IOPS Working Papers on Effective Pension Supervision, No.44

RESILIENCE OF PENSION SUPERVISION AGAINST SHOCKS: SUPERVISORY AUTHORITIES' CRISIS MANAGEMENT PLANS

Nina Paklina
June 2025

IOPS WORKING PAPERS ON EFFECTIVE PENSION SUPERVISION

As the proportion of retirement income provided by private pensions becomes increasingly important, the quality and effectiveness of their supervision become ever more crucial. The IOPS Working Paper Series, launched in August 2007, highlights a range of challenges that need to be addressed in the development of national pension supervisory systems. The papers review the nature and effectiveness of new and established pensions supervisory systems, providing examples, experiences and lessons learnt for the benefit of IOPS members and the broader pensions community.

IOPS Working Papers are not formal publications. They present preliminary results and analysis and are circulated to encourage discussion and comment. Any usage or citation should take into account their provisional nature. The findings and conclusions of the papers reflect the views of the authors and may not represent those of the IOPS membership as a whole.

IOPS WORKING PAPERS
ON EFFECTIVE PENSION SUPERVISION
are published on www.iopsweb.org

RESILIENCE OF PENSION SUPERVISION AGAINST SHOCKS: SUPERVISORY AUTHORITIES' CRISIS MANAGEMENT PLANS

Nina Paklina

ABSTRACT

The report reviews crisis management programmes adopted or being under development by IOPS supervisory authorities, based on a survey of 38 jurisdictions conducted in March 2024. Its aim was to collect experiences and to identify key elements and policy recommendations that could assist pension supervisors in strengthening their crisis management arrangements and preparedness for future crises.

The findings of the report show that about half of respondent authorities have established some formal crisis management arrangements, either within their authority or at the national level. To handle major incidents or crisis effectively, supervisors emphasise the need for a clear mandate and appropriate powers, allowing for flexibility to respond swiftly to various crisis scenarios.

Crisis management programmes are generally part of a supervisor's risk management framework and encompass internal governance arrangements, and business continuity and disaster recovery plans. For some respondents, the framework also includes resolution plans. Most often, multi-layered risk governance and management structures are used, which involve various management bodies and functions, each operating within their respective governance scope. The survey revealed a broad diversity of internal governance arrangements and structures that supervisory authorities put in place to anticipate and manage major crises. Some key common elements were identified such as having in place dynamic governance structures, allowing for flexibility to configure and adapt crisis planning; critical role of leadership; ensuring planned coordination actions and information exchange with supervised entities. Respondents emphasised the need for a crisis management and business continuity strategy with clear, written action plans and procedures to maintain or restore operations. Nearly half of respondents have implemented such written plans and procedures.

Business continuity and disaster recovery plans must be regularly reviewed, audited and updated. To have a holistic view of level of resilience and preparedness across the market and the compatibility of recovery strategies of financial institutions, supervisors have begun to organise industry-wide stress testing exercises.

Respondents also emphasised the importance for crisis preparation and management, strong strategic relationships and effective information-sharing mechanisms with peer supervisors and other relevant public authorities.

The report concludes with policy recommendations aiming to help policymakers enhance the resilience of pension supervision frameworks, thereby ensuring long-term sustainability and continued protection of retirement savings.

Keywords: pension supervision, private pensions, risk management, crisis management, business continuity plans, stress testing

JEL codes: G-23, G-28, H-12

Resilience of pension supervision against shocks: Supervisory authorities' crisis management plans

Background:

The resilience project aims to review crisis management arrangements and identify good practices that supervisory authorities may have in place to successfully withstand current and future shocks. The project draws on the experiences of IOPS Members and from other financial sectors. It provides a check list of key elements to assist pension Supervisory Authorities in designing crisis management programmes and strengthening oversight in this critical area.

The project started in 2024 and continues as part of the new IOPS 2025-2026 Programme of Work (POW). It expands the previous IOPS work on supervisory lessons learnt from Covid-19 pandemic[1]. It also uses the findings from the IOPS work stream on risk-based supervision (RBS), especially stress testing. The revision of the IOPS Principles is also reflected in this work.

The Project was driven by IOPS Members. Project Team Members were Chile; Hong Kong, China; Ireland; Kenya; Uganda and Zimbabwe. Mrs. Úrsula Schwarzhaupt, IOPS Vice President, Head of Regulation Intendancy, Pensions Supervisor, Chile, was the leader of this Project.

Research methods for developing the project included: IOPS survey, desk research and collection of the IOPS jurisdiction-specific examples. Definitions of terms used in the report are provided in the Glossary section.

[1] IOPS (2020), IOPS statement on pension supervisory actions to mitigate the consequences of the Covid-19 crisis, 26 May 2020, http://www.iopsweb.org/IOPS-statement-on-pension-supervisory-actionsCovid-19-crisis.pdf

Contents

Boxes

Figures

Tables

Executive Summary

A series of recent major crises have reinforced the importance for supervisory authorities and supervised entities to have in place well-designed crisis management programmes, such as business continuity management (BCM) and disaster recovery plans.

The present report reviews the strategies and main elements for crisis preparedness and management programmes that have already been adopted or are under development by IOPS supervisory authorities, based on a survey of 38 jurisdictions conducted in March 2024.

About half of the respondent authorities have established some formal crisis management arrangements, either within the authority or at the national level.

Most of the respondents have had the necessary regulatory and supervisory powers for effective crisis management, whereas in some jurisdictions, the powers for crisis management and resolution of the pension industry have only recently been expanded by legislative changes.

The survey responses indicate that **a broad diversity of internal governance arrangements** and structures have been implemented within supervisory authorities.

Crisis management structures tend to be integrated in supervisors' overall risk governance frameworks and encompass internal governance arrangements, business continuity plans, and disaster recovery plans. About 80% of the respondents have established Business Continuity Plan(s) (BCP) that are tailored to different crises to ensure continuity of essential supervisory operations and services. Crisis management frameworks can also include resolution plans. Slightly more than half of the respondents have a resolution division or team within their authorities. In about one third of the respondents, resolution teams operate as integral components of the broader crisis management framework.

A formal crisis management framework usually covers all major incidents, including financial crises and operational disruptions. Within such a broad framework, plans dedicated to a particular type of critical incident may be set up. Usually resolution plans cover financial crises, whereas business continuity plans and disaster reduction plans ensure continued business operation during an emergency.

Pension supervisors emphasised that a strong risk culture and governance framework, with clear roles and responsibilities, is essential for effective risk and crisis management. Flexible governance structures are needed to ensure a successful crisis response, allowing for adaptable crisis planning and for implementation of ad-hoc measures as the external environment changes.

Pension supervisors stressed the importance having in place comprehensive written crisis management plans. Procedures should be flexible, structured in multiple action levels and adaptable to a wide range of risks. Nearly half of the respondents have already implemented such measures.

Supervisors conduct regular testing of business continuity and disaster recovery plans as well as crisis communication protocols. The testing includes crisis simulation exercises to evaluate responses to various crisis scenarios. In some jurisdictions, supervisors also run industry-wide stress tests of business continuity plans to assess market-wide resilience and the alignment of recovery strategies across participants. Internal and external audits could be performed to ensure robustness.

Open and on-going co-operation with peer supervisors and other public authorities is crucial for effective crisis management. Pension supervisors actively participate in established bodies such as the Council of Financial Regulators or Financial Stability Committee/Commission to co-operate and undertake policy dialogue on systemic risks and crisis management. Supervisors are also reinforcing co-operation at the international level in the area of crisis management, in particular as part of their efforts to strengthen the supervision of international financial groups.

Introduction

Enhancing the stability and resilience of financial systems is one of the overarching objectives of prudential supervision. Such supervision aims, through the use of various prudential tools and practices, to contain the risks in the financial sector as a whole or its part, the pension sector. Increasingly, supervisory authorities endeavour to limit also risks that are outside the financial sector perimeter such as, for example, cyber or technological risks. Supervisors do not strive to fully eliminate risks as they cannot operate in a zero-failure regime. They achieve their goal, in part, by planning for and implementing crisis management and resolution programmes.

Covid-19 pandemic represented a deep shock and a significant disruption to the world economy. It had a profound impact on the ways companies and public authorities, including supervisory authorities, had to operate to withstand the crisis and re-organise their activities in the period of global pandemic. The pandemic offered a real-world test of the operational resilience of the supervisory authorities.

Most recently, global financial system experienced a series of another distresses, including the banking crisis in March 2023 and various macroeconomic and geopolitical shocks. Supervisory attention, in addition to these more cyclical events, is also directed to the structural transformations affecting the financial sector, such as digitalisation, climate change, demographic change[2].

An increasing interconnectedness of the global financial system, and its evolving and complex nature, heighten the risk of contagion, where shock in one financial sector can quickly propagate to other sectors and take a cross-jurisdictions dimension. Going further, risks or shocks emanating from non-financial sectors are impacting the financial industry and should be also considered.

In most jurisdictions, supervisory measures are directed to maintain or strengthen resilience of the financial sector institutions against both cyclical and structural risks. They do that by enhancing monitoring and assessing the whole range of risks weighing on the financial system.

A series of recent major crises has reinforced the importance of having in place relevant and well-defined strategies, such as business continuity management (BCM) policies and action plans. Strengthening the resilience against shocks is increasingly important for both supervisors and financial institutions themselves.

This report looks specifically at crisis management programmes by supervisory authorities. These programmes enable supervisors to maintain conduct of effective supervision of pension systems regardless of any major disruption or crisis[3], while also ensuring the safety and health of supervisory staff. In recent years, supervisory authorities have taken measures to review and reinforce their crisis management programmes or considered introducing them in case they have not yet implemented such programmes.

In March 2024, the International Organisation of Pension Supervisors (IOPS) surveyed its Members about their crisis management programmes (developed or under development). Thirty-eight Members offered their highly informative responses. Some authorities referred to confidential internal documents in relation to crisis management plans that are, therefore, not disclosed in this report. Members' responses provided a wide range of insights and experiences upon which the project has

[2] See Glossary section. The survey does not cover the ageing of population that will have significant consequences on pension liabilities in the longer run. The report defines significant incident (crisis) as a sudden and relatively not long-term phenomenon. Therefore, we exclude long-lasting shocks to pension systems that would have specific demographic implications.

[3] It is understood in the report that significant incident/crisis could be interpreted both as a market-related crisis or a major operational disruption caused by natural disaster, terrorist attack, sanitary crisis, technology failure, major cyber-attack, etc.

drawn. The respondents are almost equally divided among the integrated (20) and specialised (pension sector) supervisors (18).

The paper is divided into five sections. The first briefly discusses regulations in place in respondent jurisdictions that give powers to supervisors for crisis management. Next, it reviews the crisis management frameworks (implemented or under development) aimed at addressing the key risks and shocks that supervisory authorities could face. The third section canvasses various forms of governance arrangements and organisational structures used by supervisory authorities to anticipate and respond to major disruptions. The fourth one highlights the various types of crisis management plans and focuses on the key responsibilities and general procedures that must be followed prior to and during the crisis, including communication, incident reporting, and other key aspects. The fifth section briefly describes co-operation arrangements between supervisors and other public authorities that are aimed at taking coordinated actions when a major crisis emerges. The conclusions are presented in the final section of the report, while a separate document outlines policy recommendations that can be translated into actionable steps for supervisory authorities when developing crisis management programmes, regulatory frameworks and supervisory practices. The report also includes a list of main terms in a glossary.

1. Legislative or regulatory powers for crisis management

1.1. Supervisory Authorities' legislative and regulatory powers to effectively manage crises

Roughly **half of the respondents have in place crisis management frameworks.** These frameworks are formal governance structures such as bodies or committees established either at the level of their authority or at the national level. They aim to efficiently deal with any significant incidents or crises that may impact a supervisors' ability to conduct effective supervision of the pension systems and to deliver on their mandates.

