levels, and ideally linked to individual interests and skills. The inclusion of low-level staff can create motivation and enthusiasm and match individual objectives to management plans. Public servants must own internal control and risk management processes in order to close the gap between nominal and actual implementation.

Some concrete instruments could include:

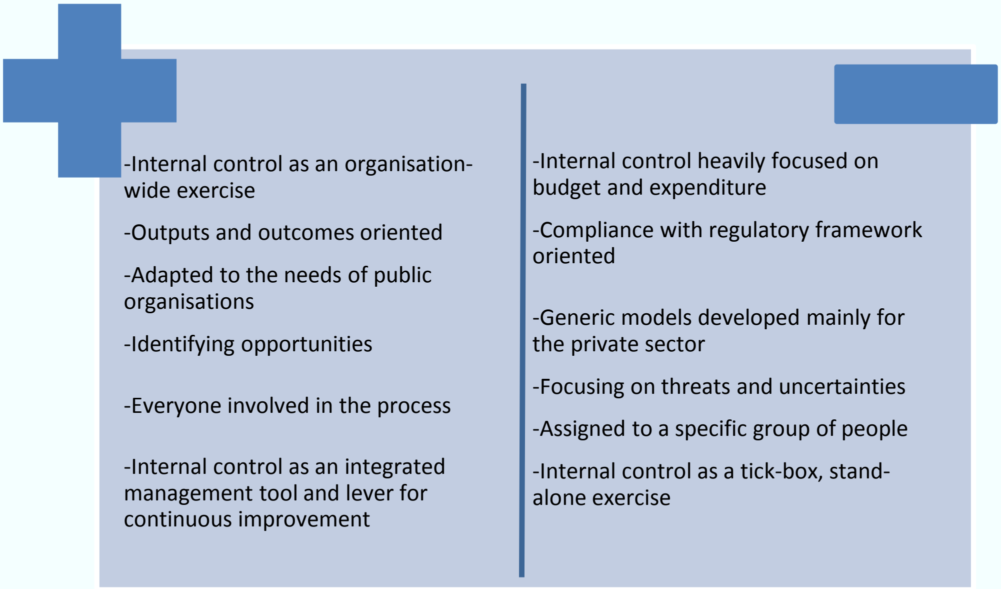
- Using awareness campaigns or events on the importance of integrating internal control and risk management activities into daily business as a tool to influence public perception and enhance the accountability, and therefore the legitimacy, of public entities.

- Providing regular feedback on the linkages between a sound internal control environment and the achievement of the entity's objectives through periodic messages (e.g. newsletter, videos) from senior management to highlight progress and achievements on improving the actual implementation and integration of the internal control requirements and activities.
- Linking issues such as budget allocation, expenditure limits and staff and payroll ceilings, especially at the regional and municipal level, with progress made in mainstreaming internal control and risk management into daily operations.

As already highlighted, the new implementation manual on internal control "*Acuerdo por el que se emiten las Disposiciones y el Manual Administrativo de Aplicación General en Materia de Control Interno*, MAAG-CI" aims to address some of these challenges by bridging the gap between nominal and actual implementation. The first significant change is the integration of the two internal control conceptual frameworks developed by the SFP and the ASF, respectively: the Standard Model of Internal Control (*Modelo Estándar de Control Interno*, MECI) and the Integrated Framework for Internal Control in the Public Sector (*Marco Integrado de Control Interno en el Sector Público*, MICI). MICI deals with mainstreaming the role of COCODI within management, and operations as a driver for continuous organisational performance improvement.

Most OECD countries view internal control as an integral part of a public organisation's governance systems. This approach is crucial to ensure that public entities can capitalise on opportunities, while offsetting the threats that may hinder the achievement of set objectives. One of the primary purposes of a robust internal control system is to support political and administrative senior management in decision making, while reducing uncertainty and effectively mitigating risks. The main challenge for Mexico seems to lie in avoiding turning internal control and risk management into a stand-alone exercise that is not integrated with the other governance systems. Box 6.7 provides a list of bad and good practice concerning the integration of internal control.

Box 6.7. Bridging the implementation gap



-Internal control as an organisation-wide exercise

-Outputs and outcomes oriented

-Adapted to the needs of public organisations

-Identifying opportunities

-Everyone involved in the process

-Internal control as an integrated management tool and lever for continuous improvement

-Internal control heavily focused on budget and expenditure

-Compliance with regulatory framework oriented

-Generic models developed mainly for the private sector

-Focusing on threats and uncertainties

-Assigned to a specific group of people

-Internal control as a tick-box, stand-alone exercise

Source: IFAC (2015), *From Bolt-on to Built-in: Managing Risk as an Integral part of Managing an Organisation*, International Federation of Accountants, New York, https://www.ifac.org/publications-resources/bolt-built.

There are several concrete actions that could lead to the greater understanding and active involvement of both management and staff regarding internal control arrangements and requirements:

- Human resource procedures for hiring, individual evaluation, selection of top managers and dismissal should reflect and underscore the organisation's mission and ethical values, which are the core foundations of a contemporary internal control system. Although the SFP cannot act alone in this field across the federal administration, it should steer the dialogue and reform initiatives.
- Job descriptions and competency profiles for managerial and high risk positions should encompass concrete tasks and responsibilities in relation to the allocation of internal control functions along the three lines of defence model.
- Communicate at the entity level (e.g. by videos, electronic messages, newsletters) the good practices and individual achievements in integrating and using internal control as a management tool.

Capacity building efforts that the SFP could consider to strengthen its existing training activities, particularly given the opportunity of the introduction of MAAG-CI, include:

- Dilemma training scenarios underpinning the attributes of a sound internal control environment (one of the five components according to the new MECI).
- Workshops on the added value of internal controls in improving management and governance systems, including some especially designed for senior and middle

management. There could be a tailored workshop for *Oficialias Mayores*, given their important co-ordination role.

- Training modules and awareness campaigns focusing on bridging the gap between organisational objectives, daily operations and internal control activities. The members of COCODIs should be actively involved in these training modules, focusing on their new tasks and their core role in linking internal control with management systems and improving the overall governance of federal organisations.

The National Auditing System (NAS) Working Group on Internal Control should use an evidence-based methodology for assessing the maturity and implementation of internal control components and processes within public entities.

Evaluation exercises (self-assessment models), conductedby Mexican public entities with the support of the respective OICs and according to SFP guidelines, have already identified the problems hampering the improvement of the maturity and implementation of internal control components and activities. OICs are responsible for reviewing answers to self-evaluations and the supporting documentation, and providing assurance to management of the quality of internal control processes. This should be the primary role of an internal audit function that acts as a third line of defence/assurance within the overall internal control system. The entire process is supported by a toolkit of analytical criteria (*Criterios para la Evaluación del Órgano Interno de Control al Informe Anual del Estado que Guarda el Sistema de Control Interno Institucional*).

There are serious challenges regarding the credibility and validity of these self-evaluation reports. The process has certain limitations, which the ASF has touched upon in its Studies No 1172 and No 1212 (*Modelo de Evaluacion de Control Interno en la Administracion Publica Estatas*). The ASF has conducted its own evaluation on the results of the self-assessment conducted by Mexican federal entities, and concluded that the application of the methodology, as well as the documentation of the answers provided, vary across entities and need to be further mainstreamed and rigorously monitored.

As a first step, the SFP should consider adopting practical steps to strengthen the credibility and accuracy of the self-assessment exercise, given the opportunity of the new manual and the new MECI. Concrete actions could include: stricter documentation requirements on the rating given by organisations, secondary sampling controls from the competent unit of the SFP, exchange of information and cross checking with assessments undertaken by the ASF, and creating a registry of certified practitioners in internal control self-assessment (CSA) techniques. These CSA techniques aim to enable managers and teams directly involved in business units, functions or processes to participate in assessing the organisation's risk management and control processes. Internal auditors can be involved in a consulting role for gathering relevant information about risks and controls; for focusing audit work on high risk, unusual areas; and to forge greater collaboration with operating managers and work teams. They should not own the process, but rather act as facilitators to help teams in the assessment of risks and controls. The SFP’s approach provides for the head of the OIC to review and assess the self-assessment findings before reporting back to the SFP. The above-mentioned steps can increase the credibility of the exercise across all internal and external stakeholders, and help prioritise and guide corrective actions towards the internal control components and activities that face the most significant challenges.

The SFP may wish to consider the Guidance (FERMA-ECIIA, 2014) on the 8th European Company Law Directive on Statutory Audit (2006/43/EC – Art. 41-2b), which provides a good example of identifying the key points for establishing and implementing a sound system of monitoring the effectiveness of internal control, internal audit and risk management systems (Box 6.8).

Box 6.8. Q&A for providing guidance to senior management and committees on monitoring the effectiveness of internal control, internal audit and risk management systems

1. Who monitors the adequacy of the internal control system? Are there processes to review the adequacy of financial and other key controls for all new systems, projects and activities?

A key part of any effective internal control system is a mechanism to provide feedback on how the systems/processes are working so that shortfalls and areas for improvement can be identified and changes implemented. In the first instance, if there is an internal control department, it will help managers implement sound internal controls. The operation of key controls will then be subject to review by internal and external audit along with other review agencies, both internal and external to the organisation. If no internal control department exists, guidance may be sought from risk management or internal audit.

2. Are arrangements in place to assess periodically the effectiveness of the organisation’s control framework?

A key requirement of many of the internal control requirements encompassed in legislation throughout the European Union (EU) and the rest of the world is an annual attestation as to the adequacy and effectiveness of the internal control system. Such attestation should be clearly evidenced. The review of the control framework will be the responsibility of the audit committee who will receive information and assurances from internal audit, risk management and the external auditors.

3. Who assesses internal audit?

The audit committee assesses the performance of the internal audit function by receiving performance information from the function itself and consulting appropriate directors and the external auditors. In addition, the function should be independently reviewed by an external agency, such as the Institute of Internal Auditors (IIA), as specified in the International Professional Practices Framework, issued by the IIA.

4. How are the proposed audit activities prioritised? Is the determination linked to the organisations’ risk management plan and internal audit’s own risk assessment? Are the internal audit plan and budget challenged when presented?

The work of internal audit should be set out in a risk-based plan challenged and approved annually by the audit committee. This plan should be informed by the work of other review agencies, such as external audit and risk management, and should contain sufficient work for the head of internal audit to be able to form an overall view as to the adequacy of the risk management process operated by the organisation. If there is no formal risk management process, or if the process is flawed, then internal audit will need to rely on some other method of assessing the key activities and controls for its review. This could be based on its own risk assessment.

Source: FERMA (2014), European Confederation of Institutes of Internal Auditing Guidance on the 8th EU Company Law Directive, 2014, Federation of European Risk Management Associations, Brussels.

The National Auditing System Working Group on Internal Control could publish the results of self-assessment exercises and build on existing procedures (i.e. ASF and SFP reviews) to reach a commonly accepted and effective model for evaluating the federal organisation's self-assessment results. These "secondary" level evaluations could be shared between federal entities, even in a ranking approach reflecting methodological approaches (e.g. practical steps, tools, techniques, documentation) and providing evidence-based data for further improving the exercise at the entity level.

Internal audit: Ensuring independence and providing assurance

In order to strengthen the independence and the assurance role of the internal audit function, the SFP should seek to better clarify the functions between the second and third lines of defence.

In Mexico, there seems to be confusion between the duties and functions assigned to each of the three lines of defence. The problem lies mainly with framing the tasks and responsible actors in the second line of defence.

The main features of second line defence tasks and processes are:

- They must be separate from the first line chain of command.
- Reliance is placed on this oversight by management.
- They are not completely independent since they are still close to management.
- There won't always be a second line depending on special circumstances, such as the size of the entity.
- The degree of maturity of oversight provided varies widely depending on the function.

Mexico could continue to work on assigning and clearly separating the roles and responsibilities of the second and third lines of defence. The second line of defence consists of management oversight functions to ensure that first line controls are properly designed, in place and operating as intended. It usually includes actors and activities such as risk management, ethics committees, controllership for financial risks and reporting, management oversight committees (e.g. IT, human resources), payment gating and sampling reviews. These functions are far from line management and first line of defence activities, but still close to management's authority so that they cannot be part of the independent third line of defence function.

It is not always easy to draw a line between the second and third lines of defence in public organisations, sometimes due to the size and structure of the organisation, as well as whether senior management consider that it is more efficient for internal audit to perform risk management, compliance or other second line of defence functions. If this occurs, and a clear separation is not achievable, there must be safeguards that the intersection between the second and third lines of assurance do not compromise the effectiveness of the internal audit function (third line). The head of internal audit should clearly communicate the impact to senior management, since if internal audit is involved in second line of defence activities, the task of providing assurance regarding these specific activities must be outsourced either externally or internally to other departments. Internal audit should not assume any managerial responsibilities regarding the audit object. In the case of undertaking new risk management or compliance initiatives, internal audit can facilitate and support the responsible actors, but should never assume ownership.

In order to clarify the tasks and functions assigned to the second and third lines of defence, Mexico could consider developing guidelines that tailor the three lines of defence model to the actual allocation of roles and responsibilities between individuals and units within federal public organisations. Such a tool would help both managers and staff understand where they stand within the overall institutional internal control system, and what is expected from them in this entity-wide approach to effectively mainstream internal control functions in management and operational processes. As noted above, this tailored approach entails taking into account the differences between public organisations in size and structure, as well as mission and objectives. Even in cases where there are not enough resources, or where internal control arrangements are not mature enough to support a clear distinction between the second and third line of defence, international professional practice standards provide for the necessary safeguards to ensure that these functions are managed and performed properly in order to add value to the organisation.

The SFP could highlight the distinct role of the internal audit function regarding fraud and corruption investigations by assessing the current structure and operational model of the OICs, while ensuring professionalism and strong capacities.

