Application Paper on operational resilience objectives and toolkit

February 2026

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard-setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard-setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

For more information, please visit www.iais.org and follow us on LinkedIn: IAIS – International Association of Insurance Supervisors.

Application Papers provide supporting material related to specific supervisory material (ICPs or ComFrame). Application Papers could be provided in circumstances where the practical application of principles and standards may vary or where their interpretation and implementation may pose challenges. Application Papers do not include new requirements, but provide further advice, illustrations, recommendations or examples of good practice to supervisors on how supervisory material may be implemented. The proportionality principle applies to the content of Application Papers.

International Association of Insurance Supervisors
c/o Bank for International Settlements
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090

This document is available on the IAIS website (www.iais.org).

IAIS

Contents

Executive summary

1. As insurers' operations become more complex, interconnected and dependent on technology and third-party service providers, the likelihood and impact of operational disruptions and the importance of operational resilience have materially increased. Operational resilience can be considered as an outcome that emerges from several governance and risk management practices and disciplines currently used by insurers. An operationally resilient insurer is one that can encounter, withstand, mitigate, recover and learn from the impact of a broad range of events that have the potential to significantly disrupt the normal course of business by affecting critical services or operations. The concept and definitions of operational resilience take as a premise the assumption that operational disruptions will occur and thus insurers should consider their tolerance for such disruptions and take this tolerance into account when devising their approach to operational resilience.
2. The focus of the International Association of Insurance Supervisors (IAIS) on insurance sector operational resilience was reinforced in its 2025–2029 Strategic Plan, which features digital innovation and cyber risks as strategic themes. In developing this Application Paper, the IAIS recognises this as an area in which supervisory practices continue to evolve.
3. The Insurance Core Principles (ICPs) establish the importance of insurers having effective risk management and governance processes. This paper supports supervisors and insurers in understanding how to assess and address operational resilience in light of the relevant ICP requirements. To this end, it considers how operational resilience can be embedded into existing risk management and governance frameworks.
4. The Application Paper consists of the operational resilience objectives (the objectives) and supporting practices and tools (the toolkit). The objectives provide an outcomes-based articulation of the application of ICPs in light of developments in operational resilience, while the toolkit provides a selection of practices that could be used to achieve (or work towards achieving) the objectives. These two components work in tandem: the objectives provide the basis for a high-level framework for meeting the ICPs, while the toolkit provides supervisors with practical implementation approaches. Such approaches will naturally evolve as risk management practices mature (in general and for a given insurer) and new risks emerge. The selection of practices and tools included in the toolkit can be implemented according to the specific context and needs of each supervisor and market.
5. The development of this Application Paper took both a top-down and a bottom-up approach. The objectives were drafted by the Operational Resilience Working Group (ORWG) first and then it developed the toolkit on the basis of a survey conducted with IAIS Members from multiple jurisdictions (see the Annex for a list of the participating jurisdictions).
6. Responses to the survey point towards a convergence in supervisory practices adopted for the governance and management of operational resilience (Objective 1). This is explainable because operational resilience has been embedded into existing governance and risk management frameworks for some time. The survey indicated a wide variety of practices adopted by supervisors for the key elements of operational resilience regimes (Objective 2).

1 Background

1.1 Background and purpose

7. The IAIS has undertaken a body of work on operational resilience. The IAIS' Global Insurance Market Report (GIMAR) special topic edition (April 2023) focused on the global cyber insurance market, the cyber resilience of the insurance sector and potential implications for financial stability. In May 2023, the IAIS published an Issues Paper identifying issues impacting operational resilience in the insurance sector with respect to cyber resilience, IT third-party outsourcing and business continuity management, and providing examples of how insurance supervisors are approaching these issues with consideration of lessons learnt during the Covid-19 pandemic.
8. Stakeholder feedback from the May 2023 Issues Paper encouraged the IAIS to take a dynamic, proportionate, risk-focused and principles-based approach to any future work on operational resilience, with the aim of encouraging consistency where possible, respecting jurisdictional differences and underscoring the benefits of information sharing, collaboration and cooperation. Given this feedback, the IAIS has developed this Application Paper with the aim of providing a sound and consistent foundation to support supervisors in developing and strengthening their approaches to supervising insurers' operational resilience.
9. As stated in the May 2023 Issues Paper, the IAIS considers operational resilience as an outcome that emerges from a wide array of practices and disciplines. While closely related, operational resilience and operational risk management are distinct but complementary concepts. Operational risk management focuses on identifying, assessing, preventing and mitigating risks from an insurer's day-to-day operations, including internal processes, people, systems and external events, whereas operational resilience focuses on ensuring *continuity* of critical services and functions when failures occur. The two are related but should not be conflated.

1.2 How ICPs support operational resilience

10. The ICPs provide a global framework for the supervision of the insurance sector and a flexible basis for supervisors to identify and respond to new and emerging risks. The ICPs are the starting point for guiding supervisory responses and supporting the sound management of operational resilience issues. A key aspect of operational resilience is that operational disruptions can have both narrow and widespread implications (for example, to a functional area of the insurer, across the organisation, sector-wide, across sectors and/or across jurisdictions).
11. A number of ICPs, both individually and when viewed collectively, support the sound supervision and management of operational resilience in the insurance sector. The ICPs relevant to the Objectives set out in Section 2 include:

- ICP 2 (Supervisor)
- ICP 3 (Information Sharing and Confidentiality Requirements)
- ICP 7 (Corporate Governance)
- ICP 8 (Risk Management and Internal Controls)
- ICP 9 (Supervisory Review and Reporting)
- ICP 10 (Preventive Measures, Corrective Measures and Sanctions)
- ICP 16 (Enterprise Risk Management for Solvency Purposes)

- ICP 24 (Macroprudential Supervision)
- ICP 25 (Supervisory Cooperation and Coordination)

1.3 Objectives and toolkit for insurance sector operational resilience

12. The IAIS conducted a survey of its Members in late 2024 that sought information about practices related to the objectives that they have in place or are planning to implement. The toolkit reflects a snapshot of the practices identified in the survey responses; therefore, it does not capture all practices across insurance supervisors and is likely to be most reflective of the characteristics of those jurisdictions that responded to the survey. The toolkit will help supervisors to consider the practices they could adopt to support the outcomes set out in the objectives. The practices noted in the toolkit provide a range of ways in which insurers and supervisors could look to meet the objectives. As operational resilience-related risks evolve and the tools to address these risks develop, some of these practices may become more or less applicable over time, and new or revised practices may evolve. The IAIS will therefore continue to monitor these practices and provide a platform for its Members to share their experiences.
13. In developing the objectives, the IAIS considered developments across the financial system, including relevant work being undertaken by the Financial Stability Board (FSB)[1] and the Basel Committee on Banking Supervision.

2 Operational resilience regulatory landscape

2.1 Supervisory approaches and frameworks

14. Jurisdictions have taken a variety of approaches to operational resilience and operational risk in relation to their supervisory materials. Nearly all jurisdictions have supervisory materials that address operational risk as part of their risk management, governance and solvency frameworks.
15. Some jurisdictions report having comprehensive supervisory frameworks that encompass most or all of the objectives. A number of surveyed jurisdictions are somewhere in the middle, as they have developed materials that focus on specific topics or areas that are components of an operational resilience approach such as business continuity management, outsourcing and change management.
16. A number of jurisdictions have indicated that they are implementing, or plan to implement, enhanced frameworks for operational resilience and others have indicated that they are actively monitoring this area for potential future work.
17. The following types of guidance and supervisory practices were reported:

- *Legal or supervisory requirements:* These are generally principles-based and are often included in requirements on topics, such as corporate governance, operational risk management, technology/cyber risk management and outsourcing/third-party risk management.
- *Supplementary guidance:* This is material in addition to the foundational requirements (set out above), such as explanatory notes, recommendations, technical standards, opinions and good practice examples. This also includes internal supervisory guidance for use in monitoring insurers' operational resilience.

[1] Financial Stability Board, *Toolkit for Enhancing Third-Party Risk Management and Oversight*, 2023

- *Supervisory engagement activities:* These include on-site inspections, thematic reviews, published supervisory priorities and supervisory reporting.
- *Insurance sector engagement:* These include information sessions, workshops, seminars, self-assessment surveys and bilateral meetings (eg with industry associations and consulting firms).

3 Objective 1: Relationship amongst operational resilience, governance and operational risk management

Objective 1.1: The insurer oversees, implements and maintains an effective approach to operational resilience that is supported by its governance framework (ICP 7).

In support of this objective, it is important for the insurer to consider how the Board:

- Provides leadership by setting a tone from the top that fosters a risk culture and supports the insurer's approach to operational resilience;
- Provides informed and engaged oversight of Senior Management's implementation of the insurer's approach to operational resilience;
- Oversees the insurer's approach to addressing and mitigating the impact of operational disruptions, including how the approach is integrated into the insurer's governance framework and incorporates measures that manage the impact of identified risks to within tolerance limits; and
- Ensures that it has sufficient knowledge, skills, experience and understanding of operational resilience matters to fulfil its responsibilities.

