

Chapter 7. Safeguarding integrity and managing risks in IMSS procurement

A sound internal control system and effective risk management are critical elements for achieving IMSS's objectives and safeguarding integrity in its procurement processes. This chapter explores the strengths and opportunities for improving the strategies that drive IMSS's internal control and risk management activities. In particular, IMSS could clarify its risk management objectives for procurement, including sharpening the focus on fraud and corruption risks. The chapter also highlights how IMSS and internal control bodies could improve tools and clarify roles for managing risks in procurement processes. Priorities include making improvements to its risk assessment processes and increasing management ownership of the internal control system.

Public procurement is a high-risk activity because of the volume and regularity of purchases, and the often complex nature of processes to procure goods and services. Fraud, corruption and abuse can all unravel the fabric of integrity within procurement processes. Strategic and operational risks – such as inefficiencies in the tendering process, delays in delivery or substandard contract performance – can also undermine the achievement of policy and programme objectives.

The effectiveness of the internal control and risk management system in Mexico's Institute of Social Security (IMSS) therefore has a direct bearing on its success in achieving its strategic goals. As the largest public purchaser of pharmaceuticals and other medical supplies in Mexico, this is particularly relevant for IMSS's procurement activities. Risk managers, internal auditors and other stakeholders in IMSS's internal control system play critical roles in not only safeguarding integrity, but also ensuring that procurement activities operate effectively and efficiently for the benefit of citizens.

In 2013, the OECD reviewed IMSS's public procurement activities, and reported on IMSS's efforts to design and implement an effective internal control system for its procurement processes (OECD, 2013^[1]). Since this review, IMSS has made improvements to manage risks and strengthen internal controls, in line with Mexican and international standards. For instance, it has developed dedicated units to lead risk management activities, such as risk assessments, and it has incorporated specific procurement risks into its risk matrices. While it has taken steps to improve risk management, it could tailor these activities further to address specific procurement risks, particularly the risk of fraud and corruption.

Building on the OECD's 2013 review, this chapter assesses ongoing challenges and risks facing IMSS, and offers recommendations for IMSS to manage risks more proactively. This includes making integrity objectives clearer in its risk management strategy, and improving efforts to monitor and evaluate the effectiveness of the internal control system.

The chapter begins with an overview of internal control and risk management in IMSS, including its application of government-wide standards. It then identifies ways that IMSS could improve its risk assessments and related guidance, as well as enhance management ownership over the internal control system. Finally, the chapter offers considerations for the SFP and Mexico's Supreme Audit Institution, as key stakeholders of the internal control system, to improve their support of IMSS's initiatives so as to better manage procurement risks. These considerations include clarifying roles and improving co-ordination. The recommendations in this chapter demonstrate the linkages between managing risks and institutional goals, recognising that citizens are the ultimate beneficiaries of a sound internal control system and risk management function.

Overview of internal control and risk management in IMSS

Internal control and risk management in the Mexican Government is grounded in the SFP's 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*, or MAAG-CI), published in the Official Gazette on 2 November 2016. The MAAG-CI introduces the System of Institutional Internal Control (SCII) as Mexico's internal control and risk management framework for federal public entities. IMSS, as an autonomous government institution, is subject to the requirements outlined in the MAAG-CI and the SCII. The SCII has the following three components (see Box 7.1 for additional details):

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

Box 7.1. The System of Institutional Internal Control and its components

As outlined in the SFP's Manual of Internal Control System (MAAG-CI), the System of Institutional Internal Control (SCII) can be defined as a set of processes, mechanisms and other organisational elements which interact with each other (Mexico's Ministry of Public Administration, 2016^[21]). An institution can apply the SCII at various levels, including planning, organisation, execution, direction, information and monitoring of its management processes. This is to ensure that the decision making is conducted in a manner that supports and promotes continuous improvement, quality, efficiency, compliance with the law, and the achievement of the institutional goals and objectives in an ethical and integral environment.

One of the three components of SCII, the Standard Model of Internal Control (MECI), is aligned with the Integrated Framework on Internal Control in the Public Sector (Marco Integrado de Control Interno en el Sector Público, or MICI), developed by Mexico's Supreme Audit Institution (Auditoría Superior de la Federación, or ASF). MECI, according to SFP officials, was an attempt to harmonise the internal control standards of SFP and ASF. MECI includes three different levels of control: strategic, executive and operational. The framework is built around the following components, drawing from the Internal Control-Integrated Framework by the Committee of the Sponsoring Organisation of the Tredway Commission: the control environment, risk assessment, control activities, information and communication, and monitoring activities.

The five components of MECI are structured around 17 principles, which are meant to aid officials in developing an effective internal control system. A successful integration of the principles contributes to the effective operation of the overarching components, and consequently to the effective operation of the overall internal control system within the entity. Moreover, the principles are meant to assist in making informed judgements when evaluating the maturity and degree of implementation of various components. When applying the framework, managers should be aware that they are expected to develop appropriate and tailored controls, since these are not articulated in MECI.

In addition to MECI, MAAG-CI also introduced the Institutional Risk Management (ARI), which provides a risk management framework and methodology. Specifically, the ARI outlines the activities an entity should undertake in order to identify, evaluate and mitigate corruption risks.

Source: (Mexico's Ministry of Public Administration, 2016^[21])

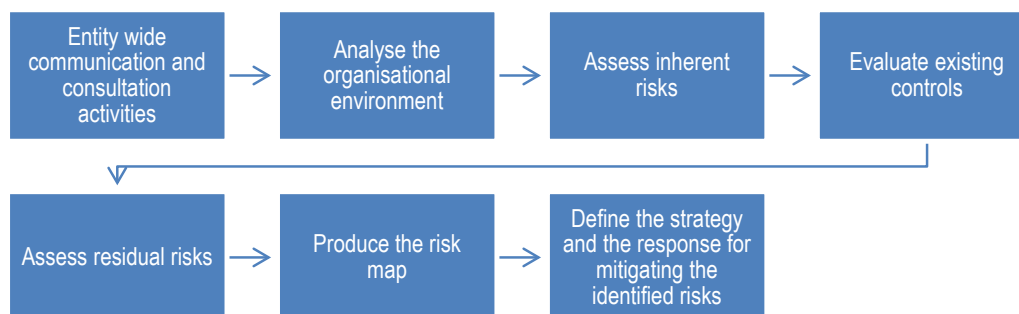
IMSS's Directorate of Administration, and a team within it referred to as the Coordination of Modernisation and Competitiveness (MC), are responsible for directing the development, issuance and updating of policies, norms, procedures and guidelines related to regulations and internal control, among other areas. Other actors support the internal

control system in IMSS. These include the Internal Control Office (*Órgano Interno de Control*, or OIC), an extension of the Ministry of Public Administration (SFP). The standards for internal control in Mexico assign a major role to the OICs to contribute to internal control and risk management activities.

The MAAG-CI requires federal public entities to produce an annual risk management matrix and an action plan, referred to as the Working Programme of Risk Management (*Programa de Trabajo de Administracion de Riesgos*, or PTAR). Within IMSS, the PTAR is developed and signed by the Director General, the Internal Control Coordinator (ICC) and the Risk Management Liaison. This is in line with the MECI, which assigns responsibility for monitoring the functioning of the internal control system to the heads of government institutions (i.e. IMSS's Director General), or when appropriate, the Governing Bodies (Mexico's Ministry of Public Administration, 2016^[2]). MECI also requires the Director General to agree on the risk management methodology with the ICC. The latter is responsible for co-ordinating, implementing and monitoring PTAR activities, including the risk matrix and action plans, as well as progress reports and an annual report on risk behaviour.

The MC conducts risk assessments of a number of IMSS's services, which it documents in its Quality and Patient Safety Plan. As the title of the plan suggests, these risk assessments focus on risks and challenges that could affect the quality of medical care and patient safety, such as handling hazardous materials, as well as the management and use of medicines (IMSS, 2016^[3]). The MC focuses its assessments on operational risks, and it co-ordinates with other IMSS directorates, as well as the OIC, to provide methodological support and follow up to other directorates in their own assessments.

Each directorate, including the procurement function, is responsible for analysing risks that are relevant to its area. In general, IMSS's approach reflects a "specific risk approach", whereby risks are identified within specific units. This is in contrast to a risk factor approach, which involves identifying risk factors shared across most, if not all, units within the institution (Wright, 2013^[4]). According to officials, IMSS relies heavily on MECI, ARI and SFP's manual, described in Box 7.1 above, to structure its risk assessments, following the steps outlined in Figure 7.1 below. As a result of this process, for the 2017 calendar year, IMSS identified 13 strategic and operational risks linked to 47 risk factors in total across a range of activities included in its work plan for 2014-2018. For instance, as a strategic risk, IMSS identified a failure to digitalise paperwork and services that can improve the quality of services provided to citizens (IMSS, 2017^[5]; see Chapter 3). Other risks focused on health services, such as the risk of poor implementation of measures to prevent diseases, leading to increased mortality rates during hospital stays.

Figure 7.1. The risk assessment process based on ARI

Source: (OECD, 2017_[6])

The CABCS (Co-ordination of Procurement of Goods and Contracting for Services area or *Coordinación De Adquisición de Bienes y Contratación de Servicios*) co-ordinates IMSS's procurement function, and is responsible for assessing risks related to procurement activities. With the support of the MC, the CABCS identifies risks in the procurement cycle using the process described above. It assesses the probability and impact of risks, and determines whether control activities are sufficient for mitigating risks within a defined risk tolerance (see next section for more on risk tolerance). The MC analyses progress towards addressing these risks, and others, on a quarterly basis. The MC also consolidates the risks into a single matrix, graphic and PTAR. The matrix functions much like a risk registry (Box 7.2) and as such, IMSS's risk assessment process reflects the experience of other countries.

Box 7.2. Development and management of risk registers – example of the Irish Health Service Executive (HSE)

The Health Service Executive develops risk registers in order to manage its risks and to obtain a high-quality overview of the services' risk status at a certain point in time. The risk register serves as a powerful tool for risk tracking, and outlines the overall system of risks and the status of risk mitigation actions.

Each line manager is responsible for developing a risk register in his/her area of responsibility. Once completed, the register is shared with all employees of the entity in a clear and comprehensible manner, while taking into consideration their level of training, knowledge and experience.

An action plan is the critical part of a risk register. It is developed to address the additional controls required to reduce the risk to a satisfactory level. Supplementary controls that cannot be managed at the service level should be transferred to the next level of management. HSE acknowledges that for various reasons not every risk can be eliminated. Consequently, at any stage of the process it may be decided to 'live with' or accept a certain level of risk. When a risk cannot be entirely eliminated, it must be recorded in the risk register along with a list of controls aiming to reduce it to an acceptable level. These risks will be then monitored on a regular basis.

Four elements have been identified as prerequisites for developing a sound risk register:

1. **Availability of risk expertise.** Staff supporting the process need suitable training and education.
2. **Use of approved support materials and tools.** To ensure consistency throughout the process, a number of approved documents and tools are to be used when developing a register.
3. **Commitment and ownership.** Visible commitment from senior management is the key success factor in the process.
4. **Availability of site support.** Administrative support is required for organising workshops and overall co-ordination.

Since risk assessment is a dynamic process, risks and their control measures should be continuously reviewed, monitored and revised where necessary. Monitoring can be conducted at service level, at service area level, or for independence assurance.

Source: (Irish Health Service Executive, 2009^[7])

Ensuring effective risk management strategies and implementation

IMSS could improve its risk management strategy for public procurement by clearly defining its goals and objectives, particularly those related to fraud and corruption risks.

The approval and signature of the Director General for the PTAR, discussed above, demonstrates a high-level commitment to risk management and internal control within IMSS. It also helps to set the tone from the top with regards to management's expectations for standards of conduct and communicating the importance of internal

control, as required in the SCII. However, IMSS's Strategic Work Plan for 2016-2018 omits any reference to the importance of internal control and risk management for the effectiveness, efficiency and integrity of IMSS's activities, including procurement. Other key documents like the PTAR and risk matrix also do not explicitly mention corruption, fraud or integrity.

The OECD's 2013 report on the IMSS, *Public Procurement Review of the Mexican Institute of Social Security: Enhancing efficiency and integrity for better health care*, recommended that IMSS establish a procurement risk management policy that was aligned with broader organisational objectives. The policy would aim to define and communicate IMSS's approach to risk, and provide high-level guidance on institutional processes and procedures for mitigating risks (OECD, 2013^[1]). IMSS has yet to implement this policy; however, as an alternative, it could consider defining and incorporating integrity objectives into its work plans, the PTAR and guidance that discusses its procurement activities. This would help to demonstrate to managers and employees the importance of corruption and fraud risk management in this high-risk area.

In particular, IMSS could define clear objectives that explicitly emphasise the importance of a culture of integrity, and managing the risks of fraud and corruption. By making a reference to integrity and combating corruption at the strategic level, and highlighting high-risk areas like procurement, IMSS can further set a high-level tone that is conducive to effective fraud and corruption risk management. This would also help IMSS to better align with MECI, which now includes a principle dedicated to managing fraud and corruption risks, noting that entities should consider the potential for fraud when assessing risks to the achievement of objectives (Mexico's Ministry of Public Administration, 2016^[2]). Box 7.3 offers examples of strategic objectives dedicated to integrity from the United States.

Box 7.3. Defining integrity objectives: the approach of the United States' Centers for Medicare and Medicaid Services

The Centers for Medicare & Medicaid Services (CMS) is a federal agency within the Department of Health and Human Services (HHS) responsible for administering the Medicare, Medicaid and the Children Health Insurance Program. When developing its strategy, CMS ensures that it is well aligned with the strategic plan updated by HHS every four years. This allows for an integrated implementation approach and for the most current priorities to be duly reflected in the CMS strategy.

CMS defines its strategic plan in a comprehensive manner, outlining the agency's vision, mission and goals, as well as strategic objectives and desired outcomes. CMS's strategic objectives determine what improvements are required to achieve specific results, and thus help monitor whether progress has been made. With the assistance of the Strategic Planning and Management Council, the agency has identified strategic objectives covering the following organisational perspectives: organisational capacity, internal processes, financial stewards, and customers and stakeholders.

According to the CMS strategy, Objective 6.0, Strengthen Program Integrity, supports financial stewardship while helping to maximise value and effectiveness within the available resources. Improvements in financial stewardship subsequently help achieve the desired outcomes for customers and stakeholders, supporting the agency's overall goals and vision.

The CMS's strategy further describes the "Strengthen Program Integrity" objective through the following features and elements:

- enhanced financial accountability due to appropriate federal and state oversight of Medicaid expenditures;
- co-operation with law enforcement
- improving bad actor detection, identifying improper payments, refining enrolment processes
- taking into account policy levers and anti-fraud mechanisms at an early stage of regulation development
- improving the proactive stance through effective programme oversight and overall risk management
- enhancing enforcement through compliance and oversight activities
- improving prevention of fraud, waste and abuse through a targeted screening process
- effective risk management and strategic investments leading to high impact and return
- improved audit processes reduce audit frequency incompatibilities
- consolidated and well-aligned data are used for decision making
- improving collaboration with States on executing the healthcare delivery reform
- maintaining CMS's accountability, reliability and transparency by providing decision makers with access to its financial information
- proactive and coherent agency programme integrity activities.

Moreover, the importance of integrity is further underscored by being listed in the

CMS strategy as one of its core values by which they live. This emphasises its commitment to the highest standards of ethical behaviour and honesty.

Source: (CMS, 2016^[8])

When defining integrity objectives, IMSS could also ensure they are echoed in the sub-objectives of IMSS's functional activities, particularly procurement. Sub-objectives relate to IMSS's functional activities and its departments, including its procurement and contracting activities. Management is responsible for linking entity-level objectives to specific sub-objectives, and co-ordinating across IMSS (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2013^[9]). By strengthening this link, IMSS could more clearly articulate the value of internal control and risk management activities for achieving goals, objectives and outcomes. This could also enhance management ownership of these activities, as discussed further below.

To complement its efforts to create a culture of integrity, IMSS could further emphasise messages that focus on integrity values as opposed to rules.

In Mexico, the three years since the onset of major anti-corruption reforms in 2014 have seen considerable advances in public sector integrity and accountability. Beginning in early 2015 with the issuance of executive orders by the President of Mexico (focusing primarily on managing conflicts of interest), Mexico has undergone a series of reforms aimed at strengthening accountability and integrity in government. The federal government has also replaced its previous ethics code (*Código de Ética de la Administración Pública Federal*, DOF 31/julio/2002) and Integrity Rules (*Lineamientos de integridad y comportamiento ético, a través de Comités de Ética*, DOF 6/marzo/2012) with the new Ethics Code and Rules of Integrity (*Código de Ética y Reglas de Integridad*, DOF 20/08/2015). All public entities at the federal level are required to update their own organisations' codes accordingly. The reforms included four initiatives to strengthen management in public procurement processes, including (OECD, 2017^[6]):

- **Protocol for Procurement Officials' Behaviour** (Protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones). This is included in the General Law on Administrative Responsibilities (Ley General de Responsabilidades Administrativas). See chapter 5 for further discussion.
- **A registry of federal public administration public servants involved in public procurement processes** (Registro de servidores públicos de la Administración Pública Federal que intervienen en procedimientos de contrataciones públicas), including classification according to their level of responsibility and their certification.
- **An online publication of sanctioned suppliers**, specifying the reason of the sanction.
- **Increased collaboration with the private sector** to reinforce transparency in procurement procedures and decision making, and to reinforce integrity through the involvement of citizens in the identification of vulnerable processes and procedures, and the development of co-operation agreements with chambers of commerce and civil society organisations.

To comply with these new integrity requirements, IMSS established a "Code of Conduct and Prevention of Conflicts of Interests of IMSS Public Officials", which was approved

by the Technical Council in December 2015. The Technical Council is responsible for issuing the guidelines that govern IMSS officials, such as those related to preventing acts of corruption. An annex to the Code of Conduct includes Integrity Rules for the Exercise of Public Service, and contains a section entitled “Public Procurement, Licenses, Permits, Authorisations and Concessions.” This section states that the officials who participate in procurement processes must: 1) act with transparency, impartiality and legitimacy; 2) focus their decisions based on society’s requirements and interests; and 3) ensure the best conditions for the government. It also describes which behaviours would violate these rules.

In addition, the Law of Social Security (LSS), the Internal Regulation of the IMSS (*Reglamento Interno del Instituto Mexicano del Seguro Social*, or RIIMSS), and the Internal Working Regulation of the Collective Work Contract (*Reglamento Interior de Trabajo del Contrato Colectivo de Trabajo*) for 2015-2017 jointly state, according to IMSS officials, that employees are bound to follow, when complying with their obligations, “the principles of responsibility, professional ethics, excellence, honesty, loyalty, impartiality, efficiency, warmth and quality in services provision and in health care to right-holders.” It also notes that “they shall be subject to civil or penal responsibilities which they might incur as persons in charge of providing a public service.”

While the Protocol of Conduct for Public Servants in Public Procurement helps to raise the profile of procurement as a high-risk area, it is largely based on rules instead of values (OECD, 2017^[6]). This notion is reflected in the above laws and regulations. A compliance-based approach emphasises prevention of fraud and corruption through the establishment of enforceable standards and telling officials what to do. In contrast, a values-based approach aims to inspire integrity and induce behavioural changes through awareness-raising about ethics, values and the public interest. The former approach risks undermining motivation and morale if officials feel they are mistrusted or perceived to be corrupt. For this reason, OECD’s Recommendation of the Council on Public Procurement, referred to in Box 7.4 below, emphasises the importance of not creating undue fear of consequences (or risk-aversion) in the procurement workforce or supplier community (OECD, 2015^[10]).

Box 7.4. Integrity and OECD Recommendation of the Council on Public Procurement**III. RECOMMENDS that Adherents preserve the integrity of the public procurement system through general standards and procurement-specific safeguards.**

To this end, Adherents should:

- i) Require high standards of integrity for all stakeholders in the procurement cycle. Standards embodied in integrity frameworks or codes of conduct applicable to public sector employees (such as on managing conflict of interest, disclosure of information, or other standards of professional behaviour) could be expanded (e.g. through integrity pacts).
- ii) Implement general public sector integrity tools and tailor them to the specific risks of the procurement cycle as necessary (e.g. the heightened risks involved in public-private interaction and fiduciary responsibility in public procurement).
- iii) Develop integrity training programmes for the procurement workforce, both public and private, to raise awareness about integrity risks, such as corruption, fraud, collusion and discrimination, develop knowledge on ways to counter these risks, and foster a culture of integrity to prevent corruption.
- iv) Develop requirements for internal controls, compliance measures and anti-corruption programmes for suppliers, including appropriate monitoring. Public procurement contracts should contain “no corruption” warranties, and measures should be implemented to verify the truthfulness of suppliers’ warranties that they have not and will not engage in corruption in connection with the contract. Such programmes should also require appropriate supply-chain transparency to fight corruption in subcontracts, and integrity training requirements for supplier personnel.

Source: (OECD, 2015^[10])

Fostering a culture that is conducive to risk management and that encourages management ownership over the internal control system requires officials who are motivated and do not feel treated as threats themselves. As such, IMSS could consider emphasising a values-based approach in its messaging and training on the code of conduct and ethics. Currently, risk management and internal control activities in IMSS are largely the responsibility of select teams and the OIC, with others involved on an ad-hoc basis for risk assessments and other activities. However, risk management and responsibility over the internal control system should permeate across the organisation, vertically and horizontally. By emphasising values-based approaches, IMSS would help to advance this idea. Moreover, sharpening the focus on integrity values in the procurement cycle would bring IMSS more into line with international standards, including the OECD's Recommendation of the Council on Public Procurement.

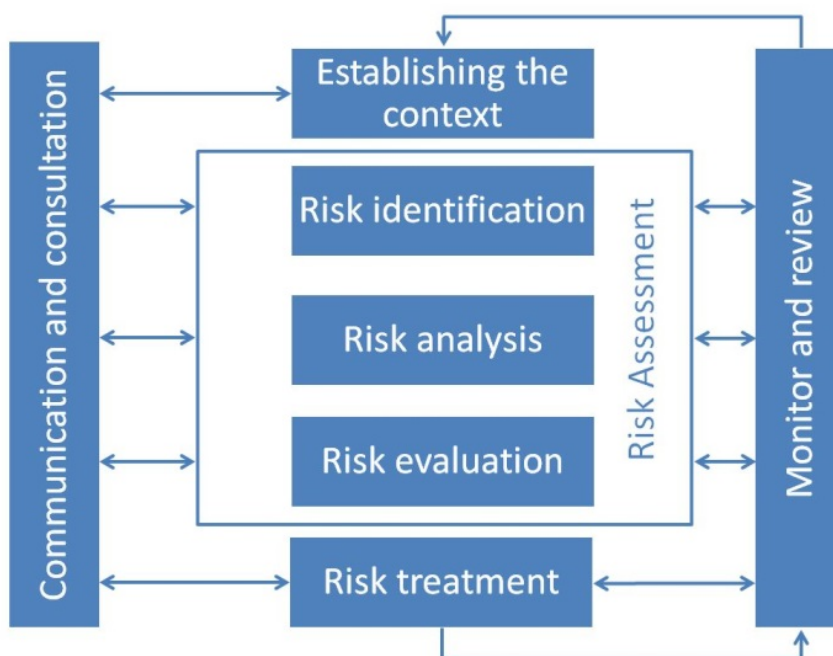
IMSS could further develop its strategy and activities for more systematically monitoring and evaluating the effectiveness of the internal control system and risk management activities.

While the IMSS Director General has the ultimate responsibility for the internal control system, according to MECI, other actors throughout the institution play critical roles, as detailed in IMSS's 2017 Organisational Manual of the Directorate of Administration (IMSS, 2017^[11]). The Directorate of Administration, and the MC within it, is responsible

for directing the development, issuance and updating of policies, norms, procedures and guidelines related to regulations and internal control, among other areas. In addition, the directorate has the duty to establish mechanisms to assess the state of the internal control system and risk management processes.

Numerous international standards exist for internal control and risk management, such as the International Standards Organisation's (ISO) 3100, *Risk Management: Principles and Guidelines*, which calls for planned monitoring and evaluation as part of the risk management process (ISO, 2009^[12]), as shown in Figure 7.2. In line with the ISO standards, the MAAG-CI requires management to evaluate results and prepare quarterly progress reports and an annual report for the PTAR. In addition, according to the manual, management should evaluate and document the results of self-assessments and independent evaluations to determine whether internal control is effective and appropriate (Mexico's Ministry of Public Administration, 2016^[2]). Management must also identify changes that have occurred in internal control, which may have resulted from institutional changes or changes to its environment.

Figure 7.2. International standards for risk management



Source: Adapted from (ISO, 2009^[13])

During interviews, IMSS officials described several activities to assess the internal control system and risk management activities, but they largely focus on evaluation rather than monitoring, and do not take into account the range of factors that could influence these functions. For instance, IMSS publishes an annual evaluation report that focuses on financial risks in the PTAR (*Evaluación de los Riesgos Financieros Considerados en el Programa de Administración de Riesgos Institucionales*). In addition, officials noted that they take into account audit findings by SFP and the Mexican Supreme Audit Institution (*Auditoría Superior de la Federación*, ASF) in order to determine where processes are failing. Based on these reviews, IMSS conducts "root cause" analyses, aimed at

addressing vulnerabilities and improving policies and procedures. IMSS could more systematically and strategically evaluate these processes in order to better understand opportunities for improving its internal control system and risk management.

The SFP communicates requirements and offers guidance on the timing and objectives of monitoring and evaluation in its Manual of Internal Control System, the MAAG-CI. However, it is not explicit about the purposes and potential areas for evaluation. According to ISO 31000, *Risk Management – Principles and Guidelines* (ISO, 2009^[12]), IMSS's monitoring and review processes should encompass all aspects of risk management in order to:

- ensure controls are effective and efficient in both design and operation
- obtain further information to improve risk assessment
- analyse and learn lessons from events (including "near-misses"), changes, trends, successes and failures
- detect changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities
- identify emerging risks.

