Public

IAIS

Public background session on the Application Papers on artificial intelligence and operational resilience

13:00 – 14:30 (CEST), 17 July 2025, Virtual

Purpose of this public background session

Purpose

1. Introduction
2. Application Paper on the supervision of artificial intelligence and Q&A
3. Draft Application Paper on operational resilience objectives and toolkit and Q&A

Application Paper on the supervision of artificial intelligence

IAIS

Forum workstreams

Artificial Intelligence

No changes needed to the Insurance Core Principles. Focused on developing supporting material.

- Application Paper
- Develop Member-only material to support AI supervision
- Analysing data as part of the Global Monitoring Exercise

SupTech

Sharing emerging practices on SupTech with a focus on understanding effective digitalisation strategies

- Forum survey and wider membership survey planned
- Develop Member-only material to effectively share practical SupTech use cases

FinTech monitoring

Horizon-scanning to monitor and understand emerging FinTech trends

- Tracking member work on FinTech developments
- Understanding what structural impact these changes could have on the global insurance sector
- Conducting crypto-assets survey to grasp its landscape in the insurance sector

ICPs and Application Papers

- The Insurance Core Principles (ICPs) form the **globally accepted framework for insurance supervision.** The ICPs seeks to encourage the maintenance of consistently high supervisory standards in IAIS member jurisdictions.
- **Application Papers** provide supporting material related to supervisory material. Supporting material aids IAIS members to put the ICPs into practice.
- 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.
- Supervisory implementation / application of materials in all Application Papers are subject to the **proportionality principle**.

Structure of the Application Paper

Risk-based supervision and proportionality

Governance and accountability

- Risk management system
- Corporate culture
- Human oversight and allocation of management responsibilities
- Use of third-party AI systems and data
- Traceability and record keeping

Robustness, safety and security

- AI system robustness
- AI system safety and security

Transparency and explainability

- Explaining AI system outcomes
- Explanations adapted to the recipient stakeholders

Fairness, ethics and redress

- Data management in the context of fairness
- Inferred causal relationships in an AI system
- Monitoring outcomes of AI systems
- Adequate redress mechanisms for claims and complaints
- Societal impacts of granular pricing

Consultation comments

Tone

Issue raised: The paper focuses excessively on the risks of AI systems and creates overly burdensome requirements.

Response: The paper:

- Now also highlights AI opportunities, including a dedicated box in the introduction.
- Acknowledges both opportunities and challenges for financial inclusion enabled by granular risk-based pricing practices.
- Further emphasises risk-based and proportionality considerations.

Definition of AI systems

Issue raised: The OECD definition of AI systems is too broad. Suggested a narrower, insurance-specific definition.

Response: Retained the definition but made edits to:

- Highlight the focus on AI systems with autonomous and adaptability features, excluding traditional mathematical models.
- Emphasise a proportionate and risk-based approach, scoping out low-risk activities.

Proportionate and risk-based approach

Issue raised: The paper is burdensome and introduces new requirements, raising compliance costs.

Response: Clarified that:

- The paper does not introduce new requirements.
- Focus is on integrating guidance into existing risk and governance frameworks.
- Emphasises a risk-based approach to supervision with a new section 2.

Consultation comments

Third-party oversight

Issue raised: Insurers are expected to have control or oversight over third parties.

Response:

- Clarified that insurers must assess whether acquiring or using third-party AI systems constitutes the outsourcing of critical services and require that such arrangements meet the oversight expectations outlined in ICP 8.8.
- Consistent with existing requirements, insurers should obtain adequate information and reassurances from third-party providers, respecting intellectual property rights eg by including relevant clauses in contracts with third parties.

Societal impacts of granular risk pricing

Issue raised: More granular risk pricing enabled by AI may negatively impact protection gaps

Response: The paper

- Highlights potential negative impacts on financial inclusion for high-risk customers, especially vulnerable consumers.
- Acknowledges that some customer groups may benefit from greater access to affordable insurance due to granular risk assessments enabled by AI systems.

Additional changes

Issue raised: Requests for additional information to be added to the paper.

Response:

- Made a limited number of additions.
- Not all requested details were included, given the importance of maintaining a concise and accessible document and the need to stay within the typical level of detail expected in an Application Paper.

IAIS

Questions?