The responses of IOPS Members show that a **diverse set of internal governance arrangements** and **institutional operational structures** have been implemented within supervisory Authorities **for crisis management**. However, they allow for several common approaches and learning experiences to be explored.

Essentially, supervisors believe they need to have appropriate powers to deal with significant incidents or crisis.[4] Respondents emphasised that laws or regulations should give supervisors a clear mandate and powers, ensuring sufficient flexibility to respond promptly and efficiently to diverse crisis scenarios. Supervisors should be able to assess the effectiveness of these powers and to take appropriate follow-up actions.

Most respondents (28 or 76%) stated that they have the necessary effective regulatory and supervisory powers for crisis management. These powers are usually described in the pension laws or in other relevant financial legislation. In some jurisdictions, the law responsible for macroprudential policy and supervision would include provisions in relation to the identification and monitoring of systemic risks, crisis management and resolution (North Macedonia, Poland). Also, standards, guidance or handbooks issued by other public authorities, including Financial Sector Committees[5] or Parliaments, could be applied to direct supervisors in the event of a financial crisis or emergency situation. In Indonesia, a special Law Number 9 on Prevention and Handling of the Financial System Crisis was issued in 2016. For the pension sector, the Indonesian supervisor (OJK) has developed

[4] See Glossary section.

[5] Or similar bodies; names change depending on jurisdiction.

Implementation regulations for the Crisis Management Protocol (CMP), based on the OJK circular letter[6].

Respondents outlined **key regulatory and supervisory powers they hold over supervised entities, both proactively and during the crisis**, including powers:

- to oversee the governance and risk management processes carried out by the supervised entities
- to obtain additional data and information, as needed (e.g. in crisis situations)
- to monitor supervised entities' business continuity plans
- to provide temporary legislative relief from certain requirements; such relieves could be extended in time and tailored to the needs of the crisis situation
- to prohibit the transfer of members between fund managers
- to introduce restrictions on free disposal of assets or setting of a capital surcharge
- to require a supervised entity via a recovery plan to reduce its risk profile (strengthen or restore the financial or liquidity situation or take other measures)
- to use enforcement and/or sanctioning powers (i.e., issue warnings and impose sanctions which could be published)
- to resolve, within the resolution planning and capability, failing or nearly to fail supervised entities
- to exercise powers of last resort (such as security fund, policy protection fund)
- to propose new regulatory reforms.

1.2. Recent developments

Recently, **in some jurisdictions amendments were introduced to the legislative framework to grant Authorities new powers to strengthen their crisis management capability and resolution**. As an example, in 2019, the Australian Prudential Regulation Authority (APRA) expanded its resolution function to include the superannuation industry (Box 1) following the collapse of a non-APRA regulated parent company causing stress to three APRA-regulated trustees (Group) and a service company[7]. The failure could have led to significant operational disruption to members from the breakdown in critical support from the parent and the services company to the trustees.

[6] The OJK Circular letter was issued in 2016 and was later updated in 2022.

[7] Effectiveness and Capability Review of the Australian Prudential Regulation Authority, Financial Regulator Assessment Authority, June 2023, https://fraa.gov.au/sites/fraa.gov.au/files/2023-07/apra-assessment-report-2023.pdf

Box 1 APRA crisis management and resolution powers, including in superannuation

Australia:

APRA crisis management powers were legislated in 2018. The Government's– *Financial Sector Legislation Amendment (Crisis Resolution Powers and Other Measures) Act 2018* (Crisis Management Amendment Act) gave APRA the powers needed to resolve failing banking and insurance entities and in 2021 the *Treasury Laws Amendment (Your Future, Your Super) Act* extended the legislative framework for the superannuation industry which covered the concept of resolution in superannuation.

Legislative amendments and elaboration of APRA cross-industry prudential standards covering recovery and exit planning (*CPS190 Recovery and Exit Planning*) and resolution planning (*CPS900 Resolution Planning*) followed by industry consultations were finalised in May 2023. APRA's resolution planning requirement came into effect on 1 January 2024 for all industries, and the Recovery and Exit Planning requirement will be effective from 1 January 2025 for the superannuation industry.

The standards in particular set out the expectations and require trustees to have credible recovery and exit plans that are regularly tested and reviewed. Strong recovery and exit plans reduce the likelihood of resolution.

In the event of a crisis, whereby the entity is deemed to no longer be in the recovery phase but is in resolution, APRA draws on its powers from the *Superannuation Industry Supervision Act 1993*. APRA uses its resolution powers as a last resort.

APRA's primary **resolution power in superannuation** include:

- Ability to remove or suspend a trustee and appoint an Acting Trustee where legislative thresholds are met. The Acting Trustee will consider implementing resolution actions, in consultation with APRA, on the basis that these actions are in the best interest of members. These may include transferring members to another fund or changing the trusteeship of the fund where the trustee is willing to accept the transfer. The appointment of an Acting Trustee is a temporary, last resort option for crisis scenarios.
- Permit trustees to temporarily cease the transfer of members' benefits to other funds. It does not prevent the payment of pension payments.
- Direct or impose a licence condition for the trustee to take reasonable steps towards a merger or transfer of members, such as identifying potential partners. However, APRA cannot force a merger or transfer of members. APRA can also direct a related entity of a trustee to undertake an action.

In comparison to the banking and insurance industries, superannuation resolution powers are relatively limited. There are inherent limitations with the use of the Acting Trustee power. The suspension or removal of trustee and subsequent appointment of an Acting Trustee is complex and has significant operational impacts.

Members of a superannuation fund bear the significant cost of implementing an Acting Trustee arrangement, and there are substantial operational complexities arising from the change of the legal trustee entity, and the challenges of maintaining a panel of organisations willing to become an Acting Trustee.

In contrast, where APRA appoints a Statutory Manager in the banking industry, it stands in the place of the board resulting in substantially less operational disruption.

APRA's own resolution activities focus on the protection of members, promoting financial stability and maintaining critical functions. APRA uses it powers to enact its resolution strategy.

Source: Based on Member' responses to the IOPS survey 2024.

In addition to legislative powers, supervisors may adopt internal rules of crisis management procedures and arrangements.

The IOPS statement[8] released during the Covid-19 pandemic, drawing on Members' collective experiences, outlines key supervisory actions taken by IOPS members during the pandemic, which covered key priority areas: communication; support of operations and business continuity; specific supervisory requirements towards supervised entities; consumer protection; co-operation and engagement.

The set of powers given by legislators to the Authorities proved to be satisfactory for acting in a crisis context. It was observed that the recent major crises, such as the Covid-19 pandemic (2020-2021), have proven to be real-world tests of the operational resilience of Authorities and supervised entities. In this regard, it was highlighted by some Authorities (Portugal, Mauritius) that their powers proved to be satisfactory in time of crisis.

A small fraction (7 or 19%) of the respondents replied that they did not have appropriate powers to handle crises.

2. Establishment of crisis management frameworks

2.1. Formal instances and committees to proactively identify and effectively manage a wide range of crisis

Crisis management structures within supervisory authorities tend to be integrated in their overall risk governance framework and encompass internal governance arrangements, business continuity plans, and disaster recovery plans. In some respondents, such frameworks included resolution plans and other relevant risk management measures. The board or senior management of an authority leads crisis management and ensures effective implementation of crisis management policies and procedures.

Notwithstanding a large variety of approaches adopted by supervisory authorities, it was observed that where a formal crisis handling framework exists, it would usually cover all major critical incidents, including major financial or market-related incidents as well as significant incidents that may cause major operational disruptions (cyber security incidents, technology failures, natural disasters, pandemics, etc). Within such a broad framework, plans dedicated to particular types of critical incidents may be set up: usually, **resolution plans** cover a financial crisis of a regulated entity/entities, whereas **business continuity plans** and disaster reduction plans ensure business operation continuation during an emergency.

Most often, multi-layered risk governance and management structures are used, which involve various management bodies (e.g. committees) and functions, each operating within their respective governance scope. In most cases, Authorities adopt a holistic approach while managing risks, with divisions or departments acting as risk owners. These entities conduct risk and control assessments, assess adequacy and quality of controls, implement risk treatment plans and report them at their level risk registers for an ongoing monitoring. Key risks are then escalated to the Senior Management for review and oversight.

Crisis management is part of the risk management framework (RMF) in a group of respondents (14 or 38%). It is used to identify, monitor, assess and manage both emerging and structural risks that

[8] IOPS (2020), IOPS statement on pension supervisory actions to mitigate the consequences of the Covid-19 crisis, 26 May 2020, http://www.iopsweb.org/IOPS-statement-on-pension-supervisory-actionsCovid-19-crisis.pdf

affect the financial industry, the Authority, or both. The framework would also include necessary control activities and mechanisms to limit the risks to an acceptable level. In cases of some Authorities, crisis management plans could be set up separately from the supervisory RMF (e.g., Mauritius).

Several jurisdictions (Costa Rica; Hong Kong, China) indicated that their RMF for operational risk management is **structured according to the three lines of defence model** proposed by the Basel Committee on Banking Supervision (BCBS)[9]. The model reinforces Authorities' risk management capabilities and cultivates a strong risk and control culture across all business units. The roles are clearly delineated for each line, with oversight provided by specific subject matter experts, senior management, and independent audit. The "High-level principles for business continuity" of the BCBS define a business continuity plan (BCP) as a "comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organisation in the event of a disruption" (Box 2).

A majority (29 or 78 %) of respondents established BCP(s) for critical incidents to ensure the continuity of essential supervisory operations and services, as well as ensure the safety and health of staff regardless any disruption or major crisis. Figure 1 outlines key stages of preparation of the BCP by the Mandatory Provident Fund Schemes Authority of Hong Kong, China.

Some Authorities align the BCP and crisis management to the ISO 22301 Standard, which is the **international standard for Business Continuity Management Systems**. The standard provides a framework for organisations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against and recover from disruptive incidents[10].

[9] Basel Committee on Banking Supervision, Revisions to the principles for the sound management of operational risks, March 2021, https://www.bis.org/bcbs/publ/d515.pdf

[10] ISO 22301 International Standard for Business Continuity Management Systems (BCMS), https://www.iso.org/standard/75106.html

Box 2 The Basel Committee on Banking Supervision (BCBS) "High-level Principles for Business Continuity" (2006)

The BCBS High-level Principles for Business Continuity apply both to financial institutions and financial authorities.

Business Continuity Management (BCM) is part of operational risk management, which includes policies, standards and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of disruption.

Effective BCM typically incorporates business impact analysis, recovery strategies and business continuity plans as well as testing programmes, training and awareness programmes, and communication and crisis management programmes.

