IAIS

Application Paper on operational resilience objectives and toolkit

Virtual, 19 February 2026

Purpose of this public background session

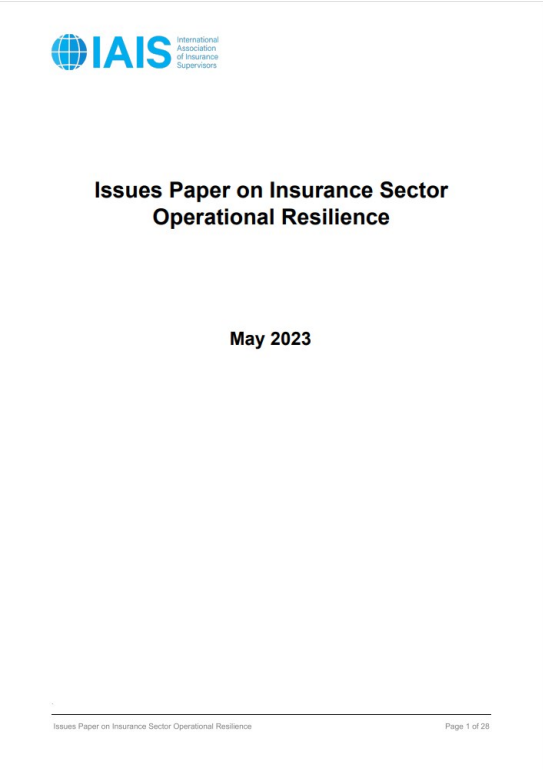
Purpose

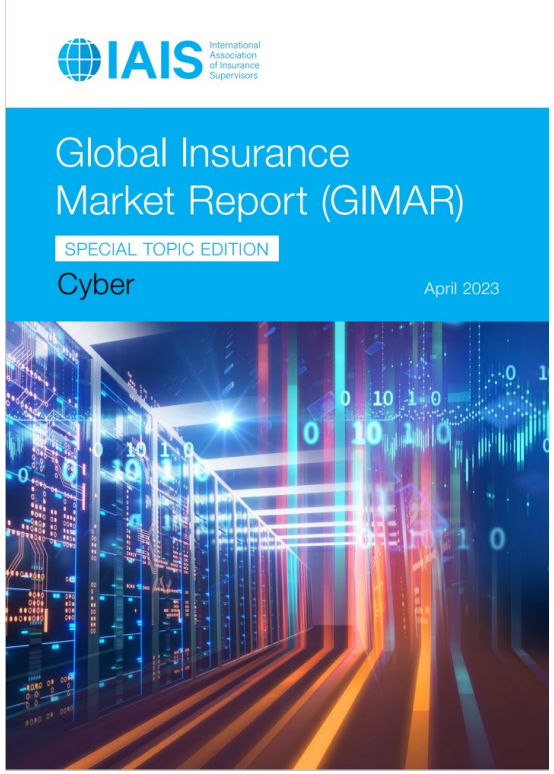
1. Background
2. Application Paper
3. Outcome of the consultation
4. Q&A

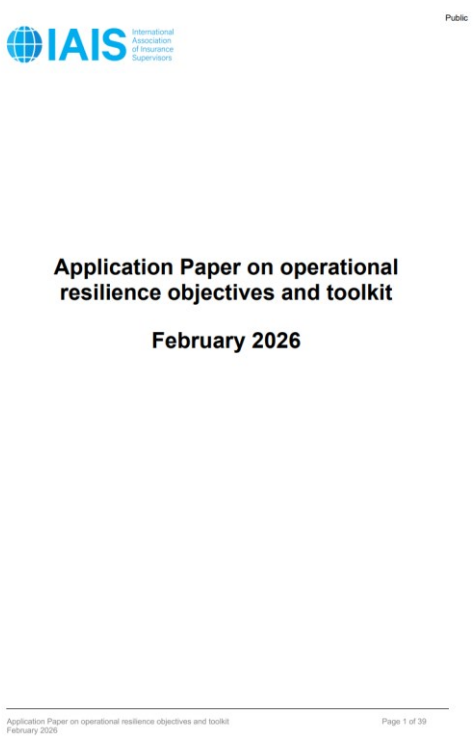
Operational resilience

"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 all definitions of operational resilience take as a premise the assumption that **operational 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."

