Paper on Insurance Sector Operational Resilience

International Association of Insurance Supervisors

ManagementSolutions
Making things happen

Executive summary of the paper

Key issues, supervisory approaches and potential areas of work

1 Executive summary of the paper
Insurance Sector Operational Resilience

The IAIS Paper on Insurance Sector Operational Resilience identifies issues impacting operational resilience in the insurance sector

Background and regulatory context

In recent years, the IAIS has published other material relevant to operational resilience:

- **2016** paper on cyber risk
- **2018** paper on supervision of Insurer Cybersecurity
- **2020** report on Cyber Risk Underwriting

The pandemic further illustrated the **need for companies** to have in place a **more comprehensive operational resilience framework.** In this context, the IAIS has published a paper on Insurance Operational resilience.

Objective of the paper

- **Identify issues impacting operational resilience** in the insurance sector and provide examples of how supervisors are approaching these developments.

Challenges/issues identified

1 Information collection and sharing

- Outline overarching issues, focusing in particular on the **importance of sound governance** to effective operational risk management, and the benefits of information sharing including public/private collaboration

2 Cyber resilience

- Challenges associated with assessing the quality of the framework established by an entity to deliver on cyber resilience, including existing **tools and metrics** available to supervisors.

3 IT third-party outsourcing

- Challenges associated with assessing **risks arising from concentration of IT providers** as a critical issue, given the increased complexity of the financial sector and the reliance on IT third-party outsourcing.

4 Business continuity

- Challenges associated with the need for **business continuity management (BCM) approaches** to evolve to meet the realities of today's environment, including in response to the pandemic.

IAIS potential future areas of work

2 Key issues, supervisory approaches and potential future areas of work (1/2)
Information collection and cyber resilience

Focus on the importance of supervisors having access to a range of information and having available the appropriate tools and metrics to assess an insurer's cyber resilience

	Challenges identified	Supervisors practices/approaches	Potential areas of work
Information collection and sharing	• Having **access** to a range of information, including on an entity's operational resilience framework and the potential threats impacting the insurance sector. • The pandemic demonstrated the importance **of effective information sharing and public/private cooperation** to support an entity's operational resilience.	• To gather this information, some supervisors proactively engage with an **entity's Board and Senior Management** to understand the effectiveness of an entity's operational resilience framework. • In some jurisdictions, **regular forums** for timely and ongoing exchanges of information on operational resilience have been put in place (e.g. BaFin, PRA, FCA) • Some supervisory authorities publish **current state, findings, and thematic review reports as well as best practices** relevant to operational resilience in the insurance sector.	• **Facilitate mechanism** for sharing information or leverage existing information sharing mechanisms. • Explore how **definitions and terminologies** relevant to operational resilience could be **better aligned.pppp**

Cyber resilience	• Identify the most **effective** supervisory tools and approaches to cyber resilience **monitoring** that can keep pace with the changing nature of cyber-attacks and the speed with which entities are adopting new technologies.
	• **Absence of greater consensus around best practices** for assessing an insurer's cyber resilience.
		• The use of the following tools and techniques:
		  • **Self-assessment Questionnaires**: involves insurer's performing self-assessments of the quality of their framework to deliver on cyber resilience.
		  • **Vulnerability Assessments**
		  • **Cyber Incident Reporting**
		  • **Scenario-Based Testing**
		  • **Red Team Tests**
		  • **Threat Led Penetration Tests**
			• **Discussion on metrics and tools used** to evaluate the quality of an insurer's framework to deliver on cyber resilience and emerging cyber risks associated with the use of new or developing technologies.
			• **Analysis of the impact on cyber resilience of large-scale IT transformations** as insurers make increasing use of new technologies.
			• **Developing proactive, consistent and proportionate approaches** to the development, supervisory evaluation, and implementation of an insurer's framework to deliver on cyber resilience,

2 Key issues, supervisory approaches and potential future areas of work (2/2)

Third-party outsourcing and BCM

Challenges associated with assessing risks arising from concentration as a critical issue and the challenges associated with the need for BCM approaches to evolve to meet the realities of today's environment, including in response to the pandemic

	Challenges identified	Supervisors practices/approaches	Potential areas of work
IT third-party outsourcing	• Ongoing management of risks arising from **concentration** associated with the provision of critical IT services to companies by third-party service providers. • Addressing risks arising from concentration stemming from **third-party service providers** (e.g. use of the cloud of a third-party IT service that may present risks arising from concentration at the individual entity)	• Many supervisory authorities require or are planning to require insurers to provide **information on services outsourced to third parties**. • Certain jurisdictions are **moving forward with legislation** and/or guidance on third-party service providers, examples of which include the EU's DORA and the UK Treasury policy statement. • Risks arising from concentration can also be partially addressed through **novel risk management practices**, such as the adoption of multi-cloud	• **Alignment and report definitions and requirements** for terms relevant to IT third-party outsourcing (eg such as critical services, outsourcing, third parties etc) • **Exchange information on practices and methodologies** used by supervisors. • **Explore implications of larger insurers** considering a multi-vendor strategy and the implementation of data portability arrangements and environments across providers.

Business continuity management	• Multitude of **interconnections and interdependencies between various systems**, participants, and service providers in the insurance sector.
	• **Complex** functioning of the sector
	• Identification of **major operational events** likely to pose a threat to the critical activities of an insurer, such as natural disasters
		• Supervisors are taking action to address the changed risk environment in relation to BCM. Policy and/or supervisory work have focused on:
		  • **Improvements to BCPs** based on risks that arose during the pandemic
		  • **Integration of the BCM** system requirements across business functions to identify business continuity risks
		  • Increasing the **breadth** and **frequency** of vulnerabilities assessments to help ensure a thorough knowledge of critical business services
			• Draw out the **links between business resilience and BCM**.
			• **Exchange information on best practices and methodologies** used by supervisors, including: i) how the sector is approaching evolutions in BCM best practices; ii) the scope of BCM; and iii) how existing or recently revised BCPs have or will evolve to remain fit for purpose in consideration of the changed work environments that emerged during the pandemic.

Management Solutions
Making things happen

International *One Firm*
Multiscope Team
Best practice *know-how*
Proven Experience
Maximum Commitment

Marcos Fernández Domínguez
Partner at Management Solutions
marcos.fernandez.dominguez@msspain.com

Efrén Manuel Hernández Domínguez
Director at Management Solutions
efren.manuel.hernandez@msspain.com