Draft Application Paper on Operational Resilience Objectives [and Toolkit]

10 September 2024

14:00-15:00 CEST

Background

- **Phase 1**: draft **Objectives for Operational Resilience published in August,** under consultation until **11 October**
- **Phase 2:** development of a non-exhaustive collection of **Supervisory Tools ("Toolkit)**
- Objectives and Toolkit to form a single **Application Paper** following the consultation of each

Objectives

- Grounded in ICPs, high-level and principles-based
- Reinforces that operational resilience is an outcome emerging from an array of practices and disciplines
- Establishes a sound and consistent foundation to support authorities supervising insurers' operational resilience

Toolkit

- Operationalise the Objectives by setting out examples of relevant supervisory practices
- Will provide options, while not being prescriptive, to driving consistency where possible, while respecting jurisdictional differences and proportionality

Draft Objectives

Overview

Operational resilience, governance, and operational risk management

Key elements of a sound approach to operational resilience

Operational Resilience Objectives

Objectives for insurance supervisors

Overview

Operational resilience, governance, and operational risk management

- An insurer's approach to operational resilience is supported by its governance framework
  - Board responsibilities
    - ✓ Oversight of the approach to operational resilience
    - ✓ Integration with the governance framework
    - ✓ Collective knowledge, skills etc, relevant to operational resilience
    - ✓ Tone at the top that fosters a risk culture
    - ✓ Oversight of risk management vis-à-vis risk tolerance limits
    - ✓ Informed and engaged oversight of Senior Management
  - Board and Senior Management Responsibilities
    - ✓ Effective communication across the organisation and amongst key stakeholders
    - ✓ Clearly defined roles, responsibilities and reporting lines, including escalation mechanisms
    - ✓ Sufficiency of resources

Overview

Operational resilience, governance, and operational risk management

- An insurer's approach to operational resilience leverages, and is integrated with, its operational risk management framework in a consistent, comprehensive and robust manner
  - A risk management system is in place that identifies, assesses, monitors, mitigates and reports on operational risks
  - The approach identifies and manages all risks that may severely disrupt operations, including on the delivery of critical services
  - The approach is embedded in the system of internal controls and sets out roles and responsibilities in consideration of the three lines of defence

Overview

Key elements of a sound approach to operational resilience

- The insurer identifies and maintains an up-to-date inventory of its critical services and interdependencies
  - Critical services and related dependences are identified and documented end-to end
  - Resource and risks involved in the delivery of critical services are understood

- The insurer sets impact tolerances for disruption to its critical services
  - Maximum disruption/impact levels are quantified in view of an insurer's risk tolerance, financial soundness and impacts to customers and the wider financial system
  - Impact tolerances are pre-defined and form a useful basis for evaluating the need for changes to operational and strategic decisions, including the need for further investment

Overview

Key elements of a sound approach to operational resilience

- 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
  - Scenario testing includes assessing the insurer's ability to withstand and recover from severe but plausible operational disruption, and incorporates lessons learnt

- The insurer effectively manages operational incidents, including but not limited to cyber incidents, affecting critical services
  - Operational incidents are effectively managed to prevent and respond to – and recover from – their occurrence to minimise disruption to critical services
  - Clear processes for identifying, reporting and responding to incidents are in place, including at third- and nth-party service providers
  - Communication plans reinforce reporting on incidents to relevant stakeholders

Overview

Key elements of a sound approach to operational resilience

- 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
  - Stable and resilient technology environment through appropriate risk management practices
  - Effective management and testing of access to technology, systems, premises, networks, key people and information assets
  - Good cyber hygiene practices
  - Regular technology and cybersecurity assessments
  - Ongoing training, awareness and collaboration with industry peers on threat intelligence, including on responses to identified incidents
  - Regular testing of the approach, and incorporating effective situational awareness and threat intelligence

Overview

Key elements of a sound approach to operational resilience

- The insurer plans, tests, and implements changes in a controlled manner
  - Change management framework considers impacts of change on operational resilience
  - Changes managed through the change lifecycle with a view to minimising disruption and planning for contingencies
  - Change management capabilities are regularly reviewed with a view to understanding and improving operational effectiveness, and addressing identified gaps

- 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
  - Clear recovery objectives and comprehensive contingency plans are established
  - BCPs consider the results of business impact analyses
  - Recovery objectives are validated against a range of severe but plausible scenarios

Overview

Key elements of a sound approach to operational resilience

- The insurer effectively manages relationships with third-party service providers, including intra-group and nth-party relationships
  - Effective management and oversight of supply chain risks, including those stemming from the use of third-party service providers that are critical to the business
  - Effective management of the potential impact of disruption throughout the lifecycle of its relationships with third-party service providers

Overview

Objectives for insurance supervisors

- In evaluating the insurer's operational resilience, supervisors coordinate within the supervisory authority to capture all potential areas of vulnerability
  - Communications within a supervisory authority aim to minimise a "siloed" approach
- Supervisors share information and cooperate with other supervisors with a view to minimising risks
  - Approach supports sharing information and cooperating with other supervisors, including with domestic supervisors, supervisors in other jurisdictions and across sectors
  - The approach aims to minimise legal and other impediments
  - Supervisory authorities consider how they use 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 party service providers
  - Supervisory authorities support formalising sharing arrangements