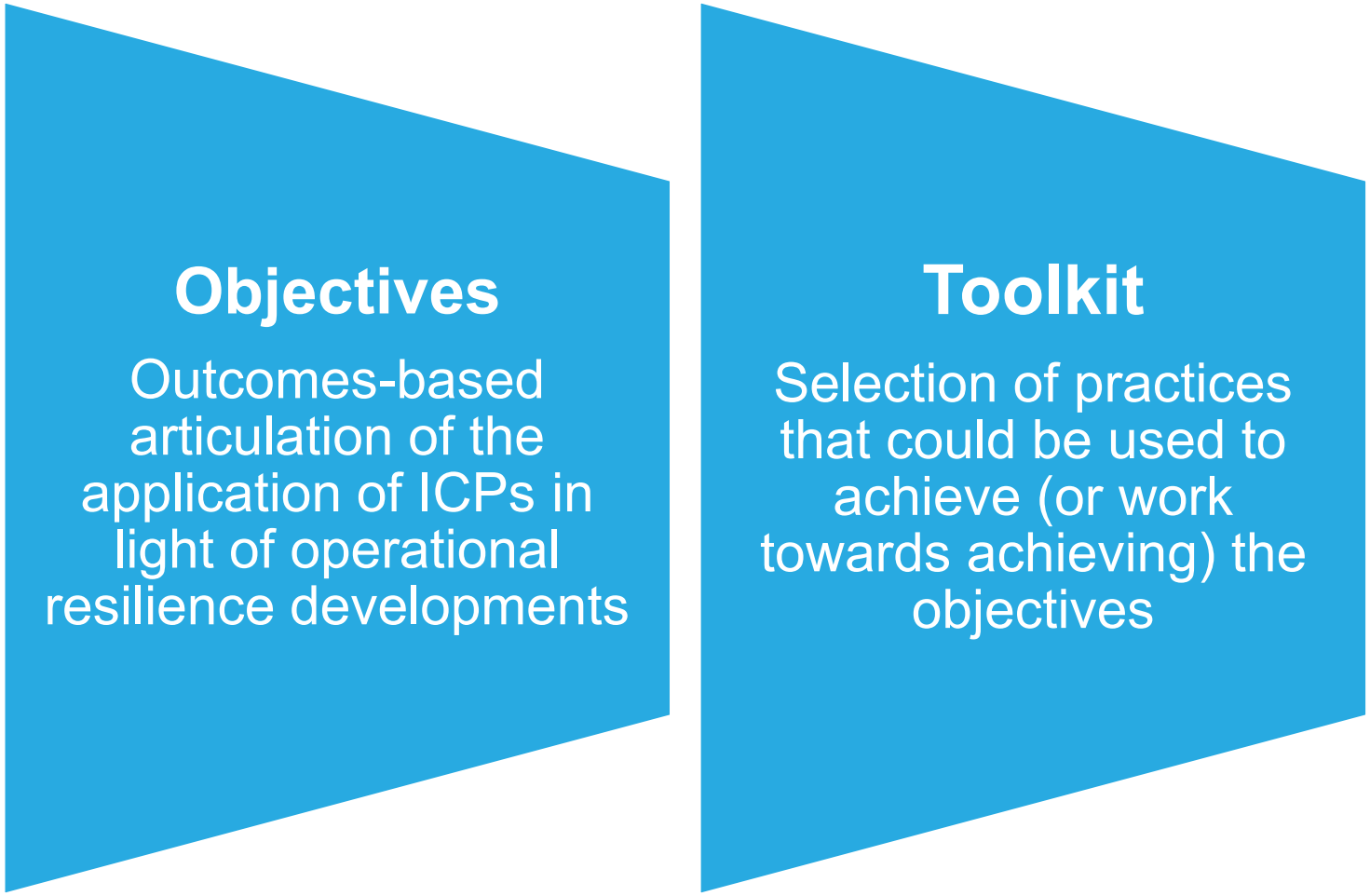
Evolving operational resilience work







Application Paper structure: objectives and toolkit



Two components work in tandem:

- Objectives: provide the basis for a high-level framework for meeting the ICPs;
- Toolkit: provides supervisors with practical implementation approaches that 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.

Application Paper

Objectives

Practices

Examples

- *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

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

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

leadership by setting a tone from the top that fosters a risk culture and supports the approach to operational resilience;

informed and engaged oversight of Senior Management's implementation of the approach to operational resilience;

the insurer's approach to addressing and mitigating the impact of operational s, including how the approach is integrated into the insurer's governance framework orates measures that manage the impact of identified risks to within tolerance limits;

hat it has sufficient knowledge, skills, experience and understanding of operational matters to fulfil its responsibilities.

ditionally important for the insurer to consider how the Board and Senior Management:

ures effective systems and processes are in place that support the insurer's approach to ional 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 robu ernance framework that specifically addresses digital, information and communications hnology (ICT) and cyber resilience risks. This could be in addition to requirements on how e governance framework of the insurer more broadly supports its approach to operational res ence.

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 opera

Bermuda: The Bermuda Monetary Authority (BMA) published an op outsourcing code and guidance in September 2025. The framework reinfo roles the Board and Senior Management play in maintaining and st resilience, overseeing outsourcing arrangements and ensuring com expectations. It details the respective roles as follows:

- The Board is responsible for strategic oversight, approval and acco resilience and outsourcing policies, ensuring alignment with regul appetite and the insurer's strategic objectives; and
- Senior Management is responsible for implementing, and managing outsourcing arrangements, including the development and execution controls and ongoing monitoring and evaluation.

See: Operational resilience and outsourcing code.

Canada, Quebec: The Autorité des marchés financiers (AMF) sets out ations on sound governance structure to foster compliance with operational risk m gement 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;

Toolkit

Inputs from IAIS members through a survey, points towards:

Objective 1: **Convergence in supervisory practices** adopted for governance and management of operational resilience. Operational resilience has been embedded into existing governance and risk management frameworks for some time.

Objective 2: **Wide variety of practices** adopted by supervisors for the key elements of operational resilience regimes.

Objective 1

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

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

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).

Objective 2

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

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

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

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).

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

Objective 2

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

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).

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

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).

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

Objective 3

Objective 3: Objectives for insurance supervisors

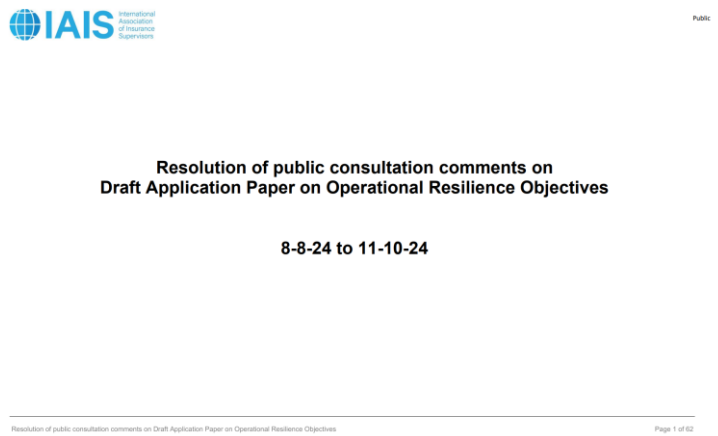
3.1: In evaluating the insurer's operational resilience, **supervisors coordinate** within the supervisory authority to capture all potential areas of vulnerability (ICPs 2 and 24).

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

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

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

Consultation: objectives and toolkit



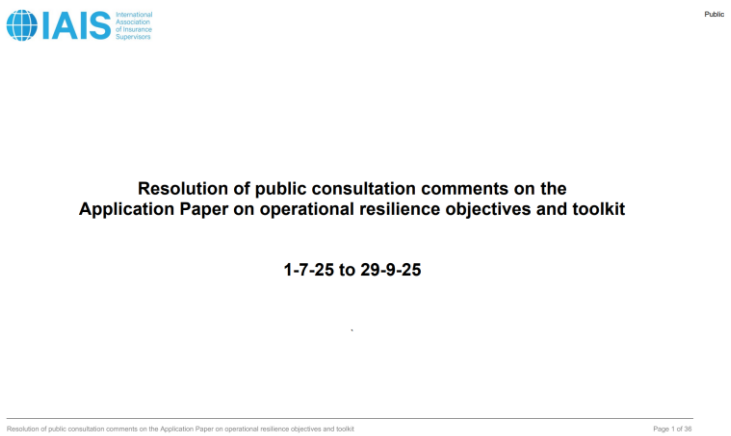
IAIS International Association of Insurance Supervisors

Public

Resolution of public consultation comments on
Draft Application Paper on Operational Resilience Objectives

8-8-24 to 11-10-24

Resolution of public consultation comments on Draft Application Paper on Operational Resilience Objectives Page 1 of 62



IAIS International Association of Insurance Supervisors

Public

Resolution of public consultation comments on the
Application Paper on operational resilience objectives and toolkit

1-7-25 to 29-9-25

Resolution of public consultation comments on the Application Paper on operational resilience objectives and toolkit Page 1 of 36

- Consulted on objectives in **August 2024**.
- Updated objectives based on consultation feedback:
  - Member survey of practices conducted
  - Practices developed into toolkit
- Last consultation closed in **September 2025**

2024 responses	*2025 responses*	*Category*
2	2	**Insurers**
7	6	**Trade associations**
6	1	**Members**
3	0	**Others**

- Final Application Paper, reflecting the consultation comments, published on **12 February 2026**

Consultation: summary of material changes

Comment	IAIS Response
Contextualise operational resilience as part of a broader ecosystem.	Paras 1 and 9 were updated to make clear that operational resilience encompasses severe governance and risk management practices.
Proportionality and capacity-building considerations.	The proportionality principle was reiterated. Capacity-building initiatives will be supported through Member webinars.
Board responsibilities.	Adjustments were made to ensure proportionality and flexibility, with communication strategies moved to senior management responsibilities (paras 19/20).
Objective 2.2, 2.8	Edits made to change reference to “supply chain” to “third-party providers”.
Objective 2.4	Edits made to the toolkit under Objective 2.4 to make clear the need to balance responding to an incident and reporting to supervisors.
Box 17	Additional text added on the role of supervisory colleges.
Toolkit examples	Various updates made to toolkit examples.

ORWG: 2026 Workplan

Third-party risk

IAIS will develop a Member-only report focused on third-party risk, considering emerging trends and practices by third parties. The focus in 2026 will be to: define different scenarios of third-party involvement in the insurance sector; conduct a short survey on third parties, among Members and stakeholders; share experience on development of critical function regimes and emerging trends on third-party services; consider experience from other sectors (including via FSB/BCBS/ISOCO) of manging n-th party risk; and discuss conclusions from the survey and develop a Member-only report.

Application Paper on operational resilience objectives and toolkit

Questions