It is additionally important for the insurer to consider how the Board and Senior Management:

- Ensures effective systems and processes are in place that support the insurer's approach to operational resilience;
- Effectively implement and communicate the insurer's approach to operational resilience across the organisation and amongst key stakeholders;
- Clearly define roles, responsibilities and reporting lines in relation to operational resilience across the insurer, including escalation mechanisms; and
- Ensure the sufficiency of resources to support the insurer's approach to operational resilience.

18. A majority of jurisdictions indicated that the governance framework of insurers should address the roles and responsibilities of the Board, Senior Management and Key Persons in Control Functions. Roles and responsibilities cover matters such as establishing and implementing systems, processes and policies at a high level and authorities generally appear to take this allocation of roles as extending to operational resilience. Governance frameworks can support the operational resilience approach of insurers in various ways, including:

- Supervisors could consider putting in place supervisory materials that seek to integrate operational resilience into an insurer's governance framework by identifying specific operational resilience roles and responsibilities of the Board and Senior Management.
- Supervisors could include operational resilience under roles and responsibilities of the Board and Senior Management under existing frameworks on closely related areas, such as business continuity management and operational risk.

- Supervisors could focus on the need for insurers to have a robust governance framework that specifically addresses digital, information and communications technology (ICT) and cyber resilience risks. This could be in addition to requirements on how the governance framework of the insurer more broadly supports its approach to operational resilience.

Board Members

19. There are a range of supervisory practices with respect to the operational resilience roles and responsibilities of Boards, with the level of detail varying across jurisdictions. Supervisors could consider (i) placing overall responsibility on the Board to ensure the insurer has implemented an effective approach to operational resilience and highlighting the Board's role in overseeing the implementation of this approach; and (ii) setting specific roles and responsibilities for the Board, including:

- Establishing a risk culture, clear risk appetite, risk management strategy and risk management framework that support the insurer's approach to operational resilience.
- Extending these responsibilities to reviewing and approving key aspects of the insurer's operational resilience approach, such as the insurer's impact tolerances, critical services and compliance self-assessments against operational resilience requirements.
- Ensuring the insurer's approach to operational resilience is adequately resourced, possibly highlighting the resources required to specifically address IT and cyber risks. This could extend to resourcing relevant IT security awareness programmes and digital operational resilience training and IT skills for all staff.

Senior Management

20. In most jurisdictions, the Senior Management is responsible for day-to-day management, including ensuring the implementation of the operational resilience framework and its integration with the insurers' overall risk management framework, Supervisory practices that could support this outcome include:

- Assessing whether operational resilience is included within the roles and responsibilities of Senior Management identified under an insurer's governance framework.
- Requiring insurers to allocate responsibility for operational resilience to a specific individual or individuals within Senior Management.
- Setting expectations that Senior Management are responsible for outlining a communication strategy in the event of operational risk-related incidents and setting out communication actions to relevant external stakeholders as part of their business continuity policies.

Box 1: Examples of how governance frameworks can support operational resilience

Bermuda: The Bermuda Monetary Authority (BMA) published an operational resilience and outsourcing code and guidance in September 2025. The framework reinforces the complementary roles the Board and Senior Management play in maintaining and strengthening operational resilience, overseeing outsourcing arrangements and ensuring compliance with regulatory expectations. It details the respective roles as follows:

- The Board is responsible for strategic oversight, approval and accountability for operational resilience and outsourcing policies, ensuring alignment with regulatory requirements, risk appetite and the insurer's strategic objectives; and
- Senior Management is responsible for implementing, and managing resilience measures and outsourcing arrangements, including the development and execution of detailed procedures, controls and ongoing monitoring and evaluation.

See: Operational resilience and outsourcing code.

Canada, Quebec: The Autorité des marchés financiers (AMF) sets out expectations on sound governance structure to foster compliance with operational risk management orientations, including:

For the Board to:

- Approve the operational risk management framework, the strategies in line with the risk appetite of the institutions and the operational risk tolerance;
- Supervise Senior Management to ensure that the operational risk management framework is being applied; and
- Be regularly apprised of evolving trends, emerging risks and material changes likely to alter the financial institution's risk profile.

For Senior Management to:

- Implement and maintain processes and systems reflecting the operational risk management framework in accordance with operational risk tolerance levels;
- Ensure that adequate mechanisms are set up for reporting situations where operational risk tolerance levels are exceeded;
- Ensure the availability, sufficiency and adequacy of operational risk management resources; and
- Ensure that targeted risk management training is given to managers and their teams.

See: Operational risk management guideline.

Costa Rica: The Superintendencia general de seguros (SUGESE) sets minimum governance requirements on the Board in relation to digital operational resilience, including:

- Approving the digital operational resilience policies of the insurer;
- Ensuring that digital operational resilience is incorporated into the insurer's contingency and business continuity plans;
- Approving the budgets and resources necessary to ensure digital operational resilience;

- Ensuring the implementation of response, recovery and crisis management plans to address incidents related to digital assets that could disrupt the execution of critical processes; and
- Ensuring that incident response plans related to digital assets are aligned with the risk appetite, tolerance and capacity established by the insurer.

See: General regulation on information technology governance and management.

Qatar: the Qatar Financial Centre Regulatory Authority (QFCRA) has issued requirements setting out how an insurer's governance framework must support the firm's approach to operational resilience, including:

- Setting out the Board's general obligations for overseeing an effective approach to operational resilience;
- Requiring the Board to review and approve key aspects of the firm's approach to operational resilience (such as impact tolerances and critical operations);
- Requiring the insurer to align its approach to operational resilience to its governance framework and embedding operational resilience into roles and responsibilities of Senior Management and control functions, committee structures and so on; and
- Setting specific obligations on the Board and Senior Management in relation to risk areas, notably outsourcing, technology risks and business continuity, that further integrate operational resilience into the governance framework of insurers.

See: Governance and Controlled Functions Rules 2020.

USA: The National Association of Insurance Commissioners' (NAIC) Market Regulation Handbook Financial Condition Examiner's Handbook, and Financial Analysis Handbook, provide comprehensive guidelines that support objective 1.1 by emphasising effective corporate governance, robust risk management frameworks and strong internal controls. They outline specific responsibilities for the Board and Senior Management, including setting a risk culture, approving key aspects of operational resilience and ensuring adequate resources are allocated. The Market Regulation Handbook stresses the importance of transparent communication and reporting practices, enabling insurers to embed operational resilience into their governance framework effectively. By leveraging these guidelines, insurers can enhance their governance structures to better support operational resilience, aligning with objectives outlined. Additionally, required filings such as Form F (Enterprise Risk Report), ORSA (Own Risk Solvency Assessment), and Corporate Governance Annual Disclosure (CGAD), also support objective 1.1 by emphasising effective corporate governance, robust risk management frameworks and strong internal controls.

See: NAIC Market regulation handbook.

21. Jurisdictions can apply fit and proper criteria for Board appointments and can also consider setting specific requirements or expectations regarding the Board's knowledge, skills, experience and understanding of operational resilience. These can be based on formal and informal education, as well as their professional background skills and industry experience. Jurisdictions can choose to specifically identify the need for Board members to have sufficient knowledge and understanding of IT and cyber risks and their impact on operational resilience.

Box 2: Practices on Board and Senior Management knowledge, skills and experience

Canada, Quebec: The AMF has established expectations for insurers to ensure that the Board's collective skills and experiences are sufficient to properly understand, assess and quantify the risks faced by the institution when such risks are presented by Senior Management, including ICT risk.

See: Integrated risk guideline.

China, Hong Kong: The Hong Kong Insurance Authority's expectations are that the Board should have sufficient knowledge and relevant experience of the insurance business to guide the insurer and oversee its activities, including operational risk matters, effectively.

See: Guideline on the corporate governance of authorized insurers.

European Union: Under the Digital Operational Resilience Act (DORA), the Board is expected to have the necessary knowledge and skills to validate the implementation of operational resilience and have sufficient knowledge and skills to assess ICT risk and its impact on operations.

See: Article 5 of DORA.

New Zealand: The Reserve Bank of New Zealand (RBNZ) has set expectations that both the Board and Senior Management have a sufficient understanding of the insurer's cyber risk environment, including for future resource planning purposes and for both ongoing and forecasted cyber resilience needs.

See: Guidance on cyber resilience.

Qatar: The QFCRA's view is that robust oversight and engagement on ICT matters by an insurer's Board and Senior Management play a leading role in promoting an ICT and information security risks-conscious culture within the firm. To ensure this, the QFCRA has set its expectations that the Board and Senior Management should possess sufficient knowledge and understanding of the ICT and information security risks facing the insurer and take steps so that these risks are well understood and properly managed throughout the firm.

See: Governance and Controlled Functions Rules 2020.

United Kingdom: The approach of the Prudential Regulation Authority (PRA) is to set expectations that Board members should have sufficient knowledge and skills (but not necessarily technical expertise) to meet their operational resilience responsibilities and be able to constructively challenge Senior Management.

See: Statement of policy: operational resilience.

22. Jurisdictions can consider evaluating the Board through supervisory actions. Examples of such activities include:

- Supervising the knowledge, skills, experience and understanding of operational resilience matters through the licensing procedure for Board members. These criteria can be assessed against the individual's formal and informal education, former responsibilities and positions held. Competencies appropriate for the management and conduct of business could also be tested

through interviews and candidate presentations, enabling the authority to ask questions to determine the level of candidates' knowledge, skills, experience and understanding.

- On-site supervision actions, where the responsibilities of the Board and Senior Management are evaluated with respect to the insurer's operational resilience approach, including the definition of roles and responsibilities, knowledge on the subject, approval of strategy and policies, implementation of the model, operation of the three lines of defence, assigned budget, monitoring and authority and effectiveness to correct weaknesses.
- Reviewing Board materials and periodically meeting with other Boards, which provides insights into the Board's understanding of operational resilience.

Objective 1.2: The insurer's approach to operational resilience leverages and is integrated with, its operational risk management framework in a consistent, comprehensive and robust manner (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Ensures that a risk management system is in place that identifies, assesses, monitors, mitigates and reports on the operational risks (including new and emerging risks) to which the insurer is exposed;
- Identifies and manages all risks that have the potential to severely disrupt its operations, including its ability to deliver on its critical services;[2] and
- Is embedded into its internal controls and incorporates appropriate roles and responsibilities across business lines and functions in consideration of the three lines of defence (the division of responsibilities between the business, risk management and compliance and internal audit, as referred to at ICP 8.2.3).

Practices to ensure that a risk management system is in place that identifies, assesses, monitors, mitigates and reports on the operational risks (including new and emerging risks) to which the insurer is exposed.

23. The majority of jurisdictions require insurers to address operational risk as part of their overall risk management framework. Supervisory materials and practices rely on principles-based supervisory requirements that can include requirements on areas such as corporate governance or operational risk management in general, or specifically on technology, cyber or third-party risk management. Further materials and tools could be prepared by supervisors to address the integration of an insurer's approach to operational resilience with its operational risk management framework.

- Issue supplementary materials in addition to supervisory requirements, for example guidance on technology risk, outsourcing and/or business continuity specifically addressing operational resilience of the firm. Such supplementary material may be issued for example as explanatory

[2] Consistent with the FSB *Toolkit for Enhancing Third-Party Risk Management and Oversight*, critical services are those whose failure or disruption could significantly impair a financial institution's viability, critical operations, or its ability to meet key legal and regulatory obligations.

notes, supervisory priorities, recommendations, technical standards, opinions, good practice examples.

- Set expectations that stress the integration of operational resilience into the operational risk management framework by having a single combined set of guidelines on supervisory expectations covering both operational risk and operational resilience, to emphasise the relationship between them.
- Another way to provide guidance is for the supervisory authority to hold events such as information sessions, workshops, seminars or bilateral meetings, for example with insurers, industry associations or consulting firms.
- Jurisdictions can perform specific supervision activities to assess insurers' consideration of operational resilience in their approaches to operational risk, such as self-assessment surveys, on-site inspections and thematic reviews, cyber incident response exercises, reviews of meeting minutes of the Board, the Risk Committee and other committees where these are linked to operational risk management, operational resilience and information security.
- Internal supervisory guidelines on the supervisory approach to operational resilience can include guidelines for a detailed assessment of insurers' risk management and resilience practices.
- Supervisory authorities can consider requiring that operational resilience is integrated into insurers' ICT risk frameworks, which is a core competency of the operational risk framework.

Box 3: Risk management systems

Canada, Quebec: The AMF sets out expectations for insurers to:

- Define and maintain a general risk appetite statement as well tolerance levels for material risks;
- Establish a framework to adequately manage operational risks, based on their risk appetite;
- Manage operational risk by taking into account the institution's operational risk exposure inherent to people, processes, systems or external events as well as the exposure of third parties to these risks; and
- Develop strategies, policies and procedures enabling ICT risk identification, assessment, quantification, control and monitoring.

In addition, the AMF periodically holds webinars and organise roundtables with insurers in order to promote good practices regarding operational resilience themes.

See: Operational risk management guideline.

Canada: OSFI sets out expectations regarding operational risk management practices that support operational resilience. These include:

- Having an effective operational risk management framework that includes: an approved operational risk appetite statement with operational risk limits, policies and procedures that are regularly reviewed and updated; a risk taxonomy that includes categories of risks related to people, inadequate internal processes and systems and external events and assessment; and monitoring tools to evaluate risks and controls; and
- Having a risk appetite for operational risks defined and adhered to that includes qualitative and quantitative measures, is forward looking (ie anticipates potential risks in the future) and explicitly sets out risk limits.

See: Operational risk management and resilience - guideline.

European Union: DORA requires insurers to have in place:

- A sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience;
- An internal governance and control framework that ensures an effective and prudent management of ICT risk, in order to achieve a high level of operational resilience; and
- An ICT risk management framework, which includes a digital operation resilience strategy setting out how the framework shall be implemented.

See: DORA regulation.

Qatar: The QFCRA requires insurers to have in place:

- A risk management system that identifies, measures, evaluates, monitors, reports on and controls or mitigates all internal and external sources of material risk and that should be forward looking to ensure new and emerging risks that could materialise are identified;
- A documented operational risk framework that is integrated into its risk management framework, including governance arrangements for the oversight of operational risk, monitoring, analysis and reporting of operational risk and escalation processes for operational

risk events and internal controls that are designed and used effectively for the management of operational risk; and

- An operational resilience approach that is aligned to its operational risk framework.

See Governance and Controlled Functions Rules 2020.

Practices to identify and manage all risks that have the potential to severely disrupt an insurer's operations, including its ability to deliver on its critical services.

24. Supervisory requirements on operational risk and resilience typically include the requirement for insurers to identify risks that have the potential to severely disrupt their operations, including their ability to deliver on their critical services. Where there are no specific requirements on operational risk and resilience defined, requirements on considering potential severe disruptions can be included in areas such as technology risk, outsourcing/third-party risk management risk and business continuity management.

Practices to embed operational resilience into an insurer's system of internal controls, roles and responsibilities across business lines, and the division of responsibilities between the business, risk management and compliance and internal audit.

25. While in most jurisdictions there are supervisory requirements for insurers to implement effective internal controls, including appropriate segregation of duties amongst the three lines of defence, supervisory requirements often do not specifically address the integration of operational resilience aspects into these controls. Supervisors can require insurers to adopt internal governance and control frameworks that address effective and prudent management of ICT-related risks. These frameworks can include the obligations for the management body that defines, approves, supervises and is responsible for the implementation of such governance.

Box 4: Internal controls

European Union: Requirements in DORA for insurers include:

- Assigning responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such a control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions and internal audit functions, according to the three lines of defence model or an internal risk management and control model; and
- An ICT risk management framework, other than for microenterprises, that shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.

4 Objective 2: Key elements of a sound approach to operational resilience

Objective 2.1: The insurer identifies and maintains an up-to-date inventory of its critical services and interdependencies (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Ensures an understanding of its critical services, including the resources and risks involved in the delivery of those services; and
- Identifies, maps and documents each critical service end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers.

Practices to ensure an understanding of insurers' critical services, including the resources and risks involved in the delivery of those services.

26. There are generally two approaches that could be used for the identification of critical services and related risks and resources:

- A bottom-up approach, where critical services identified are at the operational level and then aggregated information is submitted for review and approval by Senior Management.
- A top-down approach, where Senior Management sets the direction and priorities for identifying critical services, which are then set out in more detail by operational teams.

27. In choosing which approach or a combination of approaches to use for identification of critical services, insurers currently consider their size and overall risk profile and the nature, scale and complexity of their services, activities and operations. This includes, where applicable, the criticality of such services, activities and operations to the broader financial system. Similarly, supervisors can issue relevant guidance to explain how insurers can approach the identification of critical services and interdependencies, referring to examples or expectations relevant to their jurisdiction.

Box 5: Expectations on identification of critical services and interdependencies

Canada: Section 3.1 of OSFI's Guideline E-21 (on operational risk management and resilience) sets out expectations for insurers to identify, map and document their critical processes.

Practices to identify, map and document each critical service end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers.

28. A common practice is to document the approach for the identification of critical processes and interdependencies through policies and procedures, with the involvement of the Board. Such policies and procedures are periodically reviewed or audited. The identification and mapping of

critical services and their interdependencies is a holistic exercise performed by insurers that involves multiple layers of their organisations; for example, current practice is for the operational layer to perform identification and mapping, for Senior Management to review the output and for the Board to approve it. Supervisors could issue guidance on their expectations relating to the governance of this specific process.

29. To build better resilience across the financial sector, supervisors could introduce practices where insurers report results of mapping on a periodic basis to supervisors. Such mapping could include registers of critical services, outsourcing and third-party arrangements. To keep the inventory of critical services and interdependencies up-to-date, insurers could introduce periodic reviews of such inventories or introduce updating of such inventories in case of material changes to critical services or interdependencies, or after regular resilience testing or self-assessment.

30. Supervisors could issue guidance where they may specify expectations to mapping of critical services and what should be included (eg critical processes) and the resources required to deliver critical processes (IT systems, data, premises, people, other critical processes, third-party providers, any materials/supplies, etc).

Box 6: Identification of critical services

Bermuda: BMA's operational resilience code and guidance describes expectations to identify and map important business processes including all resources, people, IT systems, data and facilities essential for delivering important business services.

See: Operational resilience and outsourcing code.