Public

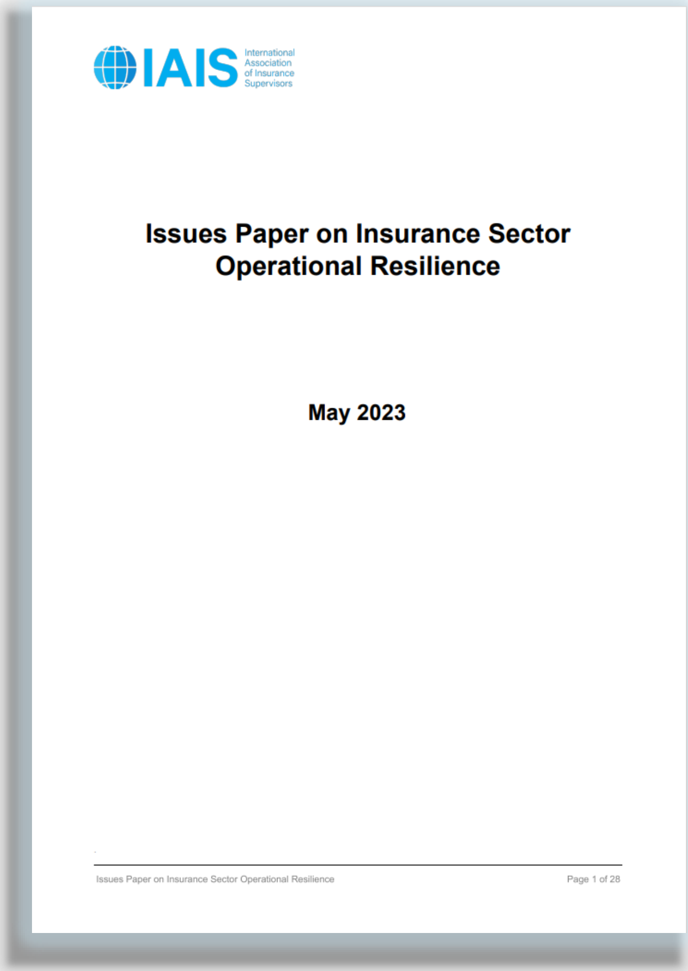
Draft Application Paper on operational resilience objectives and toolkit

IAIS

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. 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

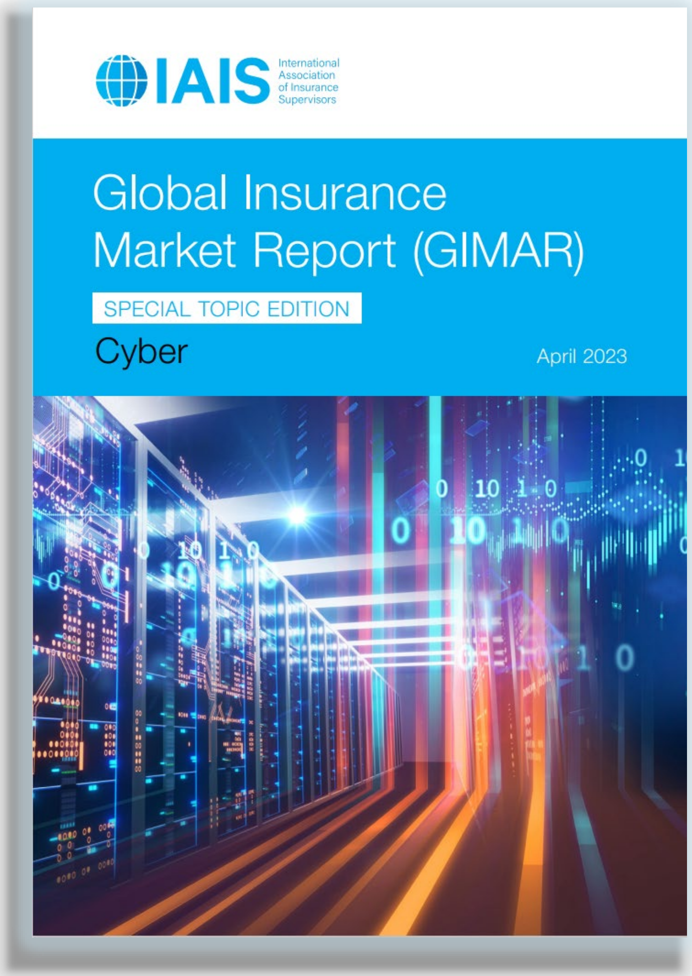


IAIS International Association of Insurance Supervisors

Issues Paper on Insurance Sector Operational Resilience

May 2023

Issues Paper on Insurance Sector Operational Resilience Page 1 of 28



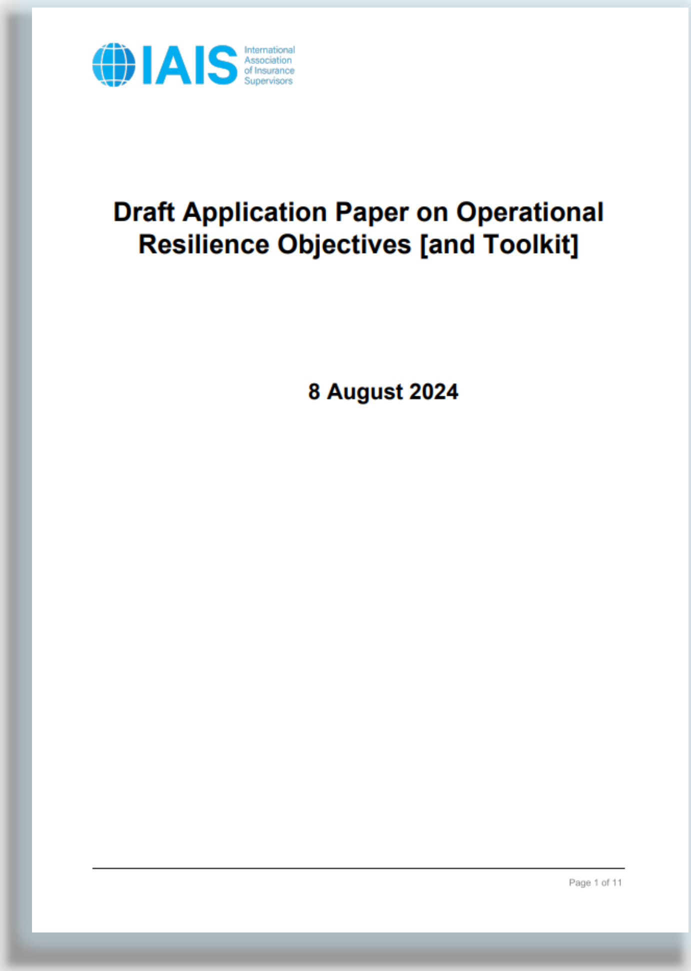
IAIS International Association of Insurance Supervisors

Global Insurance Market Report (GIMAR)

SPECIAL TOPIC EDITION

Cyber

April 2023



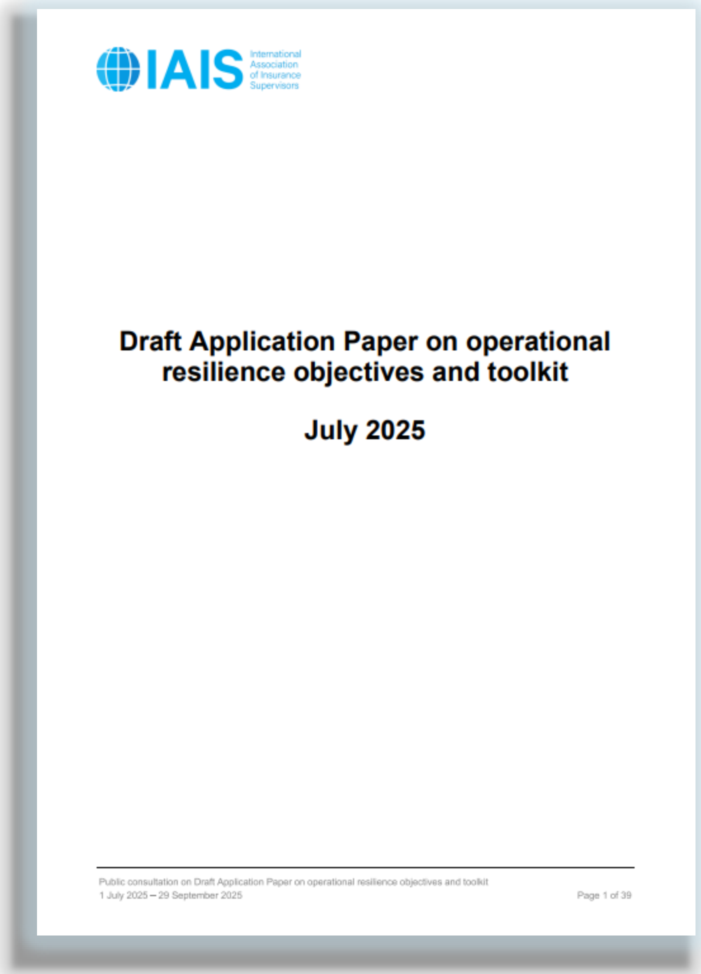
IAIS International Association of Insurance Supervisors

Draft Application Paper on Operational Resilience Objectives [and Toolkit]

8 August 2024

Page 1 of 11

Consultation: objectives and toolkit



International Association of Insurance Supervisors

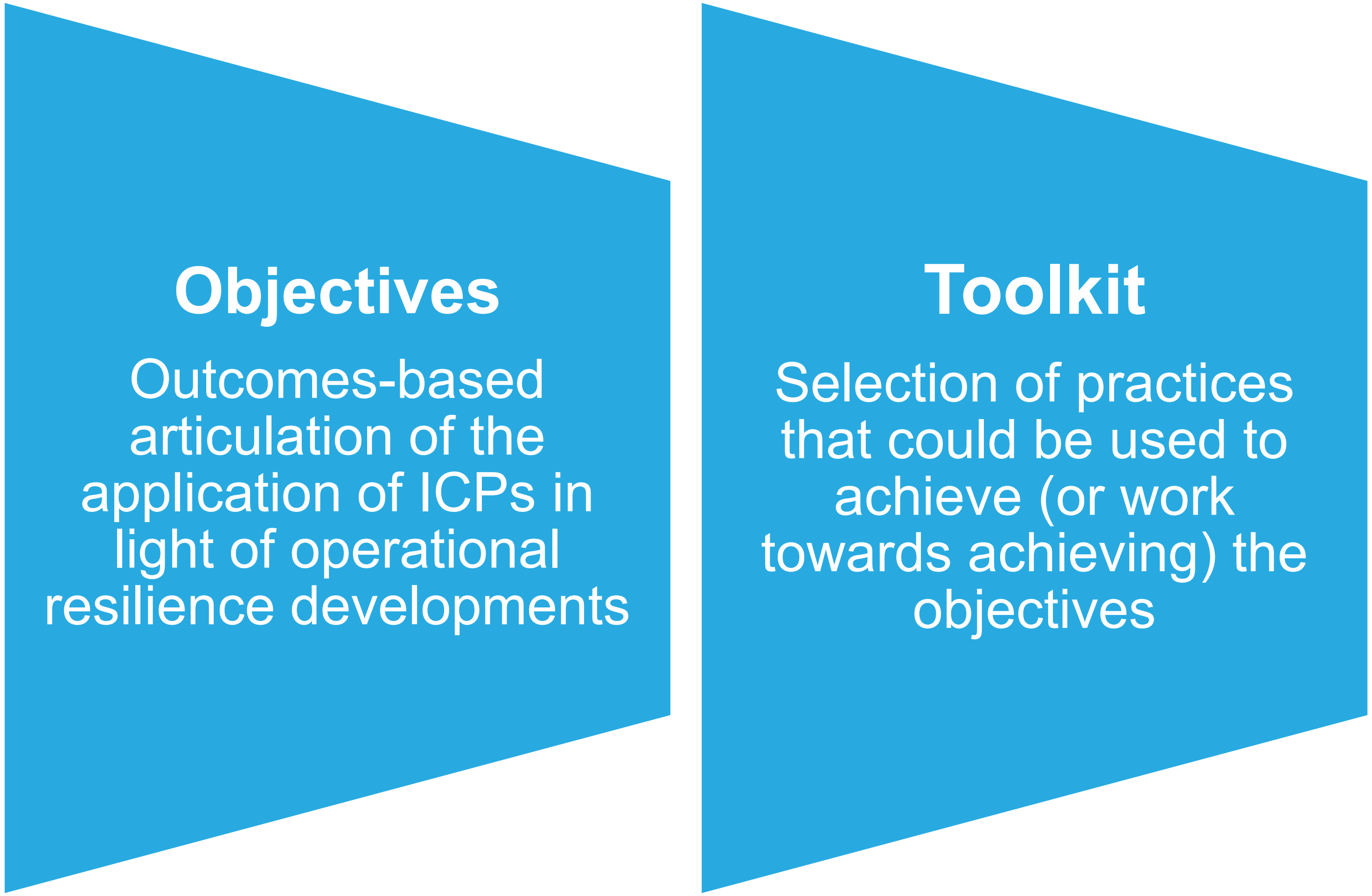
Draft Application Paper on operational resilience objectives and toolkit

July 2025

Public consultation on Draft Application Paper on operational resilience objectives and toolkit
1 July 2025 – 29 September 2025 Page 1 of 39

- Consulted on objectives in August 2024.
- Updated objectives based on consultation feedback:
  - Member survey of practices conducted
  - Practices developed into toolkit
- Current consultation runs until 29 September
- Final Application Paper subject to post-consultation edits to be published in Q1 2026

Application Paper structure: objectives and toolkit



Objectives

Outcomes-based articulation of the application of ICPs in light of operational resilience developments

Toolkit

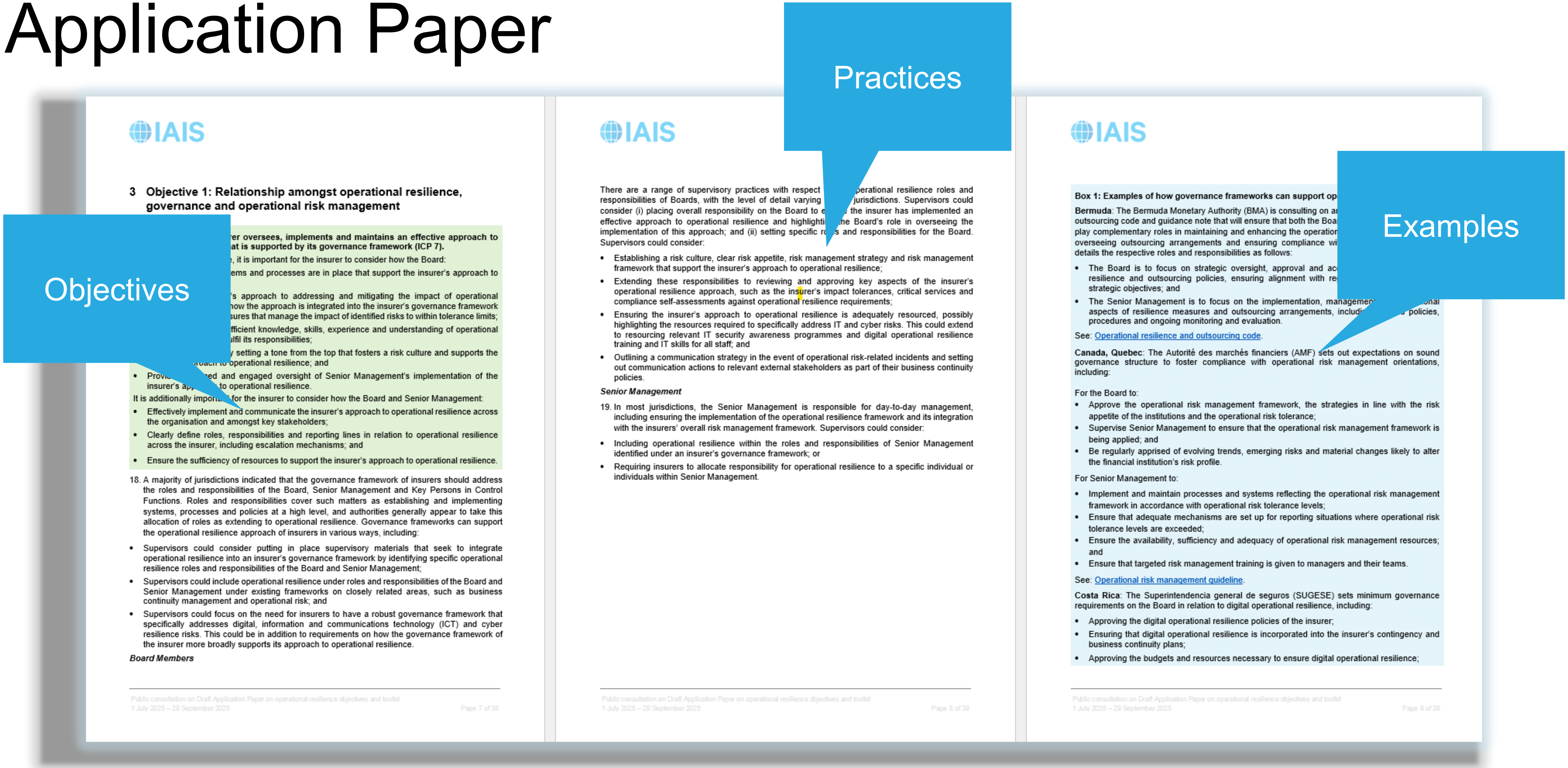
Selection of practices that could be used to achieve (or work towards achieving) the objectives

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

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

er oversees, implements and maintains an effective approach to
at is supported by its governance framework (ICP 7).

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

ems and processes are in place that support the insurer's approach to

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

fficient knowledge, skills, experience and understanding of operational
ulfil its responsibilities;

setting a tone from the top that fosters a risk culture and supports the
operational resilience; and

- Provi ed and engaged oversight of Senior Management's implementation of the insurer's ap to operational resilience.

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

- 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 such matters 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; and
- 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

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

- 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; and
- 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.

Senior Management

19. 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. Supervisors could consider:

- Including operational resilience within the roles and responsibilities of Senior Management identified under an insurer's governance framework; or
- Requiring insurers to allocate responsibility for operational resilience to a specific individual or individuals within Senior Management.

Box 1: Examples of how governance frameworks can support op

Bermuda: The Bermuda Monetary Authority (BMA) is consulting on ar
outsourcing code and guidance note that will ensure that both the Boa
play complementary roles in maintaining and enhancing the operation
overseeing outsourcing arrangements and ensuring compliance wi
details the respective roles and responsibilities as follows:

- The Board is to focus on strategic oversight, approval and ac resilience and outsourcing policies, ensuring alignment with re strategic objectives; and
- The Senior Management is to focus on the implementation, managemen onal aspects of resilience measures and outsourcing arrangements, includi policies, procedures 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:

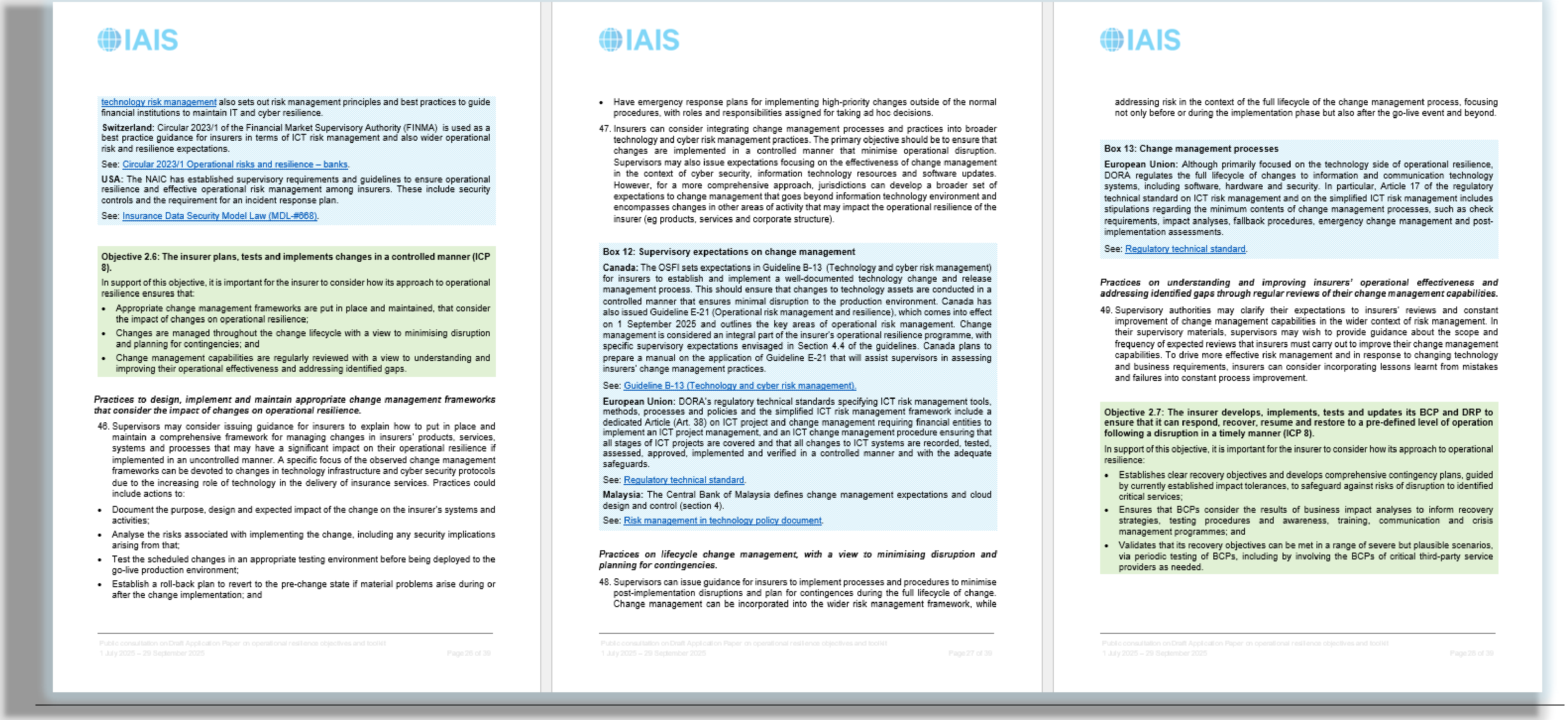
- Implement and maintain processes and systems reflecting the operational risk management framework in accordance with operational risk tolerance levels;
- Ensure that adequate mechanisms are set up for reporting situations where operational risk tolerance levels are exceeded;
- Ensure the availability, 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;