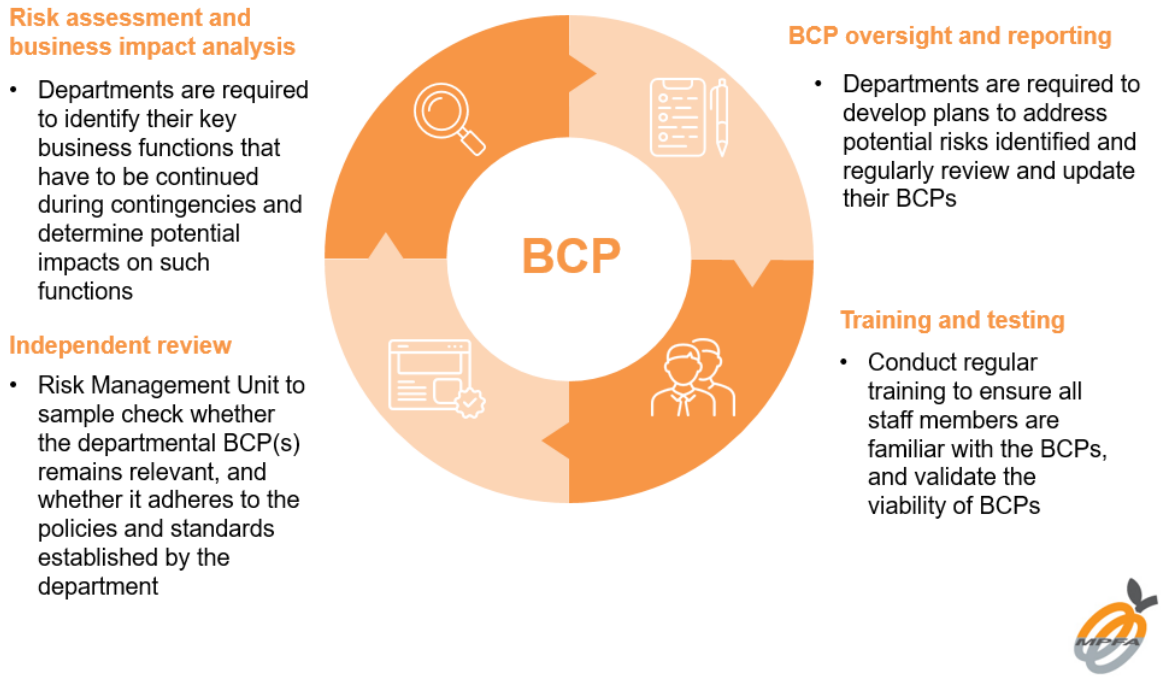
- *A business impact analysis* is dynamic process of identifying critical operations and services, key internal and external dependences and appropriate resilience levels.
- *A recovery strategy* establishes recovery objectives and priorities that are based on the business impact analysis.
- *Business continuity plans* offer detailed guidance for implementing recovery strategy. Such plan establishes the roles and allocates responsibilities for managing operational disruptions and provides clear guidance in the event of a disruption that disables key personnel. It also clearly sets out the decision-making process.

The High-level Principles for business continuity key messages are the following:

- Principle 1 emphasises that **the requirement for sound business continuity management** applies to all financial authorities and financial industry participants and that **the ultimate responsibility** for business continuity management rests with an organisation's **board of directors** and **senior managemen**t.
- Principle 2 advises organisations that they should **explicitly consider and plan for major operational disruptions**.
- Principle 3 stipulates that participants **should identify recovery objectives that are proportional** to the risk posed in order to achieve a consistent level of resilience.
- Principle 4 stresses the critical importance of **business continuity plans addressing the full range of internal and external communication issues** an organisation may encounter in the event of a major operational disruption. It especially recognises that **clear and regular communication** is essential to manage crisis and maintain public confidence.
- Principle 5 highlights critical importance of **cross-border communications** during a major operational disruption especially given interconnected nature of the financial system. It highlights the need to adopt **communication protocols**.
- Principle 6 emphasises the need to ensure that **business continuity plans are effective and necessary modifications could be introduced** through periodic testing.
- Principle 7 calls upon financial authorities **to incorporate business continuity management reviews** into their frameworks for assessing financial industry participants.

Source: The Basel Committee on Banking Supervision: "High-level Principles for Business Continuity", 2006.

Figure 1 Preparation of Business Continuity Plan by MPFA, Hong Kong, China[11]



Source: Mandatory Provident Fund Schemes Authority (MPFA), Hong Kong, China.

In Australia, business continuity management is an integrated part of the APRA risk management and control framework and aligns to supervisors' risk appetite statement.

The U.S. Department of Labor's Employee Benefits Security Administration (EBSA) has a comprehensive business continuity plan in place to maintain operations in response to a broad range of crises, including natural disasters and pandemics. All employees are required to complete annual training on continuity concepts to ensure knowledge and awareness of the agency's emergency response capabilities, thereby enabling EBSA to effectively support plan participants and beneficiaries under all conditions. In the event that the crises would impact the EBSA itself (such as a terrorist attack or new pandemic), EBSA's business continuity plan would be activated.

Several other respondents have not yet put in place formal crisis management plans and are in the process of enhancing their capacity and preparedness for crisis. This process includes the improvement of the Authorities' crisis governance infrastructure and organising continuous training for the technical staff. The Authorities from Chile, Kenya, Morocco, Portugal indicated that they were in the process of developing or finalising Business Continuity Plans and procedures. The process related to financial crisis management in the pension supervisor in North Macedonia is in the development phase.

2.2. Key risks considered by Supervisory Authority as part of crisis management plans

Supervisory Authorities are putting in place measures to strengthen resilience within the financial system. Crisis preparedness and crisis response planning by both supervisors and the industry are important parts of these efforts. It is difficult to prepare for potential future shocks owing to their uncertain character. Moreover, financial systems are becoming more complex and interconnected and

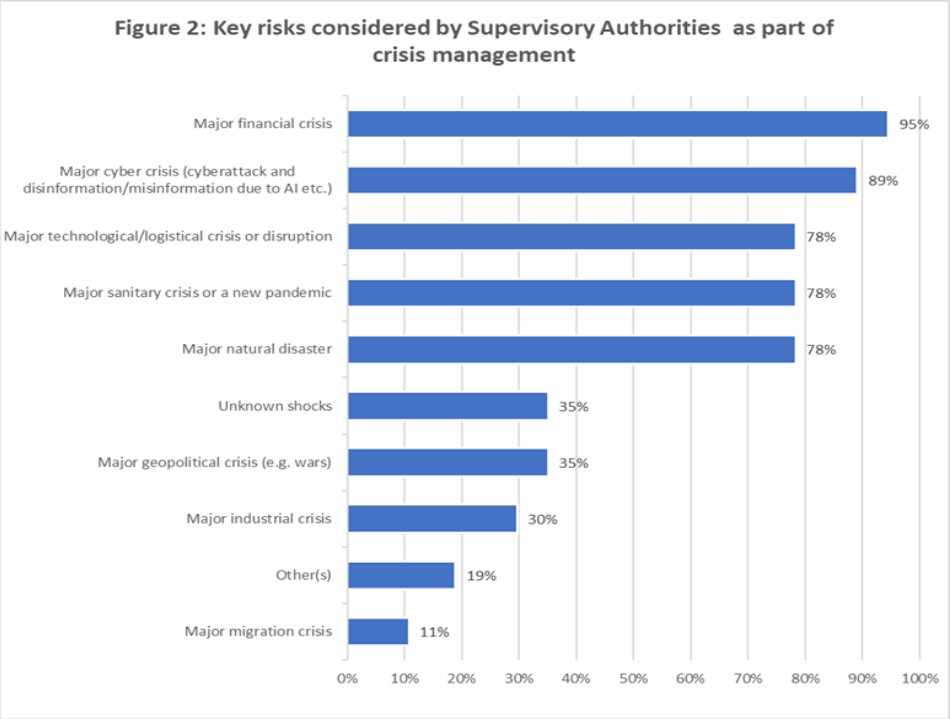
[11] Presentation by Mandatory Provident Fund Schemes Authority (MPFA), Hong Kong, China at the IOPS meeting in Mexico City, Mexico, February 2024.

the risk environment is evolving fast. As part of the IOPS survey, Members were requested to list the key risks impacting global financial systems that they consider when preparing for future crisis events.

Pension supervisory authorities believe they should adequately prepare for the following risks (Figure 2):

- **major macroeconomic/financial risks** (currently identified in various supervisory reports in the form of rising interest rates, high inflation, unstable foreign exchange) (35 or 95%);
- **growing threat of cyberattacks and scams** (such as disinformation/misinformation generated by artificial intelligence software) (33 or 89%);
- **major natural disasters** including those linked to climate change (29 or 78%); major sanitary crisis or a new pandemic (29 or 78%);
- **major technological/logistical crisis** or disruption (29 or 78%).

Figure 2 Key risks considered by Supervisory Authorities a part of crisis management



Source: Members' responses to the IOPS survey 2024.

About one-third of respondents (13 or 35%) also identified **risks stemming from geopolitical instability** affecting directly or indirectly companies in the financial sector. Supervisors highlighted an increased risk of cyber-attacks owing to major geopolitical tensions as having a high potential to damage the financial stability[12].

Several authorities also emphasised **other risks** (7 or 19%) that they consider in their crisis management programmes, such as terrorist attacks; new emerging risks, e.g., the use of artificial

[12] Financial Stability Committee, Macroprudential supervision, https://www.afs-bund.de/afs/Content/EN/Articles/Macroprudential-supervision/FSC-Communication/fsc-communication.html

intelligence; power outages; data disruption, chemical and biological hazards; changes in governmental policies on employment and retirement policies.

One-third of the respondents (13 or 35%) consider and prepare for unknown shocks. Uncertainty about how economy and financial markets will evolve is a key concern for policy makers and supervisory authorities. The concept of 'radical uncertainty' has been explored in the research literature[13]. Both financial institutions and supervisors have to deal with implications of such uncertainty. How and when major risks (e.g., macro-financial shifts, geopolitical, sanitary risks, etc.) and structural changes (digitalisation, climate change, demographic change) will materialise, and how they will affect economy and financial markets is highly uncertain. The recent European Central Bank (ECB) article[14] highlights that conventional risk models, relying on historical data, cannot assign probabilities and expected losses for future events.

In the view of supervisors, 'radical uncertainty' calls for a pivotal rethinking. They highlight the importance of developing adaptive, scenario-based strategic planning, including even greater use of alternative scenarios around the forecast that convey more of the range of possible outcomes and introduce rapid changes in the response to unexpected market movements. This also means adopting a culture of continuous learning, dynamic governance and risk management. Finally, it means building resilience in terms of capital, IT infrastructures, and operational resilience.

The major potential risks identified by supervisors are very much in line with the key global risks described in Global Risks Report (Figure 1) from the Word Economic Forum (2023)[15].

Figure 3 Global risks ranked by severity over the short- and long- terms

The colours in the table represent risk categories: Environmental, Geopolitical, Societal, Technological

Source: Global Risk Report, World Economic Forum (2023).

[13] Kay, J. and King, M. (2020) Radical uncertainty: Decision-making for an unknowable future, The Bridge Street Press

[14] https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240312~5990ccfce7.en.html

[15] Natural disasters and extreme weather events were considered as second most severe risks over the next two years by Global Risks Report 2023 from the Word Economic Forum. Global Risks Report 2025 is available on https://www.weforum.org/publications/global-risks-report-2025/.

To address new emerging operational and cyber risks and strengthen resilience, Authorities have responded by introducing a number of initiatives (Box 3).

Box 3 Members' cybersecurity initiatives

Australia:

The APRA 2020-2024 cyber security strategy is focused on strengthening cyber resilience across the financial sector by:

- Requiring establishment of baseline cyber controls, cyber hygiene and cyber-attack protocols, along with appropriate recovery plans;
- Enabling boards and executives to oversee and direct correction of cyber exposures;
- Fostering suppliers' cyber assessment; and ensuring rectification of weak links within the broader financial ecosystem and supply chain.
- Working closely with the Council of Financial Regulators (CFR) agencies to harmonise regulation and enhance supervision of cyber across the financial system as well to establish protocols to coordinate in the event of financial-system cyber incidents and system wide outages.

APRA has also required all regulated entities to undergo an independent assessment of their compliance with prudential standard CPS 234 Information Security (CPS 234), which requires adequate processes and controls to manage cyber risk. The CPS 234 tripartite assessments commenced in 2020, with most reports due to APRA for assessment by the end of 2023.

Chile:

The Chilean government has put in place a system "Computer and Security Incident Response Centre" (CSIRT) to monitor cybersecurity risks and provide coordination among government entities in case a threat is identified.

The Superintendence of Pensions (SP) has established a Security Operation Center (SOC) for internal management of cybersecurity risk. Cybersecurity crises are coordinated through the government CSIRT and the internal SP Committee/team for cybersecurity.

The United States:

The U.S. Department of Labor's Employee Benefits Security Administration (EBSA)'s focus on cyber risk has primarily resulted in promotion of preventive measures, such as improving cyber hygiene, ongoing testing and remediation of cyber vulnerabilities, and monitoring of service providers by plan sponsors.

Source: Members' responses to the IOPS survey 2024.

Some authorities have adopted a holistic approach to ensuring the resilience of the financial system, encompassing comprehensive strategies to address potential risks from multiple angles. APRA's focus on ensuring resilience in Australia's financial system and superannuation industry, from both a strategic and supervisory perspective, includes a range of initiatives such as requiring entities to establish appropriate controls (e.g., cyber controls, IT security controls and managing operational risk in key operations) and building capabilities in supervised entities. APRA focuses on assessing business continuity incidents and plans (*SPS 232 Business Continuity Management*) and information security capabilities (*CPS 234 Information Security*) of superannuation entities and where appropriate, requires improvement of these capabilities. This also includes completing some prudential thematic reviews with the learnings communicated to all superannuation entities encouraging an uplift in capabilities. Recently, APRA adopted the new prudential standard *CPS 230 Operational Risk Management)*, to recognise the critical need to better manage operational risks more broadly, and respond to business disruptions. The aim of new CPS 230, which will be effective from July 2025, and supersedes *SPS 231 Outsourcing* and SPS 232, is to:

- strengthen operational risk management through new requirements to address identified weaknesses in existing practices;

- improve business continuity planning to ensure that regulated entities are ready to respond to severe but plausible disruptions;
- enhance third-party risk management by extending requirements to all material service providers that regulated entities rely upon for critical operations or that expose them to material operational risk.

Natural disasters could also represent a major source of disruption for the supervisors' own operational resilience and capacity to deliver key supervisory services. Respondents ranked natural disasters as one of the major risks[16]. Authorities generally note an increased frequency of major natural disasters[17] and their possible impact on the financial industry[18]. Given the rising frequency and severity of natural disasters related to climate change, some authorities have included **disaster protection plans** in their crisis management frameworks, such as Disaster Recovery Plans (Ireland, South Africa) or security plans for crisis and emergency management (Namibia) to ensure that, even in crisis, they continue their work and protect critical operations. To ensure better preparedness and response for disasters resulting from natural hazards several authorities[19] have developed disaster protection plans and included them in their crisis management framework (Box 4).

Box 4 Members' initiatives on natural disaster prevention plans

Bulgaria: the Financial Supervision Commission (FSC) adopted the Disaster Protection Plan. In case of a natural disaster, the General Secretary of the FSC performs the role of the Chief Crisis Manager.

Chile: the National Disaster Prevention and Response Service (SENAPRED) monitors the variables related to natural disasters and coordinates the responses of different government authorities in case of a major event. The Superintendence of Pensions (SP) has established a plan for recovery from disasters, which aims to reestablish critical IT services that allow critical business processes in case of emergency.

Mexico: the National Commission of the Retirement Savings System (CONSAR) has implemented the Disaster Recovery and Business Continuity Plan (DRP) to ensure the continuity of the operation, in case of contingency such as natural disasters, health crises or technological interruptions. The Plan defines the integration and operation of the response groups, assigned tasks, organisation and hierarchical levels and roles of activities necessary to execute the operation continuity plan in case of contingency. The Plan is reported to the Head of the Administration and Finance Unit, who evaluates the situation and becomes the Coordinator of the actions to be implemented.

The United States: EBSA has a comprehensive continuity plan in place to maintain operations in response to a broad range of crises, including natural disasters and pandemics.

Source: Members' responses to the IOPS survey 2024.

[16] It is ranked as the second-most severe risk over the next two years by Global Risk Report, the Word Economic Forum (2023) and the first of the top ten most severe risks by the Turkish Supervisory Authority, Individual pension system 2023 Risk inventory, Pension Monitoring Centre, Türkiye.

[17] APRA Corporate Plan 2023-2024

[18] This is also recognised by the Network for Greening the Financial System, see NGFS (2024), Nature-related Financial Risks: a Conceptual Framework to guide Action by Central Banks and Supervisor, July 2024, Network for Greening The Financial System, https://www.ngfs.net/sites/default/files/medias/documents/ngfs-conceptual-framework-nature-risks.pdf

[19] Australia, Bulgaria, Chile, Mexico, the United States

Disaster protection plans could also include other disaster recovery arrangements, such as the IT Disaster Recovery Plan (Ireland; South Africa), or security plans that cover crisis, incident and emergency management (Namibia).

2.3. Acceptable risk thresholds for key risks and robust monitoring mechanisms to ensure effective oversight

Setting up a well-structured risk management framework (RMF), is a cornerstone of sound governance for the respondents. Sound internal governance practices include setting up a formalised risk appetite statement (RAS)[20], and having an appropriate risk strategy, a risk management policy, a holistic RMF and effective reporting lines to the senior management body. The RMF enables Authorities to appropriately identify, assess, manage and report the key risks relating to the Authorities' mandate. As part of their RMF structures, IOPS Members[21] are increasingly adopting Risk-based Supervisory frameworks[22], designed to identify and assess areas of greatest risk and direct resources accordingly.

To preserve and increase the resilience of the financial sector, including pension funds, Authorities have further modernised their risk management and governance frameworks and enhanced their operations by harnessing RBS to be more risk-based, forward-looking, and outcomes-focused, particularly with regard to systemic and emerging risks[23].

As an example, the Central Bank of the Netherlands (DNB)[24] further integrates risk management into its governance processes, improves management of data on emerging risks and effectiveness of controls and Key Risks Indicators (KRIs), recalibrates risk categories by simplifying the existing categorisation and improves risk culture and awareness through organisation of coordinated trainings and awareness programmes for risk professionals and other DNB staff. Also, in Australia, APRA enhances its operations by harnessing its newly established Supervisory Risk and Intensity (SRI) model to derive greater supervisory insights and intelligence and proactively keep pace with and respond to key risks and vulnerabilities[25].

The risk governance and management framework establishes an acceptable risk threshold for key risks or areas of risks (categories). This was cited by most respondent Authorities (28 or 76%). The risk governance and management framework provides mechanisms for regular monitoring (usually quarterly, but in some cases, e.g., Poland, on a daily basis) to ensure that risks are being managed within stated risk thresholds and determine any required supervisory action or intervention.

---

[20] For more information, see IOPS Risk-Based Supervision Toolkit, Module 3, https://www.iopsweb.org/rbstoolkit/Module_3_-_IOPS_RBS_Toolkit.pdf (public version).

[21] See IOPS Working Paper 38, Report on learnings from the design, implementation, use and review of Risk Based Supervision by pension supervisory authorities (internal version).

[22] Definition in the IOPS Risk-Based Supervisory Toolkit: "structured approach which focuses on the early identification of potential risks faced by pension plans or funds and the assessment of the financial and operational factors in place to manage and mitigate those risks. This process then allows the supervisory authority to direct its resources to the issues and institutions which pose the greatest threat thereby supporting timely action and escalation where determined necessary", https://www.iopsweb.org/rbstoolkit/Module_0_-_IOPS_RBS_Toolkit.pdf

[23] Effectiveness and Capability Review of the Australian Prudential Regulation Authority, 2023, https://fraa.gov.au/publications/effectiveness-and-capability-reviews-australian-prudential-regulation-authority

[24] DNB Annual report 2022, published in 2023, https://www.dnb.nl/media/zoqfezqn/76051-dnb-jaarverslag-2022_en_web.pdf

[25] APRA Corporate Plan 2021-2025, https://www.apra.gov.au/sites/default/files/2021-08/2021-25%20APRA%20Corporate%20Plan_1.pdf

Supervisory functions involve a broad range of activities to identify and respond to risk. Various experiences were offered by respondent Members.

Several respondents (Albania; Bulgaria; Ghana; Hong Kong, China; Ireland; the Netherlands; South Africa) use risk registers to identify the most significant risks and record risk assessments. Usually, each supervisory unit or department develops its own risk register, and each key risk is assigned a certain acceptable risk threshold. In some authorities, a central risk register is maintained which informs supervisory plans and approaches (Ireland, South Africa). Risk registers are periodically reviewed and most significant risks are reported to the senior management and relevant Authorities' bodies/committees.

For example, in Hong Kong, China, the Mandatory Provident Fund Schemes Authority (MPFA) utilises risk registers to record its identified risks and potential impact of risk exposure on the organisation. It also uses Key Risk Indicators (KRIs)[26] as a tool to monitor risks and to take early action to prevent or mitigate crises, as well as a risk heat map, which is a visual representation or graphical tool used to display and analyse risks.

The assessment of risks by the Central Bank of the Netherlands (DNB) involves the recording of risks and establishing management measures (controls). The effectiveness of key management measures is subject to periodic review. The KRIs are also used to measure and predict the development of risks.

In Hungary, the Central Bank uses a stress test indicator that refers to the sustainability of the operation. In Zambia, the risk appetite for various risks is outlined in the risk management policy. Key risks are assessed, monitored, and reported to the Board on a quarterly basis. In some respondents acceptable risk thresholds are defined in their Authority's Business Continuity Plan (e.g. North Macedonia).

3. Effective governance in crisis management

3.1. Implementing strong governance structures to effectively address and manage crisis

Most respondents (27 or 73%) have in place appropriate governance structures to deal with crisis management. The survey revealed **a broad diversity of internal governance arrangements and structures (bodies)** that supervisory authorities put in place to anticipate, mitigate risks, and ensure Authorities' resilience and ability to continue delivering on their mandate in the event of major disruption. Ultimately, as underlined by several responses, an effective governance structure should demonstrate clear lines of authority, accountability, and responsibilities (in particular, reporting to the senior management) with clear roles for all the stakeholders involved in crisis management at all levels of the institution (board, senior management, risk/audit functions, business lines).

Flexibility in governance structures was also emphasised as a determinant for a successful crisis response. Depending on the nature and scale of the crisis, different preparations are required. It is therefore important to have dynamic governance frameworks that allow for flexibility to configure and adapt crisis planning as the external environment changes. Ad-hoc projects and measures could be taken, where necessary, if a particular risk has emerged or developed into a significant risk for a certain sector or sectors. Likewise, this approach allows scaling down resources once the risk of disorderly failure has decreased or passed.

[26] KRIs are specific indicators or metrics that help identify risks in different business functions and provide insights into emerging risk trends by triggering thresholds or warning indicators when risk exposure surpasses acceptable levels. Source Mandatory Provident Fund Schemes Authority (MFPA), Hong Kong, China.

In general, responses by members show that sound internal governance practices and efficient risk management frameworks (RMFs) are essential to mitigate crises efficiently. Not all respondents have formal crisis management frameworks or plans in place yet. These Authorities have established several different governance structures with the aim to anticipate, mitigate risks, and act quickly in the event of a major disruption. Sound internal governance practices include setting up an appropriate risk strategy and appropriate risk appetite levels, having a holistic RMF and dedicated committees to deal with specific emergency, planning for recovery from disasters and specific contingency protocols, and establishing planning frameworks, among others.

Crisis management is usually performed through enacting Authorities' Business Continuity Plan(s) tailored to different crises to maintain the essential functions of the Authority and/or through a formal crisis handling system. Such a system includes setting up an executive crisis committee or other relevant team and well-structured formal procedures to manage a crisis. A large majority (29 or 78 %) of respondents have already established their BCP for critical incidents that aim to ensure the continuity of essential supervisory operations and services.

Typically, existing governance structures include setting up an Executive/Strategic Crisis Committee or a Senior Management Team[27]. This body, usually composed of the Head of Authority and Senior Management from key business units, such as IT, risk management and compliance, which would take a lead in ensuring the implementation of crisis handling and business continuity management strategies, policies, and plans. The Crisis Committee also oversees the BCM programme and updates.