Costa Rica: The SUGESE defines expectations for the identification of the governance and management structure, processes, services, IT infrastructure, IT goods and services providers, inventory of document types, IT projects, acquisition plans and IT risk management in its technological profile. Technology profiles are reviewed by the entity through supervision processes and during risk-based supervision visits.

See: Regulations for governance and management of IT.

South Africa: The Prudential Authority and Financial Sector Conduct Authority's joint standard on IT governance and risk management describes the requirement for financial institutions to identify business processes and information assets that support business and delivery of services, including those managed by third-party service providers and classify the business processes and information assets in terms of criticality and sensitivity, which in turn must guide the prioritisation of its protective, detective, response and recovery efforts.

See: Joint standard.

Objective 2.2: The insurer sets impact tolerances for disruption to its critical services (ICPs 8 and 16).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Defines the maximum disruption/impact that it could bear before causing intolerable harm to its financial soundness, its customers or the wider financial system, where applicable, including how such maximums relate to the wider risk tolerance of the insurer; and
- Embeds pre-defined impact tolerances as a useful basis for evaluating the need for changes to operational and strategic decisions (eg to identify, evaluate and respond to redundancies, contingencies, or the need for further investment to improve the resilience of systems and third-party providers including intragroup and nth-party providers).

Practices to set an insurer's maximum disruption/impact for disruption tolerance before causing intolerable harm to its financial soundness, its customers or the wider financial system. It may embed pre-defined impact tolerances.

31. Jurisdictions may take a non-prescriptive approach to setting supervisory requirements for insurers' impact tolerances. Practices might include requirements, guidance or expectations for insurers to assess and set their tolerance levels based on their individual business requirements, size, risks and circumstances. Where appropriate, supervisors may choose to require insurers to express their tolerances using a minimum set of metrics or elements, while providing the insurer with flexibility at firm level.
32. Insurers could assess the effectiveness of business continuity and recovery plans, including with third-party providers where applicable. Guidance could involve explaining relevant concepts such as "disruption" and "recoverability" or outlining factors the insurer should consider when setting impact tolerances.
33. To improve the likelihood of firms being able to remain within impact tolerances, supervisors could introduce practices where insurers conduct regular testing of tolerance to disruptions through scenarios and stress testing. Additionally, insurers could implement incident management processes with post-incident analysis, with conclusions from these exercises being presented to relevant governance committees.
34. To improve the approach of insurers to setting and remaining within impact tolerances, authorities can encourage insurers to participate in industry collaboration and information exchange forums. To evaluate the need for changes to operational and strategic decisions, insurers can review historical incident data to better understand impact patterns, recovery times and resource requirements.
35. Additional reported practices include periodic reviews of impact tolerances, especially but not limited to following material changes to critical processes. In this respect, supervisors could encourage insurers, for example, to:

- Regularly review and assess resilience testing scenarios;
- Monitor and adjust testing frequency based on risk assessments; and
- Review tolerance adequacy when significant process changes occur.

Box 7: Setting impact tolerances

Canada: OSFI guides insurers in setting impact tolerances for their critical services by clearly defining "tolerance for disruption" and "critical operations". Insurers are required to identify and map their critical operations, establish tolerance for disruption, then regularly test their tolerance for disruptions through scenario testing based on criticality. A variety of testing methodologies should be used, including tabletop exercises, simulations, and live systems testing. As per that guideline:

- "Tolerance for disruption" is the maximum disruption from an operational risk event a financial institution can withstand, under a range of severe but plausible scenarios. It includes things like outage time, diminishment of service, loss of data, or extent of customer impact.
- "Critical operations" are services or products that, if disrupted, would put at risk the financial institution's continued operations or safety and soundness, or harm other institutions due to its interconnectedness to the financial system.

See: Operational Risk Management and Resilience – Guideline.

European Union: DORA Article 6(8) requires European financial entities to define a digital operational resilience strategy, including methods to address ICT risk and attain specific ICT objectives by establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity and analysing the impact tolerance for ICT disruptions. Article 3 of the regulatory technical standard on ICT risk management provides further specifications in relation to the approval of the impact tolerances, including in cases when there is the need to accept residual risks exceeding those tolerance levels.

See: DORA regulatory technical standard.

United Kingdom: The Critical National Infrastructure Banking Supervision and Evaluation Testing (CBEST) is a threat-led penetration testing framework used by the Bank of England, the PRA and the Financial Conduct Authority (FCA) to assess the cyber resilience of firms and financial market infrastructures. The CBEST reports and the annual CBEST thematic reports can be used by firms to better inform their setting of impact tolerances.

See: CBEST testing framework and thematic reports

Objective 2.3: The insurer self-assesses and tests its ability to withstand and recover from severe but plausible scenarios of operational disruption and ensures that action is taken to improve operational resilience on the basis of lessons learnt (ICPs 8 and 16).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Embeds scenario testing that focuses on operational resilience and assesses the insurer's ability to withstand and recover from severe operational disruptions; and
- Incorporates lessons learnt from scenario testing, particularly when the results of testing identify that tolerances for disruption would be breached in one or more severe but plausible scenarios.

Practices embed scenario testing that focus on operational resilience and assess the insurer's ability to withstand and recover from severe but plausible operational disruptions.

36. Jurisdictions can outline supervisory expectations for insurers to test their resilience to operational disruptions through regular stress and scenario testing, documenting scenario testing and results, recovery plans and reporting requirements. Jurisdictions can set expectations for comprehensive annual scenario tests. Jurisdictions can expect insurers to document their test outcomes and ensure their plans are updated based on the test results and learnings. Supervisors may request the results of resilience tests or self-assessments on an ad hoc basis or as part of their regular supervisory reviews. Supervisory materials can also cover considerations on the comprehensiveness and adequacy of testing plus recovery objectives.

37. There are a number of practices that can support testing and self-assessment objectives:

- *Scenario testing of critical services:* Scenarios should be sufficiently severe to challenge insurers on the appropriateness of their accepted impact tolerances. The testing of their resilience responses should leverage and consider stressing their critical resources and existing arrangements for recovery and continuity. To assess insurers' ability to continue their critical operations, they could consider the time, availability of resource and the severity of a disruption scenario as additional elements of the stress testing exercise. The scope of the tests should include the assessment of resilience arrangements for critical information systems, including strategies for managing data loss.
- *End-to-end approach in testing and third parties:* To ensure that resilience responses are realistic in a test environment, insurers can consider testing not only the elements of a critical service but the recovery of all potentially affected elements in an end-to-end test, including its interlinkages and impacts to all critical services. It is good practice that insurers are aware of the resilience arrangements of their third-party service providers and ensure that resilience tests are performed jointly or in collaboration with these providers.
- *Frequency of testing:* Performing self-assessments and resilience testing at least annually is another observed practice. Insurers could perform these exercises more frequently if required (for example, in case of a material changes to critical processes or external environments).
- *Scenarios prescribed by the supervisory authority:* To ensure comprehensiveness and adequacy of the resilience testing, supervisors may consider developing stress scenarios for the insurance sector based on the sector risk outlooks or historical data for the sector to establish requirements and forecast potential shocks for the market participants.
- *Technology-specific tests:* Establishing and maintaining an enterprise disaster recovery programme, which supports the insurer's ability to deliver technology services through disruption and operate within its risk tolerance, could be considered. This programme may include plans, procedures and/or capabilities to recover technology services to an acceptable level and within an acceptable timeframe, as defined and prioritised by the insurer.
- *Proportionality and firm size:* To encourage a proportionate approach to the evaluation of the adequacy of self-assessments and scenario testing, the size and complexity of the insurer could be considered.

Box 8: Scenario testing expectations

European Union: DORA Article 11(6) requires financial entities to test their ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions. In those tests, financial entities are required to include scenarios of cyber attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and facility. Furthermore, Article 26(2) of the regulatory technical standards specifying ICT risk management tools, methods, processes and policies and the simplified ICT risk management framework details specific scenarios that should include also the lessons learnt from previous tests.

See: DORA delegated regulation.

Qatar: QFCRA Rule 8.3.7 is an example of good practices and additional regulatory guidance related to testing of impact tolerances. The operational resilience rules include supervisory expectations for insurers to test their impact tolerances, including where related to the identification of adverse circumstances and expected duration of impact, the delivery of critical operations in stress conditions, the role of the governance body and the actions in response to stress and recovery from it.

See: Governance and Controlled Functions Rules 2020.

United Kingdom: Section 15A.5 of the FCA's Senior Management Arrangement, Systems and Controls (SYSC) Handbook provides an example of regulatory expectations with regard to testing insurers' ability to withstand and recover from severe but plausible scenarios of operational disruption. Some additional guidance can be found in the FCA Policy Statement PS21/3 on building operational resilience in sections 5.13 to 5.18 and related examples.

See: FCA Handbook SYSC 15A.5 and FCA Policy Statement PS21/3.

Practices to incorporate lessons learnt from scenario testing, particularly when the results of testing identify that tolerances for disruption would be breached in one or more severe but plausible scenarios.

38. There are a number of practices relevant to identify and incorporate lessons learnt from scenario testing into the resilience practices of insurers:

- *Feedback loop and learning:* Insurers could conduct a lessons learnt exercise in the aftermath of a scenario testing or a real world disruptive event to a critical service to evaluate whether the service remained within tolerance as expected, and, if not, identify and measure what went wrong and identify actions needed to improve the resilience arrangements.
- *Governance and oversight:* To ensure awareness, accountability and oversight, the results of all scenario testing could be reported to the Board of the insurer. Senior Management may be also responsible for approving any monitoring the remediation plans to address weaknesses or vulnerabilities identified during testing in a timely manner.
- *Reporting of outcomes:* In the results of testing or self-assessments, jurisdictions can include a detailed methodology of the assumptions taken to develop testing scenarios, incorporated risks, aims and objectives of the test, as well as the test outcomes. There could be a mechanism for insurers to document their testing outcomes and retain the necessary information. This could be

used to assess sector resilience trends and leading practices, which the supervisors then can share with the insurers.

Box 9: Incorporating lessons learnt

Brazil: The Superintendência de seguros privados (SUSEP) requires supervised entities to prepare an annual report that includes the results of resilience testing, as defined in the business continuity plans (BCP).

See: Circular SUSEP nº 638/2021.

European Union: DORA Articles 6.5 and 13.3 are examples of good practices and additional regulatory guidance related to documenting lessons learnt from relevant resilience tests.

See: DORA delegated regulation

United Kingdom: The PRA Rulebook and FCA Handbook SYSC 15A.5 provide examples of regulatory expectations where the UK authorities expect insurers to report the outcomes of scenario testing as a part of their self-assessment, as well as ad-hoc data collection by the authorities. This should include a detailed methodology of the assumptions taken to develop the scenario, risks incorporated, aim and objective, as well as outcomes. The outputs of the scenario testing should be included in the yearly self-assessment to demonstrate to the authorities the insurer's ability to maintain its important business services within tolerance. Some additional guidance can be found in sections 5.13 to 5.18 of the FCA Policy Statement PS21/3 and section 6 if the PRA Supervisory Statement SS1/21 on building operational resilience.

See: FCA Policy Statement PS21/3 and PRA Supervisory Statement SS1/21.

Objective 2.4: The insurer effectively manages operational incidents, including but not limited to cyber incidents, affecting critical services (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Ensures that operational incidents, including but not limited to cyber incidents, are effectively managed to prevent, respond to, recover from and learn from their occurrence to minimise disruptions to critical services;
- Establishes clear processes for identifying, assessing, reporting and responding to incidents, including those affecting third and nth-party service providers that impact on the operations of the insurer; and
- Ensures communication plans, for example crisis communication plans, are in place to report incidents to both internal and external stakeholders, including regulatory supervisory authorities, as appropriate.

Practices to ensure that operational incidents, including but not limited to cyber incidents, are effectively managed to prevent, respond to, recover from and learn from their occurrence to minimise disruptions to critical services.

39. Jurisdictions may establish structured frameworks with explicit supervisory expectations or adopt a more flexible or evolving approach where incident management and reporting expectations can be integrated within broader risk management frameworks, particularly focusing on cyber security, ICT risk management and business continuity planning.

40. Jurisdictions may consider such frameworks to include practices required to incorporate lessons learnt from incidents, particularly in cases where the tolerances for disruption were breached.

41. Jurisdictions can use more integrated, technology-driven solutions to collect incident reports. This can include the development of centralised reporting platforms, automated monitoring systems and enhanced cross-border coordination mechanisms.

Practices to establish clear processes for identifying, assessing, reporting and responding to incidents, including those affecting third- and nth-party service providers, that impact on the operations of the insurer.

42. Jurisdictions may set explicit criteria for timely reporting material incidents, which can be linked to cyber resilience, supervisory engagement and financial stability considerations. When determining the timing of when an incident should be reported, jurisdictions may need to consider allowing insurers sufficient time to understand and respond to the incident. Jurisdictions can adopt innovative approaches to operational incident reporting, for example by encouraging the sharing of cyber threat intelligence among organisations to enhance collective resilience.

43. For efficiency purposes, supervisors can consider the implementation of centralised digital platforms for incident reporting, including sophisticated systems that allow for incident self-classification and automated tracking.

44. Jurisdictions can consider the use of standardised third-party provider reporting requirements, formalised cross-border coordination mechanisms and defined incident reporting triggers, while expanding beyond cyber risks to cover all operational incidents and the establishment of consistent materiality thresholds.

Practices related to communication plans to report incidents to both internal and external stakeholders, including supervisory authorities, as appropriate.

45. Jurisdictions may require insurers to establish crisis communication plans to ensure incidents or vulnerabilities are responsibly disclosed to policyholders, counterparties and the public.

46. Jurisdictions can mandate systematic collection and maintenance of incident records or rely on requirements through their reporting obligations.

Box 10: Incident responses and communications

European Union: Article 14 of DORA on communication requires financial entities to have in place crisis communication plans for responsible disclosure of at least major ICT-related incidents or vulnerabilities to clients and counterparts, as well as to the public. Furthermore, article 24 of the regulatory technical standards (RTS) on ICT risk management framework on ICT business continuity policy requires financial entities to define the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans and crisis communications plans. Finally, article 25 of the RTS requires financial entities to tests their crisis communication plans.

See: Regulatory technical standards on ICT risk management frameworks.

FSB Format for Incident Reporting Exchange (FIRE)

Incident reporting is one of the primary mechanisms used by financial authorities to keep track of disruptions affecting their regulated entities. Greater regulatory reporting harmonisation promotes effective financial institution supervision and facilitates cooperation and coordination among authorities in monitoring and responding to cyber risks. FIRE aims to promote common information elements for incident reporting while allowing for flexible implementation practices. FIRE addresses the fragmentation in reporting requirements, alleviating the burden on firms that operate across multiple jurisdictions. FIRE still enables authorities to determine whether to implement FIRE based on their specific requirements. Furthermore, it will provide a standard format for financial institutions to map against a variety of reporting criteria, facilitating translations between frameworks. FIRE does not set direct requirements on firms and the FSB will not collect incident reports. Rather, in order for FIRE to be usable, it would require implementation by individual authorities, or for the authority to indicate it accepts FIRE-aligned reports.

See: Final FIRE report.

USA: The NAIC's Cybersecurity Event Response Plan (CERP) provides a structured framework for Departments of Insurance (DOIs) to manage and respond to cyber security events at regulated insurance entities. This plan aligns with the NAIC Insurance Data Security Model Law (MDL #668) and includes detailed guidance on notifications, investigations, and remediation processes. By establishing clear roles and responsibilities within the DOIs, the CERP ensures a cohesive and timely response. The CERP encourages DOIs to engage with law enforcement and other regulators, fostering collaboration and information sharing, emphasising the importance of confidentiality and protection of reported cyber security event data. This systematic approach ensures that insurers can effectively manage incidents, minimising disruptions to their critical services.

See: CERP.

Objective 2.5: The insurer manages and mitigates the impact of technology risk to critical services by implementing an effective approach to operational resilience that addresses the phases of protection, detection, response and recovery (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Supports a stable and resilient technology environment through appropriate risk management practices, including for example its technology architecture, technology asset management,

patch management, service monitoring and other business continuity and disaster recovery practices;

- Ensures effective management and testing of access to information, technology, systems, premises, networks, key people and information assets to safeguard its critical services and incorporates effective protection safeguards for its information assets;
- Reinforces the adoption and maintenance of good cyber hygiene practices including conducting regular technology and cyber security assessments;
- Ensures ongoing training, awareness and collaboration with industry peers on threat intelligence, including on responses to identified incidents; and
- Supports regular testing of the approach to operational resilience, including (but not limited to cyber resilience) and incorporates effective situational awareness and threat intelligence.

Practices related to management of technology risks relevant to operational resilience, including cyber security.

47. Insurers can be subject to supervisory guidance aimed at ensuring that their technology environment is operationally resilient. Supervisory guidance can extend beyond cyber security, including aspects such as stability and scalability of the insurers' ICT landscape. Such guidance can help promote that insurers' critical services are supported by up-to-date technology infrastructure and robust operational processes. Insurers may demonstrate effective technology risk management through various documentation and processes, including risk assessments, audit findings, cyber security maturity assessments, incident management plans and evidence of regulatory compliance.

- Supervisors can conduct both on-site and off-site supervisory activities, which can include regular visits to insurers or requests for documentation submissions. Supervisors can support insurers by setting expectations on conducting the internal audit activities or assessments related to information technology, such as detailed guidelines for internal audit technology assessments, or for evaluating technology and cyber risks as part of broader operational risk management frameworks.

48. Establishing baseline technology risk management expectations can be an initial step to introduce resilience expectations.

Box 11: Supervisory expectations related to ICT risk management

Canada, Quebec: The AMF has issued a regulation on the management and reporting of information security incidents by certain financial institutions and by credit assessment agents. It establishes requirements and sets out expectations regarding the incident management process and requires insurers to report material cyber incidents.

See: Regulation on management and reporting of information security incidents.

Malaysia: The Central Bank of Malaysia has set out the bank's requirements with regard to insurers' management of technology risk.

See: Risk management in technology.

