Risk Management and Internal Control System of Deposit Insurers

Guidance Paper

November 2020

International Association of Deposit Insurers
C/O BANK FOR INTERNATIONAL SETTLEMENTS
CENTRALBAHNPLATZ 2, CH-4002 BASEL, SWITZERLAND
TEL: +41 61 280 9933 FAX: + 41 61 280 9554
WWW.IADI.ORG

Table of Contents

List of Boxes

List of Tables

List of Figures

List of Charts

Abbreviations

COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPs	IADI Core Principles for Effective Deposit Insurance Systems (also Core Principles)
DGS	Deposit Guarantee Scheme
DI	Deposit Insurer
DIF	Deposit Insurance Fund
EBA	European Banking Authority
EC	Essential Criteria
ERM	Enterprise Risk Management
IADI	International Association of Deposit Insurers
IIA	The Institute of Internal Auditors
ICS	Internal Control System
IMF	International Monetary Fund
ISO	International Organization for Standardization
RM	Risk Management
RMICSTC	Risk Management and Internal Control System Technical Committee

Key Terms

Contingency plans: the process through which an institution outlines policies, procedures and actions that it might follow in the event of unexpected developments or significant shocks and to manage a range of stress scenarios. 'Plan B.'

Enterprise Risk Management (ERM): "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004).

Governing bodies: the Board of Directors, the Supervisory Board and the Executive Board.

*Internal auditing: "*an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes" (IIA, 2019).

*Internal control: "*a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" with applicable laws and regulations (COSO, 2013).

Mandate: the set of official, jurisdiction-specific laws and/or regulations prescribing a DI's roles and responsibilities. Mandates can range from narrow to more extensive functions and responsibilities, such as preventive action and loss or risk minimisation/management, and a variety of combinations in between. These can be broadly classified into four categories (IADI Glossary):

- A "Paybox" mandate, where the deposit insurer (DI) is only responsible for the reimbursement of insured deposits;
- A "Paybox plus" mandate, where the DI has additional responsibilities, such as certain resolution functions (e.g. financial support);
- A "Loss Minimiser" mandate, where the DI actively engages in a selection from a range of least-cost resolution strategies; and
- A "Risk Minimiser" mandate, where the insurer has comprehensive risk minimisation functions that include risk assessment/management, a full suite of early intervention and resolution powers and, in some cases, prudential oversight responsibilities.

Mapping process: a process documenting all internal operational activities/processes of a DI. It follows a step-by-step analysis, identifying the responsible areas, execution timelines, inputs and outputs, risks that may occur, descriptions of existing controls and other relevant information.

Resolution: the "disposition plan and process for a non-viable bank. Resolution may include: liquidation and depositor reimbursement, transfer and/or sale of assets and liabilities, the establishment of a temporary bridge institution and the write-down or conversion of debt to equity. Resolution may also include the application of procedures under insolvency law to parts of an entity in resolution, in conjunction with the exercise of resolution powers" (IADI Glossary).

*Resolution authority: "*a public authority that, either alone or together with other authorities, is responsible for the resolution of financial institutions established in its jurisdiction, including resolution planning functions" (IADI Glossary).

Risk: the possibility that an uncertain event could occur and affect the achievement of the organisation's objectives. Uncertainty can impact on organisational objectives either positively (positive risk - opportunities) or negatively (negative risk - threats).

DI risks:

Bank failure risk: the risk that a bank fails, so that the DI has to intervene for the reimbursement of protected deposits and, depending on the mandate, other forms of intervention;

Credit risk: the amount of potential losses attributable to counterparties failing to honour their obligations towards the DI;

Currency risk: potential losses due to adverse movements in exchange rates;

Funding risk: the amount of the potential gap, if any, between the DI's funds available for interventions and the funds required for the interventions;

Interest rate risk: potential losses on the balance sheet value, due to adverse movements in interest rates on assets and liabilities, affecting future earnings and cash flows;

IT and information security risk: risks associated with the use of information systems. It involves identifying, assessing, and managing risks to the confidentiality, integrity and availability of an organisation's assets to comply with relevant legal and regulatory regimes. It also includes cyber-attack risk. These kinds of risk may be included under operational risk;

Legal risk: the risk of loss primarily caused by (1) a failed transaction, or (2) a claim being made or some other event occurring which results in a liability for the institution or other loss, or (3) taking measures to protect assets (for example, intellectual property) owned by the institution, or (4) a change in laws, or more general (5) failing to act in accordance with laws/regulations and internal policies/by-laws (compliance risk);

Liquidity risk: the risk that a DI suffers a loss as a result of having to hastily convert assets into cash to meet its funding needs or the risk that the DI cannot convert its assets quickly enough;

Market risk: the amount of potential losses attributable to adverse changes in the values of financial instruments and other investments or assets owned (directly or indirectly) by the DI, whether on or off-balance sheet, as a result of changes in market rates (such as interest rates and foreign exchange rates) or prices;

Operational risk: potential losses resulting from inadequate or failed internal processes, people and systems or from external events; it also includes legal risk;

Reporting risk: risk associated with accuracy and timeliness of information that is needed inside the DI to support decision-making processes and performance evaluation and, at the same time, outside the organisation to comply with standards, regulations, and stakeholder expectations;

Reputational risk: the risk of an event significantly affecting trust and confidence in a DI, and which could result in financial and other losses;

Strategic risk: current or prospective risk to earnings and capital arising from business and market changes and from adverse business decisions, incorrect implementation of decisions or lack of responsiveness to changes in the business environment.

Risk appetite: the amount of risk an organisation is willing to accept in pursuit of its mandate. It is established by an organisation's board and serves as a guidepost for setting strategy, goals and objectives.

*Risk appetite framework: "*the overall approach, including policies, processes, controls, and systems through which risk appetite is established, communicated, and monitored. It includes a risk appetite statement, risk limits [and risk tolerance], and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the risk appetite framework" (FSB, 2013).

Risk culture: the values, beliefs, knowledge and understanding about risk shared within an organisation with a common purpose.

Risk limit: quantitative measures that allocate the DI risk appetite statement (e.g. measure of loss or negative events) to DI "business lines, legal entities as relevant, specific risk categories, concentrations, and as appropriate, other levels" (FSB, 2013).

Risk management (RM): the set of rules, systems, methodologies and procedures aimed at identifying, assessing, managing, monitoring and reporting risks.

Risk tolerance: the risk variation the DI is willing to tolerate around specific objectives.

Risk treatment: the response activity to risk: (i) Reduce; ii) Accept; iii) Avoid; iv) Transfer.

Stress test: the exercise aimed at assessing the impact of plausible adverse scenarios on the financial and operational capacities of a DI.

Three Lines of Defence: the three groups (or lines) involved in effective risk management:

- First Line: functions/roles that own and manage risks, developed by the business management units. Functions that own and manage risks are represented by people whose activities generate the risks through their responsibilities.
- Second Line: functions/roles specialised in risk management/compliance. It challenges the first line on control of risks and facilitates risk monitoring and reporting.
- Third Line: functions that provide independent assurance to senior management and the board on the effectiveness of both first and second lines' efforts in managing risk. Internal audit acts as the third line of defence.

Executive Summary

Study on risk in economies is not new. Risk management theory and practices have developed over time under the pressure of rapid environmental changes and to address perceived gaps and weaknesses in corporate governance and controls. From the 90s the inclusion of risk management in regulation or self-regulation (i.e. Basel Committee Capital Regulation or Corporate Governance Code for Listed Companies) further underpinned the importance of risk awareness and management.

Generally speaking, 'risk management' refers to the process of identifying and assessing risks to which an entity can be exposed, with the aim of finding ways to manage them and improve the entity's ability to meet its objectives.

Notions and approaches of risk management have evolved over time. In the early stages of development, risk management was interpreted as a specific organisational function fully devoted to the identification and assessment of risks with little or no cross-cutting with the other functions and the board. But with the increasing complexity of the financial environment, risk management has rapidly morphed into a more integrated risk management awareness and modelling leading to the current configuration of 'Enterprise Risk Management' (ERM).

As with any other organisation, a DI faces different types of risk in the fulfilment of its mandate, stemming from its operational and financial activities. The DI, therefore, must know how to deal with these risks to successfully achieve its mandate. Given the role of the DI in the financial safety-net, risk management is increasing in importance and plays a key role in the performance of the DI's functions. This awareness prompted IADI to research these topics in previous years. It published two papers, directly and indirectly related to risk management.

In order to update the previous work, IADI decided to constitute a Technical Committee (The Risk Management and Internal Control System Technical Committee – RMICSTC) to investigate by means of an extended survey the most recent experience and practice among IADI Members. The goal of this paper is to set out guidance on risk management in DIs. No Core Principle (CP) specifically covers the risk management of DIs. There is an indirect reference to this topic in CP3, which emphasises that a DI must be efficiently governed. In application of this principle, Essential Criterion (EC) 4 of CP3 highlights the importance of sound governance and internal controls. The RMICSTC considered risk management to be an essential tool to achieve this goal. Furthermore, CP6 stresses the importance for a DI to have in place contingency planning, a component of overall risk management.

The RMICSTC's first step was to review the most well-known international standards of risk management applicable to all organisations. These standards would also be good practice for DIs. They are a useful conceptual guide for the general design of the risk management framework in a DI. However, their application should not be applied mechanically but adapted and fitted to the particular role of a DI mandate, size, complexity and budget limitations.

The RMICSTC designed a questionnaire and a case study template, also taking inspiration from the international standards. The aim was to collect a broad body of data on DI experience and practice of risk management. The survey was launched and a questionnaire sent to all IADI Members in September 2018. A total of 58 members (out of 83) responded. In addition, a number of focused case studies were considered, regarding 6 members, while 5 members provided supplementary in-depth documents on aspects of their risk management framework.

Analysing the empirical data was crucial for the purpose of this paper. The RMICSTC could get a picture of *if* and *how* DIs manage risk, the practices employed, policies and approaches set and followed, and the range of maturity level of the risk management frameworks in place. Furthermore, the data collected enabled a benchmark tool to be set up, with which a DI can compare itself against its peers.

The majority of DIs examined (85%) showed they have risk management in place, some with a formal and some an informal organisational structure. There was significant variation among members.

Not surprisingly, DIs with a broader mandate (risk minimisers) have very advanced risk management models. It was a similar profile for loss minimisers, albeit less formalised and structured. Paybox DIs were generally less advanced though some did reveal they exercised well-developed risk management models. Paybox Plus DIs were very varied in size and framework maturity and difficult to aggregate.

The exercise allowed the Technical Committee to set a number of guidance points on risk management for deposit insurance. The RMICSTC's main challenge was to combine established international standards into DIs' environment, in all its variety, and to come up with a table of guidance points that could be applied, without impeding DIs' flexibility and operational usefulness. The Guidance Points list the essential risk management functions a DI should have in place, with regards to its size, mandate, influence and other features of its activity.

The Guidance Points are based on the principle of proportionality since the intention is not to identify a maximum target for each individual DI, but rather a 'minimum requirement'. The level of development or maturity of the framework will then depend on the specific features of each DI.

The Guidance Points consist of a set of recommendations for the following areas of risk management: i) Governance, ii) Risk Management Process and Internal Control System, iii) Communication and Reporting, and iv) Monitoring and Improvement (Fig. 5).

The paper provides a starting point for further research involving an in-depth analysis of specific technical aspects of the risk management framework and internal control system. Handbooks or 'How to Apply' tools may also be useful to IADI Members. Finally, the RMICSTC deems the Guidance Points suitable for potential integration into the IADI CPs.

Guidance Points

The Guidance Points are the following:

- **Governance:**

1. DIs should have in place a risk management framework and an internal control system that allows them to identify, assess, manage, respond, control and report risks that could affect their ability to fulfil their mandate and achieve the public policy objectives of deposit insurance. The risk management framework and internal control system should be tailored and proportionate to the size, mandate and operational complexity of the DI. DIs should balance the costs and effectiveness of the risk management framework and internal control system.

2. The DIs' governing bodies should promote risk culture at all levels of the organisation, approve the organisational risk management policy and risk appetite, and provide appropriate resources. They should be responsible for the oversight of the risk management framework and internal control system and be assured on the adequacy and effectiveness of implementation of the framework.

3. DIs' senior management should be responsible for the design, implementation and update of the risk management framework and internal control system with the oversight of the board and other competent governing bodies. It should report periodically to the governing bodies on the risk findings and control measures.

- **Risk Management Process and Internal Control System:**

4. To promote effective risk management, DIs should ensure that all employees whose daily operations pose potential risks to the DIs are aware that they have the responsibility for identifying, assessing and responding to the risks.

5. In order to ensure that clear roles and responsibilities assigned to their governing bodies, senior management and employees involved in risk management and the internal control system, small DIs with narrow mandates should have, at least, functions or activities with appropriate rules and documented procedures, while large DIs with broad mandates should have in place a formal risk management framework and internal control system within the organisation.

6. DIs should map their operational processes and identify and measure the most significant risks embedded in their activities. Depending on their mandate, DIs should consider a broader set of risks including, at a minimum, bank failure, financial (funding and liquidity), legal, operational, IT and information security, and reputational risks.

7. DIs should have adequate tools to assess the likelihood and impact of risks and to prioritise them. DIs should have a clear understanding of the types of risk response and where further action is required to mitigate risks, and have clearly defined action plans in place. This includes contingency plans, such as business continuity and disaster recovery plans, and funding contingency plans.

8. DIs should provide an independent assurance to the governing bodies that risks are adequately identified, controls are appropriately implemented and mitigation plans are achieved. DIs that are larger in size, and have a wider mandate and higher complexity, may consider implementing the Three Lines Model approach.

- **Communication and Reporting:**

9. DIs should have in place risk reporting processes that allow for communication of risk information across all levels of the organisation.

- **Monitoring and Improvement:**

10. The risk management framework and internal control system should be monitored and reviewed periodically to ensure their adaptation to changes in the internal and external environment.

I. Introduction

All organisations, DIs included, are exposed to risks. The possibility that uncertain future events could occur and affect the achievement of the organisation's objectives is traditionally defined as a risk. Risk can also be interpreted in different ways: only negatively (negative risk - threats) or both negatively and positively (positive risk - opportunities).

The complexity of socio-economic contexts, subject to continuous and rapid change, has increased the number and interrelationships of risks to which organisations are exposed. Proper and effective risk management, therefore, has become over time an essential factor to ensure that an organisation can fulfil its mandate and meet its objectives.

Studies on risk in economies are not new (F.H. Knight, 1921). Risk management theory and practices have developed over the years. From the 90s, the inclusion of RM in regulation or self-regulation (i.e. Basel Committee Capital Regulation or Corporate Governance Code for Listed Companies) underpinned the importance of risk awareness and management in all organisations.

Generally speaking, 'risk management' refers to the process of identifying and assessing the risks to which an entity is exposed, with the aim of finding ways to deal with them in order to achieve the firm's objectives.

Notions and approaches of risk management have evolved over time. At a first stage, RM was interpreted as a specific organisational function fully devoted to the identification and assessment of risks with little or no coordination with the other functions and the board. Due to the increasing complexity of the economic context, this 'siloed' risk management approach has gradually given way to a more cross-cutting risk management philosophy. This evolution led to the current configuration of 'Enterprise Risk Management' (ERM).

ERM does not look at specific objectives concerning single functions or business areas, but considers the firm as a whole. Risk information is part of the management information that is an essential element of governance. It is an integral part of the risk culture[1] and of the strategy of the organisation.

As with any other organisation, a DI faces different types of risk in the fulfilment of its mandate, stemming from its operational and financial activities. In case of payout, for example, funding and operational risks, if not well managed, may affect the DI's capacity to reimburse insured deposits of a failed bank in the pre-defined timeframe. Legal and reputational risks may also arise.

The DI, therefore, must know how to deal with risks in order to pursue its mandate. Given the importance of the DI in the financial safety-net, risk management is growing in importance. It plays a key role in the conduct of a DI's functions.

As a general principle, the DI has to be fully aware of risks, future and incurred, and constantly monitor their evolution and possible consequences, and determine how to deal with them to enable effective decision-making. Absent or poor risk management could result in passive exposure to change and uncertainty, both of which could jeopardise the pursuit of its mandate.

Academic and practitioner literature on risk management for business and financial sectors and industries is copious. Nevertheless, there is surprisingly little research dealing with RM specifically for DIs. IADI already researched these topics, publishing two papers, directly or indirectly related to risk management.

The first paper to appear was "Organizational Risk Management for Deposit Insurers" (IADI, 2007). It was based on a survey/questionnaire to gather data on the risk management practices in six DIs, exploring the rationale and structure of the risk management framework (identification, assessment, management, monitoring and reporting of risk). A number of interesting findings on risk management emerged, such as that it has to reflect the size and complexity of operations and that it could be structured

[1] See the Key Terms.

to minimise excessive costs and reduce bureaucracy. This consideration can be seen as a seminal notion of the 'proportionality' principle.

Risk management also carries costs, both tangible (e.g. investment, hiring, defining and implementing procedures) and intangible (e.g. streamlining the decision-making process and operations). The design and implementation of risk management should be tailored to the DI's features, with due consideration of the cost-benefit balance.

The second IADI paper was "Governance of Deposit Insurance Systems" (IADI, 2009). It listed nine supporting guidance points on governance, many being still relevant for this study. It recommended that the DI should maintain a profile of desired skills for its senior executives and governing body based on competence and expertise (Guidance point 3); that the governing body should set the strategic direction of the deposit insurance system and monitor its progress (Guidance point 5); and that a deposit insurer should be transparent and disclose appropriate information on its activities, governance practices, structure and financial results (Guidance point 9).

In 2017, IADI decided to follow up its studies on risk management through an updated research project on this topic. The RMICSTC was established with members' experts. It began its work in March 2018.

The perimeters of the respective areas of risk management and internal control can be a somewhat grey area. They are two distinct concepts and have different focuses but, at the same time, are closely connected (BCBS, 2010).[2] Some use Internal Control System (ICS) as a broad umbrella covering risk management, compliance function and internal audit. Others consider risk management as a broad framework that incorporates internal controls.[3]

More generally, RM guarantees the capability to anticipate, prevent and overcome the obstacles in the way of the firm's objectives. The ICS is designed "to ensure that each key risk has a policy, process or other measure, as well as a control to ensure that such policy, process or other measure is being applied and works as intended" (BCBS, 2010, para. 70). Its main objectives are "efficiency and effectiveness of activities (performance objectives); reliability, completeness and timeliness of financial and management information (information objectives); and compliance with applicable laws and regulations (compliance objectives)" (BCBS, 1998, page 8). It is also recognised that internal control is not a one-off procedure or policy but rather a continuous one operating at all levels, all the time.[4]

The intention of this paper is to provide guidance for DIs wishing to establish a risk management framework and internal control system or to enhance those already in place. It aims at supporting the implementation of the IADI Core Principles with more detailed indications and recommendations, with particular reference to CP3, which highlights the importance for a DI to be well governed. Risk management helps to achieve this goal.[5] EC4 of CP3 further highlights the importance of sound

[2] BCBS (2010; page 25, footnote 23): "*The two terms are in fact closely related and where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each*".

[3] In this sense, COSO (2004, Foreword): "*Enterprise Risk Management – Integrated Framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process*".

[4] According to BCBS (1998, page 8), "*Internal control is a process effected by the board of directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank."*

[5] CP3: "*The deposit insurer should be operationally independent, well-governed, transparent, accountable, and insulated from external interference*".

governance and internal controls.[6] CP6 refers to the importance of having in place contingency plans (Plan B), essential in overall risk management.

The project updates the previous research. An extended survey of IADI Members' practices was carried out and a number of case studies requested, based on the significant diverse sample of selected DIs.

The Committee proceeded as follows. It first reviewed international standards. It recognised that standards apply to all organisations and, therefore, they also apply to DIs. Their application cannot be mechanical: they need to be adapted to the specific context of DIs, their operations, size, mandate and operational complexity. An aim is to avoid unnecessary complications and excessive costs. The RMICSTC designed the questionnaire and the case study template, also taking inspiration from international standards.

A total of 58 (out of 83) IADI Members responded to the survey. Six focused case studies were drafted and five members provided in-depth documents on some aspects of their risk management framework. Gathering empirical data was crucial for the purpose of this paper. The RMICSTC was able to get a picture of whether, and if so how, DIs manage risks; what practices were employed; what policies and approaches were set and followed; and, more generally, the range of maturity level of the risk management frameworks among IADI Members. Finally, based on the data collected, a risk management tool was set up with which a DI could self-benchmark its own risk management framework against its peers.

This allowed the RMICSTC to assess first if guidance points were necessary and then how to set their contents and scope. Based on the findings of the survey, a number of industry-specific guidance points on risk management for deposit insurance have been set. They represent the core risk management functions a DI should have in place, with reference to the size, mandate, and other features of the DI's activity. The principle of proportionality has been followed since the intention is not to identify a maximum target for each DI but rather the blueprint for a 'minimum requirement' for all DIs.

The paper takes a somewhat bird's-eye view, not entering into overly detailed aspects of the risk management framework and internal control system (e.g., risk assessment methodologies, detailed contents of policies and procedures). The writing style is intentionally simple and limits the use of technicalities. It also takes, where possible, an example-based approach, drawing from the experience of the most advanced members' approaches.

The paper aims to raise awareness of the topic and to highlight the fundamental principles to follow in designing and implementing a risk management framework and internal control system in a DI. In this view, the recipients of this paper are mainly those DIs having an early-stage risk management system or lacking such a framework or willing to enhance it. DIs with more advanced risk management frameworks may still benefit from this paper, as they may find points of interest and input to benchmark their practices. The paper is not intended to be a handbook.

The paper recommends further research that may regard in-depth analysis of specific technical aspects of the risk management framework and internal control system. Handbooks or 'How to Apply' tools may also be useful to IADI Members. Finally, the RMICSTC deems the Guidance Points suitable for potential integration into the IADI CPs.

The paper is structured as follows.

Section 2 points out the main reasons and rationale justifying the adoption of a risk management framework in a DI. Section 3 analyses the most important international standards on risk management. Section 4 presents the methodology and findings of the survey of practices among IADI Members and also the selected examples of good practice. It also presents a self-benchmarking risk management tool, based on the data collected. Section 5 concludes and provides the Guidance Points.

[6] "*The deposit insurer is well-governed and subject to sound governance practices, including appropriate accountability, internal controls, transparency and disclosure regimes. ...*".

The Annexes contain the lists of Technical Committee Members and participants in the research, survey statistics and the questionnaire.

II. Why Risk Management in Deposit Insurers?

Like any other organisation, DIs in carrying out their activities, are subject to uncertainty. Future events could negatively impact the DI causing losses and/or impeding it from achieving its targets and accomplishing its mandate.

Risks in DIs may have a different nature, size, complexity and manageability; some of them are specific to the DI's activities; others are common to any other organisation. The first category of risks depends on the DI's mandate.

There is, however, a minimum common denominator of risks for all DIs and of the subsequent risk management activities and objectives; it relates to the payout function, which is the common element of all DIs. Categories of risk expand with the breadth of the mandate.

So, if we consider a Paybox DI, we can identify risks affecting its core macro-processes: funding; investment of resources; Single Customer View (SCV)[7] files production and control; operational procedure for the reimbursement of deposits, payments to depositors, communications to depositors. Each of these macro-processes may be composed of various operational micro-processes, which entail different kinds of risk.

Therefore, there could be the risk that a DI's available funds are not sufficient for the interventions required (funding risk); or there could be the risk that a DI may suffer losses from the investment of its financial resources or from having to hastily convert assets into cash (to meet its funding needs), or the risk that the DI cannot convert its assets quickly enough (liquidity risk). Looking at operational processes, risks may arise from inadequate internal processes, people and systems (operational risks/IT risks) which could negatively impact on the procedures established for the reimbursement of depositors in a specific timeframe. Also, there can be strategic risks deriving from changes in the business environment (e.g. Political, Economic, Social, Technological, Legal and Environmental factors – PESTLE). These risks may interplay and impact significantly on confidence in the DI, which could result in reputational risk.

A sound and well-governed DI has to be aware that risk could lie latent in its operations. It should be vigilant in spotting, managing and controlling whatever arises, learning to assess the probability of an occurrence and/or how to mitigate the impact. The presence of a well-designed risk management framework and internal control system equips the DI to respond proactively to the unforeseen and potential surprises, by having in place a risk-based approach and appropriate information to enable more effective decision-making. Poor risk management or none at all, on the other hand, can seriously jeopardise its ability to pursue its mandate.

In today's financial environment, the DI is essential for a robust safety net and is crucial in preserving financial stability. DI mandate[8] varies across jurisdictions; there may be additional functions and responsibilities in terms of bank resolution and, in some cases, prudential supervision of banks. The broader the mandate, the larger the threats and the greater the need for policies, tools and procedures.

[7] SCV files are files containing individual depositor information necessary for the payout, including the aggregate amount of eligible deposits of every depositor.
[8] IADI classifies DI mandates into four groups: Paybox, Paybox Plus, Loss Minimiser, Risk Minimiser; see 'Key Terms'.

IADI Members, generally, recognise the importance of risk management and voluntarily include it in their governance system. The survey shows that 75% of respondents (37 out of 51 respondents with answers not mutually exclusive) declared that the introduction of their risk management was on a voluntary basis; 35% attributed its implementation to law/regulation.

Regulators seem to be increasingly stressing the importance of risk management for the DI. In Europe, for example, the European Banking Authority (EBA), following the European Deposit Guarantee Scheme Directive (DGSD, 2014/49/EU), published 'Guidelines on stress tests of deposit guarantee schemes' (EBA, 2016), setting out principles and methodologies for assessing the risk that the operational and funding capabilities of a DI might not be sufficient for depositor payout in the event of a bank failure.[9] They are aimed at helping designated authorities and DIs to increase the resilience of deposit insurance within the European Union.

III. The International Standards on Risk Management

The speed and evolving complexity of changing factors, internal and external, impacting the activities of organisations, negative knowns and unknowns, risk of varying intensity, has underpinned the expansion in studies on risk management. Pooling experiences, short-lived local crises and longer-term global ones pushed the need for recognised, agreed, overall standards that could be referred to for a broad outline of risk management that an individual organisation could put in place as a foundation on which to fine-tune its specific policy, strategy and practice.

Major international bodies specialising in risk management consequently drew up and published standards and/or guidance fit for most organisations and contexts, 'off the peg' as it were, not 'tailormade'. Among the international standards on risk management, the RMICSTC selected two of the best-known standards: the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management - Integrated Framework (ERM) and the International Organization for Standardization (ISO) Standard. Both provide bases for risk identification, assessment, treatment, control and monitoring, with indications for updating, reviewing, and identifying new risks and new crises.

The most important features of these two sets of international standards are described below.

III.A. The COSO Frameworks

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) "which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on internal control, enterprise risk management, and fraud deterrence designed to improve organizational performance and oversight and to reduce the extent of fraud in organizations" (COSO, 2013). In September 2004, the COSO Committee published its first framework, *Enterprise Risk*

[9] According to EBA Guidelines, DIs should define a programme of simulation/stress test exercises, over a certain period, regarding their ability to fulfil their tasks in all the types of intervention set out in the DGSD (i.e. payout, resolution financing, preventative measures and alternative measures in the context of national insolvency proceedings).

Management – Integrated Framework, which gained broad acceptance by organisations in their efforts to manage risk.

According to COSO, Enterprise Risk Management is the *"process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".*

The 2004-ERM consists of eight interrelated components (Internal Environment; Objective Setting; Event Identification; Risk Assessment; Risk Response; Control Activities; Information and Communication; Monitoring) needed to pursue company objectives (Strategy; Operations; Reporting; Compliance) structured by entity units (Entity level; Division; Business Unit; Subsidiary).

In 2017, the COSO Board published an updated version of the *Enterprise Risk Management – Integrating with Strategy and Performance* (COSO, 2017). The document highlights the importance of considering risk in both the strategy-setting process and in driving performance. The Framework is composed of a set of 20 principles organised into 5 interrelated components (Fig.1):

- Governance & Culture,
- Strategy & Objective-Setting,
- Performance,
- Review & Revision,
- Information, Communication & Reporting.

Figure 1 – COSO Enterprise Risk Management

Source: COSO *Enterprise Risk Management – Integrating with Strategy and Performance (2017)*.

The ERM incorporates the COSO internal control framework. The publications are different and have distinct focuses but, at the same time, are closely connected.

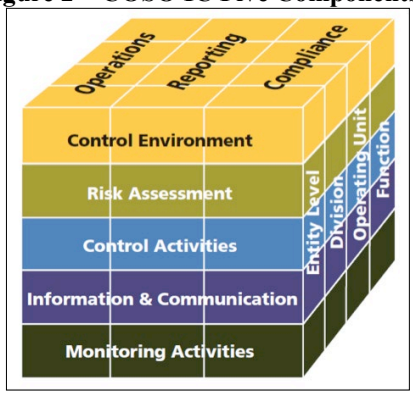
The Internal Control – Integrated Framework (COSO IC), updated in 2013 (originally published in 1992), represents a suitable framework for an organisation to design, implement, conduct and assess the effectiveness of internal control, defined as "a *process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance*".

The essence of the COSO standard is that proper risk management and internal control assist organisations in making informed decisions about the risk level they want to take and in implementing the necessary controls to pursue their objectives. Successful organisations integrate effective

governance structures and processes with performance-focused risk management and internal control at every level of the organisation and across all operations.

COSO IC consists of five components operating together in an integrated manner (Fig. 2): i) Control Environment, ii) Risk Assessment, iii) Control Activities, iv) Information and Communication, and v) Monitoring Activities. COSO guidance illustrates the IC model in the form of a cube, pointing out the links between objectives and the five components, which represent what is needed to achieve the objectives. The third dimension represents the organisation's units portraying the model's ability to focus on parts of the organisation as well as the whole.

Figure 2 – COSO IC Five Components



Source: COSO IC (2013).

Both COSO ERM and COSO IC propose structuring risk and control processes in line with the 'Three Lines of Defence' model (COSO, 2015). The *three lines of defence* is a conceptual framework introduced by the Institute of Internal Auditors, IIA (IIA, 2013).[10] It distinguishes between three groups (or lines) involved in effective internal controls and performing different roles:

- First line: This is seen as functions/roles (processes) that own and manage risks. These functions are the result of process mapping. The first line lies with people whose activities generate the risks through their daily responsibilities. The first line owns the risk and the design and execution of the organisation's risk response. The first line is the internal controls embedded within the operational processes in the organisation, which may consist of divisions, offices and other units (controls like current, comprehensive policies and procedures; segregation of duties; supervisory and secondary reviews; reconciliations, etc.).

[10] The Institute of Internal Auditors has recently updated the 2013 model (IIA, 2020). The new framework, now called "IIA's Three Lines Model" (no longer referring to 'defence') revamps the previous version of the model with the purpose of supporting strong risk management and governance in organisations operating in an uncertain, complex, interconnected and volatile world, while preserving the approach of the previous model.

The updated model places great emphasis on the importance of having balanced and thoughtful risk management 'focusing on the contribution risk management makes to achieving objectives and creating value', rather than exclusively 'defence' against risk. The new model also recognises that the separation between the three lines can be unclear because 'first and second line roles may be blended or separated'. Another important revision relates to internal audit. While the independence of internal audit is confirmed, the new framework points out that 'independence does not imply isolation'. Regular and structured interaction between internal audit and management is needed. Last but not least, a major emphasis is placed on the role of the governing body in effective risk management.

- Second line: This consists of functions/roles that oversee or specialise in risk management and compliance by providing assistance with managing risk. Second-line roles include supporting management policies, defining roles and responsibilities, setting targets for implementation, providing enterprise risk management guidance, and supporting management to identify trends and emerging risks. The second line normally monitors the effectiveness of risk responses and the timely remediation of deficiencies, and reports to management and the board for awareness and potential action.
- Third line: Third-line functions provide independent assurance to senior management and the board over both the first and second lines' efforts in risk management. Internal audit acts as the third line of defence. The third line of accountability is recognised by a high level of independence, objectivity and the authority to evaluate and make recommendations to management on the design and operating effectiveness of the entity overall so as to support the achievement of the organisation's objectives.

III.B. ISO Standard

Another important set of international standards is the ISO 31000 Standard.[11]

This standard can be used by any organisation regardless of its size, activity or sector. ISO covers three main aspects of risk management: Principles, Framework, and Process.

The "**Principles"** represent eight characteristics of effective risk management. Among them, ISO recommends that RM should be an integral part of organisational activities and should be customised and proportionate to the specific organisational context. RM should adapt to internal and external changes and events on a timely basis. Information should be timely, clear and available to stakeholders, accounting for any limitations or uncertainties. RM should continually improve through learning and experience.

The "**Framework"** represents a set of activities which an organisation could follow to develop its own RM framework, which are customised to meet the needs and context of the organisation and integrated into its governance.

The activities are: a) *Leadership and Commitment*: risk management should be integrated into all organisational activities with appropriate leadership commitment; b) *Integration*: risk management should be integrated into the organisation's activities, structure, context and culture; c) *Design*: the design of the framework should take account of the organisation's internal/external context; set out management commitment to risk management; provide clear roles, authorities, responsibilities and accountabilities for risk management; allocate appropriate resources to risk management; communicate to all stakeholders; d) *Implementation*: an effective risk management plan should be developed, with adequate resources; e) *Evaluation*: risk management performance should be periodically evaluated; f) *Improvement*: the organisation should continue to monitor and adapt its risk management framework.

The "**Process"** encompasses policies, procedures and practices for managing risk. It explains that the process covers different activities (Table 1).

[11] The International Organization for Standardization ("ISO") updated, in 2018, the International Standard for Risk Management (ISO 31000:2018), replacing the previous version of the standard, ISO 31000:2009.

Table 1 – ISO 31000:2018 - Process

Communication and consultation	To be undertaken at all stages of the process to ensure stakeholders understand risk.
Scope, context and criteria	Defining the scope of the process with reference to the internal and external context within which the organisation seeks to define and achieve its objectives. Defining risk criteria involves specifying the amount and type of risk that it may or may not take.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation: - Risk identification: Identification and articulation of risks to the organisation's objectives (including both threats and opportunities). - Risk analysis: Comprehension of the nature and level of the risk, including accounting for the likelihood and consequence of the risk. - Risk evaluation: Involves comparing the risk analysis with the risk criteria to determine where additional action is required.
Risk treatment	The process of selecting and implementing options for addressing risk, chosen with regard to the organisation's objectives, risk criteria and available resources, and including implementation of appropriate risk treatment plan.
Monitoring and review	Ongoing monitoring and periodic review of the risk management process and its outcomes integrated in the overall process.
Recording and reporting	The process and its outcomes should be documented and reported through appropriate mechanisms.

III.C. Applicability of Standards to DIs

Standards, as presented above, have a number of commonalities and some differences (RIMS 2011; D. Gjerdrum, M. Peter 2012).

Focusing on commonalities, the standards point out the importance of full integration of risk management in the organisation, at every level, from the board to management as well as to the first line of operations. Another important commonality is that there is no 'one size fits all' risk management framework. Organisations first need to fully understand the context in which they operate before designing the framework accordingly. Furthermore, both standards envisage an active approach to risk management and the strengthening of the risk culture within organisations.

With regard to differences, the COSO ERM was designed to provide an applied and very detailed risk management approach to firms' internal controls, with more emphasis on the board's governance of risk management and the interrelationship with corporate strategy. The level of detail of the ERM provides relevant information for those organisations willing to implement it but, at the same time, organisations may deem it too complex and difficult to be used effectively. ISO provides "a more streamlined approach".

Generally speaking, these international standards can be a useful reference for DIs aiming to establish or develop a risk management and internal control framework.[12] The application of standards to DIs

[12] In this regard, see as examples: i) FSCS (UK) "Following the implementation of a revised Enterprise Risk Management Framework (ERMF) in 2016/17, testing of core controls was performed during 2017/18. The control testing enabled more detailed reporting of residual risks to take place and for improvement activities to be targeted for any ineffective controls. We have further improved this element of the ERMF during 2018/19, by adopting a broader assurance approach, beyond just control self-assessment, to include other sources across the three lines of defence" (Annual Report, 2018/2019). ii) CDIC (Canada): "CDIC is exposed to a variety of internal and external risks that could influence its ability to achieve its mandate and vision. To ensure that these risks are properly identified, assessed and managed, CDIC maintains an Enterprise Risk Management (ERM) program which includes a comprehensive assessment of key corporate risks on a quarterly basis" (Annual Report, 2019). iii) FITD

should be tailored to reflect the specific context in which DIs operate and the size, risk profile, complexity and other characteristics of the DI (proportionality principle).[13] In that respect, standards may represent conceptual guides inspiring the general design of the risk management framework in a DI. Practical implementation of the framework is a challenge, because it should take into consideration the specificities of the case, in order to avoid unnecessary complexity leading to excessive compliance costs for a DI.

IV. Survey of Practices among IADI Members

IV.A. Data and IADI Members Sample

The survey of risk management and internal control system practices was carried out by means of a questionnaire consisting of three sections, aimed at investigating the main aspects of RM and ICS of DIs (Table 2). It was launched in September 2018.[14]

Table 2 – Questionnaire Structure

Section	No. of questions	General aims	Aspects
1	7	Identify the DI in terms of organisation, mandate, year of foundation, number of employees, budget size, functions.	
2	31	Identify the presence of a **formal/informal risk management structure**; investigate the **motivation** for implementing the function; collect information about the **reporting** to the governing bodies and their **responsibility** for defining and formalising policies and for overseeing the function; assess if and how **operational processes are mapped** and ranked by risk order; **which risks are identified;** if tools have been implemented to manage the **risk of bank failure** and to face **unexpected shocks**; and verify if stress tests are used. Investigate how DI **self-assesses** its own risk management framework.	(1) Risk governance (2) Risk appetite (3) Organisational structure (4) Mapping process and risk identification (5) Risk assessment (6) Managing bank failure risk (7) Contingency planning
3	12	Identify the presence of a **formal/informal internal control system**; investigate the **motivation** for implementing the function; investigate the implementation of the **three lines of defence approach**; verify the **responsibility** of governing bodies for defining and formalising policies and overseeing the function; collect information about tools to support the function. Investigate communication and reporting, and how DI self-**assesses** its internal control system.	(8) Internal control system (9) Three lines of defence approach (10) Communication and reporting

(IT) "FITD established a system of internal controls in line with best practices of international standards, on the basis of proportionality which takes into account size, complexity and nature of business" (Annual Report, 2020).

[13] The 'proportionality principle' is well known and developed in the Basel regulatory framework. Basel Committee on Banking Supervision (2011, page 5): "*In the context of the standards imposed by supervisors on banks, the proportionality concept is reflected in those Principles focused on supervisors' assessment of banks' risk management, where the Principles prescribe a level of supervisory expectation commensurate with a bank's risk profile and systemic importance*".

[14] The questionnaire is attached in the Annex.

The number of IADI Member respondents is significant: 58 [15] out of 83 (70%) IADI Members/Associates responded to the questionnaire (see Annex). 78% of respondents are public (government) owned. In terms of mandate, 48% of respondents are "Paybox Plus" DIs, 17% are "Paybox", 22% "Loss Minimiser" and 12% "Risk Minimiser". With reference to total IADI population, 45% of Paybox DIs replied to the questionnaire, 82% of Paybox Plus, 81% of Loss Minimiser and 64% of Risk Minimiser.

Regarding the size, the table below (Table 3) shows the average number of employees in the respondent DIs according to their mandates. There is a high size variance within the groups. The Paybox DIs are the smallest, the largest DIs have a Risk Minimiser mandate. There are also large DIs in the Paybox Plus group.

Table 4 reports the breakdown of respondents by function performed: 38 DIs out of 58 (66%) are pure DIs; 22%, together with deposit insurance, perform resolution functions; 12% perform deposit insurance, resolution and supervision functions.

Table 3 – Respondents - Size Distribution

Mandate	**Employees**		
	Min	Average	Max
Paybox	3	20	69
Paybox Plus	4	82	782
Loss Minimiser	4	151	416
Risk Minimiser	14	1094	5880

Table 4 – Respondents - Functions

Functions	**No.**
Deposit insurance*	38
Deposit insurance + Resolution (Authority)	13
Deposit insurance + Resolution (Authority) + Supervision	7
	58

**: One IADI Associate included.*

In addition to the questionnaire, an in-depth analysis was conducted by means of a detailed case study template sent to a limited number of IADI Members, selected on the basis of mandates and sizes.[16] A total of 6 out of 11 members contacted responded to the case study analysis (mandates: 2 Paybox, 3 Paybox Plus and 1 Risk Minimiser). In addition, 5 members provided supplementary in-depth documents on some aspect of their risk management framework. Contents of the case study analysis are summarised in the following table.

[15] As at December 2018, there were 83 IADI Members and 10 IADI Associates. In addition, one IADI Associate and one DI, not an IADI Member, replied to the survey. Statistics in text are based on IADI Members only.

[16] Case studies were collected during October–December 2018.

Table 5 – Case Study Analysis

	Section	No. of questions	Aims
1	Risk management	12	• Provide information on the main operational processes of the DI; • assess how risks to the main processes are identified, measured, monitored and reported; • collect information about the risk appetite and its reassessment; • investigate what approach is used to identify risks; • verify the presence of risks unrelated to operational processes (bank failure risk) and provide a description of how they are assessed; • assess if there is a risk system for management and reporting and if there is any mitigation mechanism; • explain the process for formalising policies; • investigate how Islamic banks under the DI make a difference to the risk management policies.
2	Internal control system	6	• Verify if operational processes are mapped and documented, who is responsible for building the process, and investigate the role of the risk management and internal control functions and the role of the stakeholders in mapping; • explain how the implementation of the three lines of defence approach reinforces risk awareness across the organisation and how the internal control structure interacts with other functions; • provide information on the additional challenges of a DI for Islamic banking if applicable.
3	Extraordinary events and contingency planning	6	• Explain the relation between risk management and contingency planning; • provide information about the contingency plans already in place and how they are structured; • investigate the robustness of the operational processes during extraordinary events and the capability of the DI to perform in such situations.

IV.B. Findings

1. Risk Governance

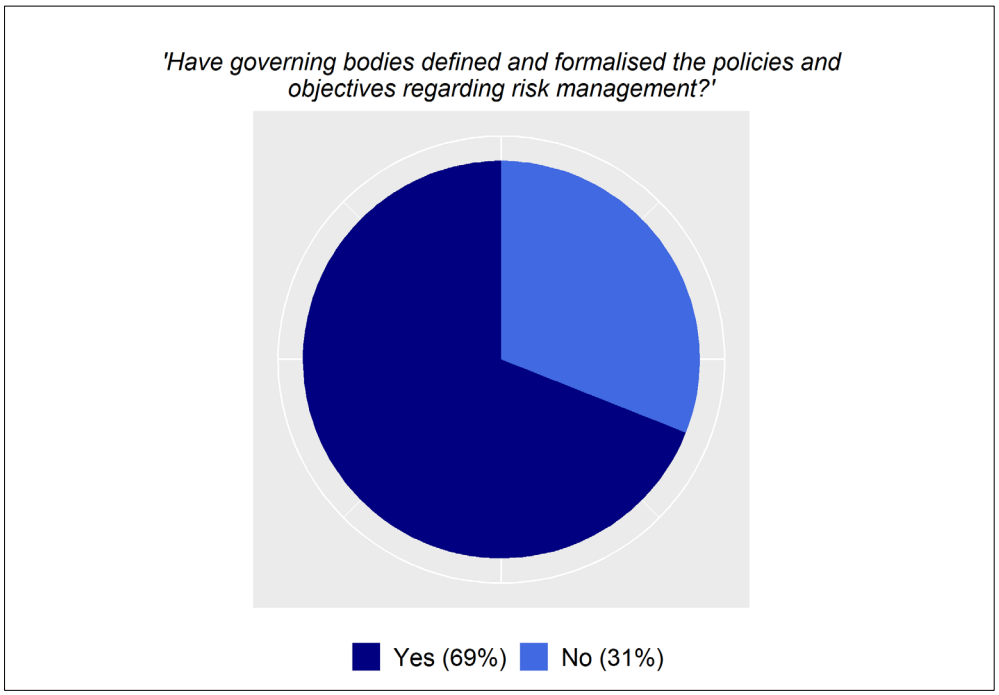
Risk governance represents a crucial element of success for every organisation. It requires that all components of the organisation are aware of the risks incurred in the performance of their activities and are prepared to deal with them according to the rules established for that purpose, with specific roles and responsibilities.

The DI's board plays a fundamental role in risk governance. International standards stress the importance of a clear commitment of the board on risk management. An effective 'tone at the top' lays a strong foundation for effective risk management in a DI and for promoting the risk culture at all levels of the organisation. The board, therefore, is responsible for the definition of the risk management framework and its approval, which includes risk policy, risk appetite and risk limits, and oversight of their application over time, given the information provided by the management. Well-managed

information flows within the organisation and extensive reporting across all risk areas to the board is, therefore, crucial for the success of risk management.

This survey investigated all these aspects. It found that, in most cases, DIs are well structured in risk management governance: 69% of respondents indicated governing bodies have defined and formalised policies and objectives regarding risk management (Chart 1). Percentages are higher in DIs with a broader mandate (Loss and Risk Minimiser).[17] Furthermore, 79% of DI boards are responsible for overseeing the function. By contrast, 31% of DIs do not have formalised policies and objectives on risk management. This cluster of DIs consists of 22% Paybox respondents and 56% Paybox Plus.

Chart 1 – Governing Bodies and Risk Management Policies



*: 58 respondents.

Examples, taken from case study analysis, of risk management policies and the board's responsibilities on risk management are reported in boxes 1 and 2 respectively.

Box 1 reports an extract of a well-designed risk management policy approved by the board of a large DI with a Paybox Plus mandate. It formalises the importance and the objectives of risk management. It also lists the main components and activities of the framework.

Box 2, which was extracted from a well-organised Loss Minimiser DI's Board Charter, lists the duties of the board.

[17] See Annex – Survey Statistics.

Box 1 – Risk Management Policy - Example

DI with a Paybox Plus mandate

…

Risk management is central to the strategic objectives and corporate governance of the DI. The DI recognises that there are risks inherent in the deployment and management of processes, systems and people involved in meeting its objectives. Constant, consistent and effective management of risk is therefore an integral component of the effective operation of the DI.

It is the objective of risk management to ensure that risks to the DI are identified, assessed and controlled to within tolerance. Risk management aims to reduce both the probability and impact of risks that might prevent it from achieving the DI's objectives, achieving its stated mission and/or meeting the obligations placed on the DI.

The DI seeks to be 'confidently in control' of all risks to the DI's mission, aims and objectives. It is recognised that the DI, as a result of its function and obligations, is exposed to risks and issues where it may have limited control. Risk will be managed at an organisation-wide level and at business function level using a central risk function supplemented by risk-focused resources based across the business and supported by appropriate policies, procedures and methodologies.

…

The DI has established a Risk Management Framework under which it:

(1) Sets risk policy and procedures;
(2) Identifies and controls risks;
(3) Assesses the control of risks;
(4) Remedies and improves controls; and
(5) Monitors and reports on risk and controls.

Executive responsibility for the Risk function resides with the Director of DI. Responsibility for the delivery of the Risk function's activities rests with the Head of Risk Management Department.

…

Risk management culture and the "Three Lines of Defence"

It is inherent in the culture of the DI that everyone, under the direction of all managers, is responsible for identifying and controlling risks, and furthermore that all colleagues have a role in this. These efforts are supported by the Risk function and related policies and procedures.

…

Risk Management governance

Executive responsibility for the Risk function resides with the Director of Department ...
Responsibility for the delivery of the activities of the Risk function rests with the Head of Risk.
…
The Risk function establishes and maintains a 'Risk Universe'. This is a comprehensive categorisation of the risks to which the Scheme is exposed. An assessment of risks of each business function must be conducted at least quarterly by its management using the Risk Universe and communicated to the Risk function. This includes an assessment of the completeness of the Risk Universe, the inherent and residual impact and likelihood of the relevant identified risks for their function.

…

Review and Assessment

The Head of Risk will conduct an annual review of the policy and submit it for formal approval.

Box 2 – Board of Directors Charter and Risk Management – Board's Duties - Example

DI with a Loss Minimiser mandate

…

The Board of Directors will:

(1) obtain an understanding of the significant risks to which DI is exposed;

(2) establish appropriate and prudent risk management policies for those risks and review these policies on a regular basis, but at least annually, to satisfy themselves that they continue to be appropriate and prudent; and

(3) obtain reasonable assurance, on a regular basis, but at least annually, that DI has an effective ERM process and that risk management policies are being adhered to.

2. Risk Appetite

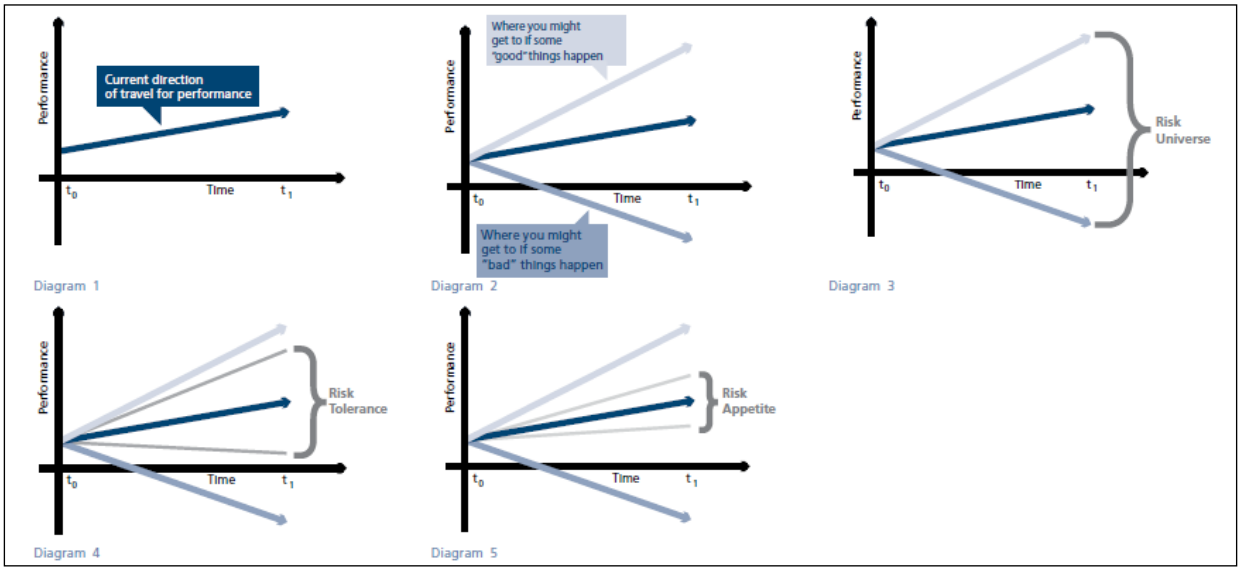
There are numerous definitions of organisational 'risk appetite', but "they all boil down to how much of what sort of risk an organisation is willing to take" (HM Treasury, 2006). Risks need to be considered in terms of both opportunities and threats – not necessarily confined to money – that impact on the capability of the organisation, its performance and reputation. Risk tolerance is the risk variation the organisation is willing to tolerate around specific objectives (Fig. 3).

Organisations can choose to have high or low risk tolerance.

Zero-tolerance (or near-zero tolerance) is usually associated with those risks an organisation wishes to avoid in consideration of their strong impact on the objectives of the organisation (e.g. fraud, corruption, regulatory and law violations).

For a DI, the ability to handle risk may be driven by elements such as its mandate, its financial and operational resources or the characteristics of the financial system (financial/banking market concentration, risk of failure of member financial institutions). Tolerances can be applied to detailed areas such as depositors' data security, deposit reimbursement, deposit insurance fund losses or timing of intervention, depending on the mandate of the DI. As to risk limits, they are often defined as the granular operational controls (expressed in quantitative metrics) on specific risks, which are practical to monitor.

Figure 3 – Risk, Risk Tolerance and Risk Appetite

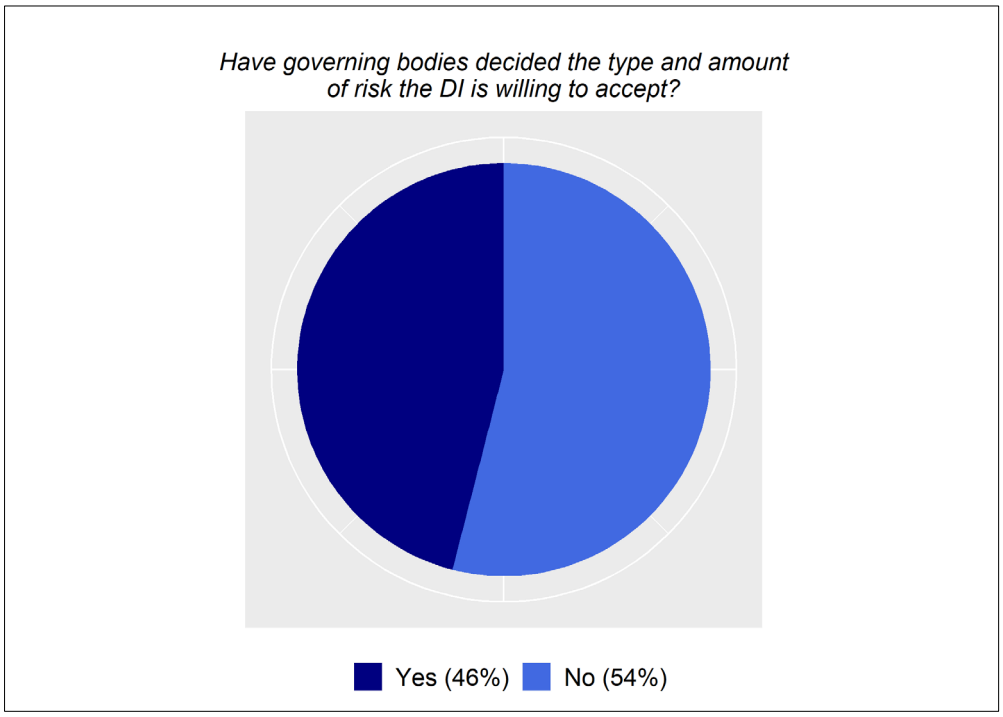


Source: IRM (2015), page 18.

On the question "Have governing bodies decided the type and amount of risk the DI is willing to accept?", the sample of DIs is split into two groups: 46% of DIs responded affirmatively; 54% negatively (Chart 2).

A well-designed risk appetite statement example, taken from a large Risk Minimiser DI, is reported in Box 3, together with an application on operational risk.

Chart 2 – Risk Appetite



*: 57 respondents.

Box 3 – Risk Appetite: Statement and Application on Operational Risk – Example

DI with a Risk Minimizer mandate

DI Risk Appetite Statement **May 2019**

What is risk appetite? Risk appetite is the amount of risk an organization is willing to accept in pursuit of its mission. It is established by an organization's most senior leadership and serves as a guidepost for setting strategy and goals and objectives. The risk appetite statement is a central component of the DI's enterprise risk management (ERM) program and communicates the DI's views about the level of risk taking that is acceptable in pursuit of its strategic goals and objectives.

What is the DI's overall risk appetite? Overall, the DI has a low appetite for risk and is conservative in its actions in order to maintain stability and public confidence in the nation's banking system and the DI's excellent reputation. The DI may consider some targeted risks, for example, to leverage new technology or seize a promising opportunity. The DI has a very low appetite for risks that could compromise its core values, such as integrity and fairness. The Risk Appetite Statement categorizes risks into the following four risk levels:

Risk Appetite Level	Definition
Very Low	Areas in which the DI seeks to avoid, minimize, or eliminate risks because the potential downside costs are intolerable. DI seeks to maintain a very strong control environment.
Low	Areas in which the DI seeks to minimize risks because the potential downside costs are significant. DI seeks to maintain a strong control environment.
Moderate	Areas in which the DI seeks to balance potential upside benefits and potential downside costs of a given decision to seize an opportunity or achieve a more favorable outcome. DI seeks to maintain a moderate control environment.
Higher	Areas in which the DI has a preference for targeted and disciplined risk-taking to seize an opportunity or achieve a more favorable outcome. The potential upside benefits outweigh the potential costs.

… …

Risk Appetite applied on Operational Risk

Operational Risk include risks that the DI's financial resources or the deposit insurance fund could be impaired because of adverse economic conditions, inefficient resource utilization, improper payments, or fraud. As steward of the deposit insurance fund, the DI must maintain the fund within statutory limits and at a level sufficient to address industry risk. The DI must ensure that deposit insurance pricing methodologies are fair and risk-based. The DI must also make sure that it has reliable contingent sources of funding, such as through the Ministry of Finance or Treasury Department, to respond to systemic risk events. The DI has internal controls in place to safeguard assets and defend against fraud, waste, and abuse. Examples include:

Theft, Fraud	The DI has a very low appetite for risks that threaten its ability to guard against theft, fraud, or misuse of corporate assets.
Insurance Pricing Deposit Insurance Fund Management	The DI has a low appetite for risks that threaten its ability to ensure that deposit insurance pricing is properly calibrated and risk based and that assessments are properly levied and collected.
Investing in Tomorrow	The DI is willing to take a higher level of risk by incurring short-term financial expenses to achieve longer-term benefits to the DI, such as investing in IT infrastructure and pursuing succession and leadership management efforts.

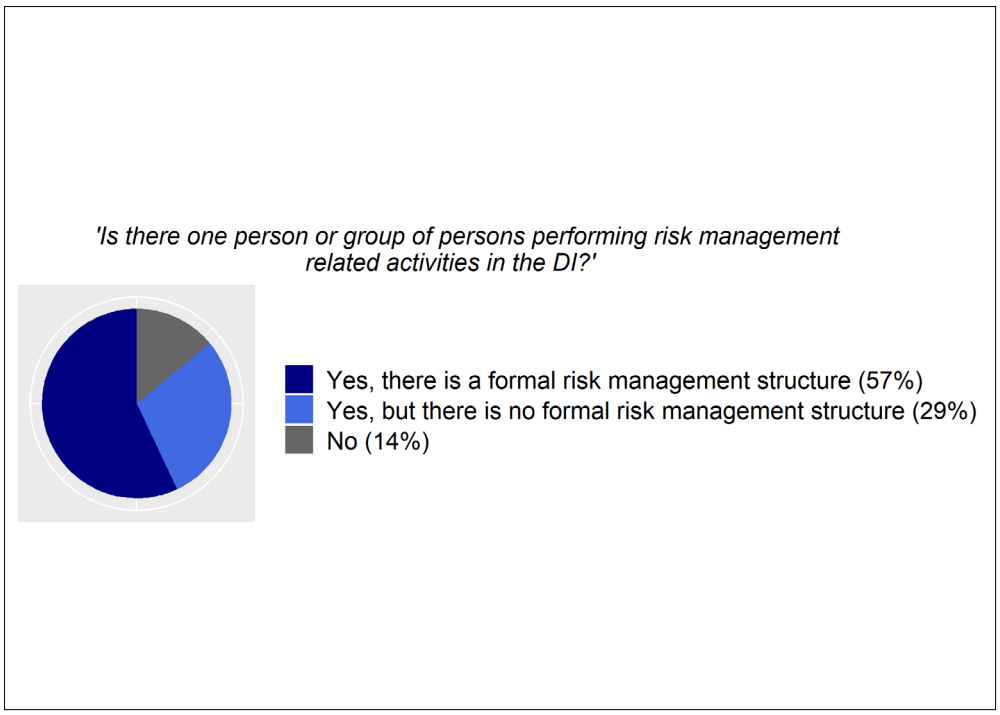
3. Organisational Structure

Another important aspect of this analysis concerns the presence of a formal or informal organisation structure for risk management within the DI and the motivation for implementing the risk management function.

The majority of DIs carry out risk management activities (86%; Chart 3). In more detail, 57% of DIs have implemented a formal risk management structure, and 29% have, at least, one person – or a group of persons – performing risk management-related activities.

14% of DIs do not have a person in charge of performing risk management activities. However, 68% of these DIs are planning or considering a future implementation of this function.[18]

Chart 3 – Risk Management Organisation



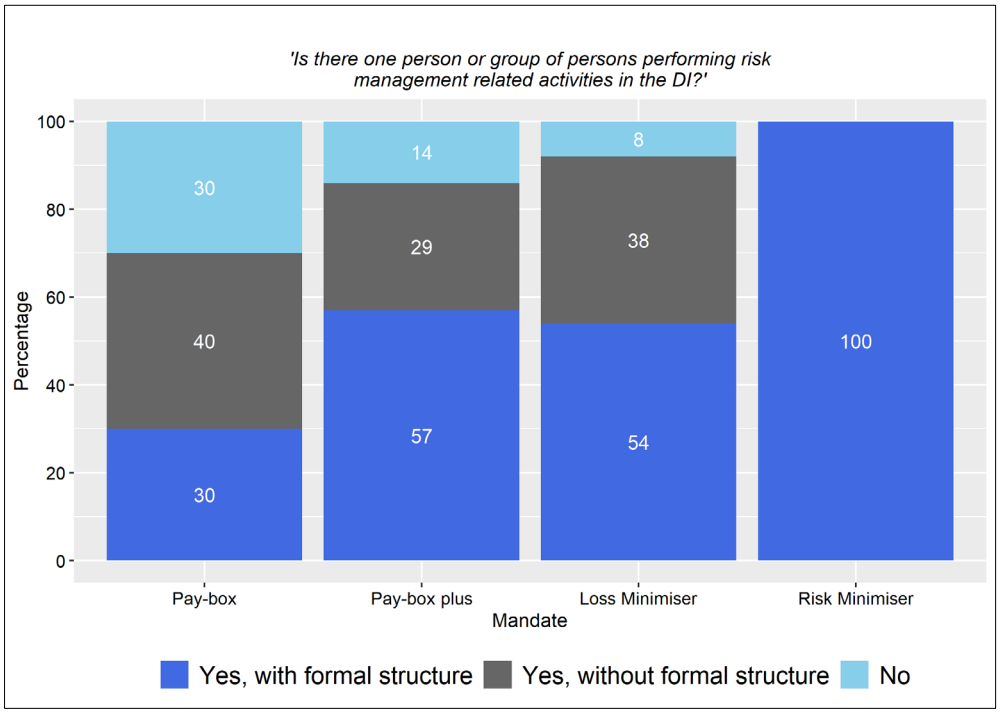
*: 58 respondents.

The presence of a formal risk management structure seems to be correlated with the complexity of the DI mandate. All Risk Minimiser DIs have a formal risk management structure, as do the slight majority of Loss Minimiser (54%) and Paybox Plus DIs (57%). 30% of Paybox DIs do not have a person in charge of performing risk management activities (Chart 4).

The motivation for implementing risk management functions comes mostly from decisions of the governing bodies. For a small percentage it comes from laws/regulatory demands and corporate by-laws.

[18] See Annex – Survey Statistics.

Chart 4 – Risk Management Organisation - Breakdown by mandate



*: 58 respondents: 10 Paybox, 28 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser.

4. Mapping process and identification of risks

A risk management process has different phases. It provides a framework for identifying risks, ranking their priority, and assessing likelihood and potential severity. It supports preventive or mitigating actions, controlling risks internally, constant monitoring of the adequacy of the overall framework, and necessary adjustments.

Identification of risks is the first step of risk management. Internal risks stem from operations, and hence the need to have in place a mapping process.

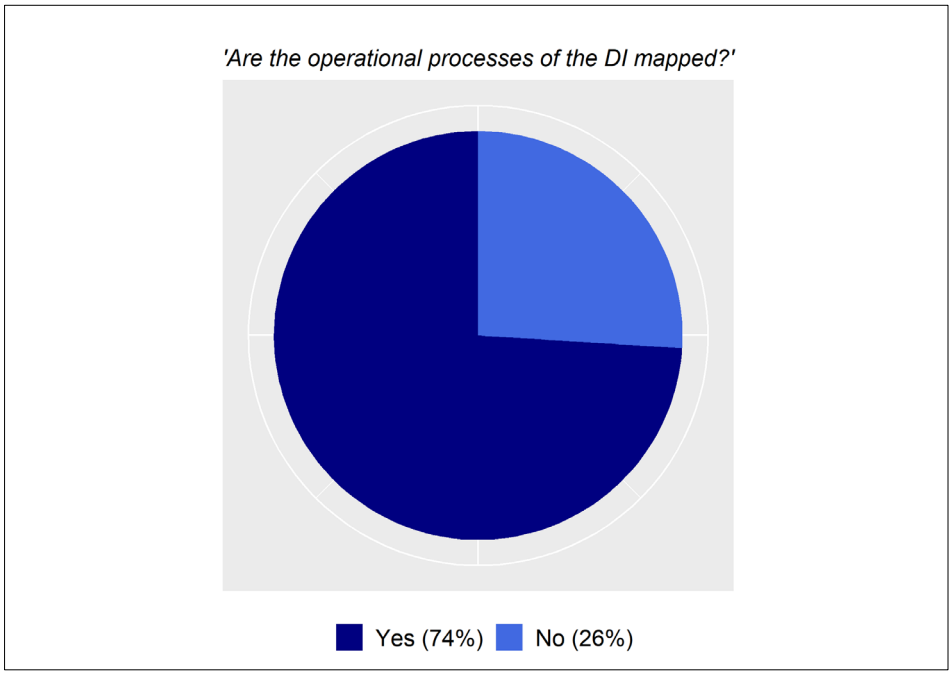
Mapping consists in documenting all internal operational activities/processes of a DI. It follows a step-by-step basis, identifying areas of activity, execution timelines, inputs and outputs, risks that may occur, descriptions of the existing controls to prevent or detect error and failure during execution, source databases and systems used, and all other relevant information. Usually, besides a written document, mapping includes a flow chart showing the process graphically from start to finish. It is important that those responsible for the activities in the execution of the processes participate in the mapping process. In the case of a narrow mandate DI (Paybox), we can identify some main macro-processes, such as funding, investment, and operational processes regarding the reimbursement of depositors; each of them can also be broken down into further processes. Different risks can occur in each process.

The survey found that 74% of DIs declared they map the operational processes (Chart 5). In the majority of cases (62%), the process is ranked by risk order (for example low, medium or high).

The majority of DIs (68%) apply distinct oversight policies according to the different types of risk. Of these, 78% develop mandatory action plans to reduce the exposure to riskier processes.

Some examples of main operational processes in DIs are shown in Box 4.

Chart 5 – Mapping Process



*: 58 respondents.

Box 4 – Mapping Process - Examples

Example 1:
DI with a Paybox Plus mandate

Main operational processes of the DI:

- Pay-out processes;
- SCV files testing;
- Asset management;
- Liquidity management;
- Credit risk management;
- ICT (Information and Communications Technology) infrastructure;
- Information security;
- Legal infrastructure.

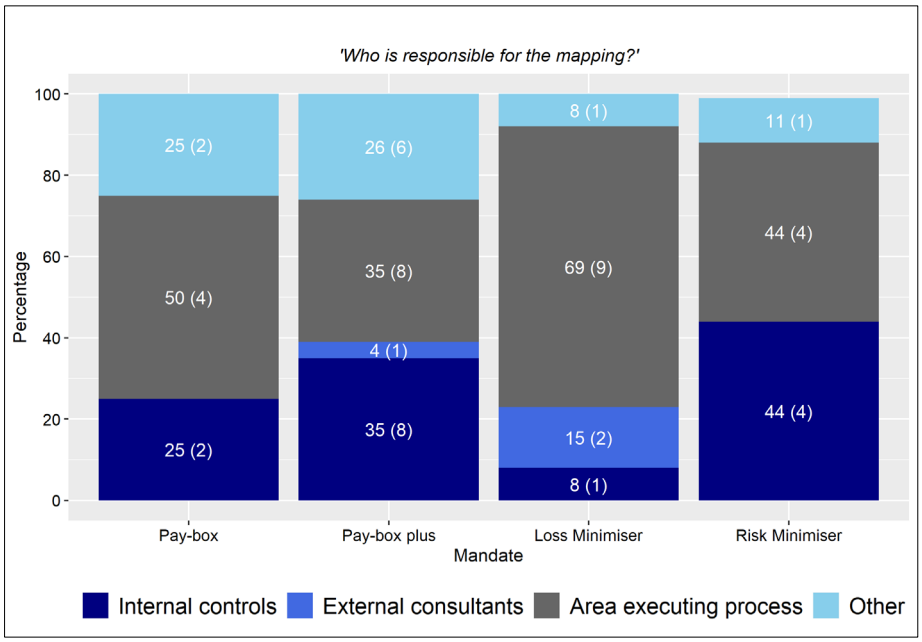
Example 2:
DI with a Paybox Plus mandate

Main operational processes of the DI:

- Collection of premiums charged on eligible deposits;
- Analysis of collateral placed by financial institutions and limit approval;
- Calculation of the current funding requirement of the Fund, measurement of the funding gap risks, measurement of the amount of total liquid assets of the Fund and definition of the share of the monthly contribution that must be destined to Reserve. Calculation of the minimum immediate liquidity requirement;
- Analysis of the requests for financial assistance transactions, design of an acceptable structure for the assistance deal – if viable, propose for the approval of the relevant authority level in the internal governance, prepare all loan and collateral documentation, make disbursement;
- Guarantee of payout to depositors in the event of bank liquidation.

On responsibility for mapping, the survey revealed that in the majority of cases, the party executing the process is, most frequently, the one responsible for mapping. The internal control structure also has an important role. Few DIs declared they employ external consultants (Chart 6).

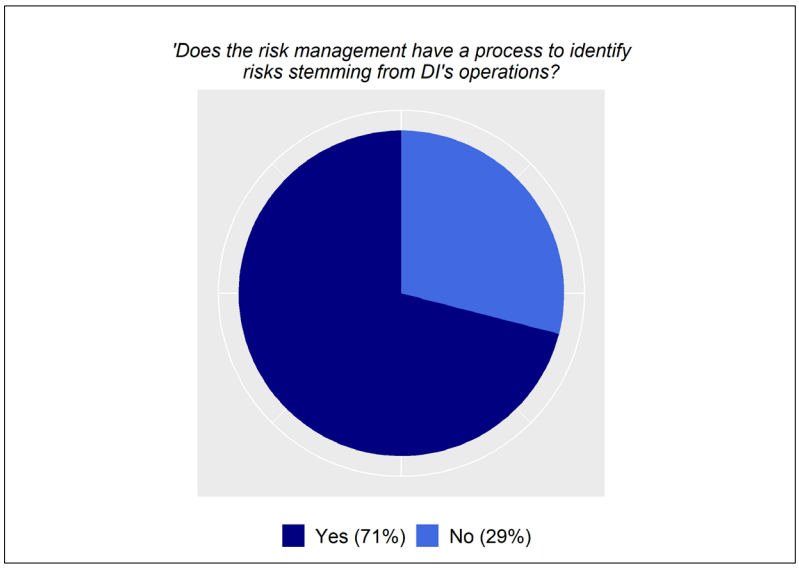
Chart 6 – Responsibility for Mapping - Breakdown by mandate



*: 40 respondents: 7 Paybox, 18 Paybox Plus, 10 Loss Minimiser, 5 Risk Minimiser.
Answers given by respondents are not mutually exclusive. Absolute frequency values are in brackets.

With regard to risk identification, 71% of DIs have a process in place to identify risks that may arise from the DI's activities (Chart 7). A slight majority of DIs have a formalised list of risks, including their definitions (53%). It seems that the presence/absence of a list of inherent risks is not linked to the type of DI mandate.[19]

Chart 7 – Identification of Risks



[19] See Annex – Survey Statistics.

Findings on the types of risk considered by IADI Members are reported in the following table. The table shows the risks identified by DIs according to their mandate. The first column indicates the overall frequency of responses, and shows the amount of DIs that consider a specific risk calculated as a percentage of the total number of respondents. The other columns show the amount of Paybox, Paybox Plus, Loss Minimiser and Risk Minimiser DIs that consider a specific risk, as a percentage of total respondents per mandate. The most frequent risks considered by all respondents are: "operational", "IT", "liquidity" and "reputational". The number of risks increases with the breadth of the DI's mandate.

Table 6 – List of Risks

Type of risks	Mandate				
	All	Paybox	Paybox Plus	Loss Minimiser	Risk Minimiser
Credit	69%	43%	62%	82%	100%
Interest rate	60%	29%	57%	82%	67%
Funding	67%	29%	62%	91%	83%
Operational/Legal	93%	71%	95%	100%	100%
IT and information security	76%	43%	67%	100%	100%
Strategic	56%	29%	48%	73%	83%
Market	64%	43%	62%	73%	83%
Currency	36%	14%	29%	55%	50%
Liquidity	84%	43%	86%	100%	100%
Bank failure	62%	29%	62%	73%	83%
Reputational risk	73%	43%	71%	82%	100%
Others	33%	29%	29%	27%	67%

*: Value in green > 70%; 45 respondents: 7 Paybox, 21 Paybox Plus, 11 Loss Minimiser, 6 Risk Minimiser.

Two examples of the most comprehensive risk category lists are reported in Box 5. Both are taken from large DIs with Paybox Plus mandates.

Box 5 – List of Risk Categories - Examples

Example 1:
DI with a Paybox Plus mandate

DI ability to fulfil its mission depends on its ability to deliver the following identified critical requirements:

- Providing a well-understood service which delivers accurate compensation payments.
- Achieving a level of service that meets customers' reasonable expectations and service standards.
- Maintaining the security of information.
- Ability to respond to major failures of banks or crises.
- Maintaining awareness among consumers.

Consequently, in order to achieve these goals, the DI has identified principal risk areas underpinning DI Risk Management Framework and surrounding which the Board has instituted risk tolerances. Risks categories are as follows:

- Governance and strategy risk;
- Financial risk;
- Legal and compliance risk;
- Technology and information risk;
- Operational risk;
- People risk.

Example 2:
DI with a Paybox Plus mandate

DI has identified the following risk categories:
1) Credit Risk;
2) Market Risk;
3) Interest Rate Risk;
4) Funding Risk;
5) Liquidity Risk;
6) Operational Risk

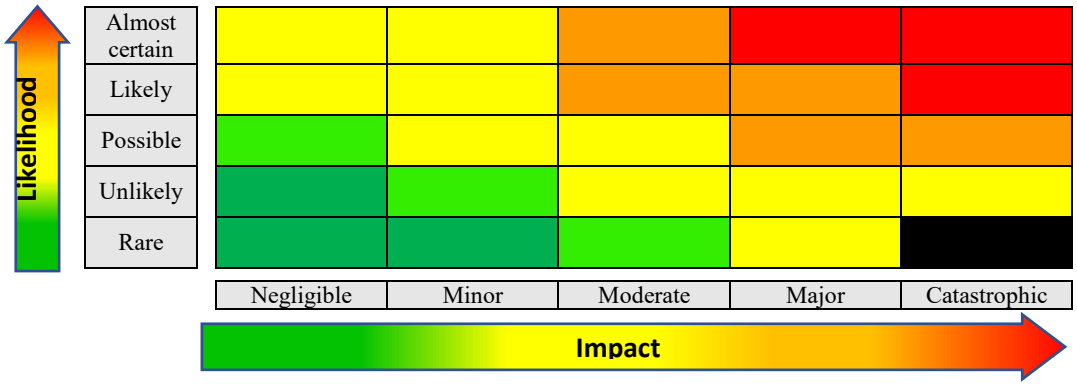
Operational Risk is divided into 8 subcategories and losses should be estimated accordingly:

- Internal fraud
- External fraud
- Labour demands
- Inadequate practices towards clients, products or services
- Damage to fixed assets, owned or in use by the company
- Financial events that lead to operational disruption
- Information technology system failure
- Failure in the execution, meeting of deadline or management of the activities of the company

5. Risk assessment

No matter what form risk takes, two factors have to be considered: the likelihood of the event occurring and the expected severity (impact) when the event occurs. Different likelihoods and impact levels can be specified, as illustrated in Figure 4, by means of a '**Risk Matrix**'. The matrix is useful for assessing and prioritising risks and for selecting the appropriate response for each risk identified.

Figure 4 – Risk Matrix



Insignificant consequences: These risks should not receive much attention because they have a low likelihood and a low impact.

Minor consequences: These risks should receive a little more attention than risks with insignificant consequences, but less attention than risks with moderate consequences.

Moderate consequences: These risks should be monitored actively because they have a higher likelihood or a higher impact than risks with insignificant or minor consequences.

Major consequences: These risks should receive special attention because they have a relatively high likelihood and their effect on the organisation would be severe.

Catastrophic consequences: These risks have unacceptable levels because they are very likely and would have a catastrophic effect on the organisation. They must be dealt with immediately.

Risks in the black area have very low probability of occurrence but would have a catastrophic effect. These risks are sometimes called 'black swans', and are usually dealt with by contingency plans.

*: Adapted from Hannes Valtonen (2014), page 151.

Some risks can be easily measured, for example the maximum or average monetary loss that could occur as a consequence of a specific event, but other risks are not measurable (e.g. strategic, reputational risks). Also, risks can be assessed on an inherent and/or residual basis, after risk mitigation.

The survey found that 59% of respondent DIs do not quantify risks in monetary terms. DIs applying monetary measurement have various mandates (3 Paybox, 5 Paybox Plus, 6 Loss Minimiser and 2 Risk Minimiser) .[20]

Box 6 provides an example of general practice in risk assessment showing inherent and residual risk.
Box 7 shows an application of the risk matrix.
Box 8 provides an example of a risk management scale.

[20] See Annex – Survey Statistics.

Box 6 – Risk Assessment - Inherent and Residual Risk - Example

DI with a Paybox Plus mandate

The Risk function establishes and maintains a 'Risk Universe'. This is a comprehensive categorisation of the risks to which the DI is exposed. At least quarterly, an assessment of risks to each business function must be conducted by the business function management using the Risk Universe and communicated to the Risk function. This includes an assessment of the completeness of the Risk Universe and the inherent and residual impact and likelihood of the relevant identified risks for their function.

Risk Type (related to core business operations or from a separate functional area)	
Date of last risk assessment	
Inherent Risk (i.e. before controls or mitigation)	Likelihood (1-5)
	Impact (1-5)
	Priority
Risk Mitigation	
Residual Risk (i.e. with benefits of controls or mitigation)	Likelihood (1-5)
	Impact (1-5)
	Priority
Executive Key Risk or Tolerance Risk	

Box 7 – Risk Assessment - Risk Matrix - Example

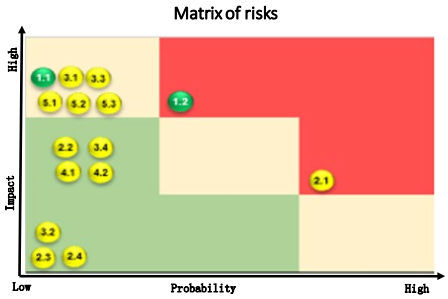
DI with a Paybox Plus mandate

The Matrix shows that five processes had their individual risks placed in the matrix according to probability (frequency) and impact before mitigation or controls. The overall residual risk of each process is represented by the colour in the legend.

For example, risks 1.1 and 1.2 have high impact and therefore are placed in red areas of the graph. However, after mitigation the overall residual risk of the process is low. Thus, their legend is green. Another example is the green area referring to low impact-low probability. All risks placed there have yellow legend. These risks are related to processes for which overall residual risk was deemed (evaluated) medium in spite of mitigation.

Matrix of risks - Relevant processes

The vulnerabilities were associated with the 5 relevant processes to fulfill the mission of the DI



Process 1: overall residual risk ➔ Low
- Risk 1.1 Probability: low Impact: high
- Risk 1.2 Probability: medium Impact: high

Process 2: overall residual risk ➔ Medium
- Risk 2.1 Probability: high Impact: medium
- Risk 2.2 Probability: low Impact: medium
- Risk 2.3 Probability: low Impact: low
- Risk 2.4 Probability: low Impact: low

Process 3: overall residual risk ➔ Medium
- Risk 3.1 Probability: low Impact: high
- Risk 3.2 Probability: low Impact: low
- Risk 3.3 Probability: low Impact: high
- Risk 3.4 Probability: low Impact: medium

Process 4: overall residual risk ➔ Medium
- Risk 4.1 Probability: low Impact: medium
- Risk 4.2 Probability: low Impact: medium

Process 5: overall residual risk ➔ Medium
- Risk 5.1 Probability: low Impact: high
- Risk 5.2 Probability: low Impact: high
- Risk 5.3 Probability: low Impact: high

Box 8 – Risk Assessment – Risk Measurement Scale - Example

DI with a Loss Minimiser mandate

Risk Measurement Scale: Impact		
Rating	**Descriptor**	**Definition**
1	Minor low	Could cause a nearly null effect on the Institute's operations, delaying or affecting the accomplishment of institutional objectives by 10%.
2	Minor	Could cause small effects on the Institute's operations, delaying or affecting the accomplishment of institutional objectives by 20%.
3	Minor high	May damage the institutional image or resources, to an extent that can be corrected in the short run, delaying or affecting the accomplishment of institutional objectives by 30%.
4	Low	May damage the institutional image or resources, to an extent that can be corrected in the mid run, delaying or affecting the accomplishment of institutional objectives by 40%.
5	Moderate low	Could cause strong damage to the fulfillment of institutional objectives, delaying or affecting their accomplishment by 50%.
6	Moderate high	Could cause significant damage to the fulfillment of institutional objectives, delaying or affecting their accomplishment by 60%.
7	Major low	Could causes severe damage to the fulfillment of institutional objectives, affecting their accomplishment by 70%, and altering the institutional work program.
8	Major high	Affects directly the fulfillment of the institutional mission, vision, goals and objectives by 80%.
9	Severe	Affects directly the fulfillment of the institutional mission, vision, goals and objectives by 90%.
10	Critical or catastrophic	Makes impossible to fulfill the institutional mission, vision, goals and objectives.

Risk Measurement Scale: Likelihood		
Rating	**Descriptor**	**Definition**
1	Rare / Almost Null	The risk can occur once every 15 years, or has a probability of occurrence of 1% to 12%.
2	Rare / Low	The risk can occur once every 10 years, or has a probability of occurrence of 13% to 24%.
3	Unlikely / Low	The risk can occur once every 5 years, or has a probability of occurrence of 25% to 37%.
4	Unlikely / Moderate Low	The risk can occur once every 3 years, or has a probability of occurrence of 38% to 50%.
5	Possible / Moderate	The risk can occur once every 2 years, or has a probability of occurrence of 51% to 62%.
6	Likely / Moderate	The risk can occur once a year, or has a probability of occurrence of 63% to 74%.
7	Very Likely / Moderate	The risk can occur once every semester, or has a probability of occurrence of 75% to 82%.
8	Very Likely / High	The risk can occur once every quarter, or has a probability of occurrence of 83% to 89%.
9	Frequent / Very High	The risk can occur once a month, or has a probability of occurrence of 90% to 95%.
10	Frequent / Continuous	The risk can occur once a week, or has a probability of occurrence of 96% to 100%.

Once risks have been identified and assessed, the DI must determine the appropriate treatment and response. Broadly speaking, there are four choices for risk treatment: i) Reduce - DI takes action to reduce the likelihood or impact of the risk; ii) Accept - DI does nothing on the basis it is willing to accept the impact of the risk; iii) Avoid - DI takes action to avoid or eliminate risk by preventing exposure to the risk event (e.g. divest, prohibit, stop activities); iv) Transfer - DI takes action to transfer or share ownership and liability of risks to/with third parties (e.g. insurance, outsourcing, hedging, etc.).

In determining the preferred risk response, consideration should be given to: the DI's public policy objectives and mandate; the cost of any treatment as compared to the amount of risk reduction (cost benefit analysis); the DI's capabilities to implement the remedial actions.

Finally, the survey investigated if DIs stress test their risk management framework: 45% of DIs responded affirmatively; this result tends to be correlated with the breadth of mandate.[21]

6. Managing Bank Failure Risk

The survey provided an in-depth analysis on whether DIs have implemented tools to manage the risk of bank failure. However, it should be noted that the failure of a bank is not a risk in itself for a DI but rather it represents its 'raison d'être'. It is when the DI is fulfilling its mandate that certain risks can come to the fore.

Findings revealed that only a slight majority of DIs (54%) have tools to manage this kind of risk.[22]

Not surprisingly, these findings are strongly related to the type of mandate. Indeed, only two out of eight Paybox respondents (25%) have tools to manage bank failure risk, whereas all Risk Minimiser respondents (100%) have tools to manage this risk.

There are many tools used to manage bank failure risk. The table below shows the number of responses for each tool used. The highest frequency are on the following tools:

- Use of DI internal credit ratings models,
- Monitoring of key risk indicators for all banks based on regulatory and bank-internal reporting,
- Communication and coordination with other financial safety-net participants to find a risk mitigation strategy.

Table 7 – Tools to Manage the Risk of Bank Failure

Tools	All			Paybox	Paybox Plus	Loss Min.	Risk Min.	Total
	No.	%						
Risk mitigating tools								
Regular risk-based audits carried out by the DI	12	38%		0%	33%	25%	42%	100%
Use of DI internal credit ratings models applied on financial institutions	18	56%		0%	45%	22%	33%	100%
Ongoing monitoring of key risk indicators for all banks based on regulatory and bank-internal reporting (banks are required to report regularly to the DI)	23	72%		4%	36%	30%	30%	100%
Trigger talks with other financial safety-net participants to find a risk mitigation strategy	21	66%		10%	32%	29%	29%	100%
Special requirements on banks (e.g. limitation of amount of covered deposits, definition of higher capital ratios, other limitations)	10	31%		10%	30%	10%	50%	100%
Apply supervisory framework or intervention guidelines	12	38%		0%	33%	33%	33%	100%
Resolution tools								
Provide liquidity assistance loans	9	28%		11%	22%	22%	45%	100%
Provide loans to shareholders for capital injection	6	19%		0%	17%	50%	33%	100%
Early intervention measures (e.g. acquisition of troubled bank and subsequent silent resolution, which is often cheaper than the compensation of depositors)	13	41%		0%	15%	38%	47%	100%
Others	6	19%		0%	50%	17%	33%	100%

*: 32 respondents.

[21] See Annex – Survey Statistics.
[22] See Annex – Survey Statistics.

7. Contingency planning

Contingency planning is conducted "by the deposit insurer and other financial safety-net participants, individually as well as jointly, to outline policies, procedures and actions that they might follow in the event of unexpected developments and significant shocks; it helps identify measures for preserving the operational and financial situation of the safety-net agency" (IADI, 2019). Areas of contingency planning may include a business continuity plan, funding plans, payout plan, communication plan, etc.

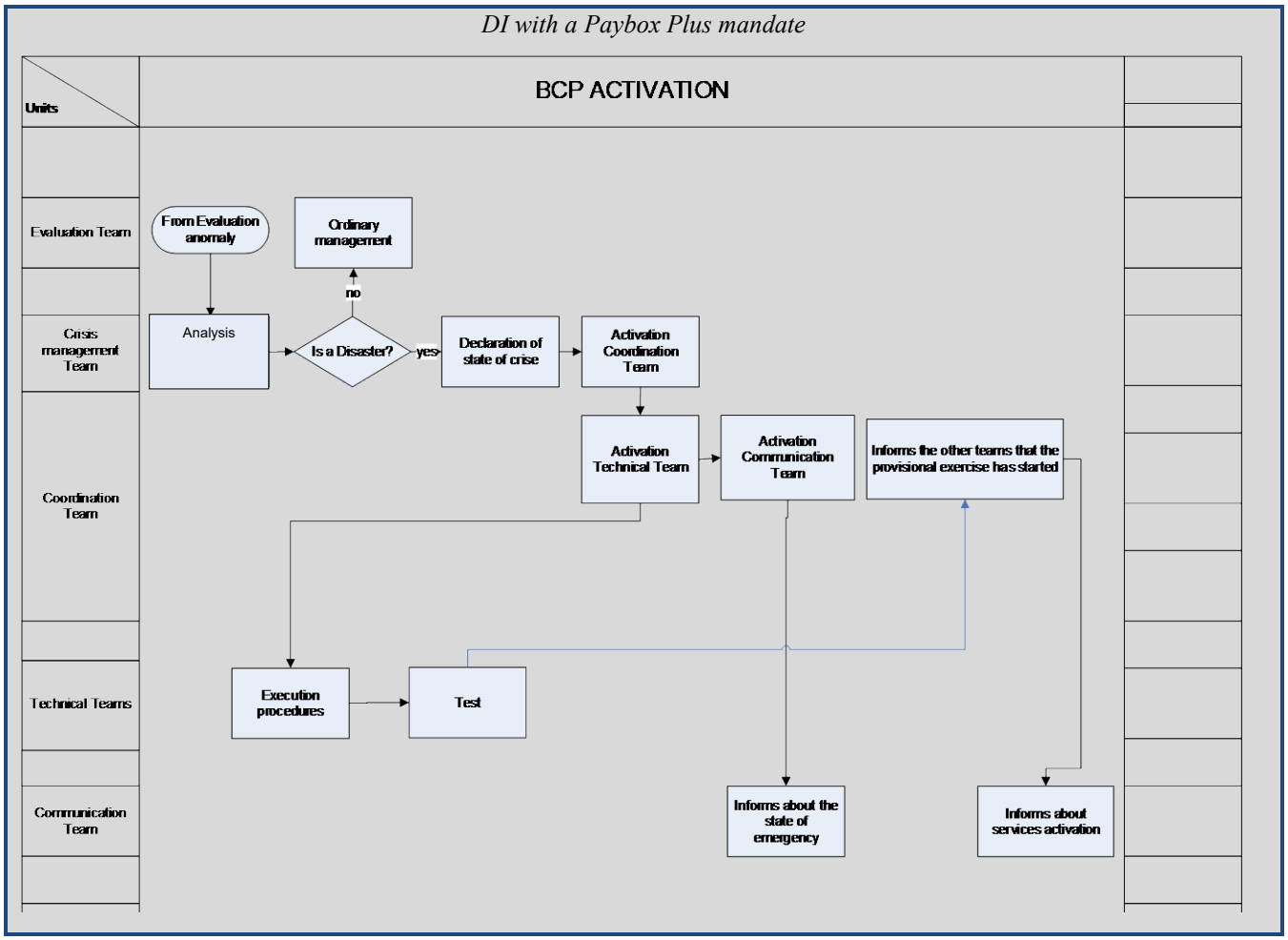
The survey shows that 64% of DIs are able to deal with unexpected extraordinary risks or shocks using appropriate tools.[23] Examples of areas of contingency planning, based on the case studies, are reported in box 9 below. Box 10 sketches the main phases of the business continuity implementation plan.

Box 9 – Areas of Contingency Plans - Examples

Example 1: *DI with a Paybox Plus mandate*	**Example 3:** *DI with a Risk Minimiser mandate*
The contingency planning estate covers *continuity* and *contingency*. For *continuity*, planning arrangements cover the following scenarios: Loss of utilities; Loss of communications (public and/or private); Loss of IT systems and/or data; Staff absenteeism; Building availability; Reputation protection; Financial loss. From a *contingency* viewpoint, the DI has plans in place to ensure that compensation is delivered to customers within seven days of the failure of the deposit-taking institutions.	Contingency planning covers business continuity of the organisation as well as recovery planning and resolution planning for Systemically Important Financial Institutions (SIFIs) of the jurisdiction. Different idiosyncratic and systemic scenarios are considered in recovery and resolution plans.

[23] See Annex – Survey Statistics.

Box 10 – Business Continuity Plan Implementation – Phases - Example

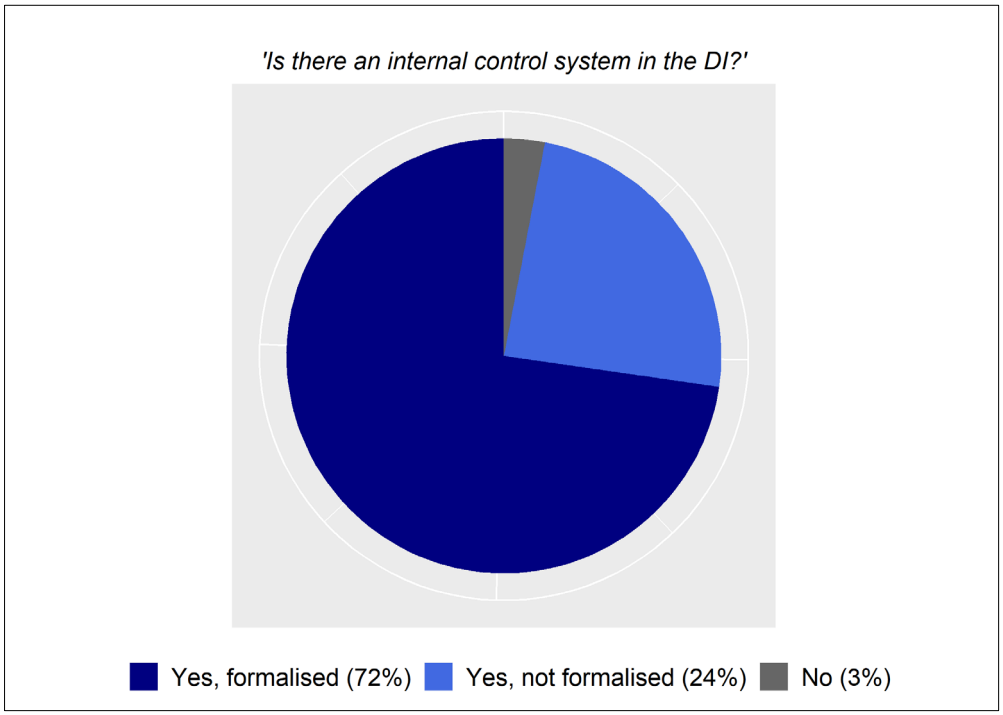


8. Internal Control System

Risk management ensures the capability to identify, prevent and overcome the obstacles to achieving the firm's objectives, and the internal control system helps to ensure risk responses are correctly and effectively implemented. It provides reasonable assurance that objectives will be achieved. The internal control system aims to ensure effectiveness and efficiency in the organisation's activities, management fairness, information reliability, and compliance with applicable laws and regulations. Continuity of controls over time is another fundamental requisite: internal control should not just be performed at a single point in time, but rather it should operate continuously and at all levels of the organisation.

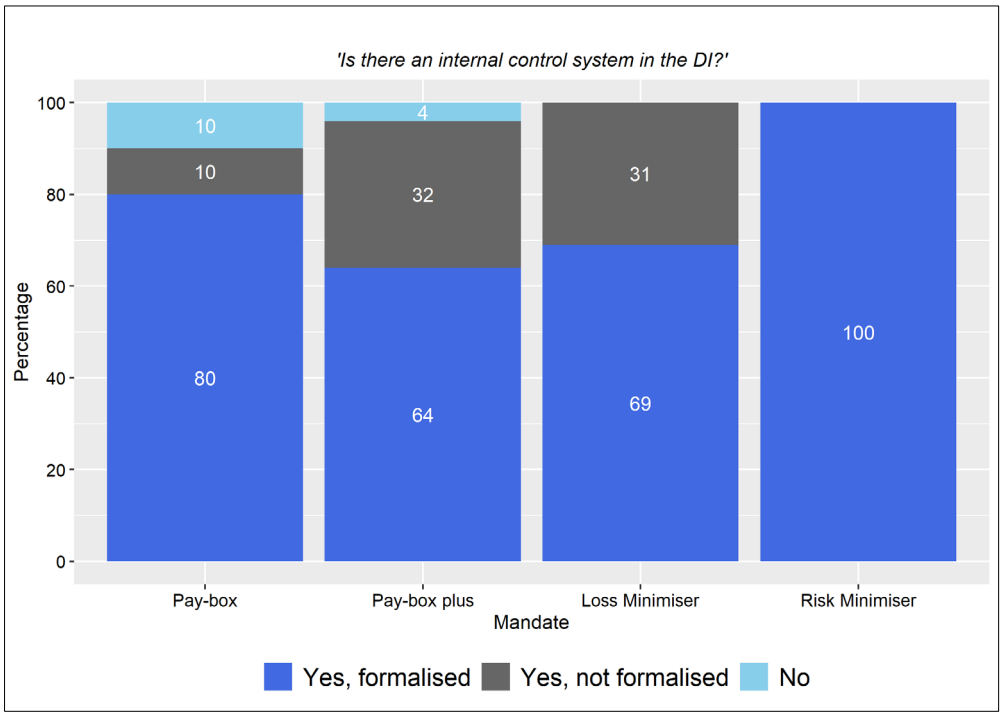
The survey found that 72% of DIs had implemented a formal internal control system (Chart 8). 24% of DIs have an internal control system, but without a formalised structure. Only 3% do not have any internal control system. Data breakdown by mandate shows that the presence of internal control is common to all the categories. 100% of Risk Minimiser DIs, not surprisingly, have internal controls in place (Chart 9).

Chart 8 – Internal Control System Structure



*: 58 respondents.

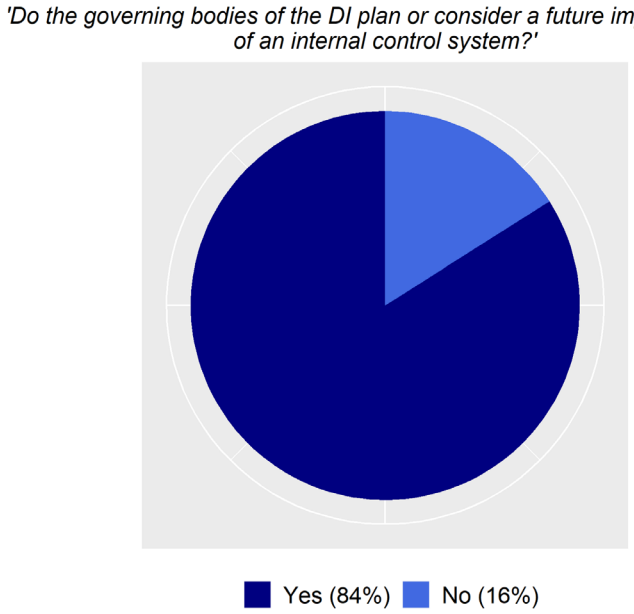
Chart 9 - Internal Control System - Breakdown by mandate



*: 58 respondents. 10 Paybox, 28 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser.

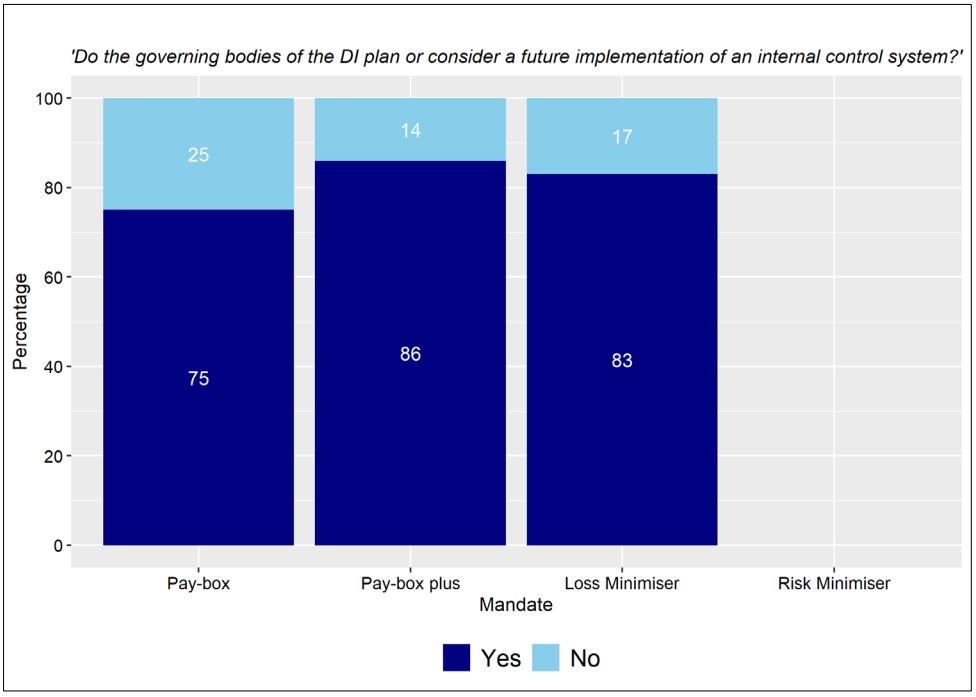
Finally, the survey found that a great majority of DIs that do not have a formal ICS (84%) are considering implementing it in the near future (Chart 10). This evidence is slightly correlated with the breadth of the mandate (Chart 11).

Chart 10 — Future Implementation of ICS



*: 17 respondents.

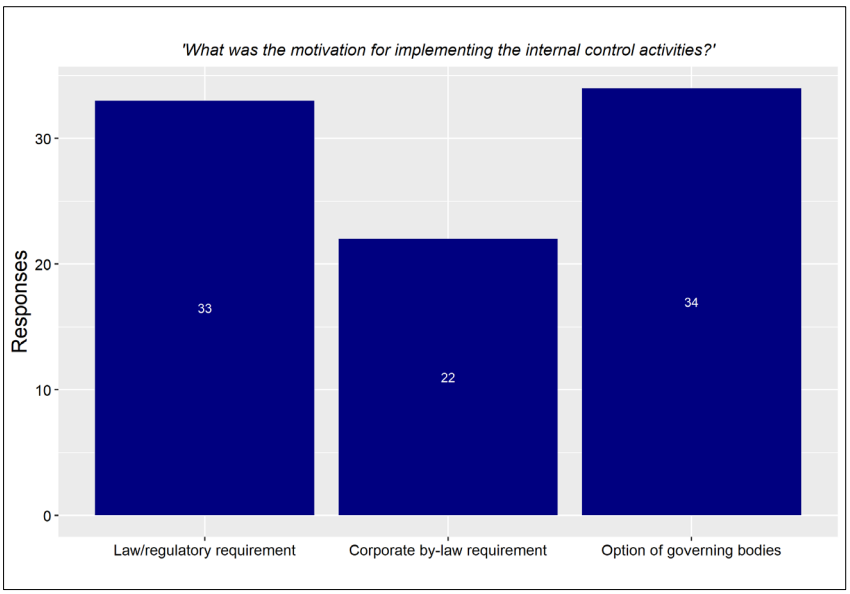
Chart 11 – Future Implementation of ICS - Breakdown by mandate



*: 17 respondents.

83% of the governing bodies of the DIs have formalised policies and objectives for the internal control system. This finding is apparently not related to the type of mandate.[24] In addition, DIs declared that, in almost all cases, governing bodies are responsible for overseeing internal control activities. The main motivations for implementing internal control activities arise from law/regulatory requirements and options of the governing bodies (Chart 12).

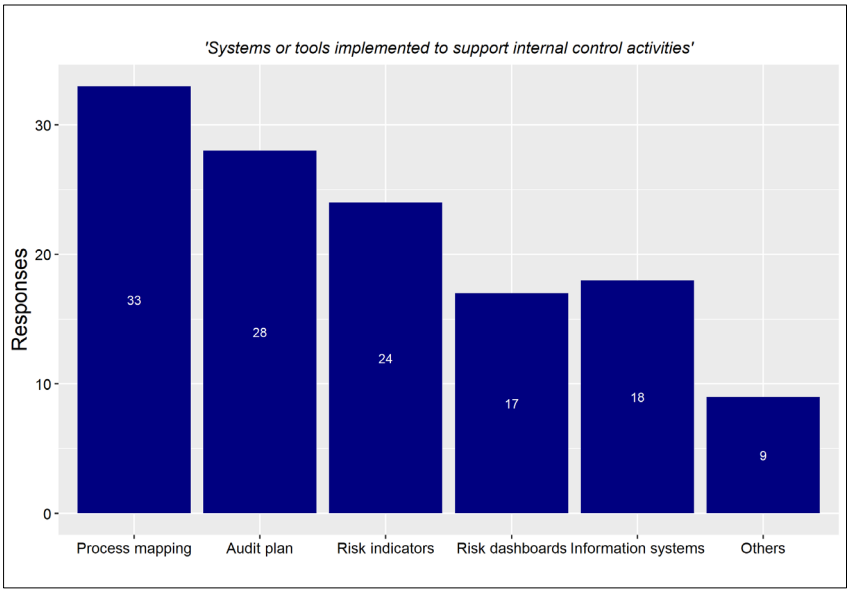
Chart 12 – Motivation for Implementing ICS - Absolute values



*: 58 respondents. Answers are not mutually exclusive.

Moreover, it was found that 74% of DIs have implemented systems or tools to support internal control activities. Mapping operational processes, preparing plurennial audit plans based on risk assessment and using key risk indicators are the most common systems or tools implemented by DIs (Chart 13).

Chart 13 – Implementation of Systems or Tools



*: 43 respondents. Answers are not mutually exclusive.

[24] See Annex – Survey Statistics.

9. Three Lines of Defence approach

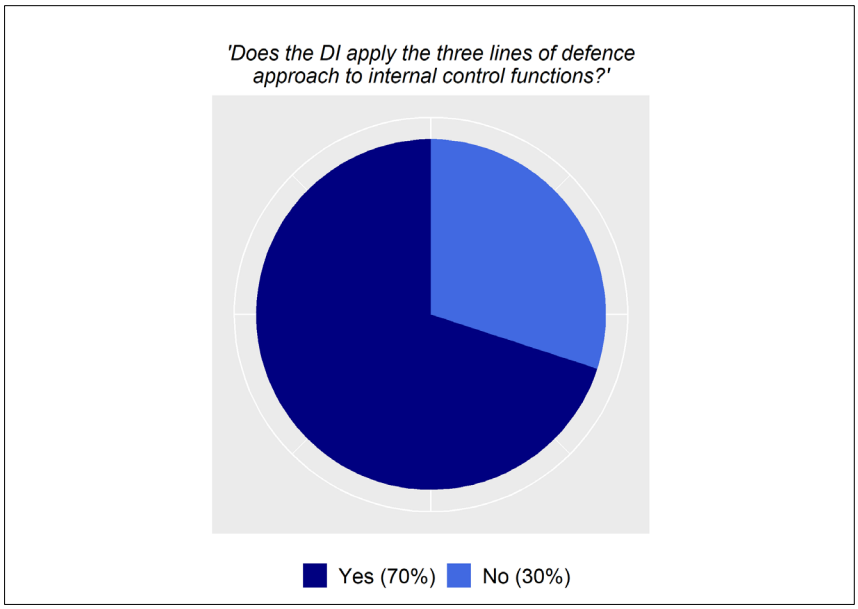
The Three Lines of Defence approach is a framework for how risk and control processes should be structured. The model is based on three lines of control. The First Line refers to functions/roles that own and manage risks that are represented by people whose activities generate the risks through their daily responsibilities. The Second Line oversees or specialises in risks management and performs the compliance function to comply with laws, regulations, rules, related self-regulatory organisation standards, and codes of conduct. The Third Line provides independent assurance over both the first and second line efforts in risk management (Internal Audit).

The survey shows that 70% of DIs use The Three Lines of Defence approach (Chart 14). The use of this control approach is fairly well spread over all the mandate categories of DIs (Chart 15)

Among the DIs that apply the Three Lines of Defence Approach, 69% have implemented an internalised audit function. Among DIs with an externalised audit function, 64% have someone at the DI as a contact person.[25]

Box 10 provides an example of a Three Lines of Defence Policy of a large DI with a Paybox Plus mandate. Box 11 reports an advanced organisational structure of risk management (of a Loss Minimiser DI), where there is a Risk Committee, Chief Risk Officer (CRO) and all the Three Lines of Defence in place.

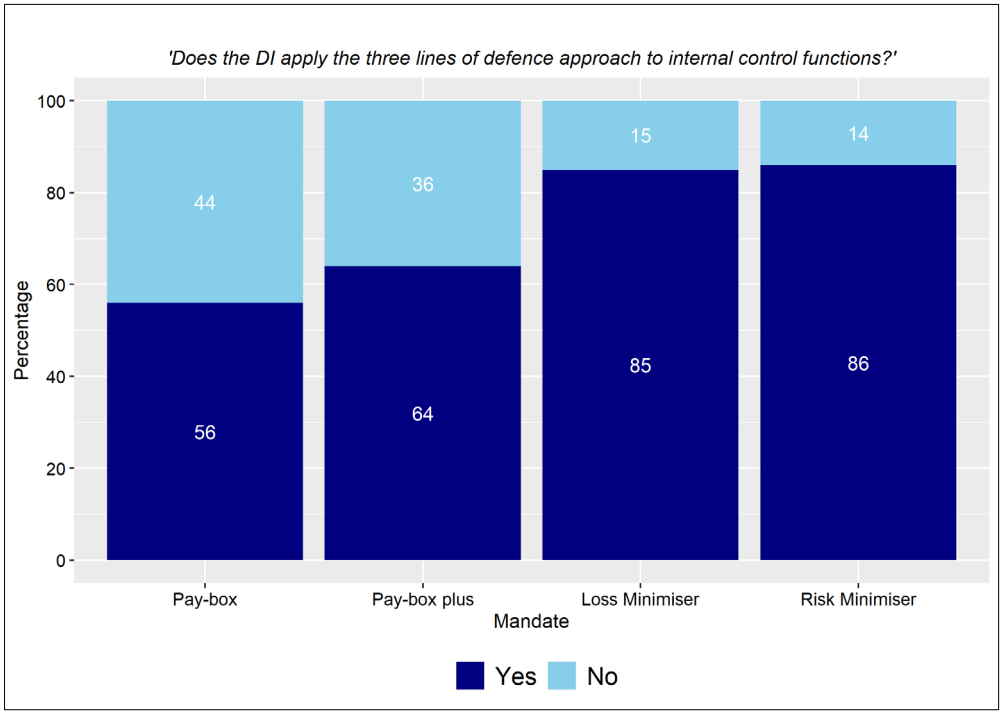
Chart 14 – Three Lines of Defence Approach



*: 57 respondents.

[25] See Annex – Survey Statistics.

Chart 15 – Three Lines of Defence Approach - Breakdown by mandate



*: 57 respondents: 9 Paybox, 28 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser.

Box 11 – *Three Lines of Defence* Policy - Example

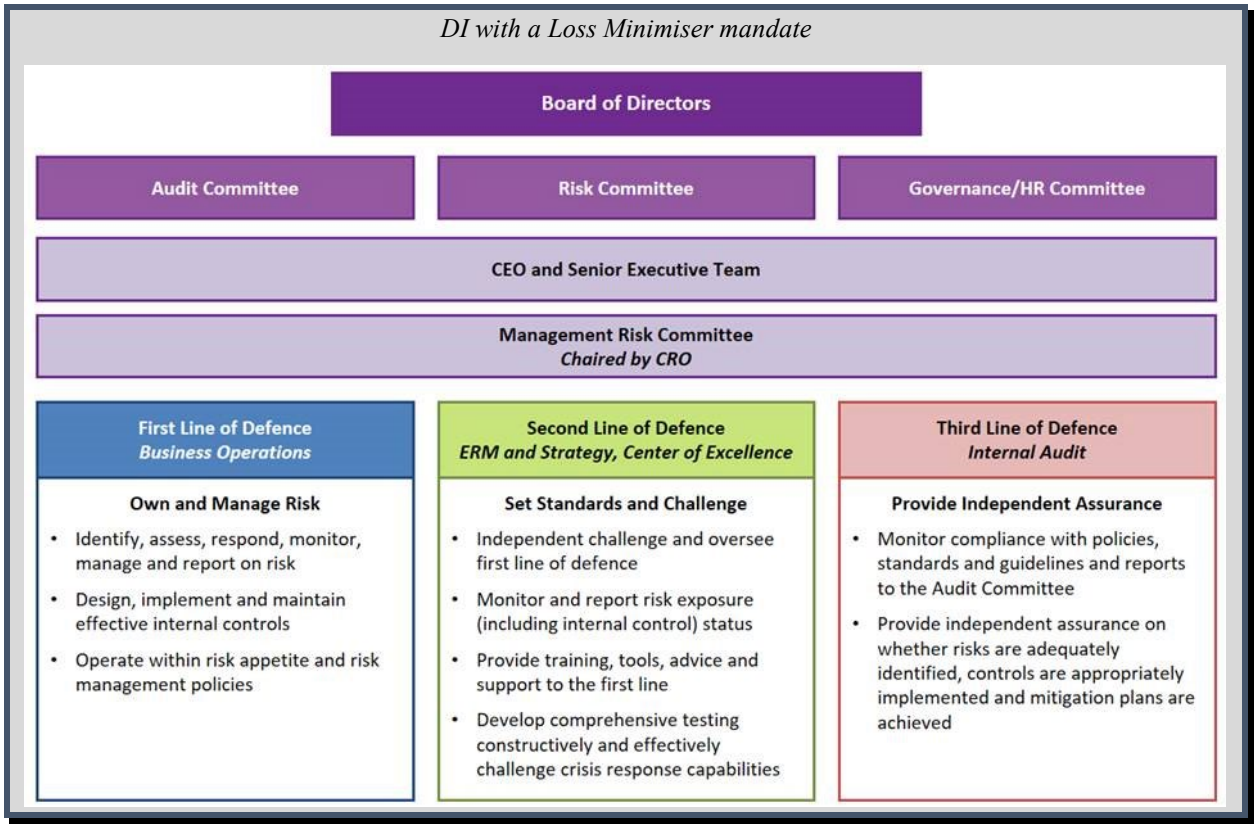
DI with a Paybox Plus mandate

The First Line of Defence is the management of the DI's business functions and business processes and is responsible for identifying risks, Assessing risks, designing and implementing operating controls to primarily mitigate risks, maintaining documentation of risk and controls; reporting on management within their areas of responsibility; and taking remedial action in response to identified control weaknesses.

The Second Line of Defence is the Risk function, headed up by the Head of Risk. The function is accountable to the Board's Risk Committee and has an open and unfettered reporting line to its Chairman. It is responsible for: establishing and maintaining the risk framework, the risk policy and relevant standards, methodologies and tools; facilitating risk identification and assessment by the First Line; monitoring and reporting on risk exposure against tolerance and progress in addressing deficiencies in risk and control.

The Third Line of Defence is the independent Internal Audit function, headed by the Head of Internal Audit and reporting to the Board's Audit Committee. It is responsible for providing independent assurance over internal control, risk management and governance …

Box 12 – Risk Management Organisational Structure - Example



10. Communication and Reporting

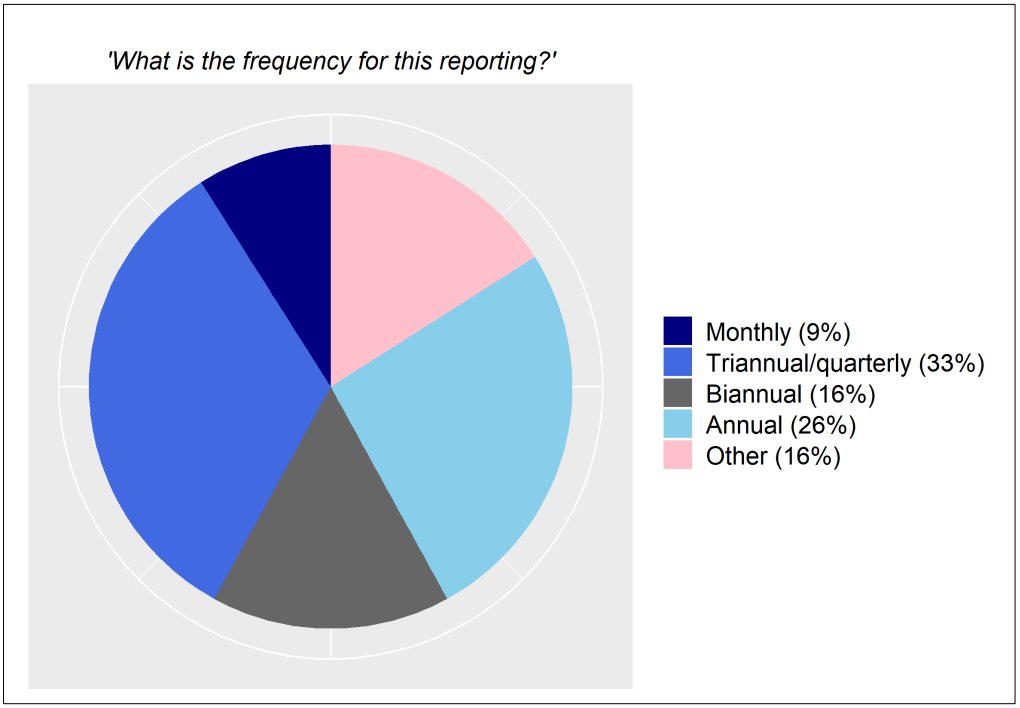
Communication and reporting are considered essential elements of the risk management and the internal control frameworks.

The survey investigates whether the DI report risk management to the governing bodies. It was found that 72% of DIs report to the board. This finding correlates with DIs' mandates: 100% of Risk Minimiser DIs, and 60% of Payboxes, report to the board.[26]

With regard to the frequency of this reporting, 33% of DIs report three to four times a year, 16% twice a year and 26% annually (Chart 16).

[26] See Annex – Survey Statistics.

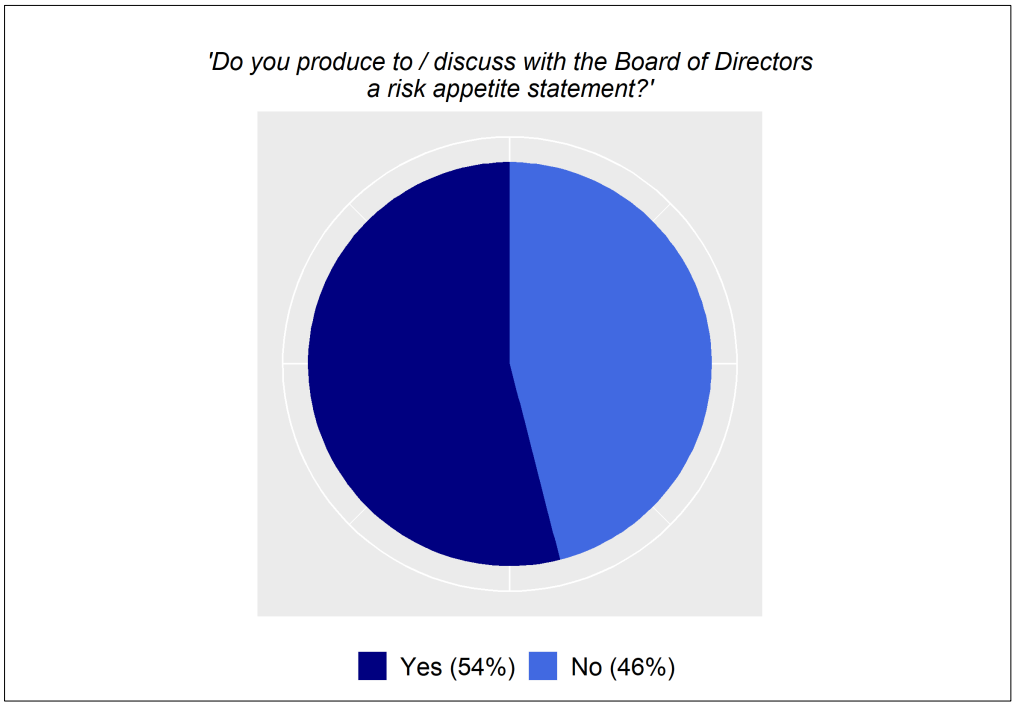
Chart 16 – Frequency of Risk Management Reporting



*: 42 respondents: 6 Paybox, 18 Paybox Plus, 11 Loss Minimiser, 7 Risk Minimiser.

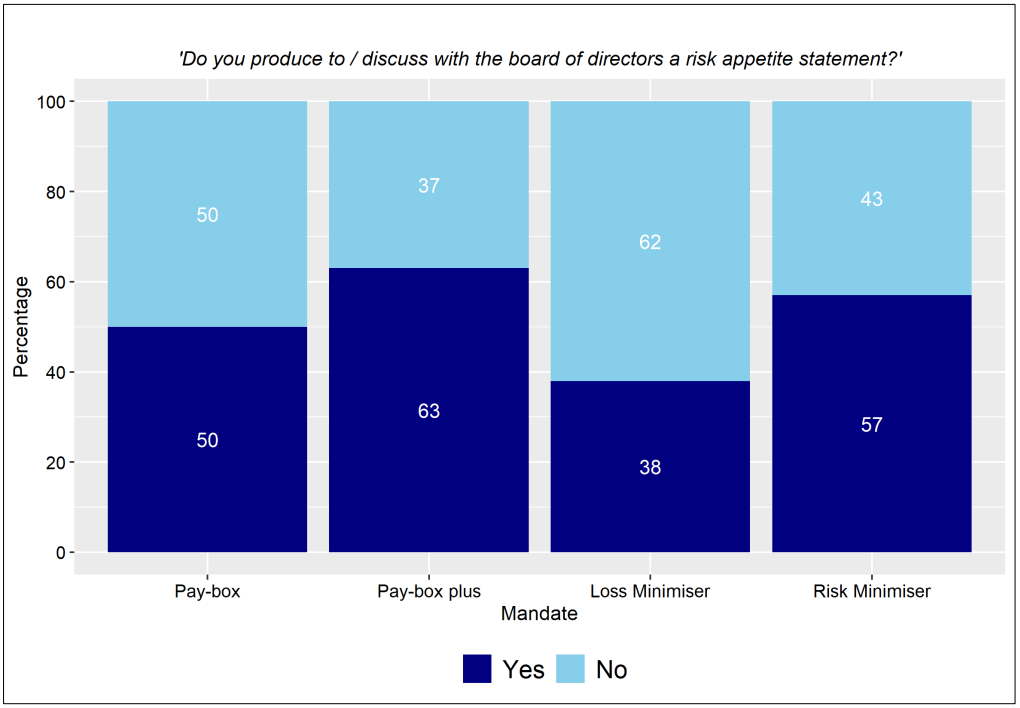
The survey investigated communication activities with regard to the risk appetite statement. Accordingly, Chart 17 shows that 54% of DIs communicate with the governing bodies on the risk appetite framework. The breakdown by mandate shows similar evidence for all types of DIs (Chart 18).

Chart 17 – Communication on Risk Appetite Statement



*: 57 respondents.: 10 Paybox, 27 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser

Chart 18 – Communication on Risk Appetite Framework - Breakdown by mandate



*: 57 respondents: 10 Paybox, 27 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser.

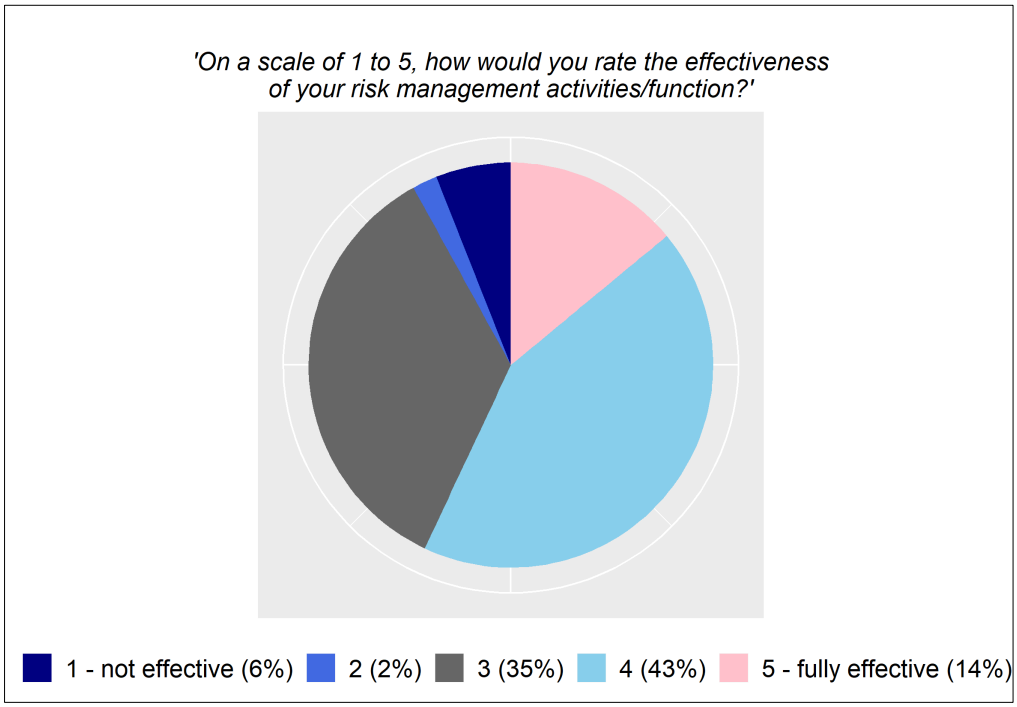
IV.C. Benchmarking Tool

The survey investigated how the DI evaluates itself and rates its own risk management framework and internal control system. This is a simple exercise of subjective assessment because DIs were left free to self-assess their framework without any specific pre-defined criteria. Overall, responses can be interpreted as a general proxy of how DIs perceive the quality of their risk management and internal control framework. This self-assessment can then be compared with peer findings by means of a benchmarking table that is presented later in this paragraph.

The survey shows that the majority of DIs (78%) evaluate themselves quite well: at an intermediate/upper level in terms of their risk management structure (Chart 19). In particular, 14% consider their structure excellent; only 6% of respondents rate the effectiveness of their risk management structure at a basic level.

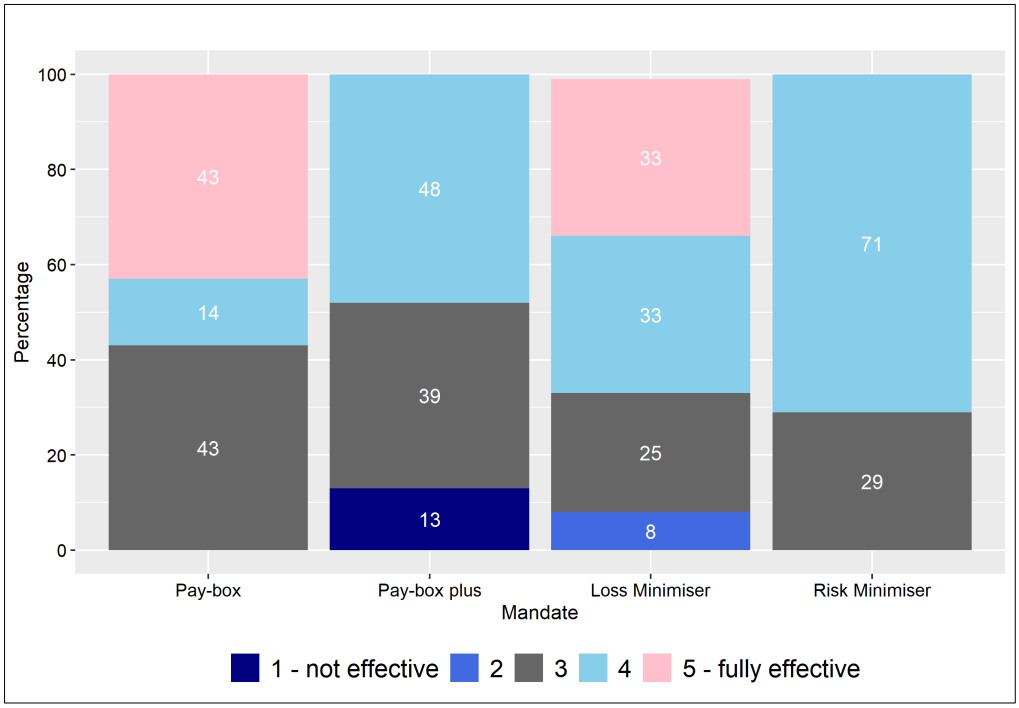
Chart 20 shows the breakdown by DI mandate. None of the Risk Minimisers rated their framework at the highest level. By contrast, 43% of the Payboxes perceived their RM and ICS frameworks to be excellent.

Chart 19 – Risk Management Self-Assessment



*: 49 respondents.

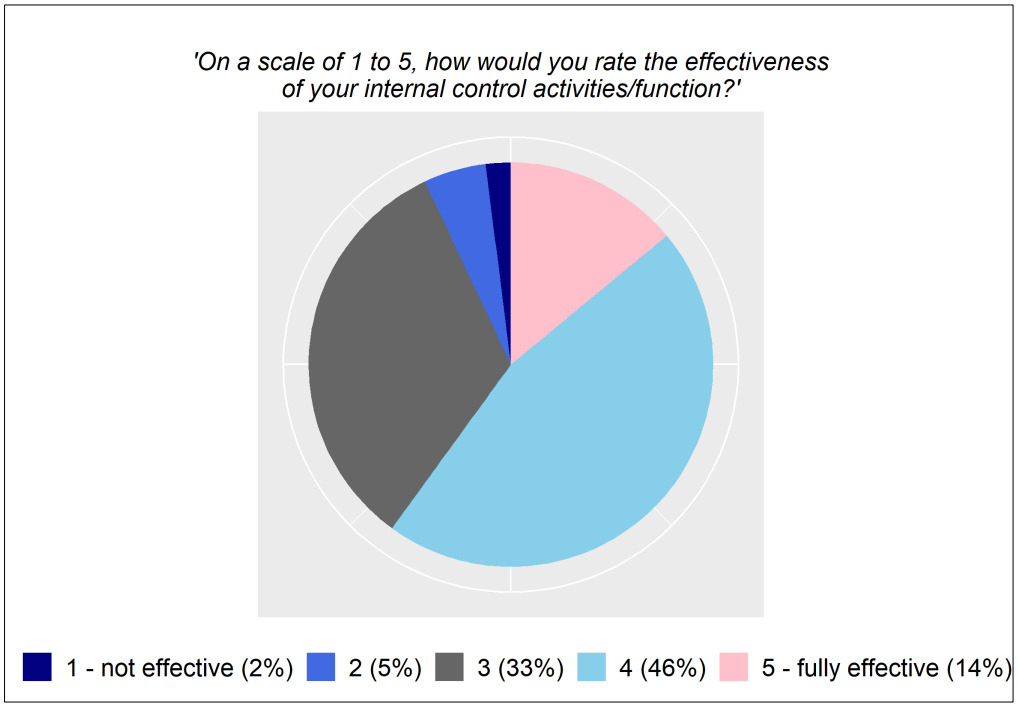
Chart 20 – Risk Management Self-Assessment - Breakdown by mandate



*: 49 respondents: 7 Paybox, 23 Paybox Plus, 12 Loss Minimiser, 7 Risk Minimiser.

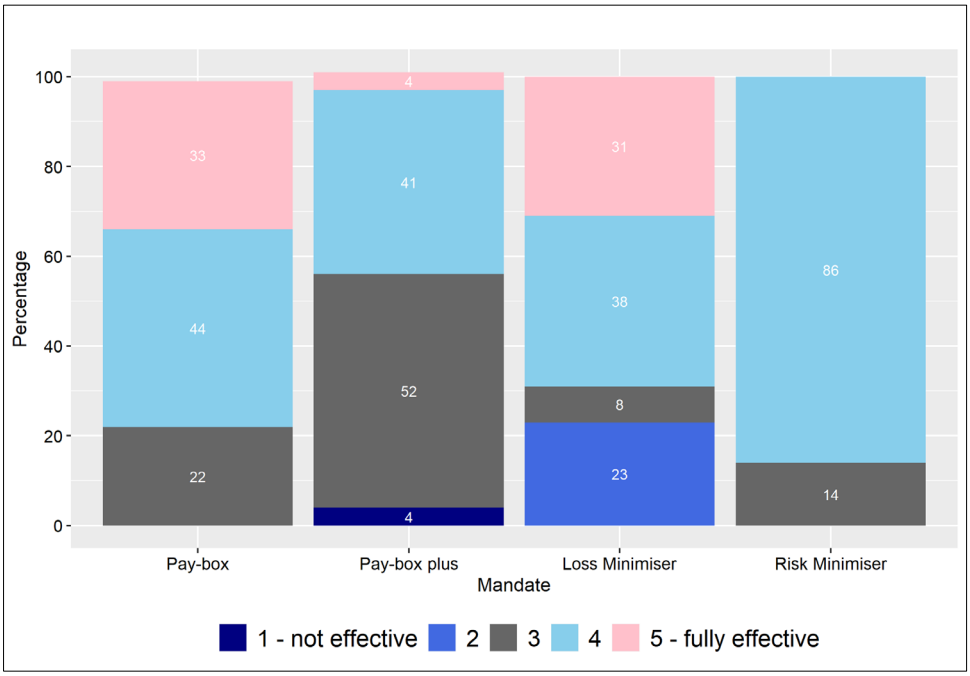
The results of self-assessment conducted with regard to ICS are consistent with those of risk management. Indeed, a great majority of DIs (79%) rate the effectiveness of this function at an intermediate/upper level. 14% evaluate themselves as fully effective and only 2% of respondents rate their internal control activities as not effective at all (Charts 21 and 22).

Chart 21 – Internal Control System Self-Assessment



*: 56 respondents.

Chart 22 – ICS Self-Assessment - Breakdown by mandate



*: 56 respondents: 9 Paybox, 27 Paybox Plus, 13 Loss Minimiser, 7 Risk Minimiser.

As already anticipated, survey findings allow a DI to objectively benchmark its self-assessment rating against peer statistics.[27] To this end, survey statistics are codified on a scoring scale and reported in Table 8. It lists all the most relevant questions of the survey questionnaire. For each question, a possible score is reported, computed on the basis of possible answers.[28] The table can be used as a self-benchmarking tool: a DI wishing to benchmark itself against its peers' profiles from the survey can first compute its own score and then compare it with mean peer scores.

Table 8 – Benchmark - Questionnaire[29]

N.	Questions:	Q. n.	Possible answers amd scores	Max Score	Paybox	Paybox Plus	Loss Min.	Risk Min.	Mean
1	3) Is there one person or group of persons performing risk management-related activities in the DI?	Q3	1) Yes, there is a formal risk management structure =2; 2) Yes, but there is No formal risk management structure = 1; 3) No = 0	2	0.9	1.4	1.5	2.0	1.4
2	e) Have governing bodies defined and formalised the policies and objectives regarding risk management?	Q3e	1) Yes = 1; 2) No = 0	1	0.5	0.6	0.8	0.9	0.7
3	f) Have governing bodies decided the type and amount of risk the DI is willing to accept?	Q3f	1) Yes = 1; 2) No = 0	1	0.4	0.4	0.5	0.7	0.5
4	g) Are governing bodies responsible for overseeing risk management?	Q3g	1) Yes = 1; 2) No = 0	1	0.5	0.8	0.8	1.0	0.8
5	12) Overall, do you provide to / discuss with the Board of Directors a risk appetite statement?	Q12	1) Yes = 1; 2) No = 0	1	0.5	0.6	0.4	0.6	0.5
6	g) Have governing bodies defined and formalised the policies and objectives regarding internal controls?	Q14g	1) Yes = 1; 2) No = 0	1	0.9	0.8	0.8	1.0	0.9
7	h) Are governing bodies responsible for overseeing internal controls?	Q14h	1) Yes = 1; 2) No = 0	1	0.9	0.9	0.9	1.0	0.9
8	b) Do distinct oversight policies apply according to the risk of the process?	Q18b	1) Yes = 1; 2) No = 0	1	0.3	0.4	0.5	0.6	0.5
9	4) Does the risk management have a process to identify risks stemming from the DI's operations?	Q4	1) Yes = 1; 2) No = 0	1	0.5	0.6	0.8	1.0	0.7
10	5) Does the risk management function have a list of risks, and their definitions?	Q5	1) Yes = 1; 2) No = 0	1	0.5	0.5	0.5	0.6	0.5
11	6) Does the DI have tools to manage the risk of bank failures?	Q6	1) Yes = 1; 2) No = 0	1	0.2	0.4	0.7	1.0	0.6
12	8) Do you have plans regarding steps, measures, or actions that the DI might follow to prepare for unexpected and extraordinary risks or shocks (contingency plans)?	Q8	1) Yes = 1; 2) No = 0	1	0.3	0.5	0.8	1.0	0.7
13	10) Do you use stress testing risk management processes?	Q10	1) Yes = 1; 2) No = 0	1	0.2	0.3	0.7	1.0	0.5
14	11) Do you assess how to transfer part of the risk portfolio to third parties such as insurance companies?	Q11	1) Yes = 1; 2) No = 0	1	0.0	0.1	0.2	0.0	0.1
15	c) Does the DI apply the "three lines of defence"; approach to internal controls functions?	Q14c	1) Yes = 1; 2) No = 0	1	0.6	0.7	0.8	0.9	0.7
16	e) If the answer to (14d) is externalised, does the DI have someone as a contact person?	Q14e	1) Yes = 1; 2) No = 0	1	0.1	0.1	0.3	0.0	0.1
17	15) Are there any systems or tools supporting the internal controls function?	Q15	1) Yes = 1; 2) No = 0	1	0.7	0.6	0.9	0.9	0.8
18	17) Are the operational processes of the DI mapped?	Q17	1) Yes = 1; 2) No = 0	1	0.7	0.6	0.8	1.0	0.8
19	18) Are the operational processes ranked by risk order (e.g. low, medium, high risk)?	Q18	1) Yes = 1; 2) No = 0	1	0.5	0.6	0.8	0.6	0.6
20	a) Are the risks quantified in monetary terms (e.g. maximum or average loss that could occur as a consequence of an event)?	Q18a	1) Yes = 1; 2) No = 0	1	0.5	0.3	0.6	0.5	0.5
21	c) Is it mandatory to develop action plans to reduce the exposure to riskier processes?	Q18c	1) Yes = 1; 2) No = 0	1	0.7	0.8	0.9	1.0	0.9
22	d) Does the DI report on its risk management to the governing bodies?	Q3d	1) Yes = 1; 2) No = 0	1	0.6	0.6	0.8	1.0	0.8
23	di) What is the frequency of this reporting?	Q3di	1) Monthly = 1; 2) Three to four times a year = 1; 3) Twice a year = 0; 4) Once a year = 0; 5) Other = 0	2	0.4	0.4	0.3	0.8	0.5
24	7) Do you prepare a plan of corrective measures adopted / intended to reduce the level of particular risks below the risk appetite level within the specified time limits?	Q7	1) Yes = 1; 2) No = 0	1	0.4	0.4	0.5	0.9	0.5
25	7i) How often is the plan updated?	Q7i	1) Quarterly = 1; 2) Semi-annually = 1; 3) Annually = 0; 4) Ad hoc = 0; 5) Other = 0	1	0.8	0.6	0.5	0.3	0.5
26	b) The risk management related activities are carried out by:	Q3b	1) An appointed Chief Risk Officer (CRO) = 1; 2) Another executive who doubles as CRO = 0; 3) Other = 0	1	0.1	0.3	0.2	0.3	0.2
27	13) Is there an internal control system in the DI?	Q13	1) Yes, there is a formalised internal control structure = 2; 2) Yes, but there are No formalised internal control structure = 1; 3) No = 0	2	1.7	1.6	1.7	2.0	1.8

[27] The validity of the benchmarking exercise is limited to the survey results.

[28] For example, for question *3 "Is there one person or group of persons performing risk management related activities in the DI"*, the score is attributed as follows:

- if the answer is "Yes, there is a formal risk management structure", the score = 2;
- if the answer is "Yes, but there is no formal risk management structure", the score = 1;
- if the answer is "No", the score = 0

On this basis, the average score for each of the 4 mandates was computed and reported in the table.

[29] Green: score values > average.

V. Final Remarks

This paper updates IADI's previous research on risk management in DIs. It draws on the well-known international standards and on a specific survey of practices among IADI Members. International standards have been essential for the analysis, since they provide views and approaches on frameworks, processes and practices of risk management applicable to all organisations. They proved to be a useful conceptual guide for the design of a risk management framework for DIs.

However, the application of the standards to the DIs should not be mechanical because of the special nature of the DI's activity and the different features of mandates and responsibilities.

The survey allowed the RMICSTC to detect how DIs currently manage their risk in terms of policy, procedures and processes. By means of a questionnaire and case studies, structured on the basis of the international standards and the RMICSTC expertise, a range of practices have been identified, showing different policies and approaches among IADI Members.

The analyses conducted showed that the majority of DIs participating in the research have a risk management framework and internal control system in place, with either a formal or informal organisational structure. The level of development/maturity of the framework varies significantly across members.

Not surprisingly, DIs with a broader mandate (Risk Minimisers) have very advanced risk management models. The 'tone at the top' clearly indicates the commitment of the governing bodies to risk management, as an essential component of corporate governance. In these cases, Boards and Audit Committees are strongly committed, with formalised risk policies and risk appetite frameworks in place, in line with their objectives and long-term strategy. The risk management processes are well structured and formalised, involving all levels of the organisation. The Three Lines of Defence model is the usual control system applied by these DIs. Monitoring and reporting activities are well organised. The risk management profiles of Loss Minimiser DIs are similar to the above, although less formalised and structured.

At the opposite end, there is the group of Paybox DIs, mostly characterised by simpler risk management frameworks, but with some exceptions. DIs with a Paybox Plus mandate are quite heterogeneous in terms of size and risk frameworks and practices. The level of diversity does not allow specific common features to be detected. However, the category would seem to include two major clusters of DIs sharing common features with, respectively, Paybox and Loss Minimiser groups.

Based on the outcomes of the analyses conducted, the RMICSTC extensively discussed the potential to define specific guidance for DIs, given the presence of international standards generally applicable to all realities. The final decision was a positive one, in the sense that the RMICSTC recognised the importance and usefulness of making available recommendations for all DIs, irrespective of the level of maturity of each system.

The RMICSTC had to face the main challenge of combining established international standards into the DI environment, in all its variety, and to come up with a table of guidance points that could be applied, without impeding DIs' flexibility and operational usefulness.

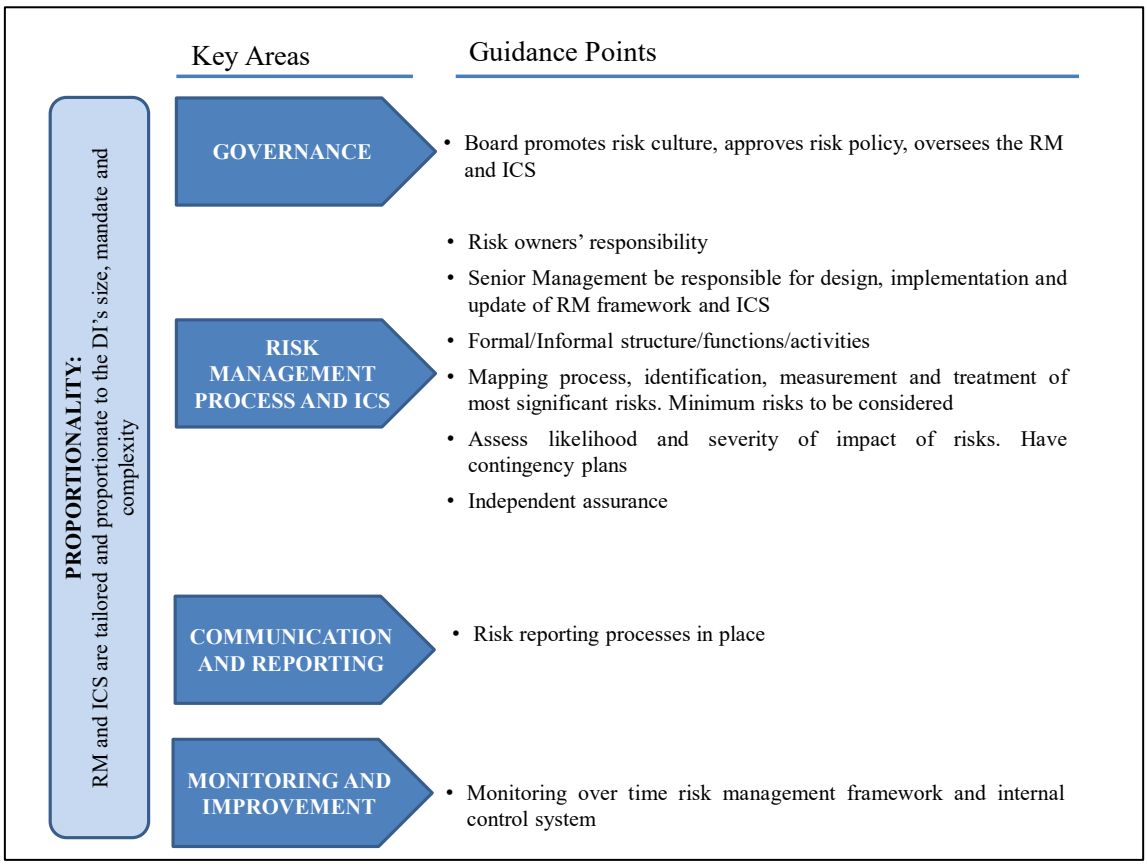
The Guidance Points consist of a set of recommendations for the following areas: i) Governance, ii) Risk Management Process and Internal Control System, iii) Communication and Reporting, and iv) Monitoring and Improvement (Fig. 5).

The Guidance Points are presented below and they are accompanied with the 'Key rationale' and the 'Text references' to easily link the guidance content to the analysis.

Future developments of this paper may look at in-depth technical analysis of the risk management framework and internal controls as well as handbooks or 'How to Apply' tools.

Finally, the RMICSTC deems that IADI CPs may benefit from considering some insights and findings coming from this research, including in CP3 a more specific provision regarding risk management within the governance provisions.

Figure 5 – Guidance - Summary



The Guidance Points are the following:

- **Governance:**

1. DIs should have in place a risk management framework and an internal control system that allows them to identify, assess, manage, respond, control and report risks that could affect their ability to fulfil their mandate and achieve the public policy objectives of deposit insurance. The risk management framework and internal control system should be tailored and proportionate to the size, mandate and operational complexity of the DI. DIs should balance costs and effectiveness of the risk management framework and internal control system.

Key rationale: *The survey found that the majority of IADI Members have a risk management framework and an internal control system. Some, however, do not yet have a framework in place. The level of formality/maturity of frameworks varies across members and increases as a DI and its mandate grows in size and is widened. The risk management framework should be proportionate to DI size and mandate and overall operational complexity. The need to customise RMICS frameworks is recommended by international standards too.*

This guidance point is related to IADI CP3 – EC4 and provides further elements on the 'sound governance' recommendation.

Text references: *§ IV.B.3; § IV.B.8; § IV.A.; § III.A and B.*

2. DIs' governing bodies should promote risk culture at all levels of the organisation, approve the organisational risk management policy and risk appetite, and provide appropriate resources. They should be responsible for the oversight of the risk management framework and internal control system and be assured on the adequacy and effectiveness of implementation of the framework.

Key rationale: *The survey found that, in most cases, IADI Members are well equipped in risk management governance. Governing bodies have set and oversee risk management policies and internal control systems. Best practices indicated that DIs have an internal audit function which provides independent assurance on risk management adequacy and effectiveness. One-third of surveyed IADI Members do not yet have a risk management policy; half have no risk appetite statement.*

This guidance point is related to IADI CP3 – EC4 and EC9 and provides further elements on the 'sound governance' recommendation regarding risk management and internal control. Guidance is also consistent with CP3 – EC7 and related additional information in the CP Assessor Handbook.

Text references: § IV.B.1; § IV.B.2; § IV.B.9; § III.A and B. DIs' best practices are reported in Boxes 1, 2, 3, 11 and 12.

3. DIs' senior management should be responsible for the design, implementation and update of the risk management framework and internal control system with the oversight of the board and other competent governing bodies. It should report periodically to the governing bodies on the risk findings and control measures.

Key rationale: *First, it emphasised the separation of role and duties between the board and the executive structure: while the oversight of the risk management framework and internal control system is a task of governing bodies, the design, implementation and update reside with the organisation. Case studies showed that in DIs with well-developed frameworks, roles and responsibilities are clearly separated and formalised. Second, risk communication is crucial for effective risk management. The survey showed that roughly a quarter of DI respondents do not report to the board on risk management. Role separation, clear allocation of responsibilities, and communication are recommended by international standards.*

This guidance point is related to IADI CP3 – EC4 and EC9. It provides further elements on the 'sound governance' recommendation regarding risk management and internal control.

Text references: *§ IV.B.10; § III.A and B. DIs' best practices are reported in Boxes 1 and 2.*

- **Risk Management Process and Internal Control System:**

4. To promote effective risk management, DIs should ensure that all employees whose daily operations pose potential risks to the DIs are aware that they have the responsibility for identifying, assessing and responding to risks.

Key rationale: *Best practices showed that effective risk management is not restricted to certain people in the DI but everyone contributes to risk management, notably for identifying and controlling risks. Compare the Three Lines of Defence approach, referred to in Guidance Point 8. This control approach is recommended by international standards.*

The guidance is related to IADI CP3 – EC3 and 4. It provides further elements on the 'human resources capacity and capabilities' and 'sound governance' recommendations.

Text references*: § III.A and B. DIs' best practices are reported in Boxes 1, 11 and 12.*

5. In order to ensure that clear roles and responsibilities are assigned to governing bodies, senior management and employees involved in Risk Management and the Internal Control System, small DIs with narrow mandates should have, at least, functions or activities with appropriate rules and documented procedures. Large DIs with broad mandates should have in place a formal risk management framework and internal control system within the organisation.

Key rationale: *The survey showed that some DIs have a formal risk management structure while others perform risk management activities without a formalised structure. According to the proportionality principle (stated in the first Guidance Point), the Technical Committee feels that small DIs with narrow mandates can follow the latter option. This guidance point is related to IADI CP3 – EC4. It provides further elements on the 'sound governance' recommendation.*

Text references*: § IV.B.3; § IV.B.8.*

6. DIs should map their operational processes, and identify and measure the most significant risks embedded in their activities. Depending on their mandate, DIs should consider a broader set of risks including, at a minimum, bank failure, financial (funding and liquidity), legal, operational, IT and information security, and reputational risks.

Key rationale: *The survey found that most IADI Members mapped and identified their risks. About 25% do not map their operational processes and, consequently, are unable to identify related risks. The survey also detected the most frequent risks identified by DIs. Based on these findings, the Technical Committee selected a minimum set of risks DIs should consider and focus on. Mapping processes and risk identification are recommended by international standards as usual steps in the risk management process.*

This guidance point is related to IADI CP3 – EC4 and EC7. It provides further elements on the 'sound governance' recommendation and EC7 comments in the CP Assessor Handbook on key DI risks.

Text references*: § IV.B.4; § III.A and B. DIs' best practices are reported in Boxes 4 and 5.*

7. DIs should have adequate tools to assess likelihood and impact of risks and to prioritise them. DIs should have a clear understanding of the types of risk response and where further action is required to mitigate risks, and have clearly defined action plans in place. This includes contingency plans, such as business continuity and disaster recovery plans, and funding contingency plans.

Key rationale: *While best practices indicated that likelihood and severity has to be assessed and mitigated, the majority of surveyed DIs do not perform risk quantitative assessment. Risk assessment is recommended by international standards*.

This guidance point is related to IADI CP3 – EC4 providing further elements on the 'sound governance' recommendation. The guidance point consistently refers to the recent IADI paper on "Deposit Insurers' Role in Contingency Planning and System-wide Crisis Preparedness and Management" (2019).

Text references*: § IV.B.5; § III.A and B. DIs' best practices are reported in Boxes 6, 7, 8 and 9.*

8. DIs should provide an independent assurance to governing bodies that risks are adequately identified, controls are appropriately implemented and mitigation plans are achieved. DIs that are larger in size and have a broader mandate and higher complexity may consider implementing the Three Lines Model approach.

Key rationale: *While the survey showed that most of the respondents use three lines of risk control, one-third of respondents do not. A well-organised application of the Three Lines of Defence approach was found in those DIs larger in size and with a broader mandate. Given these findings and in line with the proportionality principle, the Technical Committee suggests that full application of a Three Lines of Defence approach may be recommended, mainly, for larger and more complex DIs. Instead, the presence of the Third Line (internal audit), providing independent assurance on risk management adequacy, should be considered as a minimum requirement for all DIs. This guidance point is also related to guidance point 2.*

This guidance point is related to IADI CP3 – EC4/EC7 and related comments in the CP Assessor Handbook, providing further elements on the 'sound governance' recommendation and internal audits.

Text references*: § IV.B.9. DIs' best practices are reported in Boxes 11 and 12.*

- **Communication and Reporting:**

9. DIs should have in place risk reporting processes that allow for communication of risk information across all levels of the organisation.

Key rationale: *This guidance point recalls the importance of communication mentioned in guidance point 3. Here, more emphasis is put on communication and reporting across all levels of the organisation and not only between top management and the board. DI best practices showed that risk reporting generally involves the whole organisation. Each line of defence, for example, has to report on risks. Detailed risk reporting and clear communication across the organisation are recommended in international standards. This guidance point is related to IADI CP3 – EC4 and provides further elements on the 'sound governance' recommendation.*

Text references*: § IV.B.10; § IV.B.2; § III.A and B. DIs' best practices are reported in Boxes 1 and 12.*

- **Monitoring and Improvement:**

10. The risk management framework and internal control system should be monitored and reviewed periodically to ensure their adaptation to the changing internal and external environment.

Key rationale: *DIs' best practices showed that a risk management framework has to be reviewed periodically to assess its adequacy and appropriateness. Similar indications are given by international standards.*

This guidance point is related to IADI CP3 – EC4 and provides further elements on the 'sound governance' recommendation.

Text references*: § III.A and B. DIs' best practices are reported in Boxes 1 and 2.*

References

BCBS (1998), Basel Committee on Banking Supervision, Framework for Internal Control Systems in Banking Organisations, https://www.bis.org/publ/bcbs40.pdf.

BCBS (2010), Basel Committee on Banking Supervision, Principles for enhancing corporate governance, https://www.bis.org/publ/bcbs176.pdf

BCBS (2012), Basel Committee on Banking Supervision, Core Principles for Effective Banking Supervision, https://www.bis.org/publ/bcbs230.pdf

BCBS (2015), Basel Committee on Banking Supervision, Guidelines on Corporate governance principles for banks, https://www.bis.org/bcbs/publ/d328.pdf

Hannes Valtonen (2014), Chapter 18 - Risk Management, CFA Institute; https://www.cfainstitute.org/-/media/documents/support/programs/investment-foundations/18-risk-management.ashx?la=en&hash=537A7C3DEAC8FC053854B19B24D3160F8120BE68

COSO - Committee of Sponsoring Organizations of the Treadway Commission (2013), Internal Control – Integrated Framework, https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf

COSO - Committee of Sponsoring Organizations of the Treadway Commission (2004), Enterprise Risk Management — Integrated Framework Executive Summary September 2004; https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

COSO - Committee of Sponsoring Organizations of the Treadway Commission (2015), Leveraging COSO Across the Three Lines of Defence, https://www.coso.org/Documents/COSO-2015-3LOD.pdf

COSO - Committee of Sponsoring Organizations of the Treadway Commission (2017), Enterprise Risk Management Integrating with Strategy and Performance, https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Dorothy Gjerdrum, Mary Peter (2012), The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework; https://na.theiia.org/standards-guidance/Public%20Documents/7-2-%20Article_on_ISO_for_Auditors_rev7-20.pdf

European Banking Authority - EBA (2016), Guidelines on stress tests of deposit guarantee schemes under Directive 2014/49/EU https://eba.europa.eu/documents/10180/1627818/EBA-GL-2016-04+GL+on+DGS+stress+test_EN.pdf

FSB - Financial Stability Board (2013), Principles for an Effective Risk Appetite Framework, https://www.fsb.org/wp-content/uploads/r_131118.pdf

HM Treasury (2006). Thinking about risk - Managing your risk appetite: A practitioner's guide, https://webarchive.nationalarchives.gov.uk/20130102234654/http:/www.hm-treasury.gov.uk/d/tar_practitioners_guide.pdf

IADI (2007), Organizational Risk Management for Deposit Insurers, Research Paper; https://www.iadi.org/en/assets/File/Papers/Approved%20Research%20-%20Discussion%20Papers/Risk_Management_for_DIs.pdf

IADI (2009), Governance of Deposit Insurance Systems, Guidance Paper, https://www.iadi.org/en/assets/File/Papers/Approved%20Guidance%20Papers/Governance%20Final%20Guidance%20Paper%206_May_2009.pdf

IADI (2019), Deposit Insurers' Role in Contingency Planning and System-wide Crisis Preparedness and Management Guidance Paper, https://www.iadi.org/en/assets/File/Papers/Approved%20Guidance%20Papers/IADI%20Guidance%20Paper_DI%20role%20in%20contingency%20planning%20&%20crisis%20management.pdf

IADI Glossary, https://www.iadi.org/en/core-principles-and-research/publications/glossary/.

IIA – The Institute of Internal Auditors (2013), The Three Lines of Defense in Effective Risk Management and Control, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

IIA – The Institute of Internal Auditors (2019), Definition of Internal Auditing, https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

IIA – The Institute of Internal Auditors (2020), The IIA's Three Lines Model, https://na.theiia.org/about-ia/PublicDocuments/Three-Lines-Model-Updated.pdf

IRM (2011), The Institute of Risk Management, Risk Appetite and Tolerance, Guidance Paper, https://www.theirm.org/media/3779216/64355_Riskapp_A4_web.pdf

IRM (2012), The Institute of Risk Management, Risk Appetite and Tolerance, Guidance Paper, https://www.theirm.org/media/885907/Risk_Culture_A5_WEB15_Oct_2012.pdf

Frank H. Knight (1921), Risk, Uncertainty, and Profit, Hart, Schaffner, and Marx Prize Essays, No. 31. Houghton Mifflin, Boston and New York.

Official Journal of the European Union, Directive 2014/49/EU of The European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes – DGSD.

Risk and Insurance Management Society – RIMS (2011), An Overview of Widely Used Risk Management Standards and Guidelines; www.RIMS.org.

ANNEXES

ANNEX I: List of Technical Committee Members

No.	Name	Organisation	Jurisdiction
1	Giuseppe Boccuzzi (Chair)	Interbank Deposit Protection Fund	Italy
2	Akylzhan Baimagambetov	Kazakhstan Deposit Insurance Fund	Republic of Kazakhstan
3	Alain Angora	Autorité des marchés financiers	Québec, Canada
4	Alex Kuczynski	Financial Services Compensation Scheme	United Kingdom
5	Andrea Bayancela	Corporación del Seguro de Depósitos (COSEDE)	Ecuador
6	Carlos Vianna	Fundo Garantidor de Créditos	Brazil
7	Christa Walker	Canada Deposit Insurance Corporation	Canada
8	Eloise Williams Dunkley	Jamaica Deposit Insurance Corporation	Jamaica
9	Gregor Frey	esisuisse	Switzerland
10	Kumudini Hajra	IADI Secretariat	India
11	Ignatius Martin Kojo Wilson	Ghana Deposit Protection Corporation	Republic of Ghana
12	Lennart Funk	Auditing Association of German Banks	Germany
13	Margaret Chuang	Central Deposit Insurance Corporation, Chinese Taipei	Chinese Taipei
14	Martin Hlavnicka	Financial Market Guarantee System	Czech Republic
15	Natalia Vasilieva	Deposit Insurance Agency	Romania
16	Nina Johannessen	The Norwegian Banks' Guarantee Fund	Norway
17	Ridwan Nasution	Indonesia Deposit Insurance Cooperation	Indonesia
18	Said Draoui	Bank Al-Maghrib	Morocco
19	Thierry Dissaux	Fonds de Garantie des Dépôts et de Résolution	France

ANNEX II: List of DIs Participating in the Research

No.	Deposit Insurer	Survey	Case Study	Information on specific RM aspects
1	Albanian Deposit Insurance Agency – Albania	✓		
2	Autorité des marchés financiers – Québec (Canada)	✓		✓
3	Banco de Guatemala as Administrator of Fund for Savings Protection – Guatemala	✓	✓	
4	Bangladesh Bank – Bangladesh	✓		
5	Bank Deposit Guarantee Fund – Romania	✓		
6	Bulgarian Deposit Insurance Fund – Bulgaria	✓		
7	Canada Deposit Insurance Corporation – Canada	✓		✓
8	Central Deposit Insurance Corporation – Taiwan (Chinese Taipei)	✓		
9	Compensation Scheme of German Banks – Germany	✓		
10	Corporación de Protección Del Ahorro Bancario – Uruguay	✓		
11	Deposit Insurance Agency of Serbia – Serbia	✓		
12	Deposit Insurance and Credit Guarantee Corporation – India	✓		
13	Deposit Insurance Corporation – Bahamas	✓		
14	Deposit Insurance Corporation – Trinidad and Tobago	✓		
15	Deposit Insurance Corporation of Japan – Japan	✓		
16	Deposit Insurance Corporation of Mongolia – Mongolia	✓		
17	Deposit Insurance Fund – Czech Republic	✓	✓	
18	Deposit Insurance Fund – Macedonia	✓		
19	Deposit Insurance of Vietnam – Vietnam	✓		
20	Deposit Protection Agency – Thailand	✓		
21	Deposit Protection Agency of the Kyrgyz Republic - Kyrgyz Republic	✓		
22	Deposit Protection Corporation – Zimbabwe	✓		
23	Deposit Protection Fund – Montenegro	✓		
24	EAS Liechtenstein – Liechtenstein	✓		
25	esisuisse – Switzerland	✓	✓	
26	Federal Deposit Insurance Corporation - United States	✓		✓
27	Financial Services Compensation Scheme - United Kingdom	✓	✓	
28	Fondo de Garantias de Instituciones Financieras – Colombia	✓		
29	Fondo de Seguro de Depósitos (FOSEDE) – Honduras	✓		
30	Fonds de Garantie des Dépôts et de Résolution – France	✓		
31	Guarantee Deposit Fund – Paraguay	✓		
32	Fundo Garantidor de Créditos – Brazil	✓	✓	
33	Fundo Garantidor do Cooperativismo de Crédito – Brazil	✓		
34	Depositor's Insurance Fund – Libya	✓		
35	Guarantee Fund for Financial Services – Kingdom of Belgium	✓		

36	Hellenic Deposit & Investment Guarantee Fund (TEKE) - Greece	✓		
37	Hong Kong Deposit Protection Board – China	✓		
38	Indonesia Deposit Insurance Corporation – Indonesia	✓		
39	Instituto para la Protección al Ahorro Bancario – Mexico	✓		
40	Interbank Deposit Protection Fund – Italy	✓		✓
41	Jamaica Deposit Insurance Corporation – Jamaica	✓		
42	Jordan Deposit Insurance Corporation – Jordan	✓		
43	Kazakhstan Deposit Insurance Fund JSC – Republic of Kazakhstan	✓		
44	Kenya Deposit Insurance Corporation – Kenya	✓		
45	Malaysia Deposit Insurance Corporation – Malaysia	✓		
46	Moroccan Deposit Insurance Corporation – Morocco	✓		
47	National Deposit Insurance Fund of Hungary (NDIF) – Hungary	✓		
48	Nigeria Deposit Insurance Corporation – Nigeria	✓		✓
49	Palestine Deposit Insurance Corporation – Palestine	✓		
50	Philippine Deposit Insurance Corporation – Philippines	✓		
51	Deposit Insurance Fund of Kosovo – Republic of Kosovo	✓		
52	Savings Deposit Insurance Fund – Turkey	✓		
53	Singapore Deposit Insurance Corporation – Singapore	✓		
54	State Corporation Deposit Insurance Agency – Russian Federation	✓		
55	Swedish National Debt Office (SNDO) – Sweden	✓		
56	The Bank Guarantee Fund – Poland	✓		
57	The Norwegian Banks' Guarantee Fund – Norway	✓	✓	
58	West African Monetary Union Deposit Insurance and Resolution Fund – Senegal	✓		
59	Deposit and Credit Guarantee Fund of Nepal – Nepal	✓		
60	The Auditing Association of German Banks – Germany	✓		

ANNEX III: Survey Statistics

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q2(a)	a) Organisation	Government	78%	20%	42%	24%	13%	45
		Private	22%	8%	69%	15%	8%	13
Q2(c)	c) Mandate	Paybox	17%					
		Paybox plus	48%					
		Loss minimiser	22%					
		Risk minimiser	12%					
Q2(f)	f) Is the DI the Supervisor of the covered Financial Institutions?	Yes	12%	14%	14%	14%	57%	7
		No	88%	18%	53%	24%	6%	51
Q2(g)	g) Is the DI the resolution authority?	Yes	33%	5%	16%	47%	32%	19
		No	67%	23%	64%	10%	3%	39
Q3	3) Is there one person or group of persons performing risk management-related activities in the DI?	Yes, there is a formal risk management structure	57%	9%	48%	21%	21%	33
		Yes, but there is no formal risk management structure	29%	24%	47%	29%	0%	17
		No	14%	38%	50%	13%	0%	8
Q3(a)	a) Are the governing bodies of the DI planning or considering future implementation of a Risk Management function/process?	Yes	68%	19%	48%	29%	5%	21
		No	32%	40%	40%	0%	20%	10
Q3(b)	b) The risk management-related activities are carried out by:	An appointed Chief Risk Officer (CRO)	24%	8%	58%	17%	17%	12
		Another executive who doubles as CRO	16%	13%	25%	38%	25%	8
		Other	60%	17%	50%	23%	10%	30

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q3(c)	c) What was the motivation for implementing the risk management-related functions? [check more than one if applicable]	Law/regulatory requirement	35%	6%	44%	33%	17%	18
		Corporate by-laws requirement	41%	10%	62%	29%	0%	21
		Option of the governing bodies	75%	19%	49%	19%	14%	37
Q3(d)	d) Does the DI report on its risk management to the governing bodies?	Yes	72%	14%	43%	26%	17%	42
		No	28%	25%	63%	13%	0%	16
Q3(di)	If yes, what is the frequency for this reporting?	Monthly	9%	0%	75%	25%	0%	4
		Three to four times a year	33%	21%	29%	14%	36%	14
		Twice a year	16%	29%	43%	29%	0%	7
		Once a year	26%	9%	55%	27%	9%	11
		Other	16%	0%	43%	43%	14%	7
Q3(e)	e) Have governing bodies defined and formalised the policies and objectives regarding risk management?	Yes	69%	15%	45%	25%	15%	40
		No	31%	22%	56%	17%	6%	18
Q3(f)	f) Have governing bodies decided the type and amount of risk the DI is willing to accept?	Yes	46%	15%	42%	23%	19%	26
		No	54%	19%	55%	19%	6%	31
Q3(g)	g) Are governing bodies responsible for overseeing risk management?	Yes	79%	11%	50%	24%	15%	46
		No	21%	42%	42%	17%	0%	12
Q4	4) Does the risk management have a process to identify risks stemming from the DI's operations?	Yes	71%	15%	44%	24%	17%	41
		No	29%	24%	59%	18%	0%	17
Q5	5) Does the risk management function have a list of risks, and their definitions?	Yes	53%	19%	45%	23%	13%	31
		No	47%	15%	52%	22%	11%	27

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q5(b)	b) What kind of risks are considered by your risk management function? [check more than one if applicable]	Credit	69%	5%	37%	32%	26%	19
		Interest rate	60%	0%	40%	40%	20%	15
		Funding	67%	5%	45%	30%	20%	20
		Operational/legal	93%	8%	46%	27%	19%	26
		IT and information security	76%	8%	42%	29%	21%	24
		Strategic	56%	7%	40%	27%	27%	15
		Market	64%	6%	38%	31%	25%	16
		Currency	36%	9%	36%	27%	27%	11
		Liquidity	84%	4%	43%	30%	22%	23
		Bank failure	62%	9%	45%	27%	18%	22
		Reputational risk	73%	11%	33%	28%	28%	18
		Others	33%	0%	25%	0%	75%	4
Q6	6) Does the DI have tools to manage the risk of bank failure?	Yes	54%	7%	40%	30%	23%	30
		No	46%	31%	58%	12%	0%	26
Q6(i)	If yes, what are they? [check more than one if applicable]	Regular risk-based audits carried out by the DI	38%	0%	33%	25%	42%	12
		Use of DI internal credit ratings models applied on financial institutions	56%	0%	44%	22%	33%	18
		Ongoing monitoring of key risk indicators for all banks based on regulatory and bank-internal reporting (banks are required to report regularly to the DI)	72%	4%	35%	30%	30%	23

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
		Trigger talks with other financial safety-net participants to find a risk mitigation strategy	66%	10%	33%	29%	29%	21
		Provide liquidity assistance loans	28%	11%	22%	22%	44%	9
		Provide loans to shareholders for capital injection	19%	0%	17%	50%	33%	6
		Definition of special requirements for banks (e.g. limitation of amount of covered deposits, definition of higher capital ratios, other limitations)	31%	10%	30%	10%	50%	10
		Early intervention measures (e.g. acquisition of troubled bank and subsequent silent resolution, which is often cheaper than the compensation of depositors)	41%	0%	15%	38%	46%	13
		Apply supervisory framework or intervention guidelines	38%	0%	33%	33%	33%	12
		Others	19%	0%	50%	17%	33%	6

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q7	7) Do you prepare a plan of corrective measures adopted/intended to reduce the level of particular risks below the risk appetite level within the specified time limits?	Yes	49%	14%	43%	21%	21%	28
		No	51%	21%	52%	24%	3%	29
Q7(i)	If yes, how often is the plan updated and how often is the fulfilment of respective measures evaluated?	Quarterly	21%	17%	67%	0%	17%	6
		Semi-annually	32%	22%	33%	33%	11%	9
		Annually	39%	9%	45%	18%	27%	11
		Ad-hoc	4%	0%	0%	0%	100%	1
		Other	4%	0%	0%	100%	0%	1
Q7(ii)	Measures evaluated	Quarterly	36%	10%	50%	20%	20%	10
		Semi-annually	29%	25%	25%	25%	25%	8
		Annually	29%	25%	50%	13%	13%	8
		Ad-hoc	4%	0%	0%	0%	100%	1
		Other	4%	0%	0%	100%	0%	1
Q8	8) Do you have plans regarding steps, measures, or actions that the DI might follow to prepare for unexpected and extraordinary risks or shocks (contingency plans)?	Yes	64%	8%	42%	31%	19%	36
		No	36%	35%	55%	10%	0%	20
Q9	9) On a scale of 1 to 5, where 1 is 'not effective at all' and 5 is 'fully effective', how would you rate the effectiveness of your risk management activities/function?	1	6%	0%	100%	0%	0%	3
		2	2%	0%	0%	100%	0%	1
		3	35%	18%	53%	18%	12%	17
		4	43%	5%	52%	19%	24%	21
		5	14%	43%	0%	57%	0%	7
Q10	10) Do you use stress-testing risk management processes?	Yes	45%	8%	28%	36%	28%	25
		No	55%	27%	63%	10%	0%	30

	QUESTION							
CODE	**QUESTIONS**	**OPTIONS**	**%**	**PayBox**	**Paybox Plus**	**Loss Minimiser**	**Risk Minimiser**	**TOTAL (No.)**
Q11	11) Do you assess how to transfer part of the risk portfolio to third parties such as insurance companies?	Yes	12%	0%	57%	43%	0%	7
		No	88%	20%	46%	20%	14%	50
Q12	12) Overall, do you provide to / discuss with the Board of Directors a risk appetite statement?	Yes	54%	16%	55%	16%	13%	31
		No	46%	19%	38%	31%	12%	26
Q13	13) Is there an internal control system in the DI?	Yes, there is a formalised internal control structure	72%	19%	43%	21%	17%	42
		Yes, but there is no formalised internal control structure	24%	7%	64%	29%	0%	14
		No	3%	50%	50%	0%	0%	2
Q14(a)	a) Are the governing bodies of the DI planning or considering a future implementation of an internal control system?	Yes	84%	21%	43%	36%	0%	14
		No	16%	33%	33%	33%	0%	3
Q14(b)	b) What was the motivation for implementing the internal control activities? [check more than one if applicable]	Law/regulatory requirement	57%	12%	45%	27%	15%	33
		Corporate by-laws requirement	38%	14%	50%	36%	0%	22
		Option of the governing bodies	59%	24%	50%	18%	9%	34
Q14(c)	c) Does the DI apply the three lines of defence approach to internal control functions?	Yes	70%	13%	45%	28%	15%	40
		No	30%	24%	59%	12%	6%	17
Q14(d)	d) If the answer to (14c) is yes, is internal audit internalised or externalised?	Internalised	69%	10%	52%	19%	19%	31
		Externalised	31%	21%	43%	36%	0%	14

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q14(e)	e) If the answer to (14d) is externalised, does the DI have someone as a contact person?	Yes	64%	11%	44%	44%	0%	9
		No	36%	20%	40%	40%	0%	5
Q14(f)	f) Have governing bodies defined and formalised the policies and objectives regarding internal controls?	Yes	83%	19%	46%	21%	15%	48
		No	17%	10%	60%	30%	0%	10
Q14(g)	g) Are governing bodies responsible for overseeing internal controls?	Yes	93%	17%	48%	22%	13%	54
		No	7%	25%	50%	25%	0%	4
Q15	15) Are there any systems or tools supporting the internal control function?	Yes	74%	19%	40%	28%	14%	43
		No	26%	13%	73%	7%	7%	15
Q15(i)	If yes, what are they?	Mapping of operational processes	79%	21%	39%	24%	15%	33
		Plurennial audit plan based on risk assessment	67%	21%	36%	21%	21%	28
		Key risk indicators	57%	17%	38%	29%	17%	24
		Dashboards of key risks	40%	6%	35%	35%	24%	17
		Internal risk management information system	43%	22%	28%	28%	22%	18
		Others	21%	0%	44%	33%	22%	9
Q16	16) On a scale of 1 to 5, where 1 is 'not effective at all' and 5 is 'fully effective', how would you rate the effectiveness of your internal control activities/function?	1	2%	0%	100%	0%	0%	1
		2	5%	0%	0%	100%	0%	3
		3	32%	11%	78%	6%	6%	18
		4	46%	15%	42%	19%	23%	26
		5	14%	38%	13%	50%	0%	8
Q17	17) Are the operational processes of the DI mapped?	Yes	74%	16%	42%	26%	16%	43
		No	26%	20%	67%	13%	0%	15

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
Q18	18) Are the operational processes ranked by risk order (e.g. low, medium, high risk)?	Yes	62%	17%	44%	28%	11%	36
		No	38%	18%	55%	14%	14%	22
Q18(a)	a) Are the risks quantified in monetary terms (e.g. maximum or average loss that could occur as a consequence of an event)?	Yes	41%	19%	31%	38%	13%	16
		No	59%	17%	52%	17%	13%	23
Q18(b)	b) Do distinct oversight policies apply according to the risk of the process?	Yes	68%	12%	46%	27%	15%	26
		No	32%	17%	50%	25%	8%	12
Q18(c)	c) Is it mandatory to develop action plans to reduce the exposure to riskier processes?	Yes	78%	13%	47%	28%	13%	32
		No	22%	33%	44%	11%	11%	9
Q18(d)	d) Who is responsible for the mapping?	Internal Controls	28%	13%	53%	7%	27%	15
		External Consultants	6%	0%	33%	67%	0%	3
		The area executing the process	47%	16%	32%	36%	16%	25
		Other	19%	20%	60%	10%	10%	10
Q18(e)	e) Who has the authority to set the risk order of the process?	The area executing the process	20%	13%	38%	38%	13%	8
		Risk Management/ CRO	32%	15%	46%	31%	8%	13
		Internal Audit	20%	13%	63%	25%	0%	8
		Audit Committee	10%	0%	75%	0%	25%	4
		CEO or Director General	27%	36%	36%	18%	9%	11
		Internal Controls/ICO	7%	0%	33%	0%	67%	3
		Management Board	24%	20%	40%	40%	0%	10

CODE	QUESTION	OPTIONS	%	PayBox	Paybox Plus	Loss Minimiser	Risk Minimiser	TOTAL (No.)
		Board of Directors	41%	18%	53%	18%	12%	17
		Others	15%	33%	33%	33%	0%	6
Q19	19) Would the DI be available to take part as a Case Study for the Project Work Group?	Yes	54%	13%	52%	23%	13%	31
		No	46%	23%	42%	23%	12%	26