In some other jurisdictions, crisis management is performed *only* through Business Continuity Plans. In this regard, the Business Continuity Team would be responsible for crisis management. For example, in Namibia, the CEO of the Supervisory Authority would appoint the members of the Business Continuity Emergency Planning Team (BCEPT), who reports to the CEO and Risk Management Committee.

The Head of the Authority, supported by Executive Management Team/Strategic Committee, takes the lead in ensuring that appropriate crisis handling and business continuity management strategies, policies, and plans are in place. This is the case for all responding authorities. The Head will usually chair the Strategic Committee or crisis management team meetings.

In some Authorities, the Board oversees the Strategic Committee's management of risk, monitors emerging strategic risks, and undertakes deep dives of key risks where considered necessary, including consistently out-of-tolerance risks. The Committees are usually supported by various technical teams that deal with the day-to-day operational decisions needed to respond quickly to a crisis situation. The committee (or Head of the Authority) establishes the crisis management team and gives the instructions to implement the crisis management plan.

Less than half (16 or 43%) of the respondents have established a Crisis Management Team. Under different governance settings, a crisis management team could be (one of) the main body responsible for preparedness, management - and within some Authorities - for resolution of the crisis. Experts from other supervisory departments can provide necessary support and expertise depending on the situation (nature of the crisis).

In Australia, for example, in terms of internal governance, APRA's Executive Board has established a number of committees including the Supervision, Enforcement and Resolution Committee. This is the primary forum for strategic oversight and review of APRA's resolution and enforcement powers, which it does so by providing advice, oversight and constructive challenge. It also regularly discusses

[27] The exact name varies depending on Authorities' governance and risk management structures. Source: Members responses to the IOPS Survey 2024.

emerging or potential matters of concern that are identified via the Supervision Risk and Intensity Model. This committee comprises senior leaders from across the organisation. In the event that an entity experiences a decline in viability or if a crisis emerges, it may establish a Resolution Workout Team to deal with day-to-day management of viability issues or crisis. For crises that have a systemic impact, the Executive Crisis Committee is a flexible governance body that can be established by APRA's Members, which has the ability to alter its make-up during a crisis, as necessary, to keep in line with the developing situation.

In Indonesia, the Financial Services Authority (OJK) has established the Crisis Management Protocol, which consists of the Board of Commissioner, Secretariat of Crisis Management Protocol, Sectoral Monitoring Coordinator, Supervision Unit, and Supporting Unit. The OJK Board of Commissioner leads the implementation of the OJK's Crisis Management Protocol, while the Deputy Commissioner leads the Secretariat of the Crisis Management Protocol and Sectoral Monitoring Coordinator.

In the United States, EBSA has established a crisis management team that reports directly to EBSA's senior leadership. The leadership consists of the EBSA Assistant Secretary (head of the Agency) as well as the Principal Deputy Assistant Secretary and Deputy Assistant Secretary for Program Operations.

Box 5 Costa Rica inter-institutional framework to deal with systemic risks in the financial system

The inter-institutional framework was adopted to deal with systemic risks in the financial system. The National Stability Commission (CEF) is responsible for analysing and proposing actions and recommendations on the systemic risks in the financial system as well as supervising the implementation of macroprudential policies for preventive management. The CEF is composed of:

- President of the Central Bank of Costa Rica (or Manager when the President is not present)
- President of the National Council for Supervision of the Financial System
- Minister of Finance.

The Commission receives support and advice from the Monitoring and Coordination Group (GSC), enabling timely and effective decisions in relation to crisis situations.

The GSC is composed of:

- Technical Secretariat of the CEF represented by the Director of the DEF, who will be the coordinator
- Superintendent(s) of Pensions, Stock Market, Financial Entities and Insurance
- Vice Minister of Finance
- BCCR Manager
- CONASSIF Technical Advisor.

In addition, inter-institutional technical working groups are created under the coordination of the CEF Technical Secretariat. The main functions of the working groups are to proactively monitor markets, update indicators and relevant data, and issue warnings about key financial risks. Other bodies could be created should circumstances warrant.

The GSC reports to the highest authorities of the Central Bank and Superintendencies in Costa Rica.

Source: Members' responses to the IOPS survey 2024

An **inter-institutional crisis management framework** that brings together key financial sector supervisors to address major crisis is implemented in two respondent jurisdictions (Costa Rica and

Colombia, Box 5 and Box 6). In this type of framework, **coordination** with other financial sector supervisory authorities is a central part of the governance structure. It allows for maximised synergies, a coordinated decision-making process and better information sharing between authorities. It also ensures coherent acts and facilitates the coordination of actions by the participating authorities in crisis management. Some similarities in the governance structures were observed as compared to the arrangements for single/integrated authorities: in particular, the main coordination committee is composed of the key financial supervisory authorities and their top representatives (Head of Authority/Board members). Such a committee is usually supported by technical sub-committees or groups that are conducting operational work. Specialists or experts are engaged with specific qualifications depending on the nature of the crisis.

Box 6 Colombia inter-institutional framework to deal with systemic risks in the financial system

The Coordination Committee for Monitoring of the Financial System (CCSSF) was established at the national level to manage crisis situations. This is the main body for coordination among the authorities of the Colombian financial sector.

The Committee is composed of the Ministry of Finance and Public Credit, the Bank of the Republic, the Financial Superintendence and the Financial Institutions Guarantee Fund of Colombia.

At its meetings, an analysis of sectoral risk is regularly presented, particularly for credit institutions and their main alerts. Likewise, the results of stress exercises are discussed to identify the resilience of the system. The Committee also examines selected regulatory projects, especially those of a prudential nature, documents from international authorities related to matters of interest to the Committee and (determines the list of systematically important financial institutions) among other topics. The preparation of the CCSSF's agenda and topics for discussion is the responsibility of a technical subcommittee.

In times of crisis, the Coordination Committee plays a central role. If proposed by the Financial Superintendent, the Committee may declare a situation to be systemic, thus activating the Financial Crisis Group (GCF). This Group is a forum for interaction and coordination to manage systemic financial crises, which will exchange quantitative and qualitative information, and will analyse and monitor the situation to propose non-binding policy options for crisis management to the CCSSF.

The GCF comprises the CCSSF technical subcommittee, members of the Intersectoral Resolution Commission, and other officials as required depending on the event. This group is only activated in times of systemic crisis.

Finally, the importance of testing the coordination among the members of the CCSSF in the event of a potential crisis by means of conducting simulation exercises should be noted. For this purpose, a Simulation Exercise Group led by FOGAFIN was established, the main task of which is to prepare and coordinate simulation exercises for the entire Network.

Source: Members' responses to the IOPS survey 2024

A quarter of the respondents (9 or 24%) have not yet put in place or begun the process of developing the internal governance structures for crisis management. In certain Authorities (Chile, Uganda) where there are no formal crisis management plans or business continuity management policy, there is a possibility to establish sub-committees or ad-hoc teams to deal with specific emergency situations. It is also worth noting that some Authorities mentioned that, although there were no formal governance structures in place specifically for crisis management, the current internal structures and procedures such as the risk management framework, proper communication within the Authority, and resources and tools, can be redirected or re-adopted to deal with crisis management.

3.2. Crisis management team collaboration with other units or departments within Supervisory Authority

Usually, the crisis management and/or business continuity procedures outline the composition and the responsibilities of teams.

Crisis management teams or committees include representatives of all key departments of a supervisory authority and are either chaired by or report to the CEO, Chairman, or Board of the Authority. In some cases, the committee also reports to a subnational crisis management group. In the Lithuania Central Bank the crisis management team, depending on the crisis, may report to the crisis management group of the ECB or the European Systemic Risk Board.

One-third of the respondents (11 or 30%) have established a function of Chief Crisis Manager. In most cases, this function is performed by the Head of the Supervisory Authority, supported by other Executive Members (leaders), heads of Directorates, etc.

The crisis management team within the MPFA, Hong Kong, China, comprises the senior management team members (the Managing Director and Executive Directors). For different types of crises, a Crisis Command Team (CCT) is established. The CCT is composed of the senior management team members and designated Crisis Duty Officers, who are usually Directors and General Managers of respective business units of the MPFA.

Similarly, in Ireland, the Pensions Authority's senior management team acts as crisis management team. The Pensions Regulator determines the severity of the incident using the incident severity level matrix as a guide and, assisted by the senior managers, decides which employees and external contractors (if required) are best suited to deal with the incident. This group can be supplemented with additional resources if needed[28].

In the Financial Superintendence of Colombia SFC, there is no specific crisis management group. However, emerging risks that may impact the entities are evaluated prospectively twice a year, with the objective of designing a supervisory plan aimed at mitigating these risks.

In almost two-thirds (23 or 62%) of respondents, their incident response teams can be expanded and supplemented with additional resources if needed during a crisis. They can draw on additional resources from experts in supervisory or resolution teams or in other specialist teams. Supervisory Authorities are taking measures to ensure that all supervisory staff have been trained and are induced in their roles.

More than half of the respondents (20 or 54%) reported having a resolution division or team in place[29]. This is a dedicated body within the Authority (Australia, Bulgaria, Lithuania) or a team/unit or a division that also performs resolution functions (like in the National Pensions Regulatory Authority (NPRA). In Ghana, the risk committee performs the resolution functions and in the National Pension Commission of Nigeria, the Surveillance Department has functional responsibility for the resolution of failing operators undergoing a crisis). In Chile and the United States, the senior management can convene a resolution supervisory team to address a particular issue should circumstances warrant.

In about one-third (12 or 32%) of the respondents, a resolution team is part of the crisis management team. In some other Authorities, crisis management is conducted by the resolution team. Some integrated supervisory authorities noted that their resolution function covers only a particular financial sector, most often not pensions. For example, the resolution function relates to banking sector

[28] Incident response plan, The Pensions Authority, Ireland.

[29] See the glossary of terms.

in the Financial Market Authority (FMA), Austria; investment firms in the Financial Supervision Commission (FSC), Bulgaria; and credit institutions and investment companies in the Central Bank of Hungary. In other supervisory authorities, the resolution regime covers all regulated institutions, including the pension (superannuation) industry (Australia, France, Indonesia).

APRA's crisis management activities are primarily conducted through a dedicated Resolution team, which engages with the relevant internal governance committees as necessary during a resolution or crisis. If considered necessary, APRA may also work with peer regulators/agencies, such as the Reserve Bank of Australia. APRA continuously improves and regularly tests its operational capacity to resolve failures and near-failures in an orderly manner.

In Chile, the Superintendence of Pensions (SP) can, as part of resolution activities, appoint its officials to become a delegated inspector in a pension fund administrator to safeguard the security of a particular pension fund. Such an appointment may not exceed six months and is renewable only once for a maximum period of six months, and must be based on the serious facts that put the security of the pension funds in imminent danger and make the adoption of urgent measures necessary.

In Ireland, the Pensions Authority's Supervision and Enforcement Unit operates as the resolution supervisory team for any occupational pension related crisis or incident. The Authority's Operations Unit is responsible for resolving any other crisis incidents.

In Ghana, the Authority currently uses the Risk Committee to perform resolution functions.

3.3 Collaboration with supervised entities in case of crisis

About half of the respondents (19 or 51%) have established planned coordination actions between the supervisory authorities and supervised entities. It was widely recognised in the responses that effective crisis management requires an enhanced coordination and information exchange among multiple stakeholders. Several authorities referred to the planned coordination actions with the supervised entities in relation to monitoring and implementing resolution plans.