Singapore: The Monetary Authority of Singapore (MAS) has a Notice on technology risk management that sets out requirements for insurers to maintain a high level of reliability, availability and recoverability of critical systems. It also requires insurers to notify the MAS as soon as possible, but not later than one hour, upon the discovery of a "relevant incident" as defined in the notice. MAS has also published an Incident reporting template, as well as Instructions on financial institutions incident notification and reporting to MAS. In addition, MAS' Notice on cyber hygiene sets out cyber security requirements on securing administrative accounts, applying security patching, establishing baseline security standards, deploying network security devices, implementing anti-malware measures and strengthening user authentication. MAS' Guidelines on technology risk management also sets out risk management principles and best practices to guide financial institutions to maintain IT and cyber resilience.

Switzerland: Circular 2023/1 of the Financial Market Supervisory Authority (FINMA) is used as a best practice guidance for insurers in terms of ICT risk management and also wider operational risk and resilience expectations.

See: Circular 2023/1 Operational risks and resilience – banks.

USA: The NAIC has established supervisory requirements and guidelines to ensure operational resilience and effective operational risk management among insurers. These include security controls and the requirement for an incident response plan.

See: Insurance Data Security Model Law (MDL-#668).

Objective 2.6: The insurer plans, tests and implements changes in a controlled manner (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience ensures that:

- Appropriate change management frameworks are put in place and maintained, that consider the impact of changes on operational resilience;
- Changes are managed throughout the change lifecycle with a view to minimising disruption and planning for contingencies; and
- Change management capabilities are regularly reviewed with a view to understanding and improving their operational effectiveness and addressing identified gaps.

Practices to design, implement and maintain appropriate change management frameworks that consider the impact of changes on operational resilience.

49. Supervisors may consider issuing guidance for insurers to explain how to put in place and maintain a comprehensive framework for managing changes in insurers' products, services, systems and processes that may have a significant impact on their operational resilience if implemented in an uncontrolled manner. A specific focus of the observed change management frameworks can be devoted to changes in technology infrastructure and cyber security protocols due to the increasing role of technology in the delivery of insurance services. Practices could include actions to:

- Document the purpose, design and expected impact of the change on the insurer's systems and activities.

- Analyse the risks associated with implementing the change, including any security implications arising from that.
- Test the scheduled changes in an appropriate testing environment before being deployed to the go-live production environment.
- Establish a roll-back plan to revert to the pre-change state if material problems arise during or after the change implementation.
- Have emergency response plans for implementing high-priority changes outside of the normal procedures, with roles and responsibilities assigned for taking ad hoc decisions.

50. Insurers can consider integrating change management processes and practices into broader technology and cyber risk management practices. The primary objective should be to ensure that changes are implemented in a controlled manner that minimise operational disruption. Supervisors may also issue expectations focusing on the effectiveness of change management in the context of cyber security, information technology resources and software updates. However, for a more comprehensive approach, jurisdictions can develop a broader set of expectations to change management that goes beyond information technology environment and encompasses changes in other areas of activity that may impact the operational resilience of the insurer (eg products, services and corporate structure).

Box 12: Supervisory expectations on change management

Canada: OSFI sets expectations in Guideline B-13 (Technology and cyber risk management) for insurers to establish and implement a well-documented technology change and release management process. This should ensure that changes to technology assets are conducted in a controlled manner that ensures minimal disruption to the production environment. Canada has also issued Guideline E-21 (Operational risk management and resilience), which came into effect on 1 September 2025 and outlines the key areas of operational risk management. Change management is considered an integral part of the insurer's operational resilience programme, with specific supervisory expectations envisaged in Section 4.4 of the guidelines. Canada plans to prepare a manual on the application of Guideline E-21 that will assist supervisors in assessing insurers' change management practices.

See: Guideline B-13 (Technology and cyber risk management).

European Union: DORA's regulatory technical standards specifying ICT risk management tools, methods, processes and policies and the simplified ICT risk management framework include a dedicated Article (Art. 38) on ICT project and change management requiring financial entities to implement an ICT project management and an ICT change management procedure ensuring that all stages of ICT projects are covered and that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner and with the adequate safeguards.

See: Regulatory technical standard.

Malaysia: The Central Bank of Malaysia defines change management expectations and cloud design and control (section 4).

See: Risk management in technology policy document.

Practices on lifecycle change management, with a view to minimising disruption and planning for contingencies.

51. Supervisors can issue guidance for insurers to implement processes and procedures to minimise post-implementation disruptions and plan for contingences during the full lifecycle of change. Change management can be incorporated into the wider risk management framework, while addressing risk in the context of the full lifecycle of the change management process, focusing not only before or during the implementation phase but also after the go-live event and beyond.

Box 13: Change management processes

European Union: Although primarily focused on the technology side of operational resilience, DORA regulates the full lifecycle of changes to information and communication technology systems, including software, hardware and security. In particular, Article 17 of the regulatory technical standard on ICT risk management and on the simplified ICT risk management includes stipulations regarding the minimum contents of change management processes, such as check requirements, impact analyses, fallback procedures, emergency change management and post-implementation assessments.

See: Regulatory technical standard.

Practices on understanding and improving insurers' operational effectiveness and addressing identified gaps through regular reviews of their change management capabilities.

52. Supervisors may clarify their expectations to insurers' reviews and constant improvement of change management capabilities in the wider context of risk management. In their supervisory materials, supervisors may wish to provide guidance about the scope and frequency of expected reviews that insurers must carry out to improve their change management capabilities. To drive more effective risk management and in response to changing technology and business requirements, insurers can consider incorporating lessons learnt from mistakes and failures into constant process improvement.

Objective 2.7: The insurer develops, implements, tests and updates its Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure that it can respond, recover, resume and restore to a pre-defined level of operation following a disruption in a timely manner (ICP 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Establishes clear recovery objectives and develops comprehensive contingency plans, guided by currently established impact tolerances, to safeguard against risks of disruption to identified critical services;
- Ensures that BCPs consider the results of business impact analyses to inform recovery strategies, testing procedures and awareness, training, communication and crisis management programmes; and

- Validates that its recovery objectives can be met in a range of severe but plausible scenarios, via periodic testing of BCPs, including by involving the BCPs of critical third-party service providers as needed.

Practices related to development, implementation and testing of BCPs and DRPs to ensure their effectiveness.

53. The evolution of supervisory expectations has shifted BCP/DRP from standalone compliance exercises to the integral components of operational resilience frameworks. Insurers are typically required to protect their critical operations against severe but plausible scenarios, including cyber attacks, climate-related events and third-party failures. In relation to this, supervisors may stress the importance of insurers' Senior Management and Boards to actively oversee and update continuity strategies. Supervisors may focus on some core supervisory expectations in several key areas such as the design of BCP/DRP frameworks, risk and impact assessments, incident response procedures, periodic testing and supervisory reporting.

54. Supervisors may set the reporting expectations by asking insurers to complete self-assessment questionnaires regarding BCP/DRP compliance or submitting annual resilience testing reports. Key risk indicators can be used to assess the effectiveness of BCP/DRP management.

55. The supervisory approach to BCP/DRP could evolve towards more comprehensive, integrated approaches to operational resilience. The focus is increasingly on ensuring that insurers can maintain critical operations under adverse conditions while adapting to emerging risks and threats.

    Supervisors can set supervisory expectations that extend beyond technology to include operations, cyber risk management, third parties and internal dependencies. Jurisdictions can integrate BCP/DRP into comprehensive resilience frameworks that emphasise regular self-assessments and annual reviews to adapt continuity strategies to changing risk profiles.

Box 14: Business continuity/disruption planning regulatory expectations

Singapore: The MAS sets out the need for firms to take an end-to-end service-centric view in ensuring the continuous delivery of critical business services to their customers.

See: Guidelines on business continuity management.

South Africa: The Prudential Authority's and the Financial Sector Conduct Authority's requirements for IT resilience and business continuity include establishing specific service-level objectives including recovery time objectives and service recovery time objectives for critical services and business processes.

See: Joint standard on IT governance and risk.

Switzerland: As part of insurers' self-regulation, the Swiss Insurance Association has issued Minimum standards and recommendations on business continuity management, which have been approved by FINMA. These standards and recommendations include guidance on performing business impact analyses, having a business continuity strategy, defining business continuity measures, performing regular tests and having defined governance structures.

See: Minimum standards and recommendations on business continuity management.

Objective 2.8: The insurer effectively manages relationships with third-party service providers, including intragroup and nth-party relationships (ICPs 7 and 8).

In support of this objective, it is important for the insurer to consider how its approach to operational resilience:

- Ensures effective management and oversight of third-party risks, including intragroup and nth-party, service providers that are critical to its business; and
- Supports effective management of the potential impact of disruption throughout the lifecycle of its relationships with third-party, including intragroup and nth-party, service providers. This lifecycle includes planning, due diligence and selection, contracting, ongoing monitoring and termination.

Practices on effective management and oversight of third-party risks, including intragroup and nth-party, service providers and practices related to managing of the potential impact of disruptions.

56. Supervisory practices on outsourcing are relatively advanced and jurisdictions have matured their approaches in recent years. Third-party risk management is an evolutional advancement of practices on outsourcing and looks at management of relationships with third-party service providers more holistically. Insurers can establish the appropriate oversight of their third-party providers usually through contractual means. This includes insurers having ensured sufficient audit, access and information rights relating to the relevant services provided by their third-party providers.

57. Supervisors can also set expectations mandating third-party service providers to extend similar audit and access rights to authorities. This may be ensured in contracts between financial institutions and their service providers or, in certain jurisdictions, through direct requirements or expectations on financial sector critical service providers.

58. Regardless of the type of third-party service relationship, the jurisdiction can expect the final accountability towards the supervisory authorities and customers remains with the financial entity and its Board and Senior Management.

59. Expectations for third-party risk management could include expectations related to the management of a third-party service relationship, including planning, due diligence and selection of a service provider, contracting, ongoing monitoring and/or oversight and termination.

60. Supervisors can set expectations about what contracts for critical services should include, where appropriate. Supervisors may also obtain assurance about the resilience of service providers and the services they provide to insurers through:

- Regular supervisory engagement with insurers, including ad-hoc information requests, individual and thematic reviews of insurers and reviews of the information that insurers receive from service providers, including audits, certifications or collaborative assurance exercises, such as pooled audits.

- Supervisory dialogue with service providers through informal engagements. Such engagements can be helpful to better understand the design and underlying risks of relevant services.

61. Since insurers increasingly use services from a limited number of large third-party service providers, there is potential for increased concentration risk. To have a better understanding of, and to mitigate for, this potentially systemic risk, jurisdictions may consider granting supervisory authorities powers to directly oversee the provision of services to financial institutions by critical third-party providers.

62. Intragroup outsourcing and service provision can be subject to the same requirements and expectations as relationships with third-party providers outside an insurer's group. Insurers can have varying control and influence related to intragroup arrangements and supervisors can expect insurers to take a proportionate approach to how they manage risks arising from the use of such arrangements, including adjusting its vendor due diligence, relying on the group's potentially stronger negotiating and purchasing power, or adapting certain clauses in outsourcing agreements.

63. Supervisors can set contractual expectations ensuring that all responsibilities and obligations of third-party service providers, including intragroup and nth-party service providers, are cascaded. They can include requirements for insures to require third-party service providers to disclose significant relationships relevant to services provided to insurers.

Box 15: Outsourcing and third-party risk management

European Union: DORA introduces specific requirements for financial entities in relation to third-party risk management. Those requirements include: (i) contractual requirements (Art. 30 of DORA); (ii) requirement to define a policy to manage ICT third-party risk, whose specifications are set out in a dedicated RTS; (iii) requirements relating to the management of ICT subcontracting set out in a dedicated RTS; and (iv) requirements to keep a register of information on ICT third-party arrangements that is to be reported on an annual basis to the relevant competent authority. Furthermore, DORA introduces a pan-European oversight framework to manage the risks that critical ICT third-party service providers pose to the financial sector.

See: DORA Chapter V, Section II.

FSB toolkit on outsourcing and third-party relationships

In response to concerns over the risks related to outsourcing and third-party service relationships, the FSB has developed a toolkit for financial authorities and financial institutions for enhancing their third-party risk management and oversight. This is a flexible and risk-based set of tools that supervisory authorities and financial institutions may consider based on their circumstances, including the legal framework and specific features of the financial services sector in their jurisdictions. At the same time, the toolkit seeks to promote comparable and interoperable approaches across jurisdictions.

The FSB toolkit comprises of:

- A list of common terms and definitions to improve clarity and consistency regarding third-party risk management across financial institutions, enhancing communication among relevant stakeholders;
- Tools to help financial institutions identify critical third-party services and manage potential risks throughout the lifecycle of a third-party service relationship; and

- Tools for supervising how financial institutions manage third-party risks and for identifying, monitoring and managing systemic third-party dependencies and potential systemic risks.

See: FSB toolkit.

New Zealand: The RBNZ's guidance outlines how an entity should plan, screen, review and use contracts to manage its relationship with third-party service providers, while also undertaking ongoing cyber risk management to ensure cyber risks arising from third parties are under control.

See: Guidance on cyber resilience.

5 Objective 3: Objectives for insurance supervisors

Objective 3.1: In evaluating the insurer's operational resilience, supervisors coordinate within the supervisory authority to capture all potential areas of vulnerability (ICPs 2 and 24).

In support of this objective, it is important for the supervisor to consider how it ensures that departments within the authority communicate frequently to avoid a siloed approach and remain aware of risks across the insurer, including people, processes, technology and financial risks.

Internal supervisory coordination practices to avoid a siloed approach and remain aware of risks across the insurance market.

64. Supervisors can rely on existing internal methodology, processes, systems and/or internal communication channels to communicate internally regarding operational resilience issues to be addressed as part of supervision of insurers matters. They may use a mix of standard communication tools, such as: (i) emails; (ii) collaboration platforms; (iii) shared document systems/internal document repository, eg SharePoint; (iv) meetings (virtual or physical, including initial coordination meetings, regular meetings between supervision and specialists and executive committee meetings); and (v) direct communication (including calls) between departments/relevant colleagues on the topic. Regular meetings, shared document systems and formal frameworks for information sharing are commonly used to facilitate communication. As discussed in Objective 3.3, supervisors may also involve external stakeholders, such as other supervisors and industry associations, to enhance coordination and ensure a holistic approach to managing operational resilience and these communications can be instructive for internal communications as well.

65. Supervisors can have centralised decision-making bodies that govern the work involving all relevant departments. Formal frameworks can be implemented for information sharing and crisis management for operational resilience. Such frameworks define a clear responsibility structure, assignation and delegation of function/roles and a monitoring and reporting process, which includes upward reporting, downward communication, cross-department information exchange, escalation and coordination, to promote relevant information that can be effectively summarised, transmitted and analysed. Supervisors can assess their internal organisation and review their supervisory frameworks to promote collaboration and adopt hybrid working environments to enhance virtual communication.

Box 16: Coordination within the supervisory authority

Brazil: The SUSEP implemented an Integrated Supervision Committee that brings together representatives from various departments, including prudential and conduct supervision. This committee promotes collaborative oversight, approves ratings assigned through its Risk and Internal Controls Analysis System and ensures consistent supervision across departments.

Malaysia: The Central Bank of Malaysia has established a comprehensive internal framework that clearly defines monitoring and escalation protocols for industry-wide crises. It has a centralised reporting system for operational incidents, with dedicated cross-departmental teams to assess potential crisis evolution and formalised roles and responsibilities during industry-wide crises and it shares aggregated operational risk trends with insurers annually.

Portugal: There is an integrated supervisory model (Modelo Integrado de Supervisão) with a governance structure that clearly defines roles and responsibilities. There is also a multidisciplinary team (Specialised Group on Digital Operational Resilience) composed of members from prudential and market conduct supervision, IT, regulation and systemic risks analysis to specifically handle operational resilience matters related to ICT.

Objective 3.2: Supervisors share information and cooperate with other supervisors with a view to minimising risks (ICPs 3 and 25).

In support of this objective, it is important for the supervisor to consider how it:

- Defines its strategy for sharing relevant information and cooperating with other supervisors;
- Ensures the strategy takes into account and aims to minimise legal impediments and other barriers to cooperation between supervisors within and across jurisdictions and across sectors;
- Uses available information to identify and mitigate potential risks to the operational resilience of the sector, such as risks arising from concentration of use of third- and nth-party service providers; and
- Supports formalising sharing arrangements, including, for example, becoming signatory to the IAIS Multilateral Memorandum of Understanding (MMoU).

Practices on effective supervisory cooperation and information exchange.

66. Supervisors can define their approach for sharing information on operational resilience and risks with other supervisors through legal agreements, memoranda of understanding and participation in international and regional forums. Information sharing can include bilateral and multilateral exchanges, coordinated responses to incidents and regular updates on emerging risks.
67. To identify and mitigate risks to the operational resilience of the insurance sector, supervisors may require insurers to consider these risks in their management of third-party and nth-party service provider risks through comprehensive frameworks, which might include risk assessments, due diligence processes, contractual agreements and ongoing oversight of outsourced functions, especially for critical operations. Supervisors may require insurers to share information on third parties to help assess potential concentration risks. Supervisors can monitor concentration risk through reporting requirements or inventories of outsourcing arrangements.

Box 17: Supervisory cooperation

European Union: In order to facilitate an effective financial sector response to a cyber incident that poses a risk to financial stability, the three European supervisory authorities (the European Banking Authority, the EIOPA and the European Securities and Markets Authority) have established a systemic cyber incident coordination framework in the context of DORA. This work has included strengthening coordination amongst financial authorities and other relevant bodies in the European Union, as well as with key actors at an international level.

See: EU Systemic Cyber Incident Coordination Framework (EU-SCICF).

International:

Supervisory colleges play a pivotal role in enhancing the effectiveness of cross-border financial supervision. These forums bring together regulators from various jurisdictions to collaboratively oversee insurers with international footprints or complex group structures. Through structured dialogue and coordinated risk assessments, supervisory colleges foster transparency, consistency in regulatory practices and timely information sharing. This collaborative approach not only strengthens the resilience of the financial system but also ensures that supervisory strategies are aligned across borders, enabling more robust oversight and proactive risk mitigation. Supervisory colleges usually have a focus on areas that include the discussion on operational resilience matters, where supervisors collectively evaluate an insurers' ability to withstand and recover from disruptions.