Overview

Objectives for insurance supervisors

- Supervisors cooperate and communicate transparently with stakeholders
  - Engagement with relevant stakeholders consider communication and cooperation on insurers' operational resilience approaches, to the extent possible
  - Supervisors integrate expectations for insurance sector operational resilience into its review and reporting frameworks and ensure timely and frequent engagement with insurers to help address problem areas
- Supervisors support a culture of continuous learning and improvement with respect to operational resilience within the supervisory authority
  - Supervisory authorities invest in staff training and recruitment, to maintain sufficient technical expertise in the areas of operational risk and information systems
  - Supervisors incorporate generative thinking/technologies into their processes

Next steps

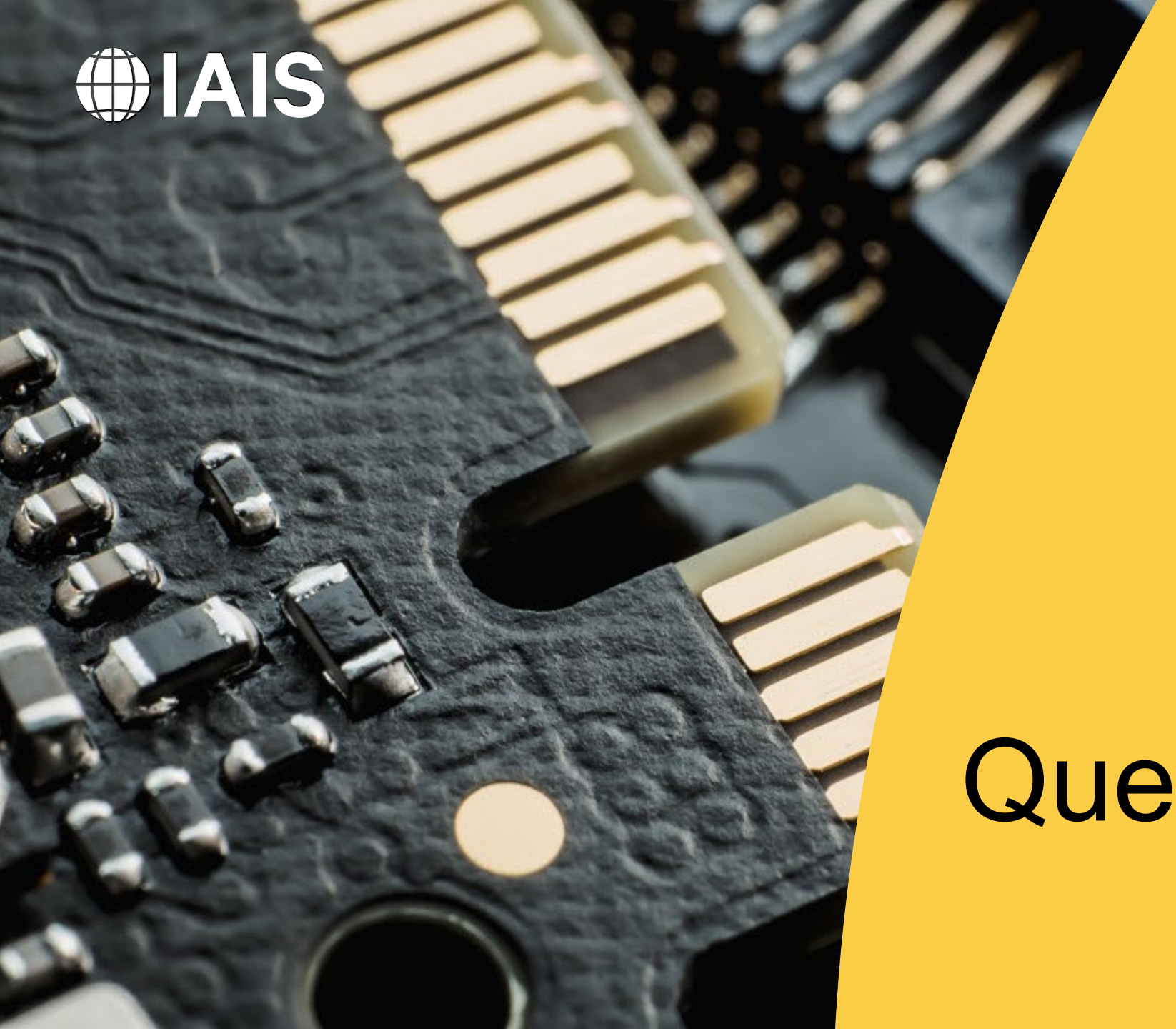
➢ Objectives (Phase 1)

- Responses to public consultation due **11 October** [Link]

➢ Toolkit (Phase 2)

- Developed in 2nd half 2024
- Information on practices relevant to the Objectives obtained via a survey of IAIS Members (currently underway)
- Consultation on Toolkit (Q2 2025)

➢ Final Objectives and Toolkit to be integrated into a single Application Paper following the consultation of each phase



Questions