The Financial Services Authority (OJK) of Indonesia applies the stress status of the pension sector as part of the Crisis Management Protocol (CMP). The stress status is determined through monitoring tools that include CMP indicators and supporting qualitative and quantitative information, such as data on global and domestic economic conditions, including the real sector, capital markets, and the banking sector that may affect pension funds. Professional judgment is applied with regard to this information. The OJK Leadership plays a key role in officially determining stress levels. The Pension Fund Stress Status Determination Committee decides on the stress status of pension funds. The Committee consists of the Chief Executive and Deputy Commissioner of Insurance, Guarantee and Pension Fund Supervision in OJK. The evaluation of the CMP indicators for pension funds is undertaken by the Pension Fund Sector Monitoring Coordinator at OJK at least once every three years.

The National Pension Commission of Nigeria has established a consultative forum, PenCom/Operators Forum, whereby responses or interventions on issues of mutual interest like crisis management are coordinated between the Commission, regulatory authority and licensed Pension Fund Operators, and the supervised entities.

3.4 Crisis management team's roles and responsibilities prior and during crisis

The risk and crisis management framework should be underpinned by a strong risk culture and governance with clear roles for all the stakeholders involved and sustainable integration of risk management practices embedded across the organisation. Respondents emphasised the role of risk culture, governance and the integration of risk management practices. Responsibilities, roles at each level of the authority (i.e. board, senior management, risk functions, business lines) during a crisis

should be clearly delineated among these groups in order to implement action plans appropriately and efficiently.

The main roles and responsibilities of the crisis management team in preparation for the crisis management. Respondent authorities highlighted that the crisis management team, usually led by business unit leaders and functional heads, should:

- Identify key functions (e.g. statutory/critical/essential functions), critical business activities and key threats
- Develop and review business continuity plans (BCPs) tailored to different crises
- Develop criteria for implementing the BCP, determine the persons who have the authority to do so and the responsibilities of each business function and level of management/staff within each function
- Monitor standards and compliance with the BCP policy

The crisis management team's roles and responsibilities include the following actions when responding to a critical incident:

- Assess the extend and impact of the critical incident and its possible systemic implications
- Consider triggering the measures provided in respective BCPs
- Consider urgent matters of supervisory or policy action as well as imminent threats to the financial system or entity/entities' stability
- Manage a crisis and consider any additional measures in light of the incident's unique circumstances
- Consider devolution of the Authority's headquarters or consider alternative work arrangements to ensure safety of the supervisory staff
- Manage recovery efforts with the aim of ensuring continuous service delivery
- Maintain necessary communication with both internal and external stakeholders
- Coordinate with the financial industry, when required, to address systemic risk situations

More broadly, respondents also highlighted the benefits of ensuring effectiveness of business continuity plans (BCP) through:

- Regular review and assessment of adequacy of BCP

  Elements of such assessments may include the loss of critical processes and systems, and provide various impacts of the loss, e.g., operational, financial, reputational impacts. It is important to undertake proportional controls to maintain processes and manage both the day-to-day operations and the change
- Regular updates of BCPs
- Regular tests of BCPs via regular exercises and revisions to ensure validity and adequacy
- Regular (annual) tests of its command-and-control communications
- Disruption event scenario testing and regular simulation exercises
- Internal audits of BCPs conducted to assess their effectiveness
- Independent reviews on BCP for continuous improvement of overall BCP process
- Awareness and regular training on Business Continuity related matters to all staff.

In the United States, the EBSA has a comprehensive continuity plan in place to maintain operations in response to a broad range of crises, including natural disasters and pandemics. All employees are required to complete annual training on continuity concepts to ensure knowledge and awareness of the agency's emergency response capabilities, thereby enabling EBSA to effectively support plan participants and beneficiaries under all conditions.

4. Crisis management plan

In line with the quoted BCBS High-level Principles, crisis management or business continuity management is understood as a whole-of-business strategy that includes policies, standards, and procedures to ensure that critical operations can be maintained and recovered in a timely manner. Its purpose is to minimise the operational, financial, legal, reputational and other negative consequences arising from the disruption[30].

A **crisis** management plan or business continuity plan is part of the overall strategy that sets out a **written plan of action** and lists necessary procedures and systems necessary to continue or restore the operations. These procedures should be documented, periodically reviewed and updated to meet the Authorities' specific needs.

Generally, **the purpose of the plan is to provide strategic direction and decision making** for overseeing the management and coordination of the recovery of Authorities' business activities, from the initial response to the point at which operations are recovered to an acceptable level.

4.1. Structure of crisis management plans

About half (18 or 49%) of the respondents have put in place crisis management (incident response) plans or procedures. Establishing a crisis management plan is considered essential for preparation and management of any major incidents that may impact a supervisor's ability to deliver its services. The plan enumerates key staff, their responsibilities, general procedures and processes, technologies, facilities that must be followed or maintained prior to and during the crisis, communication (internal and external), and incident reporting. Since there is much uncertainty about future potential crises, the designed procedures should be flexible to accommodate different types of crises and their magnitude.

An escalation process with clear lines of reporting is an essential part of a crisis plan. The plan should clearly define where the critical incidents have first been reported and then, depending on the magnitude of the crisis, whether they should be escalated to the appropriate higher level of decision taking. The incident is then triggered and the correct level of response is invoked.

A crisis management plan could consist of several action levels involving different heights of seniority (e.g., Crisis Management Team, Incident Response Team) and may cover broad categories of potential crises. For example, in Morocco, the crisis management plan covers both business and support functions and it includes:

- The Business Continuity Plan focuses on business actions for the continuation of vital operations
- The Logistics Contingency Plan describes the logistical arrangements
- The IT Disaster Recovery Plan focuses on the availability of data and IT resources

[30] The Basel Committee on Banking Supervision, High-level principles for business continuity, 2006.

- The Crisis Communication Management Plan defines the crisis structure, activation modalities of the Business Continuity Plan, specific crisis measures concerning human resources, and internal and external communication.

Similarly, The Pensions Regular (TPR), the United Kingdom, noted that their crisis management plan is modular in design and is formulated to respond to, but not limited to, five key denials:

- Denial of People (Staff Resource)
- Denial of Premises (Workspace)
- Denial of Technology (Systems and Applications) Including Cyber Attack response
- Denial of Telecommunications (Contact with customers and stakeholders)
- Denial of Supply Chain (Internal and External dependencies).

This approach ensures that the Authority has the correct departments and resources involved to respond. Each denial has a key decisions and consideration section to ensure that any risks are identified. The UK Pension Regulator has prepopulated agenda templates. Dependant on the crisis, the plan ensures that any risk crystallisation is considered and seeks to identify any emerging risks that may need to be considered. All plans in the authority are subject to Business Impact Analysis and are assessed. This includes the loss of critical processes and systems, and provides various impacts of loss, e.g., operational, financial, reputational impacts, etc.

The Central Bank of Latvia has adopted a general crisis management procedure for all types of crises and detailed business continuity, communication, and other detailed plans exist for each case.

In the Bank of Lithuania, the crisis management plan consists of three groups of action levels – strategic, tactical, operational.

The ACPR, France, stated that bearing in mind that systemic crises can be very different in nature, the Authority does not have a systematic step-by-step crisis management plan to deal with them. That said, the Authority has in place an internal resilience plan to maintain its own activity at all times.

Almost half (18 or 49%) of the respondents stated that their crisis management plans were developed internally. The process included the involvement of the representatives of each department responsible for sectors of the financial market (Poland) or in some cases the support from external consultants (Albania).

The timeline to set up a crisis management plan generally depends on factors such as the organisation's size, complexity, collaboration with and capabilities within the supervised industry, and the existing level of preparedness. Members were asked to share their experiences on the time required to develop a crisis management plan within their Authority and the factors that drove its introduction.

In Australia, CPS 900 Resolution Planning came into force on 1 January 2024. Bespoke entity resolution planning is a multi-year effort. Given that the superannuation industry is less mature in resolution compared to other industries, additional time will likely be needed to enhance industry capabilities. A significant event[31] in the superannuation sector in 2019 prompted the creation of a

[31] In 2019, APRA expanded its resolution function to the superannuation industry (Box 1) following the collapse of a non-APRA regulated parent company, which caused stress for three APRA-regulated trustees (Group) and a service company.

superannuation resolution framework, including Prudential Standard CPS 900 Resolution Planning, which applies to all industries including superannuation.

The FSC, Colombia, noted that in their case setting up a crisis management plan is typically quick, as they maintain constant off-site supervision, which allows the authority to stay in contact with pension managers when needed. The crisis management framework was introduced during the Covid crisis that provoked portfolio shocks, leading the Authority to work closely with the supervised entities to resolve operational risks, negotiate derivatives (CSA accounts), and ensure liquidity for severance funds.

The National Pension Commission of Nigeria stated that it took twelve months to develop the Business Continuity Plan, which included the Crisis Management Plan. The document is currently being reviewed in line with recent developments.

4.2. Testing and Review of crisis management or business continuity plans

Supervisory authorities should check whether a sound approach to crisis preparedness and management has been followed, by ensuring that business continuity and disaster recovery plans[32] have been periodically tested and updated. As outlined by the BCBS HPLs quoted elsewhere, testing is also important for promoting awareness and understanding among key staff of their roles and responsibilities in the event of major disruptions.

Testing and updating of crisis management programmes or business continuity management plans. All elements of the plan need to be tested regularly. As highlighted by the BCBS High-level Principles for Business Continuity, regular testing of Business Continuity Plan(s) (BCP) is considered essential to ensuring the BCP can meet its objectives. The BCP should also be periodically updated, reviewed and audited to ensure that they remain appropriate and effective.

The majority of pension supervisors perform testing of their crisis management plan regularly. Respondents indicated they test at minimum on an annual or higher (twice a year, Bank of Latvia) frequency. The test may also be conducted sooner should circumstances warrant, e.g., in the case of any significant operational or strategic change (TPR, the United Kingdom). Some Authorities stated that they are still at an early stage of testing. In Australia, APRA has not yet engaged in a testing exercise of the superannuation resolution planning programmes. APRA noted that it has previously conducted a superannuation crisis simulation (in 2014); however, this pre-dated the development of the resolution framework. Since the development of the framework, APRA has prioritised crisis simulations for banking and insurance industries.

Over half of the respondents (19 or 51%) reported conducting simulation exercises to test their crisis management plans. ACPR, France, carries out ad-hoc crisis simulation exercises involving a crisis scenario and testing their responses to the crisis.

In some jurisdictions, an independent (internal or external) audit could be used to assess the effectiveness of the organisation's testing programme, review test results, and report on findings to the senior management.

Some Authorities also carry out periodic crisis communications tests (e.g. the Pensions Authority, Ireland – see Box 8).

[32] Testing of resolution plans by supervisory authorities is not covered in this section.

In Ghana, the National Pensions Regulatory Authority tests the BCP every year to ensure continuous operations in the event of a major disruption. The test is modelled on the High-level principles for business continuity issued by the Basel Committee on Banking Supervision.

Box 7 contains additional information on the organisation of testing exercises of crisis management plans.

Box 7 Members experiences: Testing crisis management plans

Albania:

In AFSA, Albania, crisis management procedures require the plans to be tested annually or maximally every two years.

As part of the crisis management plan and Disaster Recovery Plan, the Authority's IT Infrastructure and data are periodically (daily, monthly, annually; depending on the system) backed up, and updated. Moreover, there are procedures that clearly define the steps in case of crisis such as Data Breach, Hardware Failure, Network loss, Fire, Nature Disasters, etc.

The Business Continuity Plan defines the procedures for testing backup and recovery. Drills for different scenarios of simulations are done periodically on the critical IT infrastructure and online systems. Drills for evacuation and safe gathering points in case of fire, earthquake, floods and other natural disaster are also conducted annually.

As for the security of the premises, a private security company is contracted to ensure and test annually Closed Circuit Television (CCTV) systems, check-in devices, alarm system and security guards who are deployed in case of security breach.

Hong Kong, China:

Crisis management plans for different specific crises are tested regularly at the MPFA. Before conducting, a Test Plan is created, outlining the purpose, scope, date, time, participants, and scenarios based on actual operations and likely contingencies. The Plan also specifies the procedures, required resources, and other necessary items for the test. After the completion of the test, a Testing Result Report is prepared. This report including identified improvement opportunities for enhancing the effectiveness of the BCPs is prepared for management's review.

The BCPs are tested every two years to ensure their viability and effectiveness. The scope of the test covers major components of the BCPs as well as coordination and communication with internal and external parties.

Source: Members' responses to the IOPS survey 2024.

Box 8contains additional information on the organisation and lessons learned from the recently conducted testing exercise of internal crisis communications by The Pensions Authority of Ireland.

Box 8 Crisis communications drill update - The Pensions Authority of Ireland

In September 2023, The Pensions Authority conducted a high-level internal crisis communication drill exercise as part of the Authority's Incident Response Plan. The exercise tested the senior management team's (SMT) ability to respond to an external issue emerging in the pension sector.

Several crisis scenarios were elaborated for this exercise. The initial scenario involved media concerns over the mismanagement of a large pension scheme. As the drill progressed, three additional sample scenarios were added (including a data breach, delays in public pension scheme administration and Authority-related expenses).

The SMT demonstrated:

- Strong technical awareness of the potential ramifications of a failing entity
- The need to act promptly
- Engaging rapidly with trustees
- Data collection to fully comprehend the situation
- The need to communicate with all stakeholders, including the Government.

The Authority's external communications consultants acted as independent observers of the drill exercise.

The main finding and lessons learned included:

- The response to the crisis drill was well co-ordinated, coherent and evidence based
- It was emphasised that rapid communication was critical, but not a knee-jerk, uninformed response before some basic facts had been established
- The need to balance between proactive with reactive communications
- Opening clear communication lines with key stakeholders was the priority from the outset.

The Authority also conducts twice a year IT-focused Disaster Recovery (DR) and Business Continuity Plan (BCP) tests. This includes tabletop exercises and simulated hardware failover events to the failures as realistic as possible without disrupting production work. Annual reviews of the Authority's data protection, records management and health and safety controls further strengthen the resilience.

In September 2024, the Authority's internal audit assessed business continuity, disaster recovery and cyber security incident response. The audit provided reasonable assurance of the adequacy and operating effectiveness of the Authority's business continuity and disaster recovery processes and controls. Recommendations and lessons learned from drills, tests, and audits are integrated into ongoing business continuity planning updates.

Source: Members' responses to the IOPS survey

Another important measure relates to organising industry-wide stress tests of business continuity plans. Supervisors outlined the importance of such stress tests to assess the level of resilience across the market and the compatibility of the recovery strategies of individual participants. In light of the substantial costs involved, the decision to undertake a market- or industry-wide test should be based on a thorough cost-benefit analysis. For example, in Australia, APRA is starting to plan its first financial industry-wide stress test exercise, which is an important part of APRA's supervisory toolkit. The conduct of the testing exercise may identify the need to update business continuity plans (BCPs).

Most of the respondent Authorities have relevant procedures in place to periodically review and update business continuity plans and disaster recovery plans. Overall, updates are performed at least once a year (or more frequently, if required) as a result of conducted tests or significant changes in policies, practices, risks assessment, broad environment or key personnel. In some Authorities, updates occur less often, every three or five years or for some, no fixed periodicity is set up in internal regulations. In Hong Kong, China, the MPFA crisis management plan / BCPs are reviewed and updated at least once a year or upon changes made to the plans. Table 1below provides information on BCP components that will be updated at least annually:

Table 1 MPFA, Hong Kong, China, BCP components that are subject to review and possible updates

Category	Updates
Functions	• Departmental key function lists • Back up plans • Contingent resources requirements
Contact list	• Staff (departmental) • Business partners • Service providers
Communication	• Departmental communication plan
Staff	• Staff segregation plan • Staff preservation plan • Staff evacuation plan

Source: Presentation by MPFA, Hong Kong, China at the IOPS Technical Committee, February 2024.

5. Strengthening crisis management through enhanced co-operation and information sharing with other public authorities

In the view of supervisors, an open and ongoing co-operation is essential for efficient and effective crisis management. This involves regular interactions between financial sector supervisors and other public authorities, which could take different formats and be organised at varying frequences depending on the national context.

Most respondents emphasised the importance of maintaining strategic and working relationships with governmental entities (agencies). This could be achieved through the use of memoranda of understanding and common interest agreements or reinforced by communication protocols (e.g., Colombia). A majority of respondents (22 or 57%) also established bodies such as a Council of Financial Regulators or Financial Stability Committee/Commission[33], that gather senior representatives from key financial sector authorities. Such a Committee is considered as the principal body for co-operation and policy dialogue on the matters in relation to development of financial system, including the events/risks with a systemic dimension. It is also usually responsible for assessment and recommendation-making on the systemic risks impacting the financial system, as well as for supervising the implementation of macroprudential policies for preventive management. The Financial Regulators Council enables authorities to enhance their crisis management capability and, in time of a crisis, to coordinate quickly and efficiently their actions.

Communication and exchange of information with other financial regulators during crises is also important. Effective communication during times of crisis was viewed as a decisive factor in the

[33] The exact name of the Council or Group is specific for each jurisdiction.

success of measures implemented by the responsible authorities. Several respondents underlined the importance of close co-operation with the government and other financial regulators, and related organisations, regarding communication during a crisis, and to exchange information on contingency measures and intelligence regarding the development of a crisis.

In Costa Rica, a Communication Committee was established. The Committee is responsible for developing and maintaining a comprehensive communication plan, addressing all relevant stakeholders, including the financial industry, regulatory and supervisory bodies, governmental institutions, the media, etc. The communication plan includes a regularly updated contact list of all involved parties and define clear mechanisms for timely and coordinated communication. The Committee is chaired by the coordinator of the Central Bank's Communication Office and includes a communication officer appointed by the Board of Directors of the supervisory authority.In Australia, the APRA's external engagement entails collaboration with the Council of Financial Regulators (CFR) and other government parties throughout the resolution process. APRA must escalate any resolution cases to the CFR agencies via the CFR Crisis Management Working Group and to the Australian Treasurer.

In Hong Kong, China, the MPFA works with the government, other financial regulators, and related organisations to ensure coordinated actions during major crises. This includes keeping in touch with responsible parties in the government with regard to preparation for and communication during a crisis, and to exchange information on contingency measures and intelligence regarding the development of a crisis.

In India, the Pension Fund Regulatory and Development Authority (PFRDA) is a member of the Inter Regulatory Forum (IRF) which consists of all the Financial Sector Regulators (FSRs) under the ambit of the Financial Stability and Development Council (FSDC) chaired by the Honourable Finance Minister of India. Under the IRF, the Advanced Level of Engaged Regulatory Treatment (ALERT) mechanism is present wherein the Principal Regulator will have the discretion to flag the concerns to the IRF Secretariat for activating ALERT, which will examined by the IRF Secretariat in consultation with the FSRs in IRF.

Furthermore, there is also the presence of Forum for Co-ordinated and Upgraded Supervision (FOCUS) which serves as a forum under which any of the FSRs may, at their discretion, flag concerns of systemic importance observed in interconnected entities to the IRF Secretariat.

ALERT and FOCUS serve as the critical frameworks for inter-FSR coordination and ensure a quick response to any supervisory issues that might arise which are of critical importance.

PFRDA, through Early Warning Group (EWG), which is a sub-group of Financial Stability and Development Council (FSDC), strives for early identification of cross-sectoral threats, help align responses across financial market regulators and ensures better crisis preparedness and confidence among subscribers.

In Indonesia, the coordination among related authorities takes part within the Financial System Stability Committee (KSSK). The Committee comprises the Central Bank (Bank Indonesia), Ministry of Finance, Financial Services Authority (OJK) and Indonesia Deposit Insurance Corporation (Lembaga Penjamin Simpanan, LPS). Its meetings aim to identify or confirm potential systemic impact related to a financial crisis, and to decide on the appropriate action plan to mitigate or handle the impact of the crisis. On top of the coordination with related authorities within the KSSK framework, the pension supervisor (OJK) entered into several memoranda of understanding with financial services sector supervisors in other countries, as part of the effort to strengthen supervision of the international financial groups.

The Pensions Regulator in Ireland is in regular contact with other public authorities and provides policy and technical assistance to a range of government departments, including its parent department,

the Department of Social Protection. In the case of the emergence of a major crisis, existing contacts at senior levels between the Authority and Government Departments would be utilised. Similarly, the Authority has a number of regular engagements with other regulators such as the Central Bank, or the tax authorities (Revenue).

In South Africa, the integrated supervisor, the FSCA, participates in the Financial Sector Contingency Forum.

Some respondents also stated that they maintain regular liaisons/contacts with international peers within the OECD, EIOPA, and other European supervisory institutions. These fora provide contacts that would be useful if a major international crisis emerged.

In several jurisdictions, intra- or supra-institutional collaboration in the crisis management area is not yet well developed, but work is in progress. The Retirement Benefit Authority of Kenya noted that, in addition to the work conducted by a joint financial sector regulators forum to assess the risk environment and various aspects of regulated entities that may exert systemic impact on the sector, the forum is currently in the process of augmenting the capacity for crisis preparedness within each subsector through continuous training of the technical staff. Moreover, each subsector regulator has undertaken self-assessments to identify gaps vis-à-vis international best practices, with the objective of formulating an integrated framework for crisis management and resolution for the sector.

6. Conclusions

Supervisory authorities and financial institutions operate within a complex, interconnected financial system shaped by rapidly evolving operational and risk landscapes.

Enhancing the stability of financial systems and resilience against financial and operational disruptions is one of the overarching objectives of prudential supervision. Supervisory authorities are enhancing their own crisis preparedness, while also improving the recovery, resolution, and crisis management of supervised entities.

A series of recent major crises have reinforced the importance of having in place well-designed crisis management strategies, such as business continuity management (BCM) policies and action plans.

About half of the surveyed IOPS members have implemented some formal crisis management arrangements, either within their authority or at the national level. Others are either considering or are in the process of implementing similar measures.

To handle major incidents or crisis effectively supervisors emphasise the need for a clear mandate and appropriate powers, allowing for flexibility to respond swiftly to various crisis scenarios.

Crisis management programmes are generally part of a supervisor's risk management framework and encompass internal governance arrangements, and business continuity and disaster recovery plans. For some respondents, the framework also includes resolution plans. Most often, multi-layered risk governance and management structures are used, which involve various management bodies and functions, each operating within their respective governance scope.

Supervisors have a broad diversity of internal governance and structures (bodies) for crisis management. They underscored importance of:

- Having in place dynamic governance structures, allowing for flexibility to configure and adapt crisis planning and management for different type of crises. Where formal crisis management programs are absent, supervisors should be able to implement ad-hoc measures or projects.
- Critical role of leadership, emphasising the responsibility of the Head of the Authority and Senior Management in ensuring effective crisis preparedness, business continuity strategies, and management plans. They have to set up an appropriate strategic crisis committee or crisis

management team, ensuring effective collaboration of all key departments within the supervisory Authority in times of crisis, expanding and supplementing the crisis management team with additional resources if needed.

- Ensuring planned coordination actions and information exchange with supervised entities to align crisis preparedness and management efforts.

Respondents emphasised the need for a crisis management and business continuity strategy with clear, written action plans and procedures to maintain or restore operations. Nearly half have implemented such written plans and procedures.

Business continuity and disaster recovery plans must be regularly reviewed, audited and updated. More than 55% of the respondents reported regularly testing their crisis management plans against various specific crises. Some Authorities also carry out periodic crisis communication tests using several crisis scenarios.

To have a holistic view of level of resilience and preparedness across the market and the compatibility of recovery strategies of financial institutions, supervisors have begun to organise industry-wide stress testing exercises.

The respondents believe that for crisis preparation and management, strong strategic relationships and effective information-sharing mechanisms with peer supervisors and other relevant public authorities are essential. Respondents also emphasised the importance of maintaining close relationships and co-operation with international peers, in particular as part of their efforts to strengthen the supervision of the international financial groups.

Policy recommendations are presented in a separate document entitled ‘Policy recommendations on resilience of pension supervision against shocks: Supervisory authorities’ crisis management plans’.

Glossary of terms

Business continuity management – (Adapted from the BCBS, High-level principles for business continuity, 2006): A whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption.

Conceptually, business continuity management is distinct from financial crisis management in that a financial crisis does not typically entail business continuity concerns. An event that gives rise to business continuity concerns, however, could develop into a financial crisis.

Business continuity plan – (Adapted from the BCBS, High-level Principles for business continuity, 2006): A component of business continuity management. A business continuity plan is a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organisation in the event of a disruption.

Significant incident (or crisis): The report defines event(s) that would pose serious threat to pension system and could have a long-term and important material impact on the pension system. It is understood that "significant incident" (or crisis) could imply both financial or market-related crisis, as well as major operational disruptions (caused by natural disasters, terrorist attacks, sanitary crisis/pandemic, technology failures, major cyber-attacks, etc.).

The report defines **significant incident (or crisis)** as a sudden and relatively not long-term phenomenon. Therefore, it excludes long-lasting shocks to pension systems that would have specific demographic implications. The report does not cover the issue of population ageing that will have significant consequences on pension liabilities in the longer run.

Major operational disruption – (Adapted from the BCBS, High-level Principles for business continuity, 2006): A high-impact disruption of normal business operations. In addition to impeding the normal operation of financial industry participants and other organisations, major operational disruptions typically affect the physical infrastructure.

Major operational disruptions can result from a wide range of events, such as earthquakes, hurricanes and other weather-related events, terrorist attacks and other intentional or accidental acts that cause widespread damage to the physical infrastructure. Other events, such as technology viruses, pandemics and other biological incidents, may not cause widespread damage to the physical infrastructure but can nonetheless lead to major operational disruptions by affecting the normal operation of the physical infrastructure in other ways. Events with greatest impact are referred to as "extreme events". They involve one or more of the following: the destruction of, or severe damage to, physical infrastructure and facilities; the loss or inaccessibility of personnel; and restricted access to the affected area.

Crisis management team ('CMT') (or similar terms): is a primary decision-making entity in the event of declared state of crisis, responsible for evaluation of information received and for declaration, execution, restoration and risk mitigation of a crisis. The priorities in crisis management are ensuring the safety and welfare of all employees and the surrounding community, minimising or eliminating environmental impacts, ensuring business continuity and reducing financial loss, and safeguarding the organisation's integrity.

Resolution: is understood as a process by which a Supervisory Authority or other relevant persons manage or respond to resolve failures and near-failures of a supervised entity in an orderly manner [adapted from the APRA Prudential Standard CPS 900 'Resolution Planning' definition, May 2023] According to the French legislation, the resolution regime aims to ensure the continuity of critical functions, avoid or mitigate negative effects on financial stability, protect the resources of the State

from recourse to exceptional public financial assistance and protect the rights of policyholders and beneficiaries of insurance coverage.

Risk appetite: the risk-based approach forces the authority to be explicit (and preferably articulate it to the public) about what areas it intends to focus on and the trade-offs it is forced to make. A clearly articulated risk appetite can be beneficial in setting expectations both internally and externally. Internally, the approach can support staff applying judgment to supervisory matters. Externally, it can help set stakeholder and community expectations.

Risk-based supervisory framework[34]**:** structured approach that focuses on the early identification of potential risks faced by pension plans or funds and the assessment of the financial and operational factors in place to manage and mitigate those risks. This process then allows the supervisory authority to direct [i.e. prioritise] its resources to the issues and institutions which pose the greatest threat, thereby supporting timely action and escalation where deemed necessary.

Risk management: the process of identifying, assessing, monitoring and managing the risks that may affect the achievement of the Authorities' objectives, and introducing the necessary control activities, with the aim of limiting the risks to an acceptable level. The authority implements risk management practices as part of its operational planning, specifically identifying, assessing, and managing risks related to the administration and enforcement of pension laws and related guidance. An effective risk management framework is critical for an Authority to fulfil the mission, especially in times of shocks or occurrence of critical incidents.

Systemic risk: the risk of widespread disruption to the provision of financial services that is caused by an impairment of all or parts of the financial system, and which can cause serious negative consequences for the real economy (IMF/BIS/FSB 2009)[35].

Resilience – (adapted from the BCBS, High-level Principles for business continuity, 2006): the ability of a financial industry, financial authority or financial system to absorb the impact of a significant operational disruption while maintaining critical operations and services and minimising risk to the broader economy.

Operational resilience (European Banking Authority[36]): the ability of an institution to deliver critical operations through disruption (BCBS Core Principles 2024, footnote 70). This builds on the prudential operational risk framework, encompassing internal governance, outsourcing, business continuity and relevant risk management-related aspects. Such ability enables an institution to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.

[34] RBS, IOPS definition, www.iopsweb.org

[35] Elements of Effective Macroprudential Policies

[36] https://www.eba.europa.eu/regulation-and-policy/operational-resilience

References:

Australian Prudential Regulation Authority (APRA), Prudential Standard CPS 190, Recovery and Exit Planning,

Australian Prudential Regulation Authority (APRA), Prudential Standard CPS 230, Operational Risk Management, https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf

Australian Prudential Regulation Authority (APRA), Prudential Standard CPS 900, Resolution Planning, https://www.apra.gov.au/sites/default/files/2023-05/Prudential%20Standard%20CPS%20900%20Resolution%20Planning%20-%20clean%20.pdf

Australian Prudential Regulation Authority (APRA), APRA Annual report, 2022-2023, https://www.apra.gov.au/sites/default/files/2023-10/APRA_2022-23_Annual_Report.pdf

Australian Prudential Regulation Authority (APRA), APRA moves to strengthen crisis preparedness in banking, insurance and superannuation, December (2021), https://www.apra.gov.au/news-and-publications/apra-moves-to-strengthen-crisis-preparedness-banking-insurance-and

Australian Prudential Regulation Authority (APRA), APRA Discussion paper, December 2021, Strengthening crisis preparedness, https://www.apra.gov.au/sites/default/files/2021-12/Discussion%20Paper%20-%20Strengthening%20crisis%20preparedness.pdf

Australian Prudential Regulation Authority (APRA), APRA's 2023 Supervision Priorities, https://www.apra.gov.au/supervision-and-policy-priorities

Australian Prudential Regulation Authority (APRA), APRA Corporate Plan 21-25, https://www.apra.gov.au/sites/default/files/2021-08/2021-25%20APRA%20Corporate%20Plan_1.pdf

Australian Prudential Regulation Authority (APRA), Speech, Chair John Lonsdale's speech on banking system stability, https://www.apra.gov.au/news-and-publications/apra-chair-john-lonsdale-speech-to-afr-banking-summit-2023

Australian Prudential Regulation Authority (APRA), Speech, Cahir John Lonsdale's speech to AFR Banking Summit, 26 March 2024

Basel Committee on Banking Supervision, 2021, Principles for Operational Resilience, https://www.bis.org/bcbs/publ/d516.pdf

Basel Committee on Banking Supervision, High-level principles for Business Continuity, 2006, https://www.bis.org/publ/joint17.htm

Basel Committee on Banking Supervision, Core Principles for Effective Banking Supervision, 2024, https://www.bis.org/bcbs/publ/d573.htm

Central Bank of the Netherlands (DNB), DNB Annual report 2022, published 7 July 2023, https://www.dnb.nl/media/zoqfezqn/76051-dnb-jaarverslag-2022_en_web.pdf

Central Bank of the Netherlands (DNB), DNB Visions and Strategy 2025, https://www.dnb.nl/media/jeslcpxj/dnb2025-dnb-vision-and-strategy_tcm47-387985.pdf

Central Bank of the Netherlands (DNB), DNB Supervisory Strategy 2021-2024, https://www.dnb.nl/media/yjdgeqoy/supervisory_strategy_2021_v2.pdf

Central Bank of the Netherlands (DNB), DNB Financial Stability Report 2023, https://www.dnb.nl/en/publications/publications-dnb/?p=1&l=10

European Central Bank, Speech, "The art of bending without breaking – banking on operational resilience", September 2024, https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240904~629e00231e.en.html

European Central Bank, Crisis Management, https://www.bankingsupervision.europa.eu/banking/approach/crisis/html/index.en.html

European Central Bank, Supervisory Manuel – supervision of significant institutions, 2024, https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.en.pdf

European Central Bank, "Bridges to the future: managing bank risk amid uncertainty", Speech by Claudia Buch, Chair of the Supervisory Board of the ECB, March 2024, https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240312~5990ccfce7.en.html

European Central Bank, IT and cybersecurity: no grounds for complacency, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl231115.en.html

European Union (EU), The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554, https://www.digital-operational-resilience-act.com/

Federal Financial Supervisory Authority (BaFin), Germany, Annual Reports 2022, 2023, 2024, https://www.bafin.de/EN/PublikationenDaten/Jahresbericht/jahresbericht_node_en.html

Federal Financial Supervisory Authority (BaFin), Germany, Risks in BaFin Focus 2023, 2024, https://www.bafin.de/EN/Aufsicht/Fokusrisiken/fokusrisiken_node_en.html

Federal Financial Supervisory Authority (BaFin), Germany, May 2023, Speech BaFin President "Learning the right lessons", https://www.bafin.de/ref/19621000

Financial Regulator Assessment Authority, Australia, 2023 Effectiveness and Capability Review of the Australian Prudential Regulation Authority, https://fraa.gov.au/publications/effectiveness-and-capability-reviews-australian-prudential-regulation-authority

IOPS Working Paper N38, Report on learnings from the design, implementation, use and review of Risk Based Supervision by pension supervisory authorities, 2022

ISO 22301 International Standard for Business Continuity Management Systems (BCMS), https://www.iso.org/standard/75106.html

Kay, J. and King, M. (2020) Radical uncertainty: Decision-making for an unknowable future, The Bridge Street Press

Prudential Supervisory and Resolution Authority (ACPR), Bank of France, Autorité de contrôle prudentiel et de résolution announces its work programme for 2024, Press release, January 2024,

https://acpr.banque-france.fr/en/press-release/autorite-de-controle-prudentiel-et-de-resolution-announces-its-work-programme-2024

The Bank of England, Operational resilience: critical third parties to the UK financial sector (to insert link), https://www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector

The Bank of England, Operational resilience: Impact tolerance for important business services, https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

The Bank of England, What will operational resilience look like going forward? An overview of the supervisory regulatory position – speech by Duncan Mackinnon, https://www.bankofengland.co.uk/speech/2022/may/duncan-mackinnon-speech-at-the-city-and-financial-9th-annual-operational-resilience

The Pensions Regulator, Ireland, Incident response plan

The Pensions Regulator (TPR), the United Kingdom, Cyber security principles for pension schemes (2018), https://www.thepensionsregulator.gov.uk/en/document-library/scheme-management-detailed-guidance/administration-detailed-guidance/cyber-security-principles

The Pensions Regulator (TPR), the United Kingdom, TPR Corporate Plan 2022-2023, https://www.thepensionsregulator.gov.uk/en/document-library/corporate-information/corporate-plans/corporate-plan-2022-24

The Pensions Regulator (TPR), the United Kingdom, TPR Corporate Plan 2023-2024, https://www.thepensionsregulator.gov.uk/en/document-library/corporate-information/corporate-plans/corporate-plan-2023-24

The World Economic Forum, Global Risks Report 2023, 18th Edition, 2023, https://www.weforum.org/publications/global-risks-report-2023/