Built upon ICP 3, the IAIS MMoU benefits supervisors by establishing a formal basis for cooperation and information exchange between signatory authorities regarding the supervision of insurers where cross-border aspects arise. The MMoU ensures secure, standardised sharing of confidential information, fostering transparency and trust among supervisors. Supervisory authorities must adhere to strict requirements for confidentiality and legal authority. The MMoU strengthens international supervisory cooperation, ensuring effective oversight of insurance markets and protecting policyholders while promoting the stability of the global insurance sector.

See: Details on the MMoU.

USA: The NAIC and its Financial Analysis (E) Working Group facilitate information sharing between state regulators to identify and respond to financial risks in insurers operating in multiple states. This framework enables US state insurance regulators to share information, collaborate on examinations and coordinate responses to risks affecting the insurance industry. The NAIC's Cybersecurity (H) Working Group helps regulators share cyber risk intelligence, coordinate responses to cyber incidents and develop best practices for cyber resilience. Additionally, the NAIC maintains the NAIC's financial data repository and related iSite+ tools, which provides a centralised platform where regulators can share insurer financial reports, analytical tools, examination findings and risks assessments. These systems are used by all 50 states, Washington DC and US territories to enhance regulatory oversight. The NAIC collaborates with the IAIS to align US practices with global standards, ensuring cross-border risk management.

See: Financial Condition (E) Committee; Innovation, Cybersecurity, and Technology (H) Committee.

68. Supervisors can use formal engagement mechanisms such as industry meetings, workshops, public consultations and roundtable discussions to gather feedback and share information. Supervisors can establish specialised frameworks for cyber crisis management and information sharing, or collaborate with industry associations, professional bodies and other supervisory

authorities. These engagements can contribute to developing more robust supervisory frameworks and building industry awareness.

Objective 3.3: Supervisors cooperate and communicate transparently with stakeholders (ICPs 2, 9 and 10).

In support of this objective, it is important for the supervisor to consider how it:

- Engages with relevant stakeholders, such as industry, third- and nth-party service providers, government, non-governmental organisations and policyholders regarding insurers' operational resilience approaches, taking into account confidentiality; and
- Integrates expectations for insurance sector operational resilience into its review and reporting frameworks and ensures timely and frequent engagement with insurers to help address problem areas.

Practices to improve communication and transparency with relevant stakeholders, such as industry, third- and nth-party service providers, government, non-governmental organisations and policyholders.

69. A number of steps can be considered by supervisors to improve communication and transparency:

- Review approach to regular risk assessments and reporting to ensure operational resilience is considered. Structured frameworks and scorecards can be used to assess operational resilience and determine overall risk ratings.
- Conduct supervisory assessments and industry-wide engagements.
- Assessments of risks to the insurance sector, including operational resilience risks, can be published in financial stability reports.
- Regular meetings, workshops, fora and conferences with insurers and with key industry groups, seminars, roundtables and other events can assist with engagement.

Box 18: Stakeholder engagement

France: L'Autorité de contrôle prudentiel et de résolution maintains a comprehensive engagement framework, including the Paris Resilience Group, which brings together public authorities and major financial institutions. For nearly 20 years, this group has coordinated responses to major disruptions through both formal incident response mechanisms and informal information sharing. In addition, a specific cyber-crisis protocol for less significant banking institutions and insurers, which includes structured reporting of ICT-related incidents and activation procedures for systemic events, was created in 2023.

See: Report on the Paris Resilience Group.

Zimbabwe: The Insurance and Pensions Commission engages with stakeholders through a well-structured approach that combines formal mechanisms (stakeholder consultations, policy updates and training workshops) with informal engagements (industry fora, one-on-one meetings and networking events). This multi-layered strategy allows the authority to gather diverse perspectives,

provide tailored guidance and build relationships based on open communication while systematically educating stakeholders on operational resilience principles and regulatory expectations.

70. Operational resilience may be included as part of the insurer's Own Risk and Solvency Assessment (ORSA) where major risks to capital adequacy are identified, assessed and considered as part of the current general risk management framework. Supervisors may also include a comprehensive review of the mitigation of any risks, including those related to cyber security, as part of each financial exam.

Box 19: Review and reporting

Canada: OSFI has a comprehensive approach to operational resilience integration within its supervisory framework. Its structured scorecard methodology incorporates operational resilience as one of four key categories determining an institution's overall risk rating, with the notable feature that the weakest category becomes the starting point for the overall rating, ensuring operational resilience concerns cannot be outweighed by strong performance in other areas and triggering heightened supervisory intervention when necessary.

Switzerland: There are multiple oversight mechanisms: requiring insurers to assess operational resilience risks within their ORSA and report impacts on capital adequacy; mandating submission of outsourcing arrangement inventories; and conducting both regular and ad hoc surveys on operational resilience elements, including internal controls and operational risk losses, providing a multi-faceted view of insurers' operational resilience posture.

Objective 3.4: Supervisors support a culture of continuous learning and improvement with respect to operational resilience within the supervisory authority (ICP 2).

In support of this objective, it is important for the supervisor to consider how it:

- Invests in training and recruitment of Senior Management and staff, as needed, to maintain sufficient technical expertise in the areas of operational risk and information systems and to reinforce roles and responsibilities; and
- Incorporates generative thinking/technologies into their supervisory processes to keep pace with trends in the industry.

Practices to ensure investing in training and recruitment of Senior Management and staff, to maintain sufficient technical expertise in the areas of operational risk and information systems and to reinforce roles and responsibilities.

71. Supervisors can carefully manage hiring and onboarding processes to hire and retain staff with sufficient technical expertise. Supervisors can leverage expertise through participation in workshops, training and conferences.

Box 20: Talent management considerations

China, Hong Kong: Supervisors approach technical talent management through structural and cultural elements. They actively review salary and ranking structures to remain competitive and also leverage technical staff to develop new supervisory information systems equipped with analytical tools and dashboards that improve data analysis capabilities.

Croatia: Supervisors maintain a structured development plan for the Information Security Office, which strategically addresses multiple dimensions of talent management by focusing on professional growth capacity of potential hires, implementing cyber security methodology, promoting work-life balance, providing professional education opportunities and regularly monitoring the labour market to ensure competitive compensation.

USA: Supervisors in the US insurance sector invest in training and recruitment to maintain sufficient technical expertise in areas like operational risk and information systems. The structured development plans focus on professional growth, cyber security methodology, work-life balance, and competitive compensation. US insurance supervisory authorities actively participate in national and international forums, workshops, conferences and training programmes to uplift its staff.

See NAIC training and professional development.

Practices to incorporate generative thinking/technologies into their supervisory processes to keep pace with trends in the industry.

72. Supervisors can consider using digital tools in their supervisory processes. They can use these tools in a variety of ways, from document analysis and predictive risk analytics, specialised analytical dashboards and translation and transcription, to exploratory proof of concepts. Supervisors can consider establishing formal AI usage policies for tools like Microsoft Copilot, encouraging supervisors to incorporate these technologies into daily supervisory activities. Many authorities not currently using AI or machine learning technologies are actively exploring potential applications.

6 Conclusion

73. The objectives and toolkit presented in this Application Paper provide guidance for enhancing operational resilience in the insurance sector. Underpinned by the ICPs, this paper supports supervisors in developing approaches that are consistent with global standards while remaining adaptable to local specificities. As operational resilience risks continue to evolve, particularly in areas like technology, cyber resilience and third-party dependencies, this paper provides a foundation that can accommodate new developments while maintaining focus on the fundamental goal of ensuring that insurers can withstand, adapt to and recover from operational disruptions.

Acronyms

AMF	Autorité des marchés financiers (Quebec Securities Commission)
BCP	Business Continuity Plan
BMA	Bermuda Monetary Authority
CERP	Cybersecurity Event Response Plan
DOIs	Departments of Insurance
DORA	Digital Operational Resilience Act
DRP	Disaster Recovery Plan
EIOPA	European Insurance and Occupational Pensions Authority
FCA	Financial Conduct Authority
FINMA	Financial Market Supervisory Authority
FIRE	Financial Stability Board Format for Incident Reporting Exchange
FSB	Financial Stability Board
GIMAR	Global Insurance Market Report
ICP	Insurance Core Principles
ICT	Information and Communications Technology
MAS	Monetary Authority of Singapore
MMoU	Multilateral Memorandum of Understanding
NAIC	National Association of Insurance Commissioners'
ORSA	Own Risk and Solvency Assessment
ORWG	Operational Resilience Working Group
PRA	Prudential Regulation Authority
QFRCA	Qatar Financial Centre Regulatory Authority
RBNZ	Reserve Bank of New Zealand
SUGESE	Superintendencia general de seguros (Costa Rican Superintendent General of Insurance)
SUSEP	Superintendência de seguros privados (Brazilian Superintendence of Private Insurance)

Annex

Survey responses were received from the following IAIS Members:

Belgium, National Bank of Belgium
Bermuda
Bosnia & Herzegovina
Brazil, SUSEP
Canada, AMF
Canada, OSFI
Chile
China, Hong Kong
China, Macao
Chinese Taipei
Costa Rica
Croatia
Egypt
EIOPA
France
Germany
Hungary
Ireland
Korea
Malaysia
Mexico
Moldova
New Zealand, RBNZ
Poland
Portugal
Qatar, QFCRA
Slovakia
Switzerland
United Kingdom, PRA
Uruguay
USA, NAIC
Zimbabwe