Issues Paper on Insurance Sector Operational Resilience

Public Discussion Session

31 May 2023

15:30 – 16:30 CEST

Issues Paper on Insurance Sector Operational Resilience, 31 May 2023

Technical help

Please email Alka.Sharma@bis.org or send a message to the **Host** via the WebEx **Chat** function.

Dialled-in by phone

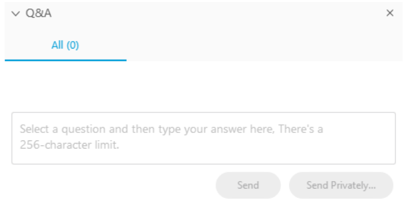
For those who have dialled-in to the webinar, please send an email to Alka.Sharma@bis.org, confirming your name and the number you have used to connect.

Video

Click on the camera icon to stop or start video. Please feel free to enable your own video. In case of bandwidth problems on your own network, you might be asked to stop video.

The Q&A function

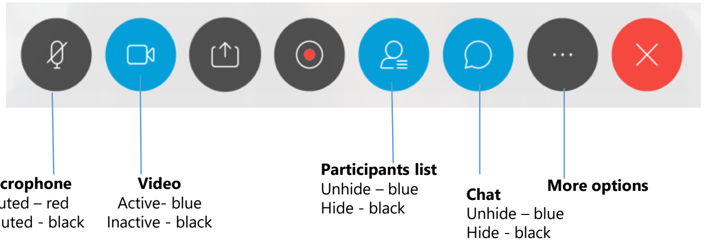
- To ask a question, or indicate that you wish to ask a question, please use the **Q&A** function:
- At the bottom right-hand corner of your screen, click on the arrow besides "Q&A". This will open a text box, which you can use to type a question or indicate that you would like to speak.



Select a question and then type your answer here, There's a 256-character limit.

- Please send your questions/indications to **all panellists**.

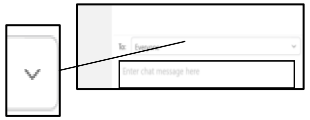
Control panel



If you cannot see the control panel, move your cursor or finger to the center lower part of your screen. The control panel should reappear.

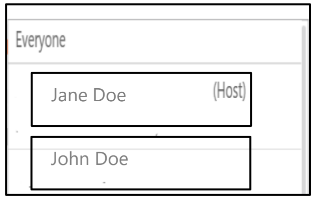
Chat function

- To see the chat function, make sure that the icon is in blue or click on the icon so that it appears on the right-hand side.
- Click on the drop-down arrow



Enter chat message here

- Click on the name of the person you would like to send a message to.

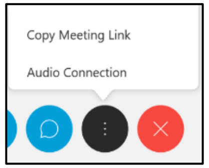


- Click on "Enter chat message here", and type in your message.

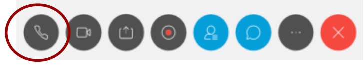
Problems with audio connection

If you cannot hear other participants, even when you have adjusted volume, please verify:

1. Is the volume adjusted for the device / headset in use? (check in PC sound settings)
2. In WebEx, go to More options ⋯ click **Audio connection** and adjust volume



3. If Audio connection does not appear under ⋯ , find the phone icon in the control panel



and select "Call Using Computer", "Call me" or "I Will Call in".

If participants cannot hear you well, you can change audio settings (e.g. to mobile phone) by clicking ⋯

1. Click on **Audio Connection**
2. Click on **Switch Connection**

Call me

Click on **Call Me**, enter your phone number and click **Call Me.** You will receive a call from WebEx.

I Will Call in

If the Call Me option does not work, choose **I Will Call In.** Dial the number listed or the Global call-in numbers. Please enter the **Attendee ID** shown below the phone number, so that you can be automatically identified.

Background

- Issues Paper on Insurance Sector Operational Resilience published on 23 May 2023
- Public consultation period took place from Oct 2022 – Jan 2023
- Public background session held in Oct 2022 to introduce the consultative draft
- 7 responses received on the consultative draft, from a combination of External Stakeholders and IAIS Members
- All comments and the IAIS responses are available on the IAIS website

Objectives of Issues Paper

- To identify issues impacting operational resilience in the insurance sector
- To provide examples of how supervisors are approaching these developments
- Address three specific operational resilience sub-topics:

Cyber resilience

Third-party outsourcing

Business continuity Management (BCM)

Relevance of operational resilience to the insurance sector

- An increasingly important area of focus in light of:
  - rapidly evolving technology and innovation
  - Changes to where and how people work
  - Increasing cyber threat landscape
- Supervisory regimes need to adapt to account for growing resilience of insurers on digital systems
- The pandemic further illustrated the need for more comprehensive operational resilience frameworks

Operational resilience and the IAIS ICPs

- The Issues Paper is derived from various sources, including a review of the IAIS Insurance Core Principles (ICPs)
- ICPs support sound management of an insurer’s operational risk, but – by their nature – do not contain specific detailed guidance on managing operational risks
- The ICP review revealed examples where further consideration for developing supporting materials could advance sound supervision of operational risks

Key issues and supervisory approaches

Governance and Board accountability

- Robust governance structures enable insurers to identify and respond to emerging risks and adapt to changing environments
- An insurer’s Board and Senior Management are well placed to oversee the establishment of a governance framework that can assess the impact of operational disruptions
- Insurers with strong and effective governance frameworks were better placed to prevent, adapt and respond to operational disruptions presented by the pandemic

Information collection and sharing among supervisors, public/private collaboration

- Effective information sharing among insurance supervisors and across the insurance sector more broadly may also help to strengthen the supervisory oversight and insurer management of operational resilience
- There are some examples of regular forums for exchange of information, and some authorities require insurers to disclose publicly or to supervisors
- However, information sharing initiatives among supervisors appear to be limited at present

Cyber resilience

- The insurance sector is heavily dependent on the use of digital technologies and this reliance has only accelerated during the pandemic as entities transitioned to remote working
- A key issue for supervisors is how to gain assurance – in a proportionate and resource effective way – that an insurer’s cyber resilience framework is effective and robust
- Cyber risks are continually evolving and growing, making potential threats to an entity/sector’s cyber resilience difficult to quantify in a structured manner

Cyber resilience – key challenges

Point in time assessments versus continuous monitoring

- Commonly used supervisory techniques provide a valuable snapshot at a point in time
- A key challenge is to identify the most effective tools and approaches to cyber resilience monitoring that keeps pace with changing cyber attacks and rapidly changing technology

Lack of standardised metrics

- Consistent approach to assess insurer’s cyber resilience can help with engaging third-party service providers that operate cross-jurisdiction
- Quantitative metrics are limited, but can be helpful in assessing parts on an insurer’s cyber resilience framework

Resourcing cyber expertise

- Supervisory authorities face challenges to developing cyber resilience oversight programmes due to a skills gap
- One consequence of skills shortages is that the advancement of supervisory frameworks over cyber resilience may lag behind the advancement of cyber-attacks

IT third-party outsourcing

- Third-party services offer many benefits, including improved operational resilience
  - Reliance on 3rd party providers also comes with increased operational risks
- Identification and management of concentration risks remains a key challenge
  - It is inherently becoming more difficult for financial supervisory frameworks to identify and mitigate potential systemic risks due to the complexity of services offered by 3rd and 4th parties
  - A single entity has limited visibility over services offered by the same 3rd or 4th party provider to multiple financial institutions across multiple jurisdictions
- Many supervisory authorities require insurers to provide information on services outsourced to third parties
  - Such collections could allow supervisory authorities to better identify concentration risks

Business continuity management

- It is important for insurers to meet commitments to its insureds and other partners through sound business continuity risk management practice

- Core elements of BCM processes include:
  - Capability to identify major operational incidents
  - Sound business continuity policies, with clear lines of responsibility, management, and communication

- Challenges related to BCM that could benefit from further analysis include:
  - Integration of BCM and risk management
  - Enhanced scope and testing of BCM frameworks
  - Ensure BCM frameworks accommodate post-pandemic practices, including remote/hybrid

Feedback from Public Consultation

- Reponses received from a number of External Stakeholders and IAIS Members
- Respondents welcomed
  - The initiative as a good way to share information on supervisory practices
  - That the paper builds on the principles based nature of existing ICPs
  - The characterisation of operational resilience as an outcome

- On areas that could benefit from future consideration by the IAIS, respondents:
  - Encouraged the IAIS to take a dynamic, risk and principles-based approach to the supervision of operational resilience
  - Emphasised the importance of harmonising requirements, instilling proportionality in supervisory approaches, and continuing to respect confidentiality requirements

Feedback from Public Consultation

- External stakeholder’s comments on areas that could benefit from future IAIS focus:
  - Aligning reporting definitions/requirements notably for incident reporting, critical services, outsourcing and third-parties;
  - Identifying and providing an inventory of potential concentration risks among third-party service providers, given regulators/supervisors' broader view of the sector;
  - Raising awareness of the impacts of data localisation rules and inadequate jurisdictional data security protocols on operational resilience; and
  - Coordinating across the financial services sector, in particular on outsourcing and third-party risk management, while remaining aware of and bringing forward insurance sector specificities

IAIS Next Steps

- IAIS is in the process of developing its next 5 year Strategic Plan and aims to launch a stakeholder survey in June to gather further input
- IAIS future work on insurance sector operational resilience will be considered vis a vis the IAIS' ongoing discussions on its strategic objectives
- Feedback received from Stakeholders is an important input to this process

Questions