IAIS International Association of Insurance Supervisors

Issues Paper on Insurance Sector Operational Resilience

May 2023

.

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard-setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard-setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

For more information, please visit www.iaisweb.org and follow us on LinkedIn: IAIS – International Association of Insurance Supervisors.

Issues Papers provide background on particular topics, describe current practices, actual examples or case studies pertaining to a particular topic and/or identify related regulatory and supervisory issues and challenges. Issues Papers are primarily descriptive and not meant to create expectations on how supervisors should implement supervisory material. Issues Papers often form part of the preparatory work for developing standards and may contain recommendations for future work by the IAIS.

International Association of Insurance Supervisors
c/o Bank for International Settlements
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090

This document was prepared by the Operational Resilience Task Force in consultation with IAIS Members.

This document is available on the IAIS website (www.iaisweb.org).

Content Overview

1 Introduction

1.1 Objectives and scope

1. The objective of this paper is to identify issues impacting operational resilience in the insurance sector and provide examples of how supervisors are approaching these developments, with consideration of lessons learnt during the Covid-19 pandemic (“pandemic”)..[1] Recognising that operational resilience is a broad and evolving area, this paper addresses three specific operational resilience sub-topics concerning areas the Task Force considers as matters of significant and increasing operational risk, and therefore of immediate interest to supervisors:
    - Cyber resilience;
    - IT Third-party outsourcing; and
    - Business Continuity Management (BCM).
2. In recent years, the IAIS has published other material relevant to operational resilience (particularly cyber resilience). The IAIS explored the topic of cyber risk in the insurance sector in an Issues Paper (2016) and in an Application Paper (2018). These papers focused on the recognition of certain fundamental elements of cyber security for financial institutions, on cyber breach case studies within the insurance sector and on cyber risk frameworks in the context of existing useful practices and guideposts. In 2020, the IAIS also published a report on Cyber Risk Underwriting, which identified challenges and supervisory considerations for sustainable cyber underwriting market development. These materials should be considered as complementary to the discussion in this paper, where relevant..[2]
3. The information in this paper is informed by a review of the IAIS Insurance Core Principles (ICPs), a stocktake of existing publications by Standard Setting Bodies (SSBs) with relevance to operational resilience, direct engagement – including roundtables – held with experts external to the IAIS membership and information shared on supervisory practices among insurance supervisors.

1.2 Relevance of operational resilience to the insurance sector

4. The digital age, as well as the accompanying risks posed by cyber threats and increasing reliance on technology, has been a reality for insurers for many decades. The concept of operational resilience is not new, though recognition of the importance of adapting supervisory regimes to account for the growing reliance by insurers on digital systems is more recent.
5. The pandemic further illustrated the need for companies to have in place a more comprehensive operational resilience framework that considers risks arising from the use of digital technology, outsourcing critical business functions to third parties and interruptions to normal business functioning due to unforeseen events. While these considerations are applicable to near-term challenges, they may also empower the Board and Senior Management (both present and future),to focus on operational resilience as an important strategic objective.

[1] The 2022-2023 IAIS Roadmap positioned operational resilience under High Level Goal 3 *Sharing good supervisory practices and facilitating understanding of supervisory issues,* as an increasingly important area of supervisory focus, particularly in light of rapidly evolving technological innovation and changes to how and where people work stemming from the Covid-19 pandemic.

[2] Issues Paper on Cyber Risk to the Insurance Sector, August 2016; Application Paper on Supervision of Insurer Cybersecurity November 2018; Cyber Risk Underwriting: Identified Challenges and Supervisory Considerations for Sustainable Market Development, December 2020.

6. Cyber-attacks grew with the spread of the pandemic and the accompanying widespread adoption of remote working. The Financial Stability Board (FSB) reported that the number of cyber activities such as phishing, malware and ransomware against financial institutions grew from fewer than 5,000 per week in February 2021 to more than 200,000 per week in late April 2021..[3] A survey among financial institutions by the Financial Services Information Sharing and Analysis Center also highlighted that, in 45% of cases, staff work-from-home overwhelmed virtual desktop infrastructure (VDI)/virtual private network (VPN) processes. The rapid move to hybrid and remote work presented risks to entities' operational resilience, in that it exposed certain new vulnerabilities to IT systems and increased the attack surface. In one third of cases, business continuity IT plans were not prepared for a long-term at-home work force. One fifth of the financial firms reported that their network operation activities were interrupted during the pandemic..[4]
7. SSBs and supervisors have sought to address operational resilience from a conceptual and component perspective, both before and during the pandemic, though the pandemic has heightened awareness and perhaps accelerated the development of supervisory materials responsive to such concerns.
8. The Basel Committee on Banking Supervision (BCBS) defines operational resilience in the banking context as "the ability of a bank to deliver critical operations through disruption." Further, the BCBS explains that "in considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption.".[5] This definition reinforces that while the prevention of harmful events is a critical part of the overall framework, recovery from inevitable disruptions is equally as vital.
9. The Organisation for Economic Co-operation and Development (OECD), in developing a very broad definition of operational resilience, articulated it as "the ability of households, communities and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty"..[6] From the OECD definition, then, it emerges that a salient element of sound operational resilience is to update and evolve aspects of the framework so as to continue to meet the mark.
10. In 2021, the United Kingdom (UK) financial supervisory authorities defined operational resilience as "the ability of firms, their groups, and the financial sector as a whole to prevent, adapt to, respond to, recover from, and learn from operational disruptions.".[7] The UK approach considers that resilience is most effectively addressed by focusing on an insurer's important business services, rather than on systems and processes in isolation. The UK policy underscores that, from time to time, disruptions will occur that prevent an insurer from operating as usual and that insurers need to consider a range of severe but plausible disruption scenarios. This approach acknowledges that blind spots can act as a substantial step towards shocks and disruptions becoming reality.
11. In 2020, in the United States (US) the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation ("the agencies") defined operational resilience in guidance as "the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard." The agencies explain that operational resilience is the outcome of effective operational risk

[3] FSB (2021), Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective: Final report (fsb.org)

[4] Bank for International Settlements (BIS) Bulletin (2021), Covid-19 and cyber risk in the financial sector

[5] BCBS (2021) BCBS Principles for Operational Resilience

[6] OECD, Risk and Resilience

[7] Bank of England, Operational resilience of the financial sector

management, combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.[8]

12. Drawing from these definitions, operational resilience can be considered as an outcome that emerges from a wide array of practices and disciplines currently used by insurers. 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 disrupt the normal course of business by impacting critical operations or systems. Operational resilience takes as a premise the assumption that disruptions will occur and that insurers should consider their tolerance for such disruptions and take this into account when devising their operational framework.

1.3 Issues paper structure

13. **Section 2** of this paper provides an overview of the general applicability of the ICPs to the broad topic of operational resilience as well as to the sub-topics noted above. This includes identification of those ICPs that support sound operational risk management in principle, noting that the risk landscape continues to change.

14. **Sections 3.1 and 3.2** 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.

15. **Section 3.3** considers 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. The importance of supervisors having available the appropriate tools and metrics to assess an insurer's cyber resilience cannot be overstated. In 2021, cyber-attacks increased globally across almost every category, with one source indicating that ransomware attacks increased 105% from 2020 to 2021.[9] This poses risks to the supervision of an entity's cyber resilience, in particular as existing tools and metrics attempt to keep pace with the evolving nature of cyber-attacks.

16. **Section 3.4** outlines challenges associated with assessing risks arising from concentration as a critical issue, given the increased complexity of the financial sector and the reliance on IT third-party outsourcing. The risks posed by a third-party outsourcing partner for IT related functions are similar across many industries, including the insurance industry. Insurers hold and handle a large amount of varied data, including personal data, financial data and intellectual property, which heightens the importance of insurers' risk management with regards to vendor relationships and how supervisors and insurers respond to the potential vulnerabilities associated with third-party risks arising from concentration.

17. **Section 3.5** sets out 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. The Joint Forum describes BCM as a "whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption." .[10] A Business Continuity Plan (BCP) is described as "a comprehensive written plan of action that sets out the procedures and systems necessary to continue or restore the operation of an organisation in the event of a

[8] US Federal Reserve Bank (November 2020), SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience (federalreserve.gov)

[9] Sonic Wall (2022), 2022 SonicWall Cyber Threat Report

[10] High-level principles for business continuity - August 2006 (bis.org)

disruption.” .[11] For the purpose of this Issues Paper, BCM is considered an overarching concept that encompasses the BCP. How operational risks evolved in the context of the pandemic, and the resulting lessons learnt during the pandemic, are of relevance to BCM. The pandemic changed the way in which many companies, including insurers, interact with employees and stakeholders by relying on the use of wide-spread remote and hybrid-working tools and technologies. Remote and hybrid working affords entities a great deal of flexibility and promotes business continuity following government mandated lockdowns (and in general). However, a critical piece of moving to hybrid and remote work environments is understanding and proactively managing the risks that arise from an increased attack surface and reliance on technology and outsourcing of IT services.

18. **Section 4** outlines a number of aspects of the risks related to cyber resilience, IT third-party outsourcing and BCM – based on observations discussed in preceding sections – that may benefit from future consideration or further analysis by insurance supervisors.

2 Applicability of ICPs to operational resilience

19. The ICPs provide a global framework for the supervision of the insurance sector. While, in most cases, they do not address specific thematic risk issues, they do afford a flexible basis for supervisors to identify and respond to new and emerging risks and/or an increased attention to rising risks – including operational risks – that the insurance sector faces. The ICPs thus serve as a natural starting point to identify foundational elements to ensuring an insurer’s operational resilience.
20. In general, the ICPs are drafted in such a way that they address a variety of risks, including operational risk; however the ICPs do not expand on the scope of the term operational resilience. For example, the ICPs reference the use of IT systems and outsourcing but do not specifically address how these may contribute to an insurer’s operational (including cyber) risks. Likewise, although the ICPs reference the identification and management of cyber risk they do not expand on the links between cyber risk management and an entity’s IT systems and processes.
21. The ICPs do nevertheless guide supervisory responses to these issues, include actions to enhance visibility and strategies for responding to operational risks and require the sound management of significant risks and implementation of appropriate internal controls, all of which promote sound operational risk management more generally, while respecting issues of proportionality.
22. The ICPs identified as supporting the supervision and management of operational resilience in the insurance sector include:
    - ICP 4 (Licensing)
    - ICP 7 (Corporate Governance)
    - ICP 8 (Risk Management and Internal Controls)
    - ICP 9 (Supervisory Review and Reporting)
    - ICP 10 (Preventive Measures, Corrective Measures and Sanctions)
    - ICP 12 (Exit from the Market and Resolution)

[11] High-level principles for business continuity - August 2006 (bis.org)

- ICP 16 (Enterprise Risk Management for Solvency Purposes)
- ICP 23 (Group-wide Supervision)
- ICP 24 (Macroprudential Supervision)

23. The ICPs have clear interactions with operational resilience and support the sound management of an insurer's operational risks. That said, by design the ICPs are set out at a principles-based level and thus do not contain specific detailed guidance with respect to defining operational resilience (and related terms) and managing operational risks.

24. A key supervisory development in recent years has been a move to consider operational resilience as an outcome, which is the ability of an entity to deliver critical operations through disruption. Operational resilience then provides a strategic context for how an entity operates and is a driver of financial resilience and potentially financial stability. Building on the principles-based nature of the ICPs, it could be useful to explore the umbrella concept of operational resilience as an outcome and to discuss and/or set out the links of this outcome-based approach to cyber resilience, IT third-party outsourcing and BCM.

25. The review of ICPs also revealed a number of examples of areas where further discussions or considerations for developing supporting materials could advance the supervision of cyber resilience, IT third-party outsourcing, and BCM as critical elements of operational risk management (which are considered among those elements outlined in section 4).

3 Key issues and supervisory approaches

26. This section sets out a range of overarching issues for insurance supervisors, relating to significant and increasing areas of operational risk and spanning across the sub-topics of cyber resilience, IT third-party outsourcing and BCM.

27. The risks associated with these sub-topics should not be viewed in a silo, as they are interdependent and interconnected. Having in place an integrated approach to managing an insurer's operational resilience could contribute to improvements in an entity's operational effectiveness and efficiency.

28. For example, insurers may rely on third parties for the provision of critical IT services, which if well managed, has the potential to improve an insurer's cyber resilience. The use of advancing technologies, such as the cloud, could provide efficiencies and improvements in cyber security as compared to in-house or legacy technology infrastructure and systems. However, dependencies on third parties can also magnify cyber risk. As noted in the G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector "cyber incidents resulting from third-party vulnerabilities could lead to fraud, disruption of services or access to sensitive customer or corporate information."[12] This is particularly important for insurers, in respect of any sensitive or personal (such as customer) data that is accessible to third-party service providers.

29. When assessing an insurer's framework to deliver on cyber resilience, supervisors may consider how dependencies on critical third-party suppliers are identified and the extent to which such dependencies create significant vulnerabilities. Including third parties in cyber resilience assessments can enhance the identification of risks and the implementation of relevant risk mitigation strategies. This could be achieved through a range of approaches from the direct

[12] G-7, Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector

participation of a third party in the assessment, to insurers themselves considering the impact of third-party dependencies when assessing their own cyber resilience.

30. There are also overlapping risks across cyber resilience, IT third-party outsourcing and BCM. For example, a cyber incident could impact business continuity and be attributed to an attack on a third party, therefore insurers need to be cognisant of the links between these risks. Integrating cyber resilience (from the perspective of the entity's in-house IT infrastructure and outsourced IT services) and BCM could help to ensure that cyber considerations are well incorporated into an insurer's broader operational resilience framework.

3.1 Governance and Board accountability

31. The ICPs emphasise the importance of robust governance structures that enable insurers to identify and respond to emerging risks and adapt to changing environments. Following on from this, the potentially broad consequences of inadequate operational resilience management elevate operational risk to a key risk necessitating appropriate attention from an insurer's Board and Senior Management.

32. An insurer's Board is ultimately accountable for overseeing the establishment of a robust governance framework that can assess the impact of operational disruptions and ensure that appropriate mitigation strategies and measures are in place to manage the impacts of these risks within tolerance limits. Senior Management, meanwhile, is responsible for ensuring the effective delivery of resilience plans.

33. While each individual member of the Board or Senior Management should not reasonably be expected to have expertise in operational risk management, Boards collectively should possess adequate knowledge, skills, and experience to provide constructive oversight to Senior Management who make decisions that have consequences on an insurer's operational resilience. Recognising that operational disruptions can have widespread impacts across an organisation, the provision of appropriate training across relevant groups within an organisation could facilitate the implementation of a sound operational resilience framework.

34. The absence of a framework for identifying and analysing the impact of severe but plausible risks to operational resilience over various durations can limit the ability to successfully enhance the insurer's overall operational resilience. Likewise, an absence of processes for identifying the people, processes, technology, facilities and information that support key operational functions, business services and lines of business in current frameworks can also impact overall resilience.

35. Integral to the effectiveness of such a framework is a risk-based process to test the effectiveness of an insurer's ability to respond to and recover from operational disruptions stemming from severe but plausible scenarios.

3.1.1 Lessons learnt from the pandemic

36. Based on external outreach with stakeholders conducted by the IAIS, insurers with strong and effective governance frameworks were better placed to prevent, adapt and respond to, as well as recover and learn from, the operational disruptions presented by the pandemic. This takes into account that many of the decisions and actions taken by insurers during this period were mandated by external parties such as governments (ie lockdowns and stay at home orders). Insurers with strong frameworks for facilitating the identification of and response to operational risks, benefitted from effective BCP activations, maintaining a sound framework to deliver and report on cyber resilience, and appropriately monitoring relationships with critical third parties.

37. External outreach further highlighted the benefits of committees within an insurer having representation from different areas of expertise across the organisation, which helped to promote a holistic approach to managing the operational disruptions presented by the pandemic.

3.1.2 Supervisory approaches

38. Many supervisory authorities currently seek assurance that insurers have sound governance frameworks and adequate Board and Senior Management oversight of resilience measures, as well as strategies to mitigate risks associated with operational disruption.[13] In this context, supervisory authorities obtain information (all or in part) from entities to aid their understanding of whether:

    - The Board and Senior Management have the appropriate knowledge, skills, experience and responsibilities to address threats to the insurer's operational resilience;
    - Roles and responsibilities regarding the management of operational disruptions are sufficiently clear and documented;
    - Resources, financial and non-financial, are appropriately allocated to support the operational resilience approach;
    - Functional groups within an entity share a coherent understanding and articulation of the entity's approach to operational resilience, including understanding their roles and responsibilities and how their work or actions interact and impact one another;
    - Risk mitigation strategies and measures put in place by insurers in the event that IT third-party outsourcing vendors cannot deliver during disruptions are adequate;
    - Governance processes include proper documentation and appropriate levels of approval; and
    - Documentation of operational resilience processes are regularly reviewed and updated.

3.2 Information collection and sharing

39. An important input for insurance supervisors when devising an effective supervisory strategy with respect to operational resilience oversight is having access to a range of information, including on an entity's operational resilience framework and the potential threats impacting the insurance sector.

40. 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. Maintaining an open and constructive communication channel can also aid both supervisors' and insurers' understanding of emerging issues of potential concern related to operational resilience.

41. 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. Cyber threats, for example, have evolved and attacks now frequently span multiple jurisdictions, sectors and industries, with implications for the operational resilience of insurers. As the International Monetary Fund (IMF) has noted "[a]ttackers show a degree of agility in cooperation across borders that authorities find difficult to match."[14]

3.2.1 Lessons learnt from the pandemic

42. The pandemic demonstrated the importance of effective information sharing and public/private cooperation to support an entity's operational resilience. For example, in the early days of the

[13] The following is taken from a May 2022 information gathering exercise among ORTF members.

[14] IMF Staff Discussion Note (2020) Cyber Risk and Financial Stability: It's a Small World After All, p. 8

pandemic some supervisory authorities benefited from frequent updates from insurers regarding the number of staff working remotely, service availability metrics, and any changes in internal control frameworks that were seen as useful to mitigating growing risks associated with the pandemic. In turn, in some cases supervisors were able to share information on approaches being considered across the insurance sector to help manage mounting operational risks during the pandemic.

3.2.2 Supervisory approaches

43. In some jurisdictions, regular forums for timely and ongoing exchanges of information on operational resilience have been put in place. These forums allow discussions on the current landscape, sources of risks or threats, mitigating strategies and measures, incidents that have occurred and lessons learnt. Various approaches are taken depending on whether participation is limited to only supervisory authorities or is inclusive of the insurance sector. Such information sharing forums in some cases also provide a platform for exploring solutions to skills gaps/training needs, as well as on how technology could be used in detection and information dissemination to better facilitate communication and coordination, in particular during crisis situations.

Examples of forums that have been created to encourage information sharing on operational resilience:

German Federal Financial Supervisory Authority (BaFin)

BaFin has in place a committee that provides a platform for information exchange. It consists of a panel of experts, including representatives of supervisory authorities, companies and related associations. The committee supports the industry in the implementation of VAIT (the Supervisory requirements for IT in insurance undertakings put forward by BaFin, including topics relevant to cyber security) and this platform is further used to discuss results from supervisory audits on a no-name basis.

UK Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA)

A Cross Market Operational Resilience Group (CMORG) is in place and leads sector-wide collective action on operational resilience. The group is made up of approximately 25 members, across the retail, wholesale, Financial Market Infrastructures (FMIs), and insurance industries, as well as financial authorities and the National Cyber Security Centre. It is co-chaired by senior executives of the PRA and UK Finance. CMORG has three core objectives. These are to:

- Identify risks to the resilience of the financial sector;
- Develop solutions to improve the operational resilience of the sector; and,
- Share knowledge.

CMORG is supported by specialist sub-groups. These sub-groups design, manage, and deliver operational resilience improvements for the sector. The work undertaken by these groups is voluntary. Sub-group chairs meet regularly to discuss CMORG's activities and identify areas that could benefit from further collaboration.

44. In addition, some authorities require insurers to disclose publicly or report to the supervisor directly updates on matters impacting their operational resilience. On the basis of such reporting, some supervisory authorities publish current state, findings, and thematic review reports as well as best practices relevant to operational resilience in the insurance sector.

45. With respect to supervisory frameworks on operational resilience, supervisors may collect a range of information, including:

- An insurer's framework and methodology to identify key operational functions, business services and lines of business, including the entity's assessment of the potential impacts of severe but plausible scenarios on tolerance limits;
- Dependencies that an insurer has on external parties including potential impacts to its operations in the event of third-party service disruptions;
- An entity's assessment of the feasibility, operational impacts and costs of switching critical services to an alternate vendor, as well as challenges anticipated;
- Operational incidents (including cyber incidents) that have occurred and lessons learnt;
- Assessments of the operational impact a disruption may have on the insurer including the identification of vulnerabilities and an insurer's testing/self-assessment of its ability to remain within its impact tolerance limits;
- Constitution of teams responsible for restoration activities and the time within which critical operations could be restored vis-à-vis a range of severe but plausible scenarios;
- Reports on training delivered in relation to operational resilience best practices, and in particular on expectations, and roles and responsibilities during periods of sub-optimal functioning;
- Reports on joint BCP testing/assessment conducted by the insurer and its third-party service providers; and
- Processes for reporting/escalating potential risks and issues on operational resilience to the Board and Senior Management, where relevant.

46. Though the benefits of information sharing on operational resilience among insurance supervisory authorities, within the sector, and among authorities and insurers are well known, such initiatives nevertheless appear to be limited at present. In this regard, supervisory colleges could provide a framework for supervisory cooperation and information sharing. Examples of potential barriers identified by the IAIS to effective information sharing include:

    - The absence of a common taxonomy, which can make it difficult for supervisors to communicate effectively across jurisdictions, and can also make it difficult to gain a consolidated view on operational resilience trends, gaps and opportunities;
    - Concerns on data protection and privacy laws (such as those in place to protect customers) that limit or prevent the sharing of information beyond an entity or jurisdiction;
    - The complexity and cost of organising and implementing formal cross border information sharing exercises;
    - The inability of supervisory authorities to obtain/share relevant information due to their legal mandate; and
    - Hesitancy of insurers to share information with supervisors because of concerns or the perception that the information could contribute to an additional scrutiny of the company's controls or an increased legal risk.

3.3 Cyber resilience

47. The insurance sector is heavily dependent on the use of digital technologies, and this reliance accelerated during the pandemic as entities transitioned to remote working. This has in turn increased the focus on entity's having in place sound frameworks for delivering on cyber resilience that can withstand and react to increasing cyber risks.

48. The FSB defines cyber resilience as "The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.".[15] Over recent years international, national and industry organisations, both public and private sector, have developed and published multiple frameworks and guidance that relate to cyber resilience, resulting in the emergence of a general consensus around the principles of an effective cyber resilience regime..[16] In 2018 the IAIS published an Application Paper on the supervision of insurer cyber security that builds upon the G-7 Fundamental Elements of Cyber Security for the Financial Sector..[17] This Application Paper puts forward building blocks for an entity to design and implement its cybersecurity strategy and operating framework.

49. A key issue for supervisors is how to gain comfort – in a proportionate and resource effective way – that the framework established by the insurer to deliver on cyber resilience is effective and robust. A particular challenge is that because cyber risks are continually evolving and growing, the forward-looking implications of potential threats to an entity/sector's cyber resilience are difficult to quantify in a structured manner, and as such widely agreed, standardised, forward-looking metrics are not fully developed. This presents challenges to a supervisor's ability to benchmark an entity's vulnerabilities to possible future disruptions stemming from cyber-attacks.

50. Direct engagement held with external experts from the insurance industry revealed that while it would not be appropriate to prescribe a 'one size fits all' approach to the supervision of cyber resilience, greater supervisory coordination could be beneficial. In particular, participants noted that a lack of mutual recognition of cyber resilience testing requirements can contribute to duplicative or inconsistent requirements for internationally active insurers.

51. Moreover, inconsistencies in approaches to evaluating an insurer's framework for delivering on cyber resilience could contribute to cyber vulnerabilities remaining undetected, threatening the stability and integrity of an insurer and bringing with it a risk of contagion to the wider financial sector. In the absence of greater consensus around best practices for assessing an insurer's cyber resilience, the mutual recognition of approaches and information sharing between supervisory authorities remains difficult. Some progress has been made in this respect, such as the Threat Intelligence Based Ethical Red Teaming (TIBER) framework in the EU (see section 3.3.2).

52. The following sets out in further detail two key challenges supervisors face when assessing the quality of the framework established by the insurer to deliver on cyber resilience.

3.3.1 Consistency of approaches for assessing cyber resilience

53. A key challenge for supervisors is to identify the most effective supervisory tools and approaches to cyber resilience monitoring that can keep pace with both the changing nature of cyber-attacks and the speed with which entities are adopting new technologies. Some of the most commonly used supervisory techniques, such as forms of testing and audit, provide a valuable snapshot of

[15] FSB (2018), Cyber Lexicon

[16] FSB (2017), Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices

[17] See G-7 Fundamental elements of cybersecurity in the financial sector and Fundamental elements for effective assessment of cybersecurity in the financial sector.

an insurer's cyber resilience at a particular point in time. However, it is challenging for supervisors to ensure that evolving and emerging cybersecurity considerations are fully integrated in all of an entity's processes and embedded in its overall information and communications technology (ICT) lifecycle.

54. At present, supervisors deploy a range of approaches with respect to monitoring. For example, supervisors may ask insurers to regularly perform in-house cyber security tests, assessments or audits, often on an annual basis. This may include an analysis of the effectiveness of the insurer's framework for delivering on cyber resilience, the systems and controls, as well as the availability of the skilled resources required to support key functions, business services and lines of business. Insurers may further be asked to report the results of these assessments to the supervisor and rectify any vulnerabilities or errors identified.

55. Having a consistent approach to assessing insurers' cyber resilience can be helpful especially when insurers are engaging third-party service providers that operate across jurisdictions (eg cloud). Some examples of supervisory approaches to assessing an insurer's cyber resilience include the analysis of reported incidents, questionnaires, on-site inspections and on-going supervisory engagement. The Bank for International Settlements (BIS) has identified that these practices "rarely produce quantitative metrics or risk indicators comparable to those available for financial risks, eg standardised quantitative metrics."[18]

56. Although limited, where quantitative metrics do currently exist authorities note that they can be helpful in assessing parts of an insurer's framework for delivering on cyber resilience. Metrics and data may assist supervisors in understanding inherent and residual risk, maturity of risk management frameworks, and identification of potential risks arising from concentration. Work in some jurisdictions is being undertaken to develop more metrics, including forward-looking indicators, with the possibility of leveraging progress having been made in other sectors. Commonly available metrics include:

- Availability – measured as percentage of time in a month a service/software is available for use (ie, 99.9% of monthly availability).
- Recovery Time Objective (RTO) – refers to the maximum acceptable delay between the interruption of service and restoration of service. This determines the acceptable timeframe for service unavailability.
- Recovery Point Objective (RPO) – refers to the maximum acceptable time since the last data recovery point. This determines the acceptable loss of data between the last recovery point and the interruption of service.

3.3.2 Resourcing cyber expertise

57. Many supervisory authorities face challenges to developing cyber resilience oversight programmes due to a skills gap. The skills required to assess cyber resilience are in high demand and there are significant shortages of appropriately qualified staff. This is compounded by the fact that within the cyber resilience field there are specific areas of specialisation that necessitate unique skills and experience and the demand for these specialised skills is outpacing supply.

58. A report on cyber security skills in the UK labour market estimates that a "high proportion of UK businesses continue to lack staff with the technical skills, incident response skills and governance skills needed to manage their cyber security".[19] This highlights that supervisory

[18] BCBS (2018), Cyber resilience: Range of practices

[19] Ipsos report (publishing.service.gov.uk)

authorities and companies alike are competing for skilled staff across sectors which intensifies the difficulty of attracting and retaining specialists.

59. One consequence of skills shortages is that the advancement of supervisory frameworks over cyber resilience may lag the growing sophistication of cyber-attacks. Supervisory authorities note that they have deployed a variety of tools to improve the recruitment and retention of cyber specialists, including deploying internal training of existing staff, the creation of accreditation programmes and encouraging knowledge sharing across national cybersecurity authorities.

3.3.3 Lessons learnt from the pandemic

60. The dynamic nature of cyber risk was brought to the forefront during the pandemic. Many jurisdictions saw significant growth in the use of sophisticated and aggressive ransomware attacks. At the same time, the increased use of remote access technologies to facilitate remote working exposed new vulnerabilities to IT systems. This threat was exacerbated by the fact that facilitating remote working necessitated rapid, large-scale IT transformation programmes by insurers. Such transformations can themselves be a source of disruption. Large and complex transitions from legacy IT systems to new technologies inevitably increase the attack surface and therefore, if managed poorly and without sufficient testing, are likely to increase an insurer's exposure to cyber risk. On the basis of feedback from consultations with external experts, many experts agreed that it is likely that the complexity of cyber-attacks will increase going forward as threat actors leverage new forms of technology, such as artificial intelligence, to exploit an entity's vulnerabilities.

Example of a systemic cyber-attack: Log4j vulnerability

Log4j is an open-source logging library used by applications and services across the internet. A recently discovered vulnerability in Log4j could, if left unfixed by insurers in their supply chain, let cyber criminals or hackers break into systems, steal passwords and logins, extract data, and infect networks with malicious software. US and European authorities, in addition to other jurisdictions, have recently addressed this challenging threat. The US Cybersecurity & Infrastructure Security Agency widely distributed information to help companies respond to the event including tools for risk mitigation and links to utilities to aid in identifying the vulnerability within company networks. At the European level, the potential spill over effects of this failure were deemed sufficiently important to organise coordinated exchanges of information between different authorities.

3.3.4 Supervisory approaches

61. Some examples of approaches taken by IAIS jurisdictions to improve cyber resilience are outlined below:

> *European Union (EU) TIBER-EU 2018*
>
> Within the European Union, a Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) framework has been developed. Each country enacts its own implementation based on the TIBER-EU guidelines. Various EU countries have so far implemented the TIBER framework. TIBER-EU and its national implementation helps to ensure coordination and mutual recognition of testing requirements. In addition, the EU Digital Operational Resilience Act (DORA) aims to establish European shared principles for IT operational resilience testing.
>
> *UK CBEST*
>
> UK CBEST provides a framework for regulators to work with entities using a simulated cyber-attack. This enables entities to explore the implications of an attack on the people, processes and technology of an entity's cyber security controls. The aim of CBEST is to test an entity's defences, assess its threat intelligence capability and assess its ability to detect and respond to a range of externally and internally initiated cyber-attack. The UK authorities base the simulated attacks on current cyber threats. These include the approach a threat actor may take to attack an entity and how they might exploit an entity's online information. An accredited service provider carries out the simulation, acting within legal, ethical and moral constraints. The objective of the exercise is to assess if the confidentiality, integrity and/or availability of systems and processes that deliver an entity's important business services can be compromised.
>
> *Tabletop Exercises*
>
> Working with US state and federal supervisors, law enforcement agencies, and other officials, under the auspices of the Treasury Department's "Hamilton" programme, the National Association of Insurance Commissioners (NAIC) facilitates tabletop exercises with insurers and supervisors to explore cyber incident response and recovery back. This aims to enhance cyber response programmes of insurers and supervisors by discussing key methods supporting pre-emptive and/or reactive responses to potential threats. These exercises are a useful means for supervisors and the insurance industry to test their ability to respond effectively to these incidents. The exercises follow a cybersecurity event (ie ransomware, insider threat, etc.) and result in dialogue among attendees about the possible repercussions from a cyber incident on impacted institutions as well as the greater insurance sector as the event progresses. These exercises help stakeholders clarify expectations for communications as events occur and allow supervisors the opportunity to emphasise the importance of selected risk mitigation practices.

62. In addition, the following tools and techniques (in isolation or combination) for assessing the quality of an insurer's framework to deliver on cyber resilience have been used by supervisors:

    - Self-assessment Questionnaires – involves insurer's performing self-assessments of the quality of their framework to deliver on cyber resilience, the responses to which provide a snapshot of the entity's cyber resilience capabilities and vulnerabilities.
    - Vulnerability Assessments – aim to identify and assess security vulnerabilities in systems and processes via automated scans that check for exploitable known vulnerabilities, culminating in a a report on risk exposure. The frequency of testing can vary depending

on the nature of systems and processes in question, though tests are generally performed on a regular basis (may be conducted as on or offsite assessments).

- Cyber Incident Reporting – reporting of micro-level data to a supervisory authority can assist in building a picture of broader systemic threats, particularly when reporting requirements are standardised.
- Scenario-Based Testing – tests an entity’s cyber resilience against a range of scenarios, including simulations of severe but plausible cyber-attacks. This helps entities to challenge the assumptions built into their detection, response and recovery practices, and associated governance arrangements and communication plans. Scenario-based tests can take the form of tabletop exercises or simulations.
- Red Team Tests – involve entities challenging their internal and external dependencies through the use of red teams to introduce an adversary’s perspective in a controlled setting. Red teams serve to test possible vulnerabilities and the effectiveness of the entity’s mitigating controls. A red team may consist of an insurer’s own employees and/or outside experts, who are in either case independent of the function being tested.
- Threat Led Penetration Tests – defined by the G-7 as “a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity’s people, processes and technology, with minimal foreknowledge and impact on operations.”[20]

3.4 IT third-party outsourcing

63. Many regulatory frameworks include specific requirements for financial institutions to identify operational risks associated with the outsourcing of business processes or functions. Consequently, applicable risk management processes have generally been implemented by insurers. However, an area where both supervisory requirements and financial institutions' risk management processes remain less advanced is the ongoing management of risks arising from concentration associated with the provision of critical IT services to companies by third-party service providers.

64. Risks arising from concentration can occur at several different levels:
    - Across the insurance or wider financial services sector of one or more jurisdictions, with many institutions using one single or a few service providers for specific services;
    - Within larger insurance legal entities or groups, where multiple entities or functions are dependent on services provided by the same or a few internal or external service providers;
    - At subcontractors used by third-party service providers; and/or
    - At the global or regional level, where many third-party service providers and/or subcontractors are located.

65. Depending on the scale, type and criticality of third-party services, there may be the theoretical possibility that risks arising from concentration could become systemic, and as such, it is

[20] G-7, Fundamental Elements for Threat-Led Penetration Testing

important to advance supervisory frameworks and practices, as well as financial institutions' management of third-party risks arising from concentration.

66. Often third-party service providers operate around the globe and across different sectors. Addressing risks arising from concentration stemming from these third-party service providers would require a coordinated approach between the industry and supervisors from multiple countries and third-party service providers.

67. The increasing complexity of the financial (including the insurance) sector, in particular with respect to the use of technology, has increased third-party risks arising from concentration over the past few years, including during the pandemic.[21] Also evident in the past few years is an increase in the use of non-regulated subcontractors and a growing dependence on complex supply chains to deliver critical services, which has the potential to move risk outside the regulatory perimeter.[22]

68. Benefits of using third-party services include faster innovation, improved customer outcomes, reduced costs, scalability, and improved operational resilience. These benefits should nevertheless be weighed against the risks that outsourcing of critical services present to individual insurers, the wider market, and financial stability at large. That said, as risks arising from concentration frequently come about due to a lack of competition and substitutability in the market, insurers may have limited capability to address the nature of this risk in isolation.[23]

69. The use of the cloud is an example of a third-party IT service that may present risks arising from concentration at the individual entity, sector and global level.[24] Disruptions at, or inappropriate access to information stored on, the cloud could result in broad system disruptions across the industry. Other examples of third-party services often used by insurers that may present risks arising from concentration include processes for annuities payroll and benefits administration, investment management, claims processing and resolving customer queries. Claims management and loss adjusting processes are also typical non-IT examples where risks arising from concentration reside due to the level of expertise required to provide these services.

3.4.1 *Lessons learnt from the pandemic*

70. The insurance sector’s response to the pandemic highlighted how third-party service providers and outsourcers can contribute to the improved resilience of institutions. The ability to transition to remote working in an effective and timely manner was, in many instances, enabled by IT service providers. These providers also contributed to financial institutions’ ability to deliver services to consumers and support other sectors of the wider economy.

71. The pandemic also stimulated advances in insurers’ digital transformation plans. It was often seen that third parties had the capability of offering technology solutions that are more secure, resilient, and flexible than financial institutions’ own existing technology solutions, which sometimes rely on legacy systems.

72. That said, the pandemic also highlighted risks associated with geographic concentrations. This was associated with entities having in place numerous arrangements in the same geographic area, resulting in a dependence on one or a few providers in that area for the delivery of services. Such situations may apply in particular to large insurance groups with service centres in low-cost jurisdictions.

[21] FSB (2020), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships.

[22] See, for example, Ernst and Young (2021), How insurers can transform by adopting public cloud.

[23] See, for example, Accenture (2019), Five benefits of cloud for insurance.

[24] U.S. Department of Treasury, The Financial Services Sector's Adoption of Cloud Services section 6.4 (treasury.gov)

3.4.2 Supervisory approaches

73. Requirements to consider risks arising from concentration vary among jurisdictions. While in most cases insurers are required to consider risks arising from concentration during their initial selection of service providers, fewer are required to consider this risk during the ongoing monitoring and risk assessment processes.

74. Existing financial supervisory frameworks have inherent limitations with respect to identifying and managing the potential systemic risks posed by third parties and outsourcers, in that a single entity has a limited visibility over services offered by the same third-party provider to multiple financial institutions across multiple jurisdictions. This may be aggravated by the limited influence a single financial institution has on large, dominant service providers. Such limitations have further implications to an insurer's ability to mitigate risks to its cyber resilience and BCM that originate within the outsourced service provider.

75. Moreover, as some third-party service providers remain outside the regulatory perimeter, the supervisory authority's ability to directly monitor and manage the resilience of services provided to insurers is limited as well.

76. Traditional supervisory approaches rely on supervisory authorities defining requirements and expectations of insurers with respect to managing risks related to third-party services and outsourcing. However, individual entities have inherent limitations in their ability to effectively assess and manage systemic risks arising from concentration and with some service providers remaining outside the regulatory perimeter, the influence of supervisory authorities is also limited.

77. Many supervisory authorities require or are planning to require insurers to provide information on services outsourced to third parties. Such information collections could allow supervisory authorities to better identify risks arising from concentration in the future, eg as information collection exercises advance. That said, improvements are needed in the consistency of reporting definitions and requirements to make the information collected more useable. 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.

78. Risks arising from concentration can also be partially addressed through novel risk management practices, such as the adoption of multi-cloud / multi-vendor approach and exit / portability strategies. Notwithstanding, there may be costs and operational complexities associated with the adoption of such solutions.

3.5 Business continuity management

79. The insurance sector is composed of a multitude of interconnections and interdependencies between various systems, participants, and service providers. An operational disruption, degradation or interruption in the activities of an insurer or any of its service providers could jeopardise its ability to meet its commitments to its insureds and other partners. Given these interconnections and interdependencies as well as the complex functioning of the sector, it is imperative that insurers adopt sound and prudent management practices to ensure business continuity in the event of an operational incident.

80. BCM starts by the identification of major operational events likely to pose a threat to the critical activities of an insurer, such as natural disasters, power outages, telecommunications failures, computer malfunctions, data breaches, terrorism and pandemics, to name a few. The identification process is an important first step towards ensuring that an insurer can assess the impact of operational incidents on the entity's operations, and to implement the necessary mitigation measures to ensure the continuity of critical business activities.

81. A sound BCM framework generally includes an established business continuity plan, dedicated and competent people with clear responsibilities and various management processes relating to planning, implementation, testing, performance assessment, review and ongoing improvement. On the basis of its plan, insurers respond to a disruption, and resume and/or restore the delivery or provision of products and services. Actions taken should be consistent with an entity's business continuity objectives and the amount and type of risks that the insurer may or may not accept following a disruption.

82. A sound BCM framework helps the insurer ensure that it has the capability to operate during disruptions. It allows the insurer to contribute to the achievement of its strategic objectives and protects and strengthens its credibility and reputation. It improves the ability to remain effective during disruptions and helps to reduce the direct and indirect costs of disruptions while taking into consideration the expectations of interested parties, building their confidence in its ability to succeed.

83. Best practices for BCM have evolved in line with changing operating environments, as well as in response to the pandemic. The following aspects of BCM are identified as challenges that could benefit from further analysis by the IAIS and/or cooperation amongst supervisory authorities:

Integration of BCM and risk management

84. In a world of increased operational disruption, the concept of operational resilience has emerged as a key outcome of effective risk management. As a result, the focus has shifted from the establishment of sound BCM to the integration of BCM practices in other relevant risk management practices and alignment to an institution's overall operational resilience. For example, there may be value in exploring how insurers may need to consider BCM in the context of their critical operations and all key internal/external dependencies (including third parties' BCPs). The linkages between BCM and overall operational resilience, as well as third-party risk management, could allow insurers to derive additional benefits from their BCM frameworks. Where BCM frameworks are siloed in nature, this is arguably an inhibitor to business continuity, particularly in respect of IT services provided by third parties and/or outsourcing arrangements.

Enhanced scope and testing of BCM frameworks

85. There may also be value in exploring how BCM could be extended to encompass a wider range of events and business operations than have previously been contemplated. For example, the need to consider availability in BCPs could be extended to consider the consequences of loss of confidentiality and integrity of information for critical business services when business impact analysis (BIA) and risk assessment are performed (information security/cyber preparedness could be integrated into broader BCM and enterprise risk management (ERM)). BCPs could also consider how the insurer would handle the loss of a significant number of employees or key personnel.

BCM adaptations in a "new normal"

86. Before the pandemic, the business continuity strategies of most institutions focused on addressing short-term impact scenarios. Continuity assumptions that proved inadequate during the pandemic have led to a review of the criticality of some existing processes and the adoption of different time frames (eg immediate, short, medium and long term) in many operational continuity strategies, depending on the results of their BIA and the needs and resources of each insurer. According to the IMF "[f]inancial regulators and firms need to shift their focus from classic business continuity and disaster recovery planning, to delivering critical services even when attacks disrupt normal operations. Resilience requires buy-in from the top leaders of companies and financial regulators and their board members. Firms need to prepare for severe but plausible

incidents that can have a systemic impact. Supervisors should require the industry to consider such adverse scenarios and test their contingency plans both individually and collectively."[25]

87. Although hybrid work arrangements might become more permanent features, in practice remote working policies may vary significantly. Some institutions may consider arrangements that limit the amount of time staff can work from home for various reasons. Possible adjustments to labour contracts could be foreseen, depending on the work arrangement that will eventually be implemented, in order to comply with a jurisdiction's legal framework.

88. This raises the question of whether existing (prepared pre-pandemic) or recently revised BCPs remain fit for purpose or require significant additional revisions. Thus, there could be value in exploring how supervisors can reflect on how the risks that have emerged from changes made to business continuity strategies can best be managed, and whether insurers have implemented procedures to identify, analyse and aggregate these risks while new working arrangements continue to evolve.

3.5.1 Lessons learnt from the pandemic

89. The following developments over the past few years have contributed to elevating the importance of insurers having in place a sound BCM framework:

    - Digital transformations within insurers and across the sector, with resulting changes to an insurer's critical activities and processes;
    - The "redesigned" workplace, in which many employees are working from home, working from "anywhere", or working in a hybrid (combination of home and office) environment;
    - Shift from a short-term focus on temporary disruptions to the consideration of business resilience over various time frames (eg immediate, short, medium and long term);
    - Growing customer expectations in relation to the time to recovery and level of recovery, and in terms of effective communication from insurers – ie when a disruption occurs, progress in recovering, and mitigation measures to ensure they can still get serviced and notification of when services are restored;
    - The use of multiple third parties and subcontractors, each with their own level of cyber/business continuity risks as well as diverse BCM frameworks; and
    - An increasing number of vulnerabilities, including vulnerabilities to cyber-attacks.

90. Based on directed consultations with external experts, while these developments coincided with the timing of the pandemic, these themes also existed pre-pandemic. Nevertheless, it was generally acknowledged that many of these developments grew in importance more rapidly due to the pandemic experience.

3.5.2 Supervisory approaches

91. Supervisors are taking action to address the changed risk environment in relation to BCM. Policy and/or supervisory work (including on and off-site examinations) have focused on a range of areas, including, but not limited to:

    - Improvements to BCPs based on risks that arose during the pandemic and as insurers pivot towards a hybrid work environment;

[25] IMF (2022), Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards (imf.org)

- The importance of support from the Board and Senior Management to set the tone at the top, set the strategic direction with regards to BCM and its implications for operational resilience, and establish risk tolerance statements;
- Integration of the BCM system requirements across business functions to identify business continuity risks associated with interconnected functions and to minimise silos;
- Increasing the breadth and frequency of vulnerabilities assessments to help ensure a thorough knowledge of critical business services and the relevant interconnections between strategic investment decisions and everyday operations;
- Robust periodic testing of BCPs, including data backup, using severe but plausible scenarios, disaster recovery frameworks and incorporating lessons learnt from test results;
- Appropriate communications and crisis management capabilities;
- Extension of expectations for BCM to outsourcing solutions at insurance companies;
- Regular review of the entire BCM process, to ensure that it is a dynamic risk management tool; and
- Regular touchpoints with entities to discuss ongoing developments/risks relating to BCM.

4 Summary of observations and potential future areas of IAIS focus

92. The following section summarises a number of key aspects of the risks related to cyber resilience, IT third-party outsourcing and BCM – based on observations made in the paper – and outlines various topics that may benefit from future consideration or further analysis by the IAIS and insurance supervisors.

Information sharing

93. Facilitating mechanisms for sharing information, or leveraging existing information sharing mechanisms, may provide new insights for the insurance sector and insurance supervisors on emerging risks and inform the development of mitigation strategies and measures, including an improved ability to detect and respond to operational incidents and systemic risks on a collective basis. This could include information sharing on best practices across the spectrum of issues related to cyber resilience, IT third-party outsourcing and BCM. There may be existing IAIS mechanisms for information sharing that could be leveraged for this purpose.

94. To facilitate information sharing among insurers, supervisors and throughout the insurance sector more widely, it could be helpful to explore how definitions and terminologies relevant to operational resilience could be better aligned. This could help minimise the unintentional use of the same terms to refer to different concepts or the use of different terms. This may also support jurisdictions in developing a more consistent approach to discussing and understanding relevant issues.

95. The remainder of this section provides concrete examples of key topics that may benefit from further information sharing and consideration, for each of the areas of cyber resilience, IT third-party outsourcing and BCM.

Cyber resilience

96. Based on the observations outlined in section 3.3, areas related to cyber resilience that may benefit from further consideration include:

    - 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. This could also usefully extend to sharing information on practices and developments with respect to insurance sector cyber incident reporting. Such sharing of information could assist the insurance sector in keeping up to date on the fast-changing cyber risk landscape, such as the latest approaches used by threat actors and emerging technologies or tools that facilitate timely detection of and response to cyber risk incidents.

    - Analysis of the impact on cyber resilience of large scale IT transformations as insurers make increasing use of new technologies, such as cloud computing.

    - Developing proactive, consistent and proportionate approaches to the development, supervisory evaluation, and implementation of an insurer's framework to deliver on cyber resilience, as well as approaches for insurers to escalate cyber incidents to the insurance supervisor. The latter could leverage the work of the FSB on Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence,[26] with additional considerations for the insurance sector. This suggestion may also be consistent with the European Systemic Risk Board's (ESRB) call for the creation of a dedicated mechanism to coordinate national responses to cyber incidents.[27]

IT third-party outsourcing

97. Based on the observations outlined in section 3.4, areas that may benefit from further consideration include:

    - Aligning, to the extent possible, reporting definitions and requirements for terms relevant to IT third-party outsourcing (eg such as critical services, outsourcing, third parties etc) with the aim of improving international cooperation among supervisors in the identification of cross-border risks arising from concentration.[28]

    - Exchanging information on practices and methodologies used by supervisors, including:

        – Implications of risks arising from concentration on cyber resilience and BCM frameworks, in particular, with respect to recovery activities. This is particularly important to mitigate the potential impact of incidents originating within a widely used service provider, which have the potential to disrupt the ability of multiple insurers to continue business and service to their customers and other stakeholders.

        – Supervisory approaches to developing catalogues of third-party service providers in each jurisdiction to help identify critical third parties used widely across the industry;

[26] FSB (2021), Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence

[27] ESRB (2022), Mitigating systemic cyber risk

[28] FSB (2020), Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion paper: the IAIS is engaged with the FSB's ongoing cross-sector work in this area

   - Approaches to shifts in focus from managing "IT third-party risk and outsourcing" to considering overall systemic dependencies and risks created by any outsourcing and third-party arrangements (dependency management);
   - Guiding principles for identifying what constitutes a critical activity (and those activities that could become critical) and identifying the users of such activities to enable mapping of interconnections and interdependencies of services and resources. The development of such mapping exercises is currently being discussed amongst supervisory authorities in some jurisdictions; and
- Exploring the implications of larger insurers considering a multi-vendor strategy and the implementation of data portability arrangements and environments across providers. However, it is recognised that these are complex and costly tools, in particular for smaller entities.

Business continuity management

98. The ICPs set out high level principles supporting processes and activities associated with ensuring an insurers' business resilience, which broadly support sound BCM. It may nevertheless be helpful to draw out the links between business resilience and BCM, to help ensure it is understood that the concept of BCM extends to considerations beyond short-term disruptions.
99. There may also be value in exchanging information on best practices and methodologies used by supervisors, including:
    - How the sector is approaching evolutions in BCM best practices, in particular in relation to the need to continue to integrate BCM with other relevant risk management functions to remove silos and ensure that BCM frameworks consider the implications of disruptions stemming from cyber and IT third-party outsourcing risks;
    - The scope of BCM, which could be extended to a wider range of events and business operations than have been contemplated in the past. Expanded sets of scenarios and stakeholders could also be considered within the scope of robust and regular business continuity exercises and testing, to demonstrate the ability of an entity to withstand severe but plausible disruptions; and
    - How existing (prepared pre-pandemic) 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.

Annex 1: Main insights from stocktake of SSB publications

The IAIS conducted a stocktake of existing SSB publications, with the aim of understanding the current landscape with respect to available standards and supporting materials relevant to operational resilience. A bibliography follows this annex, which provides the range of publications reviewed. The following elaborates on the main lessons learnt from the stocktake with respect to cyber resilience, IT third-party outsourcing and BCM.

Cyber resilience

1. Cybersecurity risks are growing, and cyber incidents can harm an insurer's ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence.
2. An insurer's cybersecurity framework should support and promote both its operational security and the protection of policyholder data (eg the ability to maintain and promote the insurer's ability to anticipate, detect, withstand, contain, and recover from cybersecurity incidents).
3. Multiple international, national and industry organisations, both public and private sector, have developed cybersecurity frameworks and guidance that have relevance to insurance supervision, and while there are benefits to consistency, a one size fits all approach would not address the unique complexities that exist across different geographies, business structures, supervisory approaches etc.
4. The significance of the risks third parties pose to the insurer is not necessarily proportionate to the criticality of their business relationship with the insurer. An insurer should identify the cyber risks that it bears from and poses to third parties.

IT third-party outsourcing

5. Assessments of risks arising from concentration in cloud computing are at an early stage and supervisors'' expectations on insurers' use of cloud computing could benefit from clarification and cross-border cooperation. This raises further questions on whether current multilateral MoUs are fit for purpose in an age where cross-border outsourcing and cloud outsourcing are becoming more commonplace.
6. Sub-contracting of outsourced activities (fourth party risk) are on the rise presenting similar risks to those associated with IT third-party outsourcing.
7. The role of supervisors in specifying the governing law that applies to contracts covering material outsourcing arrangements and how supervisors can usefully contribute to ensuring that an insurer's control functions are adequate in relation to outsourced activities could benefit from further clarification.
8. The interaction between data protection legislation and financial supervision, in particular in relation to cross-border and IT third-party outsourcing could benefit from further discussion and articulation.

Business continuity management

9. The pandemic exposed areas where traditional disaster recovery plans failed and identified new opportunities and challenges. It further demonstrated the need to integrate digital security preparedness into broader ERM and BCM.

10. Current BCM approaches could benefit from focusing on at least the following elements: infrastructure enhancements and security hardening for large-scale remote working; process development for physical access with appropriate restrictions in the workplace; and development and inclusion of external partnerships with respect to health sciences.

11. Business continuity exercises should be conducted under a range of severe plausible scenarios and support staff's operational resilience awareness.

12. Forums that facilitate the sharing of information on best practices would be beneficial in respect of systemic operational risks. This is in particular relevant to how an entity can assess and mitigate its vulnerabilities to threats to a critical IT third-party service providers' business continuity and disaster recovery mechanisms.

References

1. BIS Bulletin (2021), *Covid-19 and cyber risk in the financial sector*

2. BIS Representative Office for the Americas (2022), *Business continuity planning at central banks during and after the pandemic*

3. Bank of England, *Operational resilience of the financial sector*

4. BCBS (2018), *Cyber resilience: range of practices*

5. BCBS (2021) *Principles for operational resilience*

6. Carnegie Endowment for International Peace (2020), *International Strategy to Better Protect the Financial system Against Cyber Threats – Cybersecurity Workforces Challenges*

7. European Systemic Risk Board (ESRB) (2022), *Mitigating systemic cyber risk*

8. FSI Insights (2018), *Regulating and supervising the clouds: emerging prudential approaches for insurance companies*

9. FSB (2017), *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*

10. FSB (2018), *Cyber Lexicon*

11. FSB Discussion Paper (2020), *Regulatory and Supervisory Issues Relating to Outsourcing and Third*-Party Relationships

12. FSB (2021), *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence*

13. G-7, *Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector*

14. G-7, *Fundamental Elements of Cybersecurity in the Financial Sector*

15. G-7, *Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*

16. G-7, *Fundamental Elements for Threat-Led Penetration Testing*

17. IAIS Issues Paper (2016), *Cyber Risk to the Insurance Sector*

18. IAIS Application Paper (2018), *Supervision of Insurer Cybersecurity*

19. IAIS paper, Cyber Risk Underwriting (2020): *Identified Challenges and Supervisory Considerations for Sustainable Market Development*

20. IMF Staff Discussion Note (2020) *Cyber Risk and Financial Stability: It's a Small World After All*, Discussion Note No. SDN/20/07, December

21. IOSCO Consultative Document (2020), *Principles on Outsourcing*

22. ISO 27002 Information security controls (prevention)

23. ISO 27035 Information security incident management (after an incident)

24. OECD, *Risk and Resilience*

25. Sonicwall (2022), *2022 SonicWall Cyber Threat Report*

26. The Joint Forum (BCBS, IOSCO, IAIS) (2005), *Outsourcing in Financial Services*

27. The Joint Forum (BCBS, IOSCO, IAIS) (2006), *High-level principles for business continuity*

28. US Federal Reserve Bank (2020), *SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience*

29. World Economic Forum (2020), *Cyber resilience is critical for organizations' survival. Thoughtful reporting can help build it*

30. World Economic Forum (2020), *Cyber Resilience and Reporting*

31. World Economic Forum (2017), *Cyber Resilience Principles and Tools*