Deloitte.
デロイト トーマツ

Regulatory developments in the global insurance sector

Vol. 64 (October to November 2025)

MAKING AN IMPACT THAT MATTERS since 1845

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 October 2025	■ **The FSB published a report on monitoring adoption of AI and related vulnerabilities in the financial sector that identifies a range of potential indicators to support monitoring of AI adoption and related vulnerabilities in the financial system**. These indicators include the following. ➢ For AI adoption: Inventories of AI use cases with breakdowns along relevant dimensions, such as financial activity, types of AI and levels of materiality ➢ For third-party dependencies and concentration: Share of financial institutions' AI applications made available by third parties and registers of critical AI services and service providers ➢ For cyber: Number of AI-related cyber attacks and number of third-party AI incidents
	2	Financial Stability Board (FSB)	10 October 2025	■ **The FSB published a report titled 'G20 Implementation Monitoring Review – Interim Report'** that outlines the implementation history of the main G20 financial reforms agreed to after the global financial crisis. ■ Key messages in the report include the following. ➢ While significant progress has been achieved in advancing the G20 financial reforms, recent trends indicate a worrisome slowdown in their implementation, which could weaken the financial system's capacity to withstand future shocks. ➢ If these trends persist, there is a growing risk of divergence between the expected level of implementation and what has actually been delivered. ➢ It is critical to avoid shifting attention to new priorities at the expense of fully implementing existing recommendations.
Europe	3	Prudential Regulation Authority (PRA)	20 October 2025	■ **The PRA, together with the Bank of England and the Financial Conduct Authority, published a report that summarises effective practices with regard to cyber response and recovery capabilities in the financial services sector**. These practices include the following. ➢ Response to a high severity cyber disruption: The most mature financial institutions have considered impact tolerance metrics beyond duration-based metrics, which enables them

[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 64 report. It is advised that you refer to the respective original materials for accurate information.

				to have a more accurate articulation of the level of service they need to deliver to mitigate risk to consumer harm, market integrity and financial stability. ➢ Recovery from a high severity cyber disruption: Financial institutions have implemented a range of solutions to strengthen their resilience capabilities, which includes restoring critical data from immutable back-ups and testing their ability to conduct a bare metal recovery in a clean environment. ➢ Response to a high severity cyber disruption at a material third party: The most mature financial institutions actively ensure a third party's resilience capabilities are equivalent to those they would expect from their own infrastructure.
	4	European Supervisory Authorities (ESAs)	16 October 2025	■ **The ESAs**, which are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA), **published their 2026 Work Programme**. Priority areas highlighted in the programme include the following. ➢ **Digital operational resilience**: The ESAs will concentrate on the effective operation of the new Oversight Framework under the Digital Operational Resilience Act (DORA), including designation of critical third-party providers and their oversight. ➢ **Consumer protection and financial innovation**: The ESAs will strengthen European consumer confidence and protection in the areas of banking, insurance, pensions and securities products and services through, for example, developing Regulatory Technical Standards (RTS) regarding Key Information Documents for PRIIPs. ➢ **Sustainable finance**: The ESAs will develop guidelines on high-level principles to carry out ESG stress testing.
	5	European Insurance and Occupational Pensions Authority (EIOPA)	1 October 2025	■ **The EIOPA identified supervisory focus areas and areas for attention** as follows. ➢ Focus areas - DORA: Assess whether insurers' ICT risk management framework is fit for purpose, etc. - Sustainability risks: Assess the quality and depth of materiality assessments of sustainability risks reported in insurers' ORSA reports ➢ Areas for attention - SCR calculation related to collective investment undertakings (CIUs)

