Regulatory developments in the global insurance sector

Vol. 34 (April to May 2023)

Disclaimer: Any opinions expressed in this paper are those of the authors, and not the official opinions of the Deloitte Tohmatsu Group.

Executive summary[1]

Region	No	Organisation(s)	Date	Regulatory developments
Global	1	Financial Stability Board (FSB)	13 April 2023	■ **The FSB finalised its recommendations on cyber incident reporting (CIR)**. The objective of these recommendations is to achieve greater convergence in CIR. The presented 16 recommendations include the following. ➢ Financial authorities (FAs) should have clearly defined objectives for incident reporting. ➢ FAs should identify common data requirements and, where appropriate, develop or adopt standardised formats to exchange incident reporting information. ➢ FAs should explore the benefits and implications of a range of reporting trigger options.
Europe	2	U.K. Prudential Regulation Authority (PRA)	2 May 2023	■ **The PRA published its business plan for 2023 to 2024**. Insurance-related priorities include the following. ➢ **Solvency II review**: A series of consultations on rule changes and expectations relating to, for example, internal model approvals, the range of assets eligible for Matching Adjustment and reductions in risk margin will be published, following the decisions enacted by Parliament. ➢ **Insurance stress testing**: A timeline for the next insurance test will be published in H2 2023. ➢ **Reinsurance risk**: Close attention continues to be paid to the impact of the high level of reinsurance of longevity risk in new annuity business and the emergence of complex 'funded reinsurance'.
	3	European Supervisory Authorities (ESAs)	25 April 2023	■ **The ESAs**, comprised of the European Banking Authority, European Insurance and Occupational Pensions Authority and European Securities and Markets Authority, **released a report on risks and vulnerabilities in the EU financial system**. Policy actions proposed in the report include the following. ➢ The broader impacts on financial institutions from i**ncreases in policy rates and sudden increases in risk premia** should be accounted for in risk management. ➢ Financial institutions are expected to put further effort into **ESG risk management**. ➢ Financial institutions should have adequate skills and capabilities to ensure **ICT security**.

[1] Volumes 1 to 12 of the report 'Regulatory developments in the global insurance sector' are available only in Japanese. This executive summary is a summary of the Japanese version of the Volume 34 report. It is advised that you refer to the respective original materials for accurate information.

	4	European Insurance and Occupational Pensions Authority (EIOPA)	24 April 2023	■ **The EIOPA, together with the European Central Bank (ECB), published a discussion paper on policy options to reduce the climate insurance protection gap for consultation**. The discussion paper sets out possible actions to tackle the insurance protection gap in four layers. These actions include the following. ➢ Layer 1 (low to moderate loss layers): Incentivise policyholders to implement ex-ante measures and reduce exposure to climate-related hazards through **impact underwriting**. ➢ Layer 2 (higher loss layers): Encourage (re)insurers to incorporate climate change considerations into the design and pricing of (re)insurance products by offering **long-term contracts.** Consider using cat bonds by which catastrophe risk can be transferred to a wider set of investors over multiple years. ➢ Layer 3 (national measures): Develop **a fiscal framework at a national level** to identify and account for the cost of natural disasters. ➢ Layer 4 (EU-level measures): Strengthen European fiscal components for natural disaster relief.
Americas	5	U.S. Board of Governors of the Federal Reserve System (FED)	28 April 2023	■ **The FED published a report on a failure of a U.S. bank in March 2023**. The report examines the factors that led to the failure of the bank in March 2023 and reviews the role of the Federal Reserve, the primary federal supervisor of the failed bank. Key takeaways from the examination and review include the following. ➢ The bank's board and management failed to manage the risks inherent in their business model and strategies. ➢ Supervisors did not fully appreciate the extent of the bank's vulnerabilities, which grew rapidly in size and complexity. ➢ When supervisors identified vulnerabilities, they did not take sufficient actions due to, for instance, a lack of clarity around internal governance processes.
	6	Canadian Office of the Superintendent of Financial Institutions (OSFI)	24 April 2023	■ **The OSFI finalised its guidelines on third-party risk management**, setting out six expected outcomes and 11 principles on governance, third-party risk management, special arrangements, technology and cyber risk. The 11 principles include the following. ➢ Financial institutions should **establish a third-party risk management framework** that defines clear accountabilities, responsibilities, policies and processes for identifying, managing, mitigating, monitoring and reporting on third-party risks. ➢ The financial institution's third-party arrangements should allow the financial institution timely

				access to accurate and comprehensive information to assist in overseeing third-party performance and risks. ➢ Both the financial institution and its third party should have documented processes in place to effectively identify, investigate, escalate, track and remediate incidents to maintain risk levels within the financial institution's risk appetite.
	7	Canadian Office of the Superintendent of Financial Institutions (OSFI)	21 April 2023	■ **The OSFI released its new framework on cyber resilience testing**, the 'Intelligence-led Cyber Resilience Testing (I-CRT) Framework'. I-CRT comprises a controlled threat assessment of financial institutions' cyber resilience. **The I-CRT framework applies to all Systemically Important Banks (SIBs) and Internationally Active Insurance Groups (IAIGs)**. For these entities, a regular assessment is conducted every three years. ■ The I-CRT process has four phases. Key action items in each respective phase are as follows. ➢ Initiation phase (6 to 8 weeks): A financial institution (FI) and the OSFI agree on a scope for the I-CRT activity. ➢ Threat Intelligence phase (6 to 10 weeks): A Threat Intelligence Service Provider (TIP) develops realistic cyber threat scenarios and the FI handles finalisation. ➢ Execution phase (8 to 12 weeks): A Red-Team Service Provider (RTP) conducts real invasive activities against the financial institution. The FI, the OSFI, the RTP and the TIP hold a workshop to review the outcome of the red team test. ➢ Closure phase (4 to 6 weeks): The FI finalises its remediation plan and the OSFI issues its recommendations.
	8	U.S. Financial Stability Oversight Council (FSOC)	21 April 2023	■ **The FSOC proposed new interpretative guidance on the designation of non-bank financial companies, together with a proposed analytic framework for financial stability risks, for public consultation**. Key differences between the current and newly proposed guidance include the following. ➢ The proposed guidance **eliminates** a statement from the 2019 guidance regarding **the use of an activities-based approach** prior to considering the designation of systemically important financial institutions. ➢ **Substantive analyses** required under the previous guidance **are not required** under the new guidance; rather, these analyses are described in the proposed analytic framework.

				➢ The proposed guidance does **not require the FSOC to conduct a cost-benefit analysis or an assessment of the likelihood of a financial institution's material financial distress** prior to making a determination.
Asia Pacific	9	Monetary Authority of Singapore (MAS)	25 April 2023	■ **The MAS released a consultation paper titled 'Enhancing safeguards for proper conduct of digital prospecting and marketing activities'**. Proposed requirements for financial institutions (FIs) with regard to digital marketing include the following. ➢ FIs should assess the specificities and limitations of digital media and address the risks associated with its use. ➢ FIs should provide clear guidance and proper training to their sales representatives. ➢ FIs should monitor digital prospecting and marketing activities conducted by their representatives.
	10	Australian Prudential Regulation Authority (APRA)	13 April 2023	■ **The APRA decided to postpone the effective date of the new regulatory standards on operational resilience to July 2025**. Other updates provided by the APRA on operational resilience standards include the following. ➢ The APRA will provide transitional arrangements for pre-existing contractual arrangements with third-party service providers. ➢ A final set of regulatory standards will be published in mid-2023.

Sources:

1. FSB ‘Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report’
2. PRA ‘Prudential Regulation Authority Business Plan 2023/24’
3. EIOPA ‘ESAs call for vigilance in the face of mounting financial risks’
4. EIOPA ‘EIOPA and ECB call for increased uptake of climate catastrophe insurance’
5. FRB ‘Federal Reserve Board announces the results from the review of the supervision and regulation of Silicon Valley Bank, led by Vice Chair for Supervision Barr’
6. OSFI ‘OSFI announces new guideline to manage third-party risk’
7. OSFI ‘OSFI releases new framework to strengthen financial institutions’ resilience to cyber-attacks’
8. FSOC ‘FSOC Issues for Public Comment Proposed Analytic Framework for Financial Stability Risks and Proposed Guidance on Nonbank Financial Company Determinations’
9. MAS ‘MAS Proposes Enhanced Safeguards for Prospecting and Marketing of Financial Products’
10. APRA ‘APRA provides an update on the implementation of new operational risk standard‘

Contact:

Shinya Kobayashi
Managing Director
Financial Services
Risk Advisory
Deloitte Touche Tohmatsu LLC

Deloitte.
デロイト トーマツ