The current model of the OICs consists of four areas: internal audit, complaints management, investigation and disciplinary activities, and performance evaluation issues. The relevant institutional arrangements and roles are described in Articles 76 and 80 of the Internal Regulation of the SFP, as well as in the Agreement for the administrative entities of the SFP ("*Acuerdo por el que se adscriben orgánicamente las unidades administrativas de la Secretaría de la Función Pública y se establece la subordinación jerárquica de los servidores públicos previstos en su Reglamento Interior*"), which was published in the official gazette in December 2015. This is a broad mission mandate that stretches to areas not typically core activities of an internal audit function. SFP units identified that the anti-corruption reform makes it even more important to clearly differentiate the roles between internal audit and investigation activities. According to leading international practice, the role of internal audit is crucial for monitoring and evaluating the operation of the various components of the internal control system. This activity enables management to determine whether all components of internal control function effectively, as separate modules and as a system. An effective internal audit monitoring function provides assurance that internal control deficiencies are identified and communicated in a timely manner to the actors responsible for taking corrective action. The monitoring process involves establishing a foundation for monitoring, designing and executing monitoring procedures that are prioritised based on risk, and assessing and reporting results, including follow-up on corrective actions where necessary.

Internal auditors also have a role in the fight against corruption, although they should not be considered as the primary responsible actors. The Institute of Internal Auditors' 2110 Standard (IPPF 2015) specifically refers to the responsibility of internal audit to evaluate the existing situation and submit proposals to improve governance in order to promote ethical values and principles inside the entity. There is a practical guide on

Evaluating Ethics-related Programmes and Activities (IIA, 2012). According to the IIA's IPPF standards:

- Standard 1210.A2: Internal Auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organisation, but are not expected to have the expertise of person whose primary responsibility is detecting and investigating fraud.
- Standard 2120.A2 Risk Assessment: The internal audit activity must evaluate the potential for the occurrence of fraud and how the organisation manages fraud risk.
- Standard 2210.A2: Internal Auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.
- Standard 2060: Chief Audit Executives (CAE) must report periodically to senior management and the board on fraud risks.

While conducting audit missions, auditors should act to identify fraud and corruption indicators that can be recognised in most of the core business processes. In order to be successful in recognising these indicators, auditors must rely on their technical experience, professional judgment and good understanding of how potential fraud and corruption acts can be committed. Audit strategies should be diverted to areas and operations prone to fraud and corruption by developing effective high risk indicators. Box 6.9 provides an example of internal audit's role in curbing fraud and corruption.

Box 6.9. Fraud and corruption: Internal audit's role

It is not a primary role of internal audit to detect fraud and corruption. Internal audit's role is to provide an independent opinion based on an objective assessment of the framework of governance, risk management and control. In doing so, internal auditors may:

- Review the organisation's risk assessment seeking evidence on which to base an opinion that fraud and corruption risks have been properly identified and responded to appropriately (i.e. within the risk tolerance).
- Provide an independent opinion on the effectiveness of prevention and detection processes put in place to reduce the risk of fraud and/or corruption.
- Review new programmes and policies (and changes in existing policies and programmes) seeking evidence that the risk of fraud and corruption had been considered where appropriate and providing an opinion on the likely effectiveness of controls designed to reduce the risk.
- Consider the potential for fraud and corruption in every audit assignment and identify indicators that crime might have been committed or control weaknesses that might indicate a vulnerability to fraud or corruption.
- Review areas where major fraud or corruption has occurred to identify any system weaknesses that were exploited or controls that did not function properly and make recommendations about strengthening internal controls where appropriate.

Box 6.9. Fraud and corruption: Internal audit's role *(cont.)*

- Assist with, or carry out investigations on management's behalf. Internal auditors should only investigate suspicious or actual cases of fraud or corruption if they have the appropriate expertise and understanding of relevant laws to allow them to undertake this work effectively. If investigation work is undertaken, management should be made aware that the internal auditor is acting outside of the core internal audit remit and of the likely impact on the audit plan.
- Provide an opinion on the likely effectiveness of the organisation's fraud and corruption risk strategy (e.g. policies, response plans, whistleblowing policy, codes of conduct) and if these have been communicated effectively across the organisation. Management has primary responsibility for ensuring that an appropriate strategy is in place and the role of internal audit is to review the effectiveness of the strategy.

Source: HM Treasury (2012), *Fraud and the Government Internal Auditor*, HM Treasury, London, www.gov.uk/government/uploads/system/uploads/attachment_data/file/207217/Fraud_and_the_Government_Internal_Auditor.pdf.

In Mexico, the OICs, are responsible for the internal audit role in organisations. However, their budget is determined and heavily influenced by the ministry or organisation in which they operate. This can limit their capacity to effectively carry out their role objectively and independently.

The OICs do not appear to have adequate resources and expertise to engage in internal audit. Corruption investigators should receive specialist training, and certification of training and investigative competency would enhance the credibility of an investigator as a witness. Internal audit should assess, at the entity level, whether there is a robust ethics programme that includes: effective senior management oversight, strong tone at the top, line management involvement, organisation-wide commitment, a customised code of conduct, timely follow-up and investigation of reported incidents, consistent disciplinary action for offenders, effective ethics training, ongoing monitoring systems, and an anonymous incident reporting system. In Mexico, it appears that the enforcement of integrity policies is often limited in identifying and sanctioning people for misconduct. How senior officials react to compliance and deviation is crucial for the credibility of the control environment. Enforcement and disciplinary procedures should be clear and transparent and equally applied to everyone. It would also be helpful to communicate on cases of people exhibiting the desired behaviour.

It has been highlighted that the involvement of OICs in disciplinary procedures has created confusion among public employees regarding the exact role and mission of the internal audit function. Managers and staff often perceive OICs as policing units that focus on compliance, identify misconduct and wrongdoing, conduct investigations and sanction people. Colombia has tried to address this problem by separating the offices of internal control from the offices of disciplinary control (*Oficina de Control Interno Disciplinario*) in order to underscore the role of internal audit as a management tool that provides consultation and assurance towards improving the efficiency and service delivery of public organisations.

An independent and efficient internal audit function should place reliance upon assurance mechanisms in the first and second line of defence in order to target resources most efficiently at areas of highest risk or where there are gaps or weaknesses in other assurance arrangements. In order for internal audit to fulfil its mission it has to be independent of the first and second lines of assurance, line management and associated responsibilities. The real challenge for internal audit in the era of financial crisis and austerity is how to do more with less, such as by sharing internal audit services across multiple agencies. Audit budgets are being reduced at a time when political personnel and public senior managers need audit assurance the most. The Government Internal Audit Agency of the United Kingdom is trying to effectively respond to these challenges, and thus safeguard and even improve its ability to deliver high quality audit services to state entities.

Box 6.10. The United Kingdom's HM Treasury experience

The Government Internal Audit Agency (GIAA) was launched on 1 April 2015, following publication by HM Treasury of the Financial Management Review (FMR) in December 2013, as an executive agency of HM Treasury (HMT) to help ensure government and the wider public sector provide services effectively. The GIAA aims to expand the agency to become the single internal audit provider to government. The idea is that the GIAA will incorporate all existing internal audit units under its auspices. As of October 2016, the GIAA employs 464.8 full-time equivalents (FTE) (auditors and administrative staff) and they expect to reach a total number of about 750 people, according to their action plan. This approach will allow for the agency to benefit from the concentration of expertise, leading practices, and critical mass (e.g. concentration of fraud forensic or cyber security experts) to improve the efficiency and quality of service while reducing the financial cost; as well as to adapt and evolve the audit expertise and capacity model based on the expectations and needs of service beneficiaries. The GIAA creates the vital space for a career path for auditors, which results in a lower turnover rate. The state entities are being charged with the cost of the provided audit services, which safeguards independence and creates a motive for improved services and performance assessment. The United Kingdom has been working with shared audit services since 1990.

GIAA offers quality assurance on an organisation's systems and processes, based on an objective assessment of the governance, risk management and control arrangements it has in place. Its internal auditors look at financial risks and wider issues, such as:

- employee relations
- management structure
- relationships with stakeholders

They then offer advice on how to improve those systems and processes, based on their findings.

GIAA is responsible for:

- Reviewing the functions and activities of government and public sector organisations, and assessing their efficiencies and risks.
- Making recommendations for improvement, based on assessments.
- Adding value to public services and improving how effectively organisations provide them.

Box 6.10. The United Kingdom's HM Treasury experience *(cont.)*

GIAA's priorities are to:

1. Expand capacity and expertise in areas including:

- counter-fraud and investigations
- information systems
- programme and project management

2. Introduce a framework agreement for internal audit services that will:

- improve private sector involvement
- make use of the collective purchasing power of government internal audit
- strengthen customer support (e.g. around sharing best practice, and access to specialist skills)
- develop the framework for providing assurance around cross-government and inter-organisational risks

The UK's example depicts a model of providing audit services in the public sector, and the current approach follows a long period of working with the model of shared audit services between clusters of organisations acting in the same policy field. For example, Research Councils United Kingdom (RCUK) is the strategic partnership of the UK's seven Research Councils. The Research Councils' Internal Audit Service (RCIAS) was formed in 1992 from the separate internal audit units previously within each Research Council. In April 2012, RCIAS merged with the RCUK Assurance Programme to form the Audit and Assurance Services Group (AASG), with a principal responsibility to each council's chief executive in helping them meet their responsibilities and accountabilities to Parliament. To achieve this they undertake an annual programme of work within each Council, which is agreed by respective Chief Executives and their Audit Committees. Working to standards set by HM Treasury, the annual programmes include a range of services to help managers meet their objectives and maintain adequate control over resources.

Sources: UK Government (2017), *Government Internal Audit Agency Webpage*, www.gov.uk/government/organisations/government-internal-audit-agency (accessed March 2017).

Research Councils UK (2017), *Audit and Assurance Services Group (AASG) Webpage*, www.rcuk.ac.uk/about/aboutrcuk/aims/units/aasg/ (accessed March 2017).

Due to budgetary dependence, OIC staff often find that their positions are contingent on the ministries in which they operate, which further limits their potential independence. There are several solutions that could be considered in order to address this challenge. The heads (they should be called Chief Audit Executives, CAE) and the staff of OICs should be carefully selected based on meritocracy and individual skills. In Colombia, for example, CAEs are appointed by the president in a major step to attract competent professionals and raise awareness about the importance of the internal audit function. It is important that auditors have a fixed term, and that the head of the organisation for which they are providing internal audit services cannot terminate their appointment without proper justification and documentation. The head and the staff could be either seconded from public organisations or hired from the private sector. A common leading practice is the creation of a registry of certified internal auditors who can be appointed in internal audit units. The overall process to increase the professionalism and independence of internal audit practitioners should be based on the existence of tailored job descriptions, detailed and clear professional standards that call for specific academic background, relevant experience, expertise and skills certification, and continuous training and capacity building requirements (e.g a scheme such as the IIA's CPEs). The process should be supported by a unified and dedicated performance assessment and remuneration regime.

A significant constraint is that the Mexican public administration has not developed the right mechanisms to attract, develop and retain competent individuals with the right set of skills and ethical commitment to work in the control and audit area. Civil service management practices that ensure merit, professionalism, stability and continuity in staffing are among the core prerequisites for setting up and maintaining an effective and added value internal control environment. The new law seems promising in ensuring that recruitment, promotion and compensation will be based on merit, skills and performance. This is also important for empowering public officials to assume responsibility and be accountable for their decisions and actions as well as avoid any undue influence arsing from situations that may blur the lines regarding assigning roles and responsibilities in a sound internal control system.

A national certification policy for internal control and audit professionals could be linked with training and capacity building activities. These approaches are influenced by factors such as the exact role of the internal audit function within public entities, i.e. whether or not they are expected to undertake duties usually assigned to the second line of defense, the nature of their involvement in integrity breaches and investigations, their degree of independence, and reporting lines to senior management and audit committees. Recent reviews and relevant data from Latin America and the Middle East and North Africa (MENA) region show that a low percentage of practitioners have acquired certifications such as the IIA's Certified Internal Auditor (CIA). Moreover, in the framework of the Public Internal Control (PIC) Forum, led by the European Commission Budget Directorate General (DG Budget), these internationally recognised certifications have been occasionally criticised as being: heavily private sector oriented; difficult to pass for practitioners who do not speak any of the languages into which the exam modules and additional information have been translated; very broad and generic in relation to the specific challenges and needs of a given country; and not tailored to effectively focus on core functions such as public finance, public procurement and infrastructure projects, and health and social welfare services.

National efforts to address the issue of weak professional expertise and capacity could include the development of customised training modules in co-operation with national schools of public administration, training centres located at the Ministry of Finance or control and audit institutions (i.e. Supreme Audit Institutions [SAIs] or general inspectorates), professional chambers and associations and universities. The quality of these modules, and their actual impact on the skills and the performance of control and audit practitioners, poses serious challenges. Efforts to develop professional "certification" that is limited within a national context are mostly linked with hiring policies, career path, remuneration, and mobility issues in the control and audit field. Box 6.11 illustrates the key elements of the Canadian internal auditor recruitment and development programme (IARD) and the training for internal auditors in the public sector (TIAPS) programme, which represent two approaches to improving the capacity and skills of internal auditors in public organisations.

Box 6.11. Professionalisation and capacity building of the internal audit service

The Canadian Internal Auditor Recruitment and Development Programme (IARD Programme)

I. Benefits of the Internal Audit Recruitment and Development Programme

In addition to coaching, mentoring and professional development courses, the IARD Programme offers:

- The experience and on-the-job training needed to pursue a Certified Internal Auditor (CIA) designation.
- A development plan designed to help recruits succeed, including competency-based work objectives and support from senior staff.
- Unique on-the-job learning opportunities to learn the profession of internal audit in the Government of Canada.
- Professional development sessions offered by the Institute of Internal Auditors that are related to position and CIA certification.
- Potential for promotion.

II. Internal Audit Recruitment and Development Programme work experience

Working under general supervision, providing support and performing assigned tasks within each of the phases of an audit engagement as a member of an audit team. Audit teams typically report to the Internal Audit Principal or the Director of Internal Audit.

Audit teams are designed to:

- Provide departmental senior management with opinions on the effectiveness and adequacy of: risk management, control, and governance processes.
- Report on the results of risk-based audits.

III. The Comptroller General of Canada has developed the Internal Audit Competency Profiles and Dictionary as a tool of the overarching Internal Audit (IA) Human Resources Management Framework (HRMF)

The IA HRMF aims to support and enable a self-sufficient, quality IA community across the federal public sector. It provides an excellent infrastructure along with tools and support services to position the IA community as professionals who perform unique work within the Government of Canada that adds value to their organisations.

The IA competency profiles and dictionary are the main building blocks of competency-based management (CBM). They allow organisations to focus on how someone undertakes his or her job based on the skills, abilities and knowledge required to perform the work. CBM is the application of a set of competencies to the management of human resources (i.e. staffing, learning, performance management and human resources planning) to achieve excellence in performance and results that are relevant to organisations.

Training for Internal Auditors in the Public Sector (TIAPS)

The TIAPS initiative provides an example of public-sector-oriented internal audit certification that merges international best practices with localised regulatory concerns, delivered in the host country's language.

Box 6.11. Professionalisation and capacity building of the internal audit service *(cont.)*

I. Scope and key characteristics

The idea behind TIAPS started in Slovenia in 2002. The programme was developed to strengthen qualifications in internal audit processes in the public sector, while devoting special attention to requirements introduced by the accession processes of the European Union. The mandatory and recommended guidelines issued by the IIA have long been viewed as private-sector centric and unable to comprehensively address public sector concerns.

One of the ways TIAPS addresses such gaps is to include a customisable module on legislation and taxation, written by experts from the participating country. How standards and practices are taught is different from the IIA, as it is more rules-based than principles-based. TIAPS clearly tells its students what should be done and how, as opposed to guidance issued by the IIA, which leaves generous room for interpretation.

TIAPS targets public sector employees who hold a bachelor's degree and already have practical experience in areas such as accounting, financial oversight, and control. The programme is composed of seven modules divided into two levels, certificate and diploma. All modules, with the exception of the module on National Legislation and Taxation, were developed by CIPFA.

II. Challenges

The biggest hurdle for implementing TIAPS is also its greatest strength: localising the curriculum. This requires involved institutions to do a lot of preparation work prior to the delivery of the programme, which includes translating training material and coaching the local tutors who will deliver the content of modules in local languages.

A related issue is the need to find and hire experts to create the legislation and taxation modules. The programme-implementing team engages translators with sound knowledge of material substance, and the initial translation is checked by an editor/proofreader to make any necessary language revisions, in line with standard terminology in each respective country.

Despite being a relatively young programme, TIAPS provides specialisations. These, however, have yet to achieve the total level of equivalence to directly replace specialised certifications – such the Certified Information Systems Auditor (CISA) provided by the Information Systems Audit and Control Association (ISACA) – although there are plans to do so in the medium term.

The programme also does not have a way to monitor and ensure that its certified practitioners keep up-to-date with evolving audit trends, which both IIA and ISACA do through their continuing professional education requirements.

Sources: Government of Canada (2017a), *Webpage of the Internal Auditor Recruitment and Development Program (IARD Program) - Post-Secondary Recruitment*, https://emploisfp-psjobs.cfp-psc.gc.ca/psrs-srfp/applicant/page1800?poster=941922&toggleLanguage=en (accessed March 2017).

Government of Canada (2017b), *Webpage: Benefits of the Internal Audit Recruitment and Development Program*, http://www.tbs-sct.gc.ca/ip-pi/job-emploi/ford-rpaf/benefitsiard-avantagesrpai-eng.asp (accessed March 2017).

ADB (2016), *Training for Internal Auditors in the Public Sector: An Alternative Approach for State Internal Auditors*, Knowledge Showcases, Asian Development Bank, www.adb.org/publications/training-internal-auditors-public-sector.

Countries interested in further exploring certification programmes such as TIAPS should take a closer look at the seven modules (certificate and diploma level) currently included in TIAPS. For example, within the four certificate level modules, any existing overlap on key functions such as risk management need to be identified to ensure adequate coverage of the role of internal audit in fostering integrity and tackling fraud/corruption schemes and practices. Furthermore, the issue of developing coherent and high quality training modules that are tailored to the legislative and administrative framework and culture of a specific country poses significant challenges regarding the resources needed and adherence to predetermined quality standards. The decision on which institution will take the lead at the national level on developing the material, and which will be responsible for training and exams, also raises issues of meritocracy and objectivity. The effective follow-up and update of professional skills and expertise is also an important issue, with questions concerning whether or not TIAPS can develop a system similar to the IIA's Continuing Professional Education (CPE) Requirements, and if the certification will be recognised outside national borders. Another issue involves assessing the added value and impact of certification to individual skills and the institutional capacity of control and audit institutions. It will be important to ensure that certification will not be another tick box exercise, or an "academic" qualification with no or limited impact in real field work. There is also a question around whether or not it will be a tool for practitioners to address the problems they encounter in the labyrinth of public entities and processes. There is a significant gap to bridge between conceptual control and audit frameworks, professional certifications, and the actual integration of internal control and audit functions within the heart of public entities' daily management and operations.

SFP could consider piloting the establishment of independent Audit and Risk Boards/Committees in selected line ministries.

COCODI's role, as illustrated in the new internal control manual and guidelines, is different to that of audit committees, which should be constituted by independent members and reside "outside" the organisation. Before engaging in a pilot phase, all issues related to the appointment of independent members, the remuneration regime, institutional and hierarchical relationships, and specific tasks regarding existing actors should be discussed in detail, while taking into consideration the specific challenges and constraints (e.g. budget, existing committees and actors) of Mexican federal organisations.

Public sector audit committees usually fall under one of the following types:

- Governance audit committees
- Central audit advisory boards
- Internal audit management committees

The choice of the model, which directly relates to the roles and responsibilities assigned to the committee/board, depends on a number of factors, including the degree of sophistication of financial management and reporting, management and control arrangements, and the level of development of managerial accountability, which includes the separation between the political and administrative decision-making process and the application of risk management techniques (Hepworth and Koning, 2012). One of the main challenges when setting up this kind of committee in the public sector is to ensure the participation of independent members external to the relevant organisation. As highlighted by the IIA’s work, the public sector has fewer audit committees than other sectors, and their quality and composition can vary greatly. In some cases, this presents significant threats to internal audit independence and objectivity. It has been highlighted that one of internal audit’s key roles is to provide objective assurance to its stakeholders. A key way of achieving this is to be seen as independent from management and other stakeholders, something that is often easier said than done. Audit committees enhance and safeguard the independence and objectivity of internal auditors. National case studies reveal different approaches in establishing audit committees or equivalent bodies, especially when comparing private and public sector institutions. According to a recent IIA survey, only 55% of public sector entities in the Latin America and Caribbean region report having an audit committee, compared to 78% of private sector entities (IIARF, 2015).

There are different types of assurance that may have different strengths and may be best used in different ways. An audit and risk assurance committee (ARAC) can play a key role in seeking an optimum mix of assurance. Within an assurance framework, the role of an ARAC can be crucial. Ideally, such a committee should be composed of independent members and non-executive directors. Having a chair and other committee members with an appropriate mix of skills and experience relevant to the entity’s responsibilities is key to an audit committee’s effectiveness. These committees are not a substitute for management’s responsibility for mitigating the risks. The committee will monitor and assess the arrangements in place to provide comprehensive and reliable assurance on financial and performance reporting responsibilities, the system of internal control, risk oversight and management. This involves identifying assurance needs and the most appropriate tools to meet these needs, as well as potential assurance gaps or overlaps and ways to address them; and whether the existing framework will provide the sufficient, relevant and reliable assurance that the organisation needs to avoid surprises and to enable early decisions and actions to be taken on risk and control issues.

Box 6.12. Leading attributes of public audit committees in Australia

A good practice audit committee is distinguished by the following attributes:

- Has a formal charter that has regard to relevant legislative requirements and the entity’s broader corporate governance framework, includes the committee’s functions and responsibilities, and is approved by the accountable authority.
- Members collectively possess relevant business, financial management, ICT and public sector experience and expertise.
- Has a sound working relationship with the accountable authority, senior management of the entity and other stakeholders.
- Adopts an independent perspective, and appreciates and respects the separation of management and audit committee responsibilities.
- Is knowledgeable about the entity’s operations, particularly the entity’s risks and the arrangements in place for the management of these risks.
- Is chaired by a person who leads discussions, encourages the participation of other members, and conducts meetings in an effective manner.
- Encourages and maintains an open and constructive dialogue with other entity committees, senior management, internal audit and the Australian National Audit

Office.

Box 6.12. Leading attributes of public audit committees in Australia *(cont.)*

- Exercises judgement and discretion in determining how best to meet its responsibilities.
- Effectively plans its activities to meet its responsibilities; focuses on the important issues and risks; is forward-looking; and adopts a continuous improvement approach in its interaction with entity management.
- Is mindful of the strategic and operational environment of the entity when requesting information from entity management, and balances the resources required with the value to the committee of the information sought.
- Receives an appropriate level of support and provides committee members sufficient opportunities to keep abreast of key developments in the entity, the public sector, the business environment in which the entity operates and the wider community.

Source: ANAO (2015), *Public Sector Audit Committees: Independent assurance and advice for Accountable Authorities*, Australian National Audit Office, Canberra, www.anao.gov.au/work/better-practice-guide/public-sector-audit-committees-independent-assurance-and-advice.

A truly independent audit/risk committee with high expertise can harness political influence on control and audit activities and mitigate the potential bias of auditors assessing the quality of internal control and risk management arrangements. It can also strengthen the impact of these processes inside the organisation and towards the achievement of the entity’s objectives, thus facilitating the involvement of middle and line managers and the rest of the personnel.

Establishing a sound working relationship with the head of internal audit will assist the audit committee to meet its responsibilities, particularly those that include reviewing internal audit plans and reports, and the resourcing of the internal audit function. It would be expected that the audit committee is consulted on the appointment of the head of internal audit. To avoid a potential conflict of interest, it is best practice for the head of internal audit to be invited to attend audit committee meetings as an adviser, rather than as a committee member.

The audit committee can also have a significant role and influence in the area of values and ethics, thus fostering and safeguarding integrity. To obtain reasonable assurance regarding the public organisation’s values and ethics practices, the audit committee can:

- Review and assess the policies, procedures, and practices established by the governing body to monitor conformance with its code of conduct and ethical policies by all managers and staff of the organisation.
- Provide oversight of the mechanisms established by management to establish and maintain high ethical standards for all managers and staff of the organisation.
- Review and provide advice on the systems and practices established by management to monitor compliance with laws, regulations, policies, and standards of ethical conduct, and identify and deal with any legal or ethical violations.

A good example of establishing audit committees can be found in the Polish approach to adopting and implementing the European Union's Public Internal Control (PIC) model (Box 6.13).

Box 6.13. Audit boards and committees: The approach of selected EU member states

Ireland

In Ireland, government departments and offices and other state agencies are required to have audit committees performing the following functions:

- Act as another source of independent advice to accounting officers.
- Review the plans and reports of the internal audit unit and assure the quality of service provided by the unit.
- Assess whether appropriate action is taken to deal with key issues identified by the internal audit unit and by external audit.
- Examine and monitor the implementation of the department's risk management strategy.
- Provided they have representatives external to the department, facilitate improvements in internal audit and internal control through the exchange of information between departments/offices and the private and public sectors.

Each audit committee:

- Operates under a written charter.
- Has significant external representation (at least two members), including, in the normal course, representatives from the private sector with appropriate expertise. The chairperson of the committee should come from outside the department or office.
- Prepares an annual report to the accounting officer reviewing its operations.
- Invites the Comptroller and Auditor General, or his/her nominee, to meet the committee at least once a year.

Italy

In Italy, the legislative decree No 150/2009, which implemented Law No 15 of 4 March 2009 on improving the productivity of the public sector and the efficiency and transparency of public administrations, set up two bodies to measure and appraise the organisational and individual performances of public administrations:

1. A central body known as CIVIT (Independent Commission for the Appraisal, Integrity and Transparency of Public Administrations).
2. For each individual administration, the OIVs (Independent Performance Evaluation Bodies).

The law tasks CIVIT, which is called upon to show independence of judgement and evaluation and work in complete autonomy, with the task of directing, co-ordinating and supervising the appraisal functions to ensure the transparency of the systems adopted and the visibility of the indicators of public administrations' management performance. This task, which aims to improve the efficiency of the public sector and the quality of services to citizens, goes hand in hand with that of ensuring total administrative transparency, i.e. making the data relating to their working accessible through the online provision of a careful selection of data that helps enable institutions and citizens to take an active part in controlling how the "public domain" is managed. This function is particularly relevant because the law sees data transparency as a tool for ensuring the integrity of public administrations, and thus preventing the serious problem of corruption. The members of CIVIT are appointed by the cabinet.

Box 6.13. Audit boards and committees: The approach of selected EU member states *(cont.)*

Each administration also has an OIV that performs tasks such as:

- Monitoring the overall operation of the system of evaluation, transparency and integrity of the internal controls and drawing up an annual report on its working.
- Promptly reporting any problems to the relevant internal government and administration organs.
- Ensuring that the measuring and evaluation processes are correct in order to uphold the principle of rewarding merit and professionalism.
- Correctly applying the guidelines, methods and instruments provided by CIVIT.
- Promoting and certifying transparency and integrity.
- Checking the results and good practices arising from the promotion of equal opportunities.

In the Italian system, there are also management control units, provided for in legislative decree no. 286/1999. Under Article 4 of this legislative decree, each administration sets up individual department level units responsible for designing and implementing management controls. These units map the processes, products and aims of the administrative action of the department to which they belong; measure the results of the administrative action in terms of efficiency, efficacy and cost; and conduct periodical monitoring of the time, resources, costs and quality of the activities of the department. The main aim is specified in Article 1 of legislative decree no. 286/1999, namely checking the effectiveness, efficiency and cost of the work of the administration in order to optimise, also by prompt corrective measures, the cost-benefit ratio.

Within the general framework of the system set out in legislative decree no. 150/2009, the performance plan and the performance report provided for in Article 10 are of particular importance. In order to ensure the quality, readability and reliability of the performance reporting documents, public administrations must each year (by 31 January) draw up a three-year programme report called the “performance plan”. This plan must be consistent with the contents and cycle of financial and budgetary programming, and must set out the guidelines and strategic and operational objectives, including defining the indicators for measuring and evaluating the performance of the administration, the objectives assigned to managers, and the relative indicators regarding final and intermediate objectives and resources. A performance report must be adopted by 30 June and describe, with reference to the previous year, the organisational and individual results obtained compared with the individual programmed objectives and resources, as well as point out any slippages. The plan and the report are sent to CIVIT and to the Ministry of the Economy and Finance.

Poland

In Poland, the Act of 27 August 2009 on Public Finance, implemented in 2010, developed a new concept of management control and accountability at the higher (secondary) level of management, the minister in charge of the government administration branch, and introduced one audit committee for each line ministry. Audit committees are meant to strengthen the internal audit function in its task of assessing management control throughout the entire branch. The audit committee may inform and give advice to the minister about risks connected with the implementation of his/her objectives throughout the entire branch.

Box 6.13. Audit boards and committees: The approach of selected EU member states *(cont.)*

Mission

The aim of the audit committee is to provide consulting services with a view to ensuring adequate, efficient and effective management control and providing an efficient internal audit to the minister in charge of the branch. It should be emphasised that the scope of the audit committee guidance covers the functioning of the management control and internal audit in all units supervised by the relevant minister. One joint audit committee may be established for the branches managed by one minister. For example, the Minister of Finance established one joint committee for three branches: Budget, Public Finance and Financial Institutions.

The members of the audit committee

The audit committee shall comprise the minimum of three members, including: 1) a person in the rank of the secretary or undersecretary of state designated by the minister as the chairman of the committee; and 2) at least two independent members, i.e. people not employed in the ministry or in organisations of the branch. In the opinion of the Ministry of Finance, the optimal size of the audit committee is five to nine persons (including the chairman). This size of audit committee gives all the members a chance to actively participate in the deliberations and effectively perform the tasks of the committee. In practice, by the end of 2012, audit committees ranged from three to seven members.

Tasks of the audit committee

Tasks of the audit committee shall include the following, in particular:

- Indicating material risks.
- Indicating material weaknesses in the management control of the branch and proposing measures to improve them.
- Setting priorities for annual and strategic internal audit plans.
- Reviewing material results of internal audit activity and monitoring implementation.
- Reviewing statements on the execution of the internal audit plan and on the assessment of the management control.
- Monitoring the effectiveness of the internal audit, including reviewing results of internal and external assessments of the internal audit activity.
- Giving permission for the dissolution of employment contracts and any change in salary and employment conditions of the chief internal audit executives in organisations within the branch.

Source: European Union (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Publications Office of the European Union, Luxembourg, http://ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html.

Summary of proposals for action

- The SFP should focus on addressing the "tick box" approach to risk management by boosting its efforts on awareness and capacity-building programmes around the importance and role of effective risk management, while prioritising a specific module for fraud and corruption risk management.

- The SFP should take a more active role in monitoring and ensuring the validity and usefulness of risk maps, matrices and Work Programmes for the Management of Institutional Risks Programa de Trabajo de Administración de Riesgos Institucional, or PTARS) in the achievement of the organisations' objectives. This initiative could take the form of an online observatory to share good practice between federal entities and motivate organisations to improve their risk management procedures and tools.

- The SFP and line ministries should consider leveraging data analytics and mainstream tools, such as data mining and data matching, to improve the quality of their risk management tools and techniques. More informed and evidence-based risks maps, matrices and PTARS lead to more effective mitigation policies. These tools can be very valuable when focusing on integrity risks, as per the requirement of the new MAAG-CI.

- The SFP's new Standard Model for Internal Control is a positive step forward in mainstreaming internal control, linking it with organisational improvement and supporting management and staff in developing ownership of internal control activities. The SFP should work with other competent authorities to ensure that all human resource procedures (e.g. hiring, evaluation, promotions) reflect concrete internal control attributes as described in the new MECI. Concrete internal control tasks and responsibilities should also be introduced in selected (as an initial step) job descriptions. The systematic communication of internal control activities and progress at the entity level is also important.

- The SFP should build on the introduction of the new MAAG-CI and enhance its awareness and capacity-building activities around the importance and challenges of integrating internal control processes in management and operational systems. Specially designed modules and workshops for key actors, such as the *Oficialias Mayores* and members of COCODIs, as well as the rest of management and staff, must be delivered on a coherent and on-going basis.

- The SFP should explore practical steps to monitor and assess the validity and accuracy of the self–assessment reports developed by federal entities. These actions could involve: introducing stricter documentation requirements; creating a registry of certified practitioners in internal control self-assessment techniques; and developing a coherent review methodology in the framework of the NAS building on the experience of the SFP and the ASF in this field.

- The SFP should strengthen the assurance role of the internal audit function by ensuring that internal auditors are not undertaking second line of defence activities (i.e. risk management, compliance reviews, programme management), and by allocating clear roles and responsibilities across the three lines of defence among all staff at the entity level.

- The SFP could assess the structure and operational model of the OICs, taking into consideration the requirements of the new anti-corruption law, and the need to clearly separate the role of internal audit function in fighting corruption and the role of fraud and corruption investigations. The UK example of shared audit services could be examined when exploring ways to strengthen independence from auditees and improve the internal audit function in Mexican federal administration.

- The SFP should work closely with competent organisations to develop the right mechanisms to attract, develop and retain competent individuals with the right set of skills and ethical commitment to work in the control and audit area. Enhancing internal audit professionalisation and capacity-building efforts could draw from international practices and certifications, while developing country specific approaches and modules to address the challenges faced by Mexican practitioners and experts.
- The SFP should develop an action plan for piloting the establishment (i.e. mission, selection and appointment procedures, reporting lines) of independent audit and risk boards/committees in selected line ministries to assess their impact in strengthening reporting independence and the assurance role of internal audit, as well as the effectiveness of the risk management function.

References

ACFE (2016), *Report to the Nations on Occupational Fraud And Abuse: 2016 Global Fraud Study*, Association of Certified Fraud Examiners, Austin, TX.

ADB (2016), *Training for Internal Auditors in the Public Sector: An Alternative Approach for State Internal Auditors*, Knowledge Showcases, Asian Development Bank, https://www.adb.org/publications/training-internal-auditors-public-sector.

ANAO (2015), *Public Sector Audit Committees: Independent assurance and advice for Accountable Authorities*, Australian National Audit Office, Canberra, www.anao.gov.au/work/better-practice-guide/public-sector-audit-committees-independent-assurance-and-advice.

European Union (2014), *Compendium of the Public Internal Control Systems in the EU Member States*, Publications Office of the European Union, Luxembourg, http://ec.europa.eu/budget/pic/lib/book/compendium/HTML/index.html.

FERMA (2014), European Confederation of Institutes of Internal Auditing Guidance on the 8th EU Company Law Directive, 2014, Federation of European Risk Management Associations, Brussels.

Fountain, L. (2012), *Manager's Responsibility for Internal Control*, www.kscpa.org/writable/files/Self-Study/FGE/updated_managers_responsibility_for_internal_control-_article.pdf.

Fraud and Corruption Control - Guidelines for best practice, of the Crime and Misconduct Commission of Queensland, Australia, 2005, www.ccc.qld.gov.au/research-and-publications/publications/prevention/fraud-and-corruption/fraud-and-corruption-control-guidelines-for-best-practice-1.pdf/download.

Government of Canada (2017a), *Webpage of the Internal Auditor Recruitment and Development Program (IARD Program) - Post-Secondary Recruitment*, https://emploisfp-psjobs.cfp-psc.gc.ca/psrs-srfp/applicant/page1800?poster=941922&toggleLanguage=en (accessed March 2017).

Government of Canada (2017b), *Webpage: Benefits of the Internal Audit Recruitment and Development Program*, www.tbs-sct.gc.ca/ip-pi/job-emploi/ford-rpaf/benefitsiard-avantagesrpai-eng.asp (accessed March 2017).

Hepworth, N. and R. de Koning (2012), *Audit Committees in the Public Sector*, London-Brussels.

HM Treasury (2012), *Fraud and the Government Internal Auditor*, HM Treasury, London, www.gov.uk/government/uploads/system/uploads/attachment_data/file/207217/Fraud_and_the_Government_Internal_Auditor.pdf.

HM Treasury (2011), *Tackling Internal Fraud*, HM Treasury, London, http://webarchive.nationalarchives.gov.uk/20130129110402/http:/www.hm-treasury.gov.uk/d/managing_the_risk_fraud_guide_for_managers.pdf.

IFAC (2015), *From Bolt-on to Built-in: Managing Risk as an Integral part of Managing an Organisation*, International Federation of Accountants, New York, www.ifac.org/publications-resources/bolt-built.

IIA (2009), *Global Technology Audit Guide, Fraud Prevention and Detection in an Automated World*, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, www.iia.org.uk/media/54541/gtag13_fraud_prevention_and_detection_in_an_automated_world.pdf.

Mexico's Ministry of Public Administration Agreement on the the Manual for Internal Control ("Acuerdo por el que se emiten las Disposiciones u el manual Administrativo de Aplicacion General en material de Control Interno",) November 2016 www.gob.mx/cms/uploads/attachment/file/174036/acuerdo-disposiciones-manual-CI.pdf.

NAO/HM Treasury (2008), *Good Practice Guide: Tackling External Fraud*, National Audit Office, London.

Research Councils UK (2017), *Audit and Assurance Services Group (AASG) Webpage*, www.rcuk.ac.uk/about/aboutrcuk/aims/units/aasg/ (accessed March 2017).

UK Government (2017), *Government Internal Audit Agency Webpage*, www.gov.uk/government/organisations/government-internal-audit-agency (accessed March 2017).

US Bureau of the Fiscal Service (2017), Website of Do Not Pay, http://donotpay.treas.gov/ (accessed March 2017).

Further reading

Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control-Integrated Framework, 2013.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management, 2004.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) and Institute of Internal Auditors (IIA)), Leveraging COSO Across the Three Lines of Defence.

Corruption Risk Management Manual, Colombia's Presidency of the Republic, Bogota 2015, www.unicauca.edu.co/versionP/sites/default/files/files/guia-gestion-riesgo-corrupcion-2015.pdf.

Crime and Misconduct Commission of Queensland, Fraud and Corruption Control - Guidelines for best practice, Australia, 2005.

Institute of Internal Auditors (2016), international Professional Practices Framework, Practice Guide: internal audit and the Second Line of Defense, Altamonte Springs, Fla., USA.

Institute of Internal Auditors (2014), Global Public Sector Insight: Independent Audit Committees in Public Sector Organizations, Altamonte Springs, Fla., USA.

Institute of Internal Auditors (2013), The Three lines of Defence in Effective Risk Management and Control, IIA's Position Paper, Altamonte Springs, Fla., USA.

Institute of Internal Auditors Research Foundation (IIARF), (2015)The Global Internal Audit Common Body of Knowledge (CBOK), Auditing the Public Sector - Managing Expectations & Delivering Results.

Institute of Internal Auditors Research Foundation (2011), Internal Auditing's Role in Risk Management, The IIARF White Paper, https://na.theiia.org/iiarf/Public%20Documents/Internal%20Auditings%20Role%20in%20Risk%20Management.pdf, (accessed 20 November 2015).

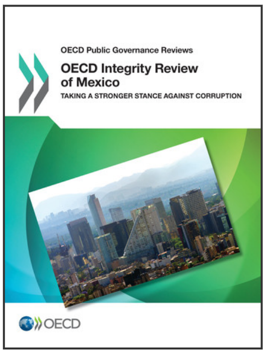
OECD (2015a), *G20/OECD Principles of Corporate Governance*, OECD, Paris http://dx.doi.org/10.1787/9789264236882-en.

OECD (2015b), *Corporate Governance of Company Groups in Latin America*, OECD, Paris.

OECD (2012), *Integrity Review of Brazil: Managing Risks for a Cleaner Public Service*, OECD, Paris.

OECD (2009), Corporate Governance and the Financial Crisis: Key Findings and Main Messages, OECD, Paris, www.oecd.org/corporate/ca/corporategovernanceprinciples/43056196.pdf.

Public Internal Control in the European Union, PIC EU-28 Conference, Assurance Maps, Paris 2015.



From:

OECD Integrity Review of Mexico

Taking a Stronger Stance Against Corruption

Access the complete publication at:
https://doi.org/10.1787/9789264273207-en

Please cite this chapter as:

OECD (2017), “Strengthening the lines of defence against corruption: Risk management, internal control and audit”, in *OECD Integrity Review of Mexico: Taking a Stronger Stance Against Corruption*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264273207-8-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.