Draft Application Paper on Operational Resilience Objectives [and Toolkit]

8 August 2024

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.iaisweb.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 was prepared by the Operational Resilience Working Group in consultation with IAIS members.

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

Contents

1 Introduction

1.1 Background and purpose

1. As insurers' operations become more complex, interconnected and dependent on technology and technology-related providers, the likelihood and impact of operational disruptions, and the importance of operational resilience, has materially increased.
2. Operational resilience is a topic that has relevance across regions and jurisdictions, with many authorities and insurers facing the same or similar challenges, hence, this is an area that can benefit from the IAIS' global perspective and reach.
3. The IAIS' work in this area is ongoing. In 2016 and 2018 respectively, the IAIS published an Issues Paper and Application Paper examining fundamental aspects of cyber security for financial institutions, cyber breach case studies within the insurance sector and cyber risk frameworks in the context of existing useful practices and guideposts.
4. 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. Most recently, the IAIS published an Issues Paper (May 2023) identifying issues impacting on 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. The IAIS' focus on insurance sector operational resilience is further reinforced in its 2024 Roadmap and cyber resilience is identified as one of the IAIS' key strategic themes under its 2020-2024 Strategic Plan. The IAIS 2025-2029 Strategic Plan, which is currently under development, also features digital innovation and cyber risks as strategic themes.
5. 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.
6. Pursuant to this feedback, the **IAIS has developed Operational Resilience Objectives** for the insurance sector, with the aim of providing a sound and consistent foundation to support supervisory authorities in developing and strengthening their approaches to supervising insurers' operational resilience. These Objectives, as set out in Section 2, are outcomes-based, do not set out new requirements, and rather provide clarity on the application of existing supervisory materials.
7. Drawing from existing definitions of operational resilience, and 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. 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 impacting critical services. Operational resilience takes as a premise the assumption that disruptions will occur and thus that insurers should consider their tolerance for such disruptions and take this tolerance into account when devising their approach to operational resilience.
8. The draft Objectives represent the first phase of a two-part consultation. The second phase, to develop a draft Toolkit, will advance in the second half of 2024 and will set out supervisory practices relevant to the Objectives. Following consultation on the draft Toolkit, the two phases of this work will be integrated into a single Application Paper.

1.2 How ICPs support operational resilience

9. The Insurance Core Principles (ICPs) provide a global framework for the supervision of the insurance sector and are set out at a principles-based level, which provides a flexible basis for supervisors to identify and respond to new and emerging risks. The ICPs thus serve as a good starting point for guiding supervisory responses and supporting the sound management of operational resilience issues.
10. A key aspect of operational resilience is that operational disruptions can have both narrow and wide-spread 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 in isolation and when viewed holistically, 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

2 Objectives for insurance sector operational resilience

12. These Objectives have been developed in the context of the modern insurance sector being a complex, interconnected, cross border system in which insurers are continuing to embrace digital innovation, rely on third-party services to support their operations some of which are critical to the insurer's business viability, and are increasingly subject to operational risks that may be systemic in nature.[1]
13. Accordingly, the Objectives address: 1) the **relationship among operational resilience, governance, and operational risk management**; 2) **key elements of a sound approach to operational resilience** that encourage the effective and holistic management of insurers' people, processes and systems with a focus on technology and cyber risk, change management, business continuity planning (BCP)/disaster recovery planning (DRP) and the use of third- and nth-party[2] services; and 3) **Objectives for insurance supervisors**. The areas covered in the Objectives are not exhaustive.
14. While the **Objectives do not set out new supervisory requirements**, they do **provide an outcomes-based articulation of the application of existing ICPs**. The ICP relevant to each Objective is indicated. While Sections 2.1 and 2.2 are directed at insurers, supervisors would also benefit from considering these outcomes when setting out their supervisory initiatives.
15. Consistent with the overarching concepts underpinning the ICPs, the **proportionality principle is applicable**. Proportionality allows the supervisor to increase or decrease the intensity of supervision according to their assessment of the risks inherent to insurers, and the risks posed by insurers to policyholders, the insurance sector or the financial system as a whole.[3]

2.1 Relationship amongst operational resilience, governance, and operational risk management

2.1.1 The insurer implements and oversees an effective approach to operational resilience that is supported by its governance framework (ICP 7)

16. In support of this objective, it is important for the insurer to consider how the Board:
    - Is accountable for overseeing 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;
    - Ensures that it has sufficient knowledge, skills, experience, and understanding of operational resilience matters to fulfil its responsibilities;
    - Provides leadership by setting a 'tone from the top' that fosters a risk culture and supports the insurer's approach to operational resilience; and
    - Provides informed and engaged oversight of Senior Management's implementation of the insurer's approach to operational resilience.
17. It is additionally important for the insurer to consider how the Board and Senior Management:

[1] The potential systemic nature of operational risks and the value of information sharing in this respect is noted in the IAIS' May 2023 Issues Paper on Insurance Sector Operational Resilience.

[2] Consistent with the FSB Toolkit for Enhancing Third-Party Risk Management and Oversight, nth-party service providers may be referred to as sub-contractors, sub-outsourced service providers or indirect service providers.

[3] ICP and ComFrame Online Tool - International Association of Insurance Supervisors (iaisweb.org)

- Effectively communicate the insurer's approach to operational resilience across the organisation and amongst key stakeholders, including regulatory authorities;
- 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.

2.1.2 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)

18. 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; and
    - Is embedded into its system of internal controls and incorporates appropriate roles and responsibilities in consideration of the three lines of defence (eg the division of responsibilities between the business, risk management and compliance and internal audit, as referred to at ICP 8.2.4 footnote 2).

2.2 Key elements of a sound approach to operational resilience

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

19. 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 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.

2.2.2 The insurer sets impact tolerances for disruption to its critical services (ICPs 8 and 16)

20. In support of this objective, it is important for the insurer to consider how its approach to operational resilience:
    - Quantifies 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 supply chains).

2.2.3 *The insurer self-assesses and tests its ability to withstand and recover from severe operational disruption scenarios, and ensures that action is taken to improve operational resilience on the basis of lessons learnt (ICPs 8 and 16)*

21. 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 but plausible 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.

2.2.4 *The insurer effectively manages operational incidents, including but not limited to cyber incidents, affecting critical services (ICP 8)*

22. 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 and respond to – and recover from – their occurrence to minimise disruptions to critical services;
    - Establishes clear processes for identifying, 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 are in place to report incidents to both internal and external stakeholders, including regulatory authorities, as appropriate.

2.2.5 *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)*

23. 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, inclusive of its technology architecture, technology asset management, patch management, service monitoring, and disaster recovery practices;
    - Ensures effective management and testing of access to technology, systems, premises, networks, key people and information assets to safeguard its critical services;
    - Reinforces the adoption and maintenance of good cyber hygiene practices (eg identity management, user authentication practices(such as multifactor authentication), access control, attack surface management etc);
    - Supports conducting regular technology and cybersecurity 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.

2.2.6 *The insurer plans, tests, and implements changes in a controlled manner (ICP 8)*

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

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

2.2.7 The insurer develops, implements, tests and updates its BCP and 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)

25. 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 the BCP's of critical third-party service providers.

2.2.8 The insurer effectively manages relationships with third-party service providers, including intra-group and nth-party relationships (ICPs 7 and 8)

26. 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 supply chain risks, including those stemming from the use of third-party, including intra-group 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 intra-group and nth- party, service providers. This lifecycle includes planning, due diligence and selection, contracting, ongoing monitoring and termination.

2.3 Objectives for insurance supervisors

27. The following Objectives support insurance supervisors in overseeing insurance sector operational resilience and responding to operational resilience related risks at both the individual insurer and macro levels. These are centred on supervisory communication, collaboration and cooperation, and are to be understood in combination with the Objectives for insurers above.

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

28. 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.

2.3.2 *Supervisors share information and cooperate with other supervisors with a view to minimising risks* (ICPs 3 and 25)

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

- Defines its approach for sharing information and cooperating with other supervisors, to take into account and minimise legal impediments or other barriers to cooperation, including with other domestic supervisors as well as supervisors in other jurisdictions and across sectors, and considering what information might be relevant to share on a case by case basis;
- 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).

2.3.3 *Supervisors cooperate and communicate transparently with stakeholders* (ICPs 2, 9 and 10)

30. 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; and
- Integrate 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.

2.3.4 *Supervisors support a culture of continuous learning and improvement with respect to operational resilience within the supervisory authority* (ICP 2)

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

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

3 Toolkit supporting Objectives for Insurance Sector Operational Resilience (placeholder)

32. As noted in the introductory section, the draft Objectives represent the first phase of a two-part consultation. The second phase involves developing a draft Toolkit in support of the draft Objectives. The development of the draft Toolkit will advance in the second half of 2024 and will set out supervisory practices relevant to the Objectives. The IAIS aims to consult on the draft Toolkit in first half 2025, following which the two phases of this work will be integrated into a single application paper.