Toolkit example: change management



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.

46. 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; and

- Have emergency response plans for implementing high-priority changes outside of the normal procedures, with roles and responsibilities assigned for taking ad hoc decisions.

47. 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: The 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 comes 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.

48. 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.

49. Supervisory authorities 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 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).

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.

Toolkit

Survey results 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 **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).

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

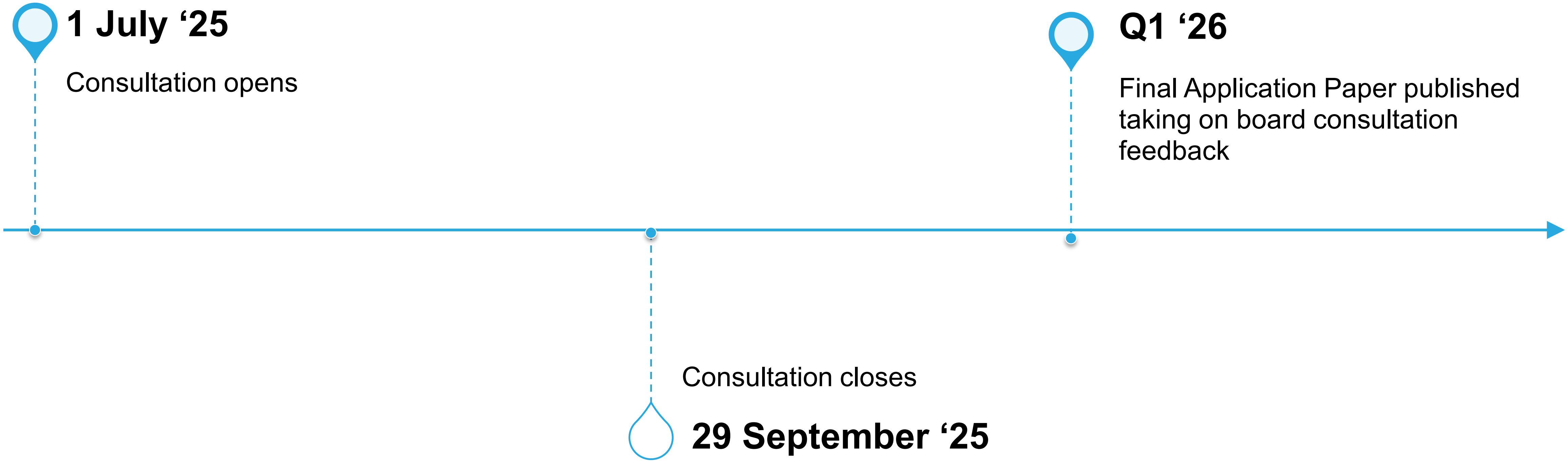
3.1: In evaluating the insurer’s operational resilience, **supervisors coordinate** within the supervisory authority to capture all potential areas of vulnerability (ICPs 2 and 24).

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).

Timeline



1 July ‘25

Consultation opens

29 September ‘25

Consultation closes

Q1 ‘26

Final Application Paper published taking on board consultation feedback

Questions?