IMSS could improve its monitoring and evaluation by going beyond financial risks to look at all aspects of the risk management process. This could include reviews of both the external and internal contexts that can affect IMSS's ability to pursue its objectives (Figure 7.3). In line with IMSS's strategic objectives, the MC and CABCS could take steps to improve evaluations of how CABCS assesses risks, and tailor these factors to procurement, keeping in mind the above purpose of evaluations.

Figure 7.3. External and internal contexts for evaluation of risk management activities

Evaluations of the context can include (but is not limited to):

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment,
- whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, and perceptions and values of external stakeholders.

Evaluating the internal context can include (but is not limited to):

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture;
- standards, guidelines and models adopted by the organization; and
- the form and extent of contractual relationships.

Source: (ISO, 2009^[12])

Improving risk assessments related to public procurement

IMSS could improve its risk assessments related to public procurement by sharpening the focus on corruption and fraud risks, as well as other strategic and operational risks that can affect the entire procurement cycle.

IMSS conducts risk assessments for a number of different areas; however, it could strengthen its assessments of its procurement functions. The risks related to the procurement cycle identified by IMSS are valid, but incomplete. IMSS primarily focuses on strategic and operational risks in the procurement cycle. It could consider additional risks, particularly those related to fraud and corruption, to ensure a thorough account of both the risks and control activities in place.

During interviews, IMSS and OIC officials highlighted a number of risks that could influence the effectiveness and efficiency of the procurement process, including insufficient planning, lack of knowledge to prepare contract requirements, and lack of collaboration between the contracting and petitioning areas, among others. However, for 2017, the risk matrix and PTAR explicitly refers to procurement risks in only two out of the 13 overall risks identified, and excludes many of the risks that officials highlighted.

One risk identified in the PTAR is the lack of co-ordination of processes for making consolidated purchases; both CABCS and the Co-ordination of Supply Control are noted as the risk owners. In addition, IMSS identifies projects that exceed their scheduled completion date as a risk. IMSS highlighted the poor detection of pensioners' deaths as a potential risk, but it does not link this to integrity, fraud or corruption. For instance, the risk of individuals who steal the identities of deceased pensioners in order to obtain goods and services that they would otherwise be ineligible to access. Neither the matrix nor the PTAR make explicit reference to risks related to fraud, corruption or integrity in any of IMSS's activities, including procurement.

Officials explained that IMSS involves various units in its assessments of procurement risks, including teams responsible not only for procurement, but also market research, control and product users. To increase the focus on fraud and corruption risks, IMSS could ensure that those who are at the frontline in preventing fraud and corruption are involved in the risk assessment (e.g. contracting officers), as well as external entities, such as contractors, ASF and regulators. Complaints, similar entities and social witnesses can also help identify risk (see Chapter 5). Interviews, surveys and focus groups are just some approaches that IMSS could use to gather information and input from these stakeholders. IMSS could also analyse individual tenders for risks. This approach could cover all phases of the procurement cycle, including pre-tendering, tendering, and post-award phases (see Table 7.1 for further discussion of such risks in the procurement cycle).

Table 7.1. Integrity, corruption and fraud risks across the procurement cycle

Risks in the pre-tendering phase	Needs assessment	<ul style="list-style-type: none"> • Lack of adequate needs assessment • Influence of external actors on officials' decisions • Informal agreement on contract
	Planning and budgeting	<ul style="list-style-type: none"> • Poor procurement planning • Procurement not aligned with overall investment decision-making process • Failure to budget realistically or deficiency in the budget
	Development of specifications/requirements	<ul style="list-style-type: none"> • Technical specifications are tailored for a specific company • Selection criteria is not objectively defined and no established in advance • Requesting unnecessary samples of goods and services • Buying information on the project specifications
	Choice of procurement procedure	<ul style="list-style-type: none"> • Lack of procurement integrity for the use of non-competitive procedures • Abuse of non-competitive procedures on the basis of legal exceptions: contract splitting, abuse of extreme urgency, non-supported modifications
Risks in the tendering phase	Request for proposal/bid	<ul style="list-style-type: none"> • Absence of public notice for the invitation to bid • Evaluation and award criteria are not announced • Procurement information is disclose and made public • Lack of competition or cases of collusive bidding: <ul style="list-style-type: none"> ◦ cover bidding ◦ bid suppression ◦ bid rotation ◦ market allocation
	Bid submission	<ul style="list-style-type: none"> • Conflict of interest and corruption in the evaluation process through: <ul style="list-style-type: none"> ◦ Familiarity with bidders over time ◦ Personal interests such as gifts or future/additional employment ◦ No effective implementation of the "four eyes-principle"
	Bid evaluation	<ul style="list-style-type: none"> • Vendors fail to disclose accurate cost or pricing data in their price proposals, resulting in an increased contract price (i.e. invoice mark-ups, channel stuffing)
	Contract award	<ul style="list-style-type: none"> • Conflict of interest and corruption in the approval process (i.e no effective separation of financial, contractual and project authorities) • Lack access to records on the procedure
Risks in the post-award phase	Contract management/performance	<ul style="list-style-type: none"> • Abuses of the supplier in performing the contract, in particular in relation to its quality, price and timing: <ul style="list-style-type: none"> ◦ Substantial change in contract conditions to allow more time and/or higher prices for the bidder ◦ Product substitution or sub-standard work or service not meeting contract specifications ◦ Theft of new assets before delivery to end-user or before being recorded ◦ Deficient supervision from public officials and/or collusion between contractors and supervising officials ◦ Subcontractors and partners chosen in an on-transparent way or not kept accountable • Deficient separation of financial duties and/or lack of supervision of public officials leading to: <ul style="list-style-type: none"> ◦ False accounting and cost misallocation or cost migration between contracts ◦ Late payments of invoices
	Order and payment	<ul style="list-style-type: none"> • False or duplicate invoicing for good and services not supplied and for interim payment in advance entitlement

Source: (OECD, 2016_[14]).

As noted in the table above, bid rigging (i.e. collusive tendering) is also a major risk that can affect the tendering phase. Bid rigging occurs when "businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods or services for purchasers who wish to acquire products or services through a bidding process" (OECD, 2009^[15]). IMSS may be particularly vulnerable to this, given the current features of the consolidated tenders it leads. Indeed, a high volume of procurement coupled with repetitive tendering processes and little changes in the scope of those tenders from one year to another could expose them to bid-rigging practices. Bid rigging and corruption can occur simultaneously and they can reinforce each other, but they each have key elements that make them distinct. For instance, bid rigging is a horizontal relationship between bidders that restricts competition; in public procurement it harms the public purchaser. Corruption involves a vertical relationship between one or more bidders and one or more procurement officials. That is, a procurement official can receive bribes or rewards at the expense of the public purchaser (or the public in general) in exchange for currying favour with a particular firm (OECD, 2012^[16]). While differences exist in the nature of the schemes, the control activities for managing the risk of both bid rigging and corruption can complement each other.

In addition to risks of fraud and corruption, several risks of strategic and operational importance to the procurement cycle are also overlooked in IMSS's current risk assessment. These may be a result of poor performance or mistakes, rather than breaches of integrity. Examples include bid challenges and complaints, poor quality of products, failure of suppliers, and inadequate contractual terms and management. Moreover, a large part of IMSS's public procurement function is highly decentralised, yet key decisions and strategies related to the procurement function have been centralised. Centralised procurement can entail risks that include market concentration and development of monopolistic structures, fit-for-purpose risks from over-standardisation of requirements, and responsiveness risks to developments in pricing and medical technology. By honing its assessments of the additional strategic and operational risks related to the procurement cycle, IMSS could intervene to prevent or mitigate the impact of these risks on procurement performance.

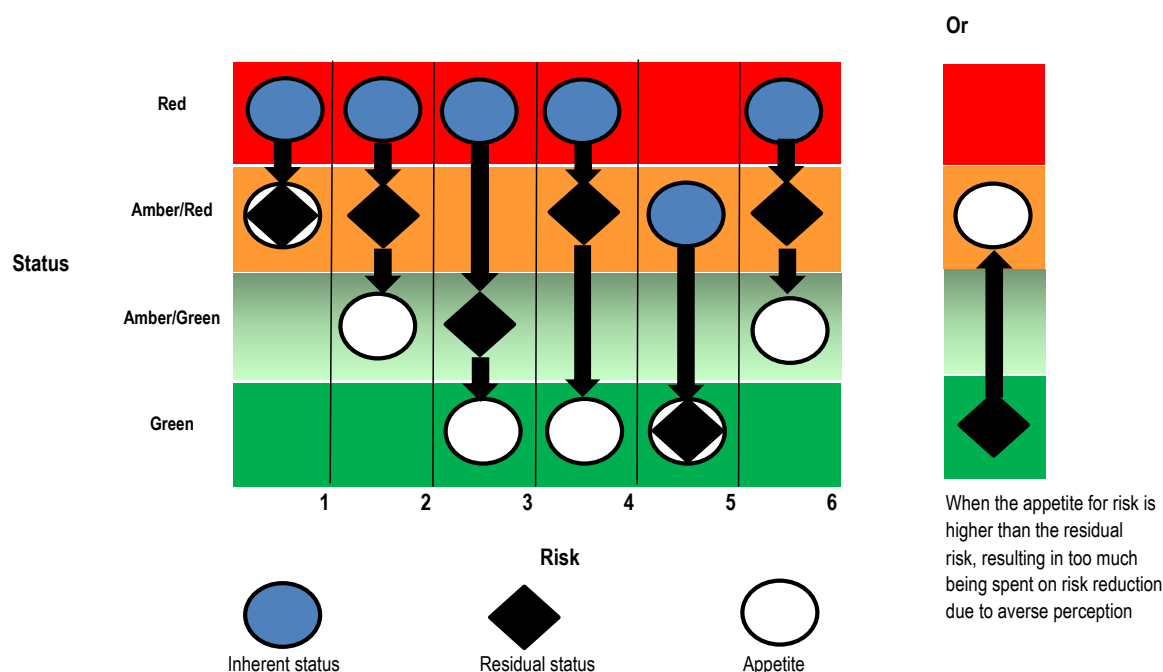
IMSS could further define risk tolerances to more effectively allocate resources and determine control activities.

The MAAG-CI requires federal public entities to define their risk tolerance relative to their strategic objectives. It further calls for the risk owners to monitor risks, using indicators, to ensure that they remain within predetermined tolerance levels (Mexico's Ministry of Public Administration, 2016^[2]). In the event that risks exceed tolerance levels, the risk owner must report this change to the Director General and the ICC. The MAAG-CI makes explicit reference to corruption risks, yet it notes that entities do not have to define a risk tolerance for corruption risks (Mexico's Ministry of Public Administration, 2016^[2]). Presumably, this is because SFP is attempting to convey that managers should have zero tolerance of any risks that could undermine the integrity of the institution.

Risk tolerance can be defined as "the acceptable level of variation in performance relative to the achievement of objectives" (Government Accountability Office, 2015^[17]). This definition underscores the idea that risk management is not only about minimising threats, but also exploiting opportunities. For instance, IMSS may identify medical equipment that it wishes to procure at a discount price. Risk tolerance can help IMSS to determine whether controls in place are effective enough (relative to the tolerance) to justify

increasing its purchase volume to take advantage of the lower price. Figure 7.4 below illustrates the practical application of risk tolerance in aiding managers to understand risk exposure and whether additional controls are needed. It depicts the relationship between inherent risks, residual risks and risk tolerance.

Figure 7.4. The relationship between inherent risks, residual risk and risk tolerance



Source: (UK HM Treasury, 2006^[18])

Risk tolerance is a critical element of effective risk assessments because it can help IMSS to make risk-based decisions about mitigation strategies. In addition, as IMSS officials have expressed the need to improve the balance between controls and efficiency in procurement process, further defining risk tolerance and providing guidance on how it is used could help IMSS to make better decisions on whether to add or reduce controls.

In 2014, IMSS strengthened its risk management framework, and incorporated risk tolerance into its assessment process. IMSS address risk tolerance in two ways. The first is in the risk matrix, where it notes the tolerance for each of the 13 risks on a scale of low, moderate, high and extreme. The second is in the PTAR, where IMSS notes an "indicator associated with risk tolerance," which links to one of the 47 risk factors IMSS has identified. For instance, the risk of uncoordinated processes when making consolidated purchases (one of the 13 risks) includes three risk factors, each of which is assigned an indicator for risk tolerance. The use of risk tolerance in the matrix and PTAR are positive signs of IMSS's attempts to incorporate this concept into decision making for determining control activities.

However, IMSS could improve its use of risk tolerances and guidance to ensure that they become more than a box-ticking exercise in response to requirements. For instance, IMSS does not define its tolerance of corruption and fraud risks, citing zero tolerance for such risks. Zero tolerance of corruption and fraud is an effective message for conveying an overall commitment to integrity; however, reducing such risks to zero has little practical

value for the purposes of managing risks. As discussed, there is need to balance controls with efficiency, innovation and other business objectives, and this is true of the procurement cycle. IMSS could develop a meaningful risk tolerance for corruption and fraud risks in procurement processes in order to make informed decisions about control activities. For example, when procuring urgently needed medical equipment, IMSS could define a "low" tolerance instead of a "very low" tolerance, with the practical effect being expedited procurement procedures for historically high-performing suppliers.

IMSS could improve its guidance and tools for conducting risk assessments related to procurement and advancing new forms of analyses on tenders and processes.

According to ISO 31000, risk management activities should be documented in order to help improve methods, tools, and overall processes (ISO, 2009^[13]). In addition, OECD's Recommendation of the Council on Public Procurement calls for government entities to not only publicise risk management strategies, but also to raise awareness and knowledge about the integration of risk management into the procurement cycle (OECD, 2015^[10]). It makes the following recommendations for achieving this:

- engaging in communication to strengthen trust between stakeholders and control activities
- organising awareness campaigns and events on the importance of integrating risk management activities into daily business practices
- providing training sessions and workshops to inform relevant public procurement entities about their risks and ways to handle the identified risks,
- circulating periodic messages using various media (e.g. newsletter, promotional poster, brochures, videos, handbook, etc.) to relevant stakeholders on the existing risk management strategies
- disseminating best practices of risk management case studies from leading organisations
- inviting public procurement entities to relevant conferences and seminars on risk management strategies.

IMSS has invested considerable resources in developing sound risk management practices and assessments, in line with the MAAG-CI and international standards. However, according to officials, it has yet to develop specific guidelines or tools to aid in identifying, monitoring and reporting risks at various stages of the procurement process. Without such guidance, a heavy burden is placed on the MC to co-ordinate, consolidate and standardise risk management practices, including risk assessments. Additional guidance for public procurement officials would help IMSS to advance a more coherent and informed approach to identifying and managing risks in individual contracts. In doing so, IMSS could draw on the experience of the Australian government (Table 7.2).

Table 7.2. Australian guidance for identifying and managing procurement risks

Sources of Risk	Examples of Risk
Contract management capability	<ul style="list-style-type: none"> • Failure to have sufficiently skilled and experienced resources to effectively manage the contract(s) • Lack of recognition of the importance of contract management • Failure to act on contractor underperformance
Contractor performance	<ul style="list-style-type: none"> • Failure to provide contract deliverables on time, to the agreed quality standards • Failure to adhere to the agreed budget • Failure to comply with all contract provisions, for example, privacy, security, recordkeeping • Fraud and/or unethical conduct by the contractor
Changes in circumstances and/or requirements	<ul style="list-style-type: none"> • Contract changes not dealt with as contract variations • Contractor not prepared to agree to contract variations to accommodate changes in entity requirements • Changes in circumstances not managed in a timely manner
Stakeholder relationships	<ul style="list-style-type: none"> • Stakeholders not consulted and/or kept informed about contract performance • Changes in stakeholder expectations not communicated to contract manager • Differing and/or conflicting stakeholder expectations

Source: (Australia National Audit Office, 2012^[19])

In developing the guidance, IMSS could consider explaining the processes and defining key terms reflected in the ARI, including the risk matrix, risk map and PTAR. These documents are meant to be tools for risk managers, and there are linkages between them that IMSS could clarify. For example, the risk matrix appears to include an assessment of inherent risks (risks in the absence of measures to address risks) and residual risks (risk exposure after applying mitigation strategies to address the risk). The residual risks are then depicted in the risk map – a standard two-dimensional representation of individual risks according to probability and impact. The PTAR then offers additional information on mitigation measures for these risks. The guidance could explain these linkages between, as well as the individual risk concepts within each to help guide and educate managers.

Improved risk assessments and guidance can also offer additional opportunities for IMSS to use the results for more advanced data analyses, particularly of tenders. Officials noted that IMSS collects information on a range of procurement risks and intends to expand its efforts to retroactively understand how tenders were carried out. IMSS could use the data it has collected on procurement risks to conduct additional analyses of individual tenders in order to aggregate risks across different procuring entities (see Box 7.5 for an example). The usefulness of this analysis depends on the quality and standardisation of the risk assessments, which in turn depend on having sufficient guidance for carrying out the process.

Box 7.5. Data-mining to identify corruption in public procurement in the European Union

In recent years, a team of sociologists has developed a new system to identify potential corruption in public procurement in Europe. The research team developed a “Corruption Risk Index” (CRI) to mine available information on public procurements to identify potential corruption issues.

To develop the CRI, the lead researcher spoke with experts on public procurement to identify 13 “red flags” that could indicate corruption in an individual contract or tender. These red flags included very short tender periods (e.g., a tender issued on a Friday and awarded the following Monday), very specific or suspiciously complex tenders compared with others in the field, tender modifications leading to bigger contracts, inaccessible tender documents, and very few bidders in highly competitive markets.

The flags were then weighted to determine a risk ranking for each contractor or firm. In a proof-of-concept conducted using data from Hungary, Slovakia, and the Czech Republic, the research team found that firms with a higher CRI score made more money than firms with lower CRIs, and were also more likely to have politicians involved as either managers or owners and to be registered in tax havens.

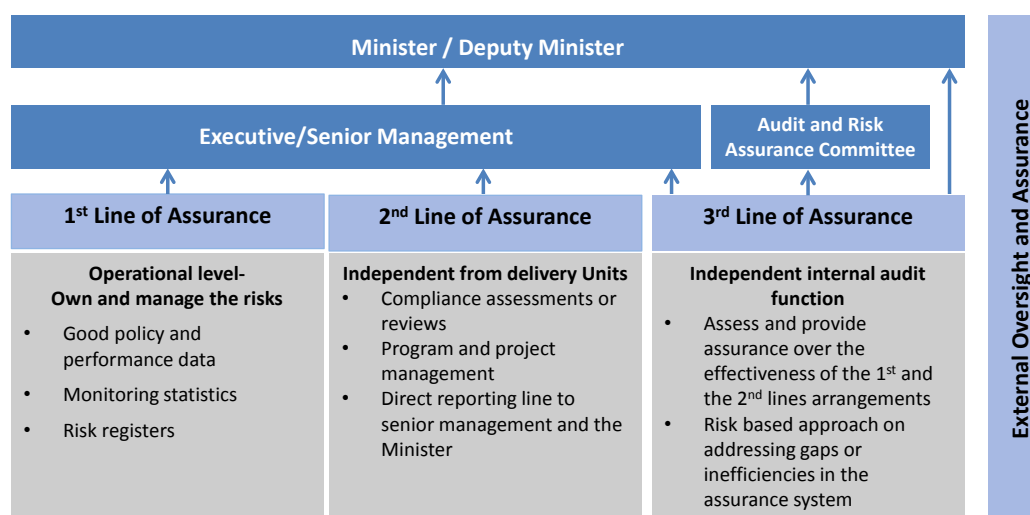
Source: (University of Cambridge, 2015_[20]).

Clarifying roles and improving co-ordination

IMSS could take steps to increase management ownership of the internal control system and risk management policies and processes, including targeted trainings and messaging for procurement officials.

SFP's standards emphasise the importance of internal control and risk management, placing responsibility squarely on managers of government entities (Mexico's Ministry of Public Administration, 2016_[21]). For instance, MECI calls for a specific corruption risk management function within government institutions as part of its risk management efforts. It also requires managers to develop a programme and policy to promote integrity and corruption prevention, involving training, disseminating a code of ethics and conduct, and whistleblowing mechanisms. These reforms are in line with international standards, and reflect the principles and practices outlined by the Institute of Internal Auditors, the Committee of the Sponsoring Organisation of the Treadway Commission (COSO) and others (Figure 7.5).

Figure 7.5. The three lines of assurance model



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.

IMSS has taken concrete measures to institutionalise the internal control system and risk management functions in line with SFP's SCII and IIA's three lines of defence. In IMSS, the contracting authority represents the first line of defence, while other units make up the second line of defence (e.g. the Change Management and Competition Unit). The OIC is the third line of defence. In addition, the MC has a sub-unit, called the Technical Coordination of Evaluation and Control (TCEC), which is entirely dedicated to improving IMSS's internal control system and risk management.

Among its many responsibilities, the TCEC designs strategies, practices and mechanisms for strengthening internal control and risk management, including following up on recommendations by OIC and the ASF. The TCEC plays the critical role of developing, implementing and evaluating the Internal Control Work Program and the PTAR. The TCEC, among other activities, is also responsible for promoting formalisation, standardisation and cross-cutting approaches, tools, methodologies and trainings for effective implementation of internal control and risk management in IMSS.

While IMSS has taken steps to institutionalise internal control and risk management as part of the overall management system, it could improve management's ownership of these functions, particularly those related to procurement processes. The challenges IMSS faces in strengthening management ownership are, in part, a function of existing policies and the structure of the internal control system in Mexico. This arrangement designates the SFP and the OICs with a mandate that blurs the division between the lines of defence. In particular, interviews with IMSS officials suggested that there is an over-reliance on the OIC to detect corruption and fraud. The omission of corruption and fraud risks in the risk matrix and PTAR further suggests the need for managers to take ownership of these functions.

In 2013, OECD reported that there is a perception within IMSS that the internal control and risk management functions, including those for preventing corruption, are the

responsibility of the OIC (OECD, 2013^[1]). To continue addressing this issue, IMSS could take steps to ensure that these functions are not seen as administrative or routine, but instead as a valuable exercise for advancing procurement objectives and broader institutional goals. Further defining and linking objectives and sub-objectives, as previously discussed, could help in encouraging ownership by management.

In addition, IMSS could develop targeted training dedicated to exploring and building knowledge about the first line of defence in the procurement process. The OECD has already recommended various communication strategies, awareness campaigns and training to promote management ownership (OECD, 2017^[6]); (OECD, 2013^[1]). Targeted training for procurement officials at both federal and state levels would help to tailor the messages so as to induce greater management ownership. These training courses could build on those carried out by the SFP, which offers courses for procurement officials on internal control and risk management. However, it is important that IMSS develops and leads its own training courses to further demonstrate that the OIC is not responsible for the internal control system. The following core messages and activities could be used in training or guidance to help create a culture of management ownership of the internal control system:

- **Making the business case for management ownership** – IMSS could improve its messaging for linking the internal control system to the success of the procurement cycle. Internal control activities are critical for the effectiveness and efficiency of procurement processes; without them, there is little assurance that goals and objectives have been accomplished. IMSS could convey the importance of internal control and risk management activities not only for preventing fraud and corruption, but also for ensuring that procurement processes are performing as expected.
- **Addressing the behavioural aspects required to induce change** – Management ownership has a strong behavioural component linked to individuals' beliefs, habits and motivations. IMSS could consider approaches for changing behaviours that first identify resistance to change, and that then develop strategies for overcoming any barriers. Change management models and "pull" strategies, such as those described in Box 7.6, could be used to encourage managers to take responsibility for the internal control system.
- **Demystifying and personalising the internal control and risk management functions** – Procurement officials may not actually realise that many of the assessments and checks they conduct are actually control activities. For instance, requiring quotes before purchasing equipment without a competitive bidding, while a common procurement procedure, is effectively a control to minimise risks of over-spending and to promote cost-consciousness. By identifying and defining officials' existing contributions to the internal control system, IMSS can reframe staff's perceptions about their daily contributions to an effective internal control system. This could also help to reinforce the notion that the OIC is not responsible for control activities or risk management.

Box 7.6. Change management paradigms to strengthen management ownership of an internal control system

Various factors can undermine the effective implementation of internal control and risk management, including institutional legacies, failure to understand complexity and a lack of leadership support. Institutionalisation also has a strong behavioural component involving the beliefs, habits and motivations of individuals. Common behavioural elements when faced with change include (Stoop, 2016^[21]):

- feeling threatened by change, as a result of consequences on power structures, prestige, individual opportunities, or careers
- a lack of understanding of the need for change or the implications of the change
- not having confidence in the promoters of change.

There are myriad change management models that could be applied to improving management ownership, and ultimately the internal control and risk management functions. For instance, in the 1950s, renowned psychologist Kurt Lewin suggested that effective change requires successful completion of a three-step process of “unfreezing” the existing behaviour, moving to a new level and “refreezing” at the new level (Hayes, 2014^[22]). Over the years, the process has evolved in different contexts to include concrete activities for each step. Lewin’s theory argues that “pull” strategies, whereby restraining forces are removed to strengthen a culture of integrity, are more effective than “push” strategies (i.e. outside pressure for change), because they are more likely to increase commitment and result in permanent change (Hayes, 2014^[22]).

Another pre-eminent change management model, developed by Harvard University Professor John Kotter, employs an eight-step process (Kotter, 1996^[23]):

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change

Other change theory models exist that can help entities to address these issues, and understand “where they are” and “where they want to go” with regards to management ownership and building a culture of integrity. One of the benefits of applying change management paradigms is that they can be flexible enough to be tailored to the individual contexts of institutions. They also are based on the notion that change is not an end state that can be reached through programmed steps, but rather an ongoing process (Paton and McCalman, 2008^[24]). Within IMSS, change management can help to bridge theory, as defined in new standards and guidelines, with practice. It also provides insights on how to manage resistance to change, which could include the following techniques (adapted from (Stoop, 2016^[21])):

- demonstrate that the status quo cannot be maintained and why
- collect information concerns and rationale for the current situation, and provide factual responses

- understand and use resistance to change for making improvements
- engage those who are promoting change
- create new perspectives that are sustainable, rooted in the medium and long-term, not only the short term.

Source: (OECD, 2017^[25])

IMSS and the OIC could take steps to clarify the roles and responsibilities for risk management and the internal control system. This could include auditor's statements of independence.

The OIC's basic structure consists of the Head of the OIC, the Responsibilities Head, the Auditing Head and the Complaints Head. Even though the OIC operates as IMSS's internal audit unit, it reports directly to SFP, not to the IMSS General Director. In 2013, the OECD recommended that IMSS establish an internal control committee in line with the SCII, which suggests that entities create an Institutional Development and Control Committee (*Comité de Control y Desempeño Institucional*, or COCODI) to monitor the implementation of the internal control system (OECD, 2013^[1]). As this is not a requirement, IMSS decided not to set up a COCODI.

OIC's presence in IMSS is organised into six areas: i) Audit for the Development and Improvement of Public Management (*Auditoría para Desarrollo y Mejora de la Gestión Pública*); ii) Internal Audit (*Auditoría Interna*); iii) Responsibilities (*Área de Responsabilidades*); iv) Complaints (*Área de Quejas*); v) Special Contingency Audit for Medical Services (*Auditoría Conatención Especial A Servicios Médicos*); and vi) Regional Co-ordination (*Coordinación de Vinculación Operativa*) (IMSS, 2017^[26]). Two of these areas (Internal Audit and Special Contingency Audit for Medical Services) conduct audits across IMSS, including procurement, construction, cross-cutting and revenue audits. In addition to the OIC areas, delegates and incumbent public commissioners (DC) contribute to monitoring and control within IMSS.

According to officials, the recent anti-corruption reforms have not led to specific changes in the internal audit functions, but the division of labour between the various entities responsible for audit has been clarified in order to ensure proper implementation, including by contracting authorities. Nonetheless, existing manuals, OIC training activities, as well as IMSS's and OIC's responses to the OECD's questions during this review suggest the need for further clarification of the roles and responsibilities in the internal control system. For instance, OIC's *Manual of Organization of the Internal Control Body for IMSS* notes that the Audit for the Development and Improvement of Public Management is responsible for "carrying out the risk assessment that may hinder the achievement of the goals and objectives of the Mexican Social Security Institute." As noted in Figure 7.6 below, international standards suggest that entities responsible for auditing should, at most, facilitate the identification and evaluation of risks. To preserve their independence, audit entities should avoid designing or implementing processes that could be the subject of audits. Segregated responsibilities from management, clear and formally defined responsibilities and working in an unbiased way, are all key elements of international standards for preserving the independence of audit entities (INTOSAI, 2010^[27]; INTOSAI, 2010^[28]).

While other divisions in IMSS have the responsibility for risk management and conducting risk assessments, statements such as those found in the OIC's manual raise

questions as to the extent and appropriateness of the OIC's involvement in conducting risk assessments. In addition, such manuals are communication tools for both IMSS and the OIC. Therefore, care should be taken to clearly define OIC's roles vis-à-vis other entities within IMSS with responsibilities for risk management and internal controls. IMSS and the OIC may find IIA guidance instructive for assessing and clarifying internal audit roles in IMSS's risk management activities (Figure 7.6).

Figure 7.6. The role of internal audit in risk management

Core internal audit roles with regards to enterprise risk management (ERM)	Giving assurance on the risk management process
	Giving assurance that risks are correctly evaluated
	Evaluating risk management processes
	Evaluating the reporting of key risks
	Reviewing the management of key risks
Legitimate internal audit roles with safeguards	Facilitating identification and evaluation of risks
	Coaching management in responding to risks
	Coordinating ERM activities
	Consolidating reporting on risks
	Maintaining and developing the ERM framework
Roles internal audit should not undertake	Championing the establishment of ERM
	Setting the risk appetite
	Imposing risk management processes
	Management assurance on risks
	Taking decisions on risk responses
	Implementing risk responses on management's behalf
	Accountability for risk management

Source: Adapted from (The Institute of Internal Auditors, 2009^[29])

Responses from IMSS and OIC officials to the OECD's questionnaire further suggest the need to ensure clear roles and responsibilities of actors in the internal control system. For example, officials said the OICs are in charge of implementing the governmental control and evaluation system. This perception of the OICs' role threatens to undermine management ownership of the internal control system, as well as the OIC's own efforts to institutionalise responsibilities for managing risks within IMSS, including procurement officials.

The OIC should further clarify its roles and responsibilities in its manual, guidance and trainings. Without this clarification, IMSS and the OIC could blur the lines between the three lines of defence, described above, and create duplicative, overlapping and fragmented internal control and risk management activities. Moreover, potential independence issues arise in the absence of clear roles and responsibilities between

operational teams and the internal audit function, as defined by international standards. For instance, the OIC carries out a number of training courses for procurement officials, including a course called the "Importance of the promotion of good practices in public contracting for improvement of public management". When conducting such courses, the OIC should avoid prescriptive guidance on how to implement internal control and risk management activities, so it is not in a position where it is auditing the very policies and practices it helped to design. To further protect the OIC from threats to its audit independence, the OIC could consider implementing internal auditor statements of independence.

The SFP/OICs and ASF could strengthen collaboration in order to more effectively provide coherent oversight over IMSS procurement processes.

In 2017, the OECD reported on the different models for internal control and risk management produced by the SFP and Mexico's supreme audit institution, *Auditoría Superior de la Federación* (ASF) (OECD, 2017^[25]). As noted, the SFP developed its own internal control and risk management framework called the System of Institutional Internal Control (SCII), accompanied by a risk management tool (*Administración de Riesgos Institucionales*, or ARI) and guidance for the OICs. In addition, in 2014, ASF developed the Integrated Framework for Internal Control in the Public Sector (*Marco Integrado de Control Interno en el Sector Público*, or MICI), as well as the Automated System for Risk Management (*Sistema Automatizado para la Administración de Riesgos*, or SAAR), which is an electronic platform accompanied by two self-assessment guides to aid practitioners in managing risks.

In 2017, OECD recommended further harmonisation of these standards developed by the SFP and Mexico's supreme audit institution, recognising the potential to cause confusion among auditors and auditees, and leaving government entities more vulnerable to fraud, waste and abuse (OECD, 2017^[30]). SFP and ASF officials confirmed that two separate models were being used when auditing IMSS's activities, citing a lack of co-ordination between these internal and external audit entities.

Co-ordination between SFP and ASF has a number of benefits, including reduced risks of fragmentation, overlap and duplication, as well as better coherence between audit findings (e.g. avoiding contradictory recommendations and findings). Effective internal and external audit co-operation, including information sharing, can also reduce the audit work of the respective entities. A joint study by the European Organisation of Supreme Audit Institutions and the European Confederation of Institutes of Internal Auditing offers insights into how external and internal audit entities can strengthen co-ordination (Box 7.7)

Box 7.7. The International Organisation of Supreme Audit Institutions' guidelines for internal control standards for the public sector

In 2014, the European Organisation of Supreme Audit Institutions (EUROSAI) and the European Confederation of Institutes of Internal Auditing (ECIIA) jointly published a study that explored the mechanisms and challenges for co-operation and co-ordination between external and internal audit entities. The report presented results from a survey of 25 supreme audit institutions (SAIs) and 42 public sector entities, all members of the ECIIA responsible for the internal audit function.

The report showed that most of the SAIs surveyed align with international standards regarding co-ordination and co-operation with internal audit institutions. Most of them refer to the International Standards for Supreme Audit Institutions (ISSAIs), International Standards on Auditing (ISA) and INTOSAI's GOV standards, such as ISSAI 1610, ISA 610, INTOSAI GOV 9140 and INTOSAI GOV 9150. Only a minority of SAIs surveyed have explicit, written internal rules, such as auditing manuals, standards, guidance, procedures or checklists, documenting and formalising the co-ordination and co-operation channels.

Co-ordination and co-operation between SAIs and internal auditors was often described as "informal", which can make it difficult to assess or ensure the quality of co-ordination. The most common benefits of co-operation and co-ordination cited include:

- promoting good governance by exchange of ideas and knowledge
- more effective and efficient audits based on a clearer understanding of the respective audit roles with better co-ordinated internal and external audit activity resulting from co-ordinated planning and communication
- refined audit scope for SAIs and internal auditors.

However, almost half of the responding SAIs stated they experience risks or identify potential risks in relation to co-ordination and co-operation. A majority of SAIs pursued co-ordination and co-operation largely in the following areas:

- evaluating the audited entity's internal control framework and risk-management arrangements
- evaluating the entity's compliance with laws and regulations
- documenting the entity's systems and operational processes.

Source: (EUROSAI and ECIIA, 2014^[31]).

One key area where ASF and SFP could improve co-ordination is early in the audit programming and planning processes. Both the SFP and ASF have their own sets of criteria for risk-based audit programming related to the procurement cycle. The risk criteria include the volume of procurement, performance indicators, reports in the media and complaints from suppliers, among others. Co-ordinating early and refining these criteria could help ASF and SFP to ensure effective coverage of the audit universe, avoid duplicating efforts and identify complementary audit subjects. In addition, audit entities can be effective inducers of change through their recommendations and audit findings. With better co-ordination between ASF and SFP, and using each other's work as inputs for programming and planning, IMSS is more likely to benefit from audit work to address

the issues described above. This could include improving management ownership of internal control systems in the procurement process, and better management of risks in the procurement cycle.

Proposals for action

Within IMSS, various stakeholders contribute to the design and implementation of an effective internal control system. This chapter has explored the activities involving IMSS staff, the OIC and the ASF, covering four lines of defence (including external audit). The first set of recommendations focus on strategic initiatives for IMSS, followed by other recommendations to improve the tools and culture of risk management. Finally, the OIC and ASF also have opportunities to improve internal control and risk management to enhance IMSS's procurement processes:

Ensuring effective risk management strategies and implementation:

- Improve IMSS's risk management strategy for public procurement by clearly defining its goals and objectives, particularly those related to fraud and corruption.
- Emphasise messages that focus on integrity values as opposed to rules to complement efforts to create a culture of integrity.
- Develop IMSS's strategy and activities for more systematically monitoring and evaluating the effectiveness of the internal control system and risk management activities.

Improving IMSS's risk assessments related to public procurement:

- Sharpen the focus on corruption and fraud, as well as other strategic and operational risks that can affect the entire procurement cycle.
- Further define risk tolerances to more effectively allocate resources and determine control activities.
- Improve IMSS's guidance and tools for conducting risk assessments related to procurement and advancing new forms of analyses on tenders and processes.

Clarifying roles and improving co-ordination:

- Increase management ownership of the internal control system and risk management policies and processes, including organising targeted trainings and messaging for IMSS's procurement officials.
- Clarify the roles and responsibilities among the SFP, IMSS's OIC and the ASF for risk management and the internal control system, potentially including auditors' statements of independence.
- Strengthen collaboration among SFP/OICs and ASF in order to more effectively provide coherent oversight over IMSS's procurement processes.

References

- Australia National Audit Office (2012), *Developing and Managing Contracts: Getting the right outcome, achieving value for Money*, Commonwealth of Australia 2012, <http://www.anao.gov.au>. [19]
- CMS (2016), “CMS Strategy: The Road Forward 2013-2017”, <https://www.nadona.org/wp-content/uploads/2016/05/CMS-Strategy.pdf> (accessed on 14 November 2017). [8]
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013), *Internal control-integrated framework*. [9]
- EUROSAI and ECIIA (2014), “Coordination and Cooperation between Supreme Audit Institutions and Internal Auditors in the Public Sector”, http://www.eciia.eu/wp-content/uploads/2014/05/EUROSAI_ECIIA_Joint_Paper_05052014.pdf. [31]
- Government Accountability Office (2015), *A Framework for Managing Fraud Risks in Federal Programs*, <http://www.gao.gov/assets/680/671664.pdf>. [17]
- Hayes, J. (2014), *The theory and practice of change management*, Palgrave, United Kingdom, <https://he.palgrave.com/page/detail/The-Theory-and-Practice-of-Change-Management/?K=9781137275349#>. [22]
- IMSS (2016), *Norm that establishes the dispositions for the implementation and maintenance of the institutional model for competitiveness*, [Norma que establece las disposiciones para la implementacion y mantenimiento del modelo insticucional para la competividad], 1000-001-003, http://www.imss.gob.mx/sites/all/statics/pdf/manualesynormas/1000-001-016_0.pdf. [3]
- IMSS (2017), *Organisational manual of the directorate of administration*, [Manual de organización de la dirección de administración], 1000-002-001, validated 22 June 2017, http://www.imss.gob.mx/sites/all/statics/pdf/manualesynormas/1000-002-001_1.pdf (accessed on 15 November 2017). [11]
- IMSS (2017), *Risk matrix and working programme of risk management*, [Programa de trabajo de administracion de riesgos]. [5]
- IMSS (2017), *Manual of organization of the internal control body*, [Manual de organización del órgano interno de control en IMSS], 0900-002-001, validated 2 February 2017. [26]
- INTOSAI (2010), *INTOSAI GOV 9100 – Guidelines for Internal Control Standards for the Public Sector*, <http://www.intosai.org/issai-executive-summaries/view/article/intosai-gov-9100-guidelines-for-internal-control-standards-for-the-public-sector.html> (accessed on 22 November 2017). [27]
- INTOSAI (2010), *INTOSAI GOV 9140 – Internal Audit Independence in the Public Sector*, <http://www.intosai.org/issai-executive-summaries/view/article/intosai-gov-9140-internal-audit-independence-in-the-public-sector.html> (accessed on 22 November 2017). [28]
- Irish Health Service Executive (2009), *Developing and Populating a Risk Register Best Practice Guidance*, http://hse.ie/eng/About/Who/OQR010_20090422_v_11Developing_and_populating_a_Risk_Register_BPG.pdf. [7]
- ISO (2009), *ISO 31000:2009 - Risk management -- Principles and guidelines*, <https://www.iso.org/standard/43170.html> (accessed on 14 November 2017). [12]

- ISO (2009), *ISO 31000 Risk management*, <https://www.iso.org/standard/43170.html>. [13]
- Kotter, J. (1996), *Leading Change*. [23]
- Mexico's Ministry of Public Administration (2016), *Agreement on 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"), <https://www.gob.mx/cms/uploads/attachment/file/174036/acuerdo-disposiciones-manual-CI.pdf> (accessed on 14 November 2017). [2]
- OECD (2009), *OECD Guidelines for Fighting Bid Rigging in Public Procurement: Helping governments to obtain the best value for money*, <https://www.oecd.org/competition/cartels/42851044.pdf>. [15]
- OECD (2012), *Session III Improving Effective Public Procurement: Fighting Collusion and Corruption*, [https://one.oecd.org/document/DAF/COMP/LACF\(2012\)15/en/pdf](https://one.oecd.org/document/DAF/COMP/LACF(2012)15/en/pdf) (accessed on 14 November 2017). [16]
- OECD (2013), *Public Procurement Review of the Mexican Institute of Social Security: Enhancing Efficiency and Integrity for Better Health Care*, OECD Public Governance Reviews, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264197480-en>. [1]
- OECD (2015), *OECD Recommendation of the Council on Public Procurement*, <http://www.oecd.org/gov/ethics/OECD-Recommendation-on-Public-Procurement.pdf>. [10]
- OECD (2016), *Preventing Corruption in Public Procurement*, <http://www.oecd.org/gov/ethics/Corruption-in-Public-Procurement-Brochure.pdf>. [14]
- OECD (2017), *Brazil's Federal Court of Accounts: Insight and Foresight for Better Governance*, OECD Public Governance Reviews, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264279247-en>. [25]
- OECD (2017), *OECD Integrity Review of Mexico: Taking a Stronger Stance Against Corruption*, OECD Public Governance Reviews, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264273207-en>. [6]
- OECD (2017), *Mexico's National Auditing System: Strengthening Accountable Governance*, OECD Public Governance Reviews, OECD Publishing, Paris, <http://dx.doi.org/10.1787/9789264264748-en>. [30]
- Paton, R. and J. McCalman (2008), *Change Management: A Guide to Effective Implementation, Third Edition*, SAGE Publications, London. [24]
- Stoop, P. (2016), *Concepts for facilitating and managing change: challenges in institutional and organisational development, with respect to the processes of regionalisation of a Supreme Audit Institution, presentation*. [21]
- The Institute of Internal Auditors (2009), "IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management", <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf> (accessed on 14 November 2017). [29]
- UK HM Treasury (2006), *Thinking about risk - Managing your risk appetite: A practitioner's guide, November 2006*, http://webarchive.nationalarchives.gov.uk/20130107005526/http://www.hm-treasury.gov.uk/d/tar_practitioners_guide.pdf (accessed on 14 November 2017). [18]

- University of Cambridge (2015), *Mining for Corruption*, [20]
<https://www.cam.ac.uk/research/features/mining-for-corruption> (accessed on 26 October 2017).
- Wright, R. (2013), *The Internal Auditor's Guide to Risk Assessment*, The Institute of Internal [4]
Auditors Research Foundation, Altamonte Springs, FL..



From:

Second Public Procurement Review of the Mexican Institute of Social Security (IMSS)

Reshaping Strategies for Better Healthcare

Access the complete publication at:

<https://doi.org/10.1787/9789264190191-en>

Please cite this chapter as:

OECD (2018), "Safeguarding integrity and managing risks in IMSS procurement", in *Second Public Procurement Review of the Mexican Institute of Social Security (IMSS): Reshaping Strategies for Better Healthcare*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/9789264190191-10-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.

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.