				- Fair treatment of consumers in claims management
	6	European Supervisory Authorities (ESAs)	1 October 2025	■ **The ESAs released a factsheet on BigTech's direct financial services activities in the EU** as part of their BigTech monitoring exercise. 13 BigTech groups are in the scope of this year's monitoring exercise. Key findings include the following. ➢ 11 of the 13 BigTech groups have subsidiaries carrying out financial services in the EU, primarily payment services, e-money issuance and insurance intermediation. ➢ Compared to the 2023 data, no new licences have been granted to BigTech subsidiaries in the EU and no new types of financial services are being carried out.
Americas	7	New York Department of Financial Services (NYDFS)	21 October 2025	■ **The NYDFS issued 'Guidance on Managing Risks Related to Third-Party Service Providers.'** Requirements provided by the guidance include the following. ➢ Identification, due diligence and selection: Financial institutions must assess the cybersecurity risks the third-party service provider (TPSP) poses to the financial institution's information systems and non-public information (NPI) when selecting a TPSP. ➢ Contracting: Financial institutions may consider incorporating some of the following provisions into their contractual agreements with TPSPs: (i) Access controls; (ii) Data encryption; (iii) Cybersecurity event notification; (iv) Data location and transfer restrictions. ➢ Ongoing monitoring and oversight: Financial institutions' TPSP risk management procedures should include layered, risk-informed oversight processes and controls designed to confirm that TPSP cybersecurity programmes are aligned with the institution's cybersecurity expectations. ➢ Termination: A financial institution must disable the TPSP's access to the institution's information systems when preparing for the end of a TPSP relationship.
Asia Pacific	8	Australian Securities and Investments Commission (ASIC)	10 October 2025	■ **The ASIC reviewed the use of offshore service providers (OSPs) by responsible entities (REs) that are licensed to operate managed investment schemes**. Better practices observed through the review include the following. ➢ Due diligence processes: REs documented due diligence processes that enable assessment of OSP's capabilities, etc., before selection and on an ongoing basis. ➢ Service level agreements: REs entered into a legally binding written contract with each OSP.

				➢ Identifying and managing cyber risks: REs documented and monitored an OSP's risk as part of the organisational risk register. ➢ Business continuity: REs required OSPs to have documented response strategies for high-risk scenarios.
	9	Insurance Regulatory and Development Authority of India (IRDAI)	9 October 2025	■ **The IRDAI released its guidelines on insurance fraud monitoring**. Regulatory requirements provided in the guidelines include the following. ➢ Fraud risk management framework: Every insurer shall strive for zero tolerance for fraud and must put in place an appropriate fraud risk management framework. ➢ Cyber or new age fraud: Insurers shall establish and implement a robust cybersecurity framework. ➢ Framework for distribution channels: Intermediaries shall recognise fraud risk to their organisation and establish an appropriate and adequate fraud risk management framework.

Sources:

1. FSB ‘G20 Implementation Monitoring Review: Interim report’
2. FSB ‘Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector’
3. PRA ‘Effective practices: Cyber response and recovery capabilities’
4. EIOPA ‘2026 Work Programme of the Joint Committee of the European Supervisory Authorities’
5. EIOPA ‘Union-wide strategic supervisory priorities - focus areas for 2026’
6. EIOPA ‘Factsheet: 2025 Joint ESA stocktaking of BigTechs’ direct financial services activities in the EU’
7. NYDFS ‘DFS Acting Superintendent Kaitlin Asrow Issues New Cybersecurity Guidance to Address Risks Associated with the Use of Third-Party Service Providers’
8. ASIC ‘Review of offshore outsourcing – Responsible entities’
9. IRDAI ‘IRDAI (Insurance Fraud Monitoring Framework) Guidelines, 2025’

Contact:

Shinya Kobayashi
Managing Director
Financial Services
Deloitte Tohmatsu Risk Advisory LLC

Deloitte.
デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Risk Advisory LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Group LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides professional services in accordance with applicable laws and regulations. With more than 20,000 people in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides leading professional services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, and enable clients to transform and thrive. Building on its 180 year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 460,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, or their related entities(collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited

© 2025. For information, contact Deloitte Tohmatsu Group.

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMS それぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory