IAIS Report on FinTech developments in the insurance sector

December 2022

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.

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 FinTech Forum in consultation with IAIS members.
This document is available on the IAIS website (www.iaisweb.org).

Content

Acronyms

AI	Artificial intelligence
API	Application programming interface
DeFi	Decentralised finance
DLT	Distributed ledger technology
DPO	Data protection officer
EIOPA	European Insurance and Occupational Pensions Authority
FSB	Financial Stability Board
GDPR	General Data Protection Regulation
IAIS	International Association of Insurance Supervisors
ICP	Insurance Core Principle
IoT	Internet of things
ISO	International Organization for Standardization
IT	Information Technology
ML	Machine learning
MRM	Model risk management
PDPA	Personal Data Protection Act
PII	Personal identifying information
SME	Small and medium-sized enterprises
TPP	Third party provider

1 Introduction

Given the rapidly increasing ease of accessibility and digital innovation in financial technology ("FinTech") and its far-reaching effects on the insurance sector, the International Association of Insurance Supervisors (IAIS) has identified FinTech as one of its strategic themes. FinTech presents significant opportunities for financial inclusion and policyholder value yet also poses potential market conduct and operational risks with the rapid expansion in alternative data sources and advanced data analytics having the potential to disrupt the insurance market or impact the trust of consumers in the sector. The IAIS uses the FinTech Forum as a platform to share supervisory perspectives, challenges and developments with respect to financial technology. Beginning in 2021, the FinTech Forum has conducted deep dive assessments into three topics:

- Use of Application programming interfaces (APIs) and open data;
- Distributed ledger technologies (DLTs) and blockchain; and
- Safe, fair and ethical adoption of Artificial intelligence (AI) and Machine learning (ML) and the use and governance of data.

Assessment activities included input gathered through member surveys and interviews with market participants and experts. The purpose of the deep-dive assessments was to better understand the current digital transformation landscape, identify issues and trends in specific areas and assess their potential implications for insurance supervision.

This report presents the high-level findings of these assessments for information purposes. It is not intended to present a final assessment on the risks and opportunities of these trends; it also does not aim to state a preference as the IAIS takes a technology neutral approach. The IAIS will continue to monitor these trends and their impact on insurers, consumers and supervisory objectives.

2 Use of Application programming interfaces and open data

2.1 Introduction

Data is a key asset for innovation, along with Information Technology (IT) infrastructure. Data exchange through APIs can facilitate innovation. Enhanced data sharing and openness, in compliance with data protection and competition rules, will arguably enable the insurance sector to embrace data-driven innovation and encourage the creation of innovative products for policyholders. It could also provide opportunities for enhanced supervision, such as more effective and responsive compliance and oversight capabilities via regulatory technology (RegTech) and supervisory technology (SupTech).[1]

The discussion around open finance has been in place for some time, primarily focusing on the banking sector ("open banking"). Data exchange of both personal and non-personal data through open APIs has become increasingly popular in insurance, as it facilitates industry-wide innovation and increases the agility of businesses when responding to changes in customer needs and expectations.

[1] See A2ii, FSI, IAIS (2022), Suptech in insurance supervision, available at http://www.iaisweb.org/2022/12/a2ii-fsi-iais-note-on-suptech-in-insurance-supervision.

Internal APIs in insurance (for example back-end communications and interactions with third-parties) have been in place for some time. Recently, there has been a shift towards opening up APIs so as to offer better services to policyholders and greater market competition. Consequently, the infrastructure for some services similar to "open insurance" is already partly in place, albeit with variations across jurisdictions. Improving such services will require negotiations, standard agreements and contracts, and work to harmonise the different standards that currently exist. In the absence of any regulatory or self-regulatory requirements (other than general data portability rules), there is limited standardisation resulting in insufficient interoperability.

Open insurance would involve standardisation or possible compulsory data sharing at the initiation and consent of the customer. It would also require robust data protection and should be developed to ensure good consumer outcomes.

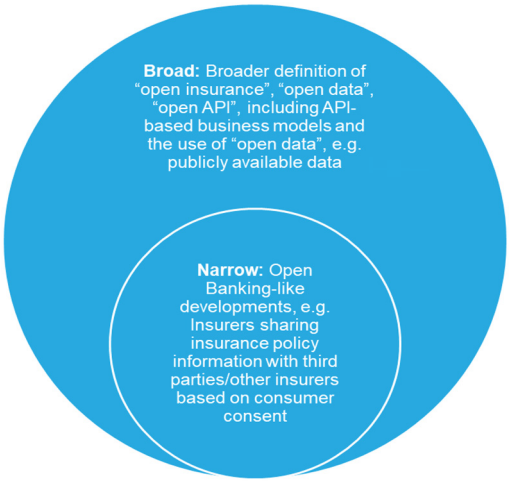
2.2 Definition of "open insurance" and use cases

There is no uniform definition of open insurance as it is a relatively new term. It is sometimes narrowly understood as compulsory data sharing across insurance policies with the explicit consent of the consumer. This could include both personal and non-personal data. Open insurance could also describe broader information sharing via APIs between different insurance market players, including in the back office and in a way that might not be directly visible to consumers. This type of insurance potentially comprises both risks and benefits for consumers, the industry and insurance supervisors. For the purpose of this report, the definition of open insurance will be kept broad.

Most IAIS FinTech Forum members reported open insurance developments in their jurisdictions. The majority of use cases seem to currently fall under the broad definition of open insurance. This includes private comparison websites, parametric insurance, Internet of Things (IoT)-based insurance solutions, embedded insurance, use of open banking data for insurance purposes (eg to identify key life events) as well as industry-led initiatives to coordinate open insurance standards.

There are less use cases of "narrow" open banking-type arrangements for which participation is compulsory, such as insurance and pension dashboards, comparison websites, or government-led initiatives such as API registers or personal data managers.

Figure 1. API and open data use cases



Source: IAIS FinTech Forum Survey on API and open data

2.3 Possible risks and challenges for developing open insurance

Notwithstanding the wide range of possible benefits from open insurance, this type of service could potentially give rise to, or amplify, a number of risks such as data security, cyber, interoperability, liability, consumer protection and financial exclusion. The potential risks to consider will depend on the concrete use case and the open insurance approach followed (ie narrow or broad).

2.3.1 Data protection and data ethics

IAIS FinTech Forum members noted the importance of a consumer first approach to mitigate potential risks, including the perpetuation of biases, and appropriately empower consumers to make informed decisions.

As previously mentioned, open insurance could include both personal and non-personal data. With an increase in data sharing, especially if combined with AI/ML tools, data protection and data ethics issues can arise. In addition, the complexity of the sharing chains may increase the risk of data misuse, financial crime, fraud or scams. Having in place clear restrictions on the sharing of data with third-parties for purposes beyond the customer's initial consent may help address these issues.

Inappropriate use of social, racial or ethnic information could lead to, or exacerbate, prejudicial biases and consumer difficulties could be entrenched if data on behaviour utilised in an ethical context is used in an unethical one.

IAIS FinTech Forum members also highlighted consumer protection measures, including:

- A common liability model across all participants, covering harms from inaccurate data, misuse of data, stolen identity and harms to third-parties;
- A common route to complaints – redress and compensation being easy, accessible, timely, and tailored;
- A clear framework of data rights around the giving and withdrawing of consent, including the appropriate duration of (and the information needed to) provide informed consent. Within this framework, simple and transparent ways or tools for the consumer to give, track and withdraw consent;
- Rules around data accuracy and consumer's rights to correct inaccurate data – inaccurate data risks are even higher when third-parties have access to make transfers, switch, open or close a product on behalf of the customer; and
- Clear and transparent rules on the legitimate use of data, and restrictions on onward sharing (eg to vendors, providers of services to third party providers (TPPs) or commercial partners).

In some jurisdictions, the existing data protection regulation may not have been designed to be fully consistent with an open insurance framework, and potential adjustments may need to be considered to ensure compatibility and suitability. Cooperation within and across jurisdictions and with relevant bodies that have data protection requirements or regulations, may help to ensure that relevant standards are aligned and the right considerations are made.

2.3.2 Financial inclusion and exclusion

Open insurance could improve financial inclusion for some high-risk consumers who previously could not access affordable coverage. Additional information could also be helpful to foster financial inclusion of customers that are less considered in traditional models (young people, first-time insured, prudent drivers in risky areas, etc.). Conversely, some high-risk consumers could encounter difficulties in accessing affordable insurance in markets where there is free competition.

The more information insurers have and share about an individual, the higher the probability that some parameters, or combination of parameters, can be used as a disqualifier or proxy for a traditional parameter. Aggregated data may expose sensitive patterns on groups (including vulnerable groups) that can be used for exclusionary or discriminatory purposes. This could threaten the risk-pooling nature of insurance provision, potentially resulting in uninsurable groups and higher prices for many.

More granular consumer data combined with AI also increases the risk that insurers identify opportunities to unfairly charge different prices to groups of consumers that are similar in terms of risk and cost-to-serve. An increased use of price optimisation practices, when setting premiums based on non-risk factors, can lead to potential unfair treatment of some consumer groups, particularly those that are more vulnerable (eg old age, low income).

Some insurers could also discontinue products sold in traditional, non-digital, ways, possibly excluding customers who lack clear access to new distribution channels or those who struggle with technology. Hence, the willingness of consumers to share very personal and sensitive data, which is not strictly necessary for risk assessments, may affect having access to insurance coverage.

2.3.3 Inconsistency in consumer attitudes

An extensive research project from one IAIS member jurisdiction identified differences between consumer attitudes, with 59% of consumers favouring insurance payments based on their exact level of risk, while the remaining 41% preferred the minimisation of information sharing, even if this resulted in higher premiums. However, the study also found that consumers have a limited understanding of how their risk is assessed, which may have affected their perspectives and priorities.

2.4 Adequacy of current framework

At this stage, there are no universal binding provisions for a holistic open insurance framework. In some jurisdictions there are ongoing discussions on extending open banking to insurance. Other jurisdictions are conducting public consultations to develop an open insurance framework. Still other jurisdictions have already begun to implement such a framework.

Overall, IAIS FinTech Forum members agreed that having an appropriate regulatory framework would facilitate the successful development of open insurance to develop successfully. Such a framework would need to protect consumers, give them the right to redress, and give them confidence that their data will only be used ethically and in a way that is consistent with their prior consent.

For jurisdictions that have frameworks already in place, most acknowledged that adjustments and specific regulatory guidance would enable them to better cope with new models. Several jurisdictions suggested that although there are no specific regulatory barriers, legal uncertainty and a lack of clarity often created significant tensions and brought up questions that would benefit from upfront clarification via a specific, perhaps harmonised, open insurance framework.

As more sensitive data might be included in open insurance compared to open banking, a careful forward-looking assessment of the interrelationship with data protection regulations and potential open insurance frameworks would be necessary as well as consideration of consumer interests in order to mitigate potential issues, including the misuse of data and the perpetuation of biases. Supervisory cooperation would also need to be intensified (eg with data protection regulators) and the issue of reliance on certain non-financial TPPs may arise (eg data providers, including IoT data providers), which would raise the question of oversight. The task of regulating open data is even

broader and more complex than other incremental changes that would need to be made to the regulatory perimeter, and this could strain regulators' expertise and resources.

2.5 Barriers, incentives and compulsion

Major barriers for existing players ("incumbents") in adopting new technologies like open insurance are centred around the restrictive impact of large legacy systems, outstanding and potential unaddressed data privacy risks, and the lack of clear interoperable standards for access.

The lack of interoperable standards and data privacy risks were again noted to be amongst the strongest barriers to accessing data for TPPs, while the difficulty of partnering with incumbents was an additional barrier cited. Examples of good practice include TPPs and insurers reciprocally auditing each other's data, which could overcome partnering difficulties and lead to speedier integrations.

The lack of consumer awareness is a critical barrier because, without it, data sharing will be limited. Consumer engagement and user-centric design should be a priority (as opposed to technology-led design) as regulation alone is not a sufficient prompt for behavioural change.

2.6 Sequencing of open insurance adoption

Interviews conducted by the FinTech Forum indicated that a "big bang" approach to open insurance was not feasible nor desirable, but rather an implementation of open insurance should be proportionate, phased and ideally driven by consideration of credible consumer propositions and use cases.

The features of the insurance market, particularly the type and nature of the data collected, will make open insurance more challenging to implement than open banking. Therefore, the development of open insurance may need to occur on a sub-sector basis, as different lines of business will develop at different speeds. However, open data frameworks for the insurance sub-sector being aligned may help provide interoperability and efficiency.

On the one hand, if compulsory data sharing is considered, sector-specific compulsory data sharing under current regulatory perimeters could be seen as a practical way forward because it reduces the amount of stakeholders involved, could possibly make policy debates clearer and could allow for a step-by-step approach before widening the approach and/or opening up market to third-parties based on bespoke regulatory/supervisory frameworks.

On the other hand, a cross-sectoral approach to open insurance may arguably allow for better consumer outcomes, including services supporting holistic overviews of their financial situation and greater economies of scale. From a supervisory perspective, it will likely demand more complex co-operation between supervisors outside of the insurance field (eg banking, securities or data) and the implementation process will arguably be more difficult.

Regarding initial use cases, it is expected that consumers would be given transparency first by allowing visibility of their insurance policies through read-only access. Once this has been proven to be successful, more complex products may emerge using write-access. Financial guidance or advice services could come on-stream where certain suitability requirements on financial advice would be layered in.

2.7 Conclusions and next steps

As open insurance develops, it is important that:

- Consumer interests are considered from the outset, including vulnerable and digitally excluded consumers; and
- The right conditions exist for open insurance to develop sustainably and securely.

Coordination will continue to be needed on multiple levels in this rapidly evolving area. Therefore, the IAIS will continue to monitor and exchange views and best practices through the FinTech Forum.

3 Distributed ledger technologies and blockchain

3.1 Introduction

As defined by the Financial Stability Board (FSB),[2] DLT is a means of recording information through a distributed ledger. These technologies enable participants (nodes) in a network to propose, validate and record state changes (or updates) consistently across the network's nodes – without needing to rely on a central trusted third-party to obtain reliable data.

DLT has the potential to lower costs and increase efficiencies in the financial services industry. These benefits could come from immutable record-keeping, atomic settlements and automation of processes. However, the use of DLT poses new risks and challenges that policymakers need to consider when assessing DLT-based applications in the financial sector.

A blockchain is one type of DLT which has a specific set of features, organising its data in a chain of blocks. Each block contains data that are verified, validated, and then "chained" to the next block.[3]

3.2 DLT in insurance

DLT can be potentially applied to all activities of the insurance value chain. It could be used to reduce duplication of processes, increase process automation, help cut costs, increase efficiency, enhance customer experience, and improve data quality, collection and analytics. It could also enable the development of new products and services – such as facilitating the uptake of insurance platforms and ecosystems, improving interaction with third-parties, promoting completely decentralised peer-to-peer insurance business models or implementing parametric insurance products.[4]

However, while promising to drive efficiency in business practices, the adoption of DLT may also trigger new risks to insurers, supervisors and consumers, such as operational risks (including fraud, technological and cyber risks), money laundering and terrorist financing risk, and legal and reputational risks. As DLT is still evolving, several emerging challenges have been noted. Given its wide range of applications and the early stage of adoption in the insurance industry, most jurisdictions are still exploring policy and supervisory responses to the adoption of DLT by insurers.

The FinTech Forum began its assessment by learning more information about three firms that offer insurance DLT use case products (B3i, Etherisc and Nexus Mutual). This should in no way be interpreted as an endorsement of any of these firms or the associated technology they are using to provide their services to customers.

[2] FSB, Decentralised financial technologies: Report on Financial Stability, Regulatory and Governance Implications, 2019.

[3] IMF, Blockchain Consensus Mechanisms: A Primer for Supervisors, 2022.

[4] EIOPA, Discussion Paper on Blockchain and Smart Contracts in Insurance, 2021.

B3i's business model that focuses on claims management and risk transfer was initially selected for a deeper dive, as both Etherisc and Nexus Mutual both used a Decentralised Finance (DeFi) model. The Fintech Forum's research and analysis was completed in early 2022, before B3i filed for insolvency under Swiss Law in July 2022. This insolvency was primarily due to unsuccessful funding for its ongoing operations.[5] Despite the fact that the firm is no longer operational, the FinTech Forum still deemed it relevant to include the findings of the analysis on B3i in this report so as to give an overview of the business model used and products proposed while also describing potential benefits, risks and regulatory and supervisory issues that are worthy of consideration.

Box 1: Short description and background on B3i

The service provider B3i Services AG was incorporated in 2018 and was owned by 21 insurance market participants around the world. Altogether, more than 40 companies were involved in B3i as shareholders, customers and community members. B3i was a globally focused company, with shareholders on six continents.

Initially formed as a consortium, B3i was tasked with developing solutions based on DLT, to reduce costs and facilitate growth within the market. As a provider of DLT solutions for the insurance and reinsurance markets, B3i developed innovative solutions for customers across the world, working closely with customers, market testers and collaborators to develop solutions for the marketplace.

3.3 Potential benefits for the insurance industry and consumers

DLT has the potential to provide benefits for the insurance industry and consumers including, that it:

- Removes the need for a central authority to act as an adjudicator, which opens opportunities for more competition and open participation.
- Provides a clear data audit trail that is shared by all participants in a network. This grants each user access to timestamps and reference links for previous transactions. Since the data is immutable and traceable, it maintains the integrity of the data in its original form. In addition, the distribution of log records ensures greater transparency, making fraud and data manipulation more difficult.

In operations, there is a potential for efficiency gains through operating autonomously. DLT results in lower operating costs (the cost of processing and storing information) for insurers. This may translate into consumers having access to products and services at a lower price.

3.4 Risks for regulatory and supervisory consideration

3.4.1 Operational and systemic risk

While promising to drive efficiency in business practices and mitigate certain existing risks, the adoption of blockchain may also trigger new risks to insurers, supervisors and consumers. As blockchain technology is still evolving, several challenges have been identified as emerging risks to the sector.

For instance, economic scaling can involve higher transaction costs. This impacts the strategy and profitability of the insurance industry. In turn, it might affect consumers, as they will pay more for the products and services being offered by the insurance company. Linked to this are the long

[5] See https://www.insurancejournal.com/news/international/2022/07/29/677926.htm

verification times that can occur during high volume periods. As a result, operational risk also increases, as long verification times may cause customers to lose patience.

DLT has the potential to disintermediate markets, reduce costs, increase speed and efficiency, and create secure records of transparent, immutable, and auditable data and activity (IMF, 2022)[6]. However, immutability is also a risk as it may slow down the process of implementing changes once a risk is identified due, in large part, to the difficulty of achieving coordinated action amongst stakeholders. In addition, if an untested solution or code is implemented, this increases risks due to the irreversibility of the transactions.

Furthermore, DLT is susceptible to IT risks. Network security risks may arise and stakeholders may require certain additional safeguards to protect their network from both internal and external threats. This may increase costs to the insurance industry, in terms of improving the resilience to cyber threats In addition, data security risks may arise due to shared networks (ie data may fall in the wrong hands resulting in litigations and reputational loss for the market). Lastly, in view of a broad and rapid development of new applications, the insurance industry may engage faulty or exposed vendors to implement DLT. This may increase the vendor risk if due diligence is not undertaken properly.

Governance challenges could also exist, especially due to risks related to potential high dependency on external platforms and IT suppliers. Therefore, it is important to have in place recovery plans to address and manage potential risks, including enhanced information and communications technology (IT), cyber resilience, etc. Similarly, there could be risks related to maintaining efficient internal controls, risk management and compliance functions. Performance and scale-up risk might also occur (eg the business risk of not arriving at profitable blockchain operations while having invested heavily in this technique). In addition, setting-up a blockchain solution would require the availability of technical personnel with a specific skillset (or accepting a high risk of dependency on third-parties). Interoperability risk could occur between different blockchains and there could be a lack of integration with internal legacy systems or issues related to the migration of legacy data to the new systems.

Concentration risk and vendor/service provider risk (lock-in risk) could occur (eg when using few external data vendors, oracles or other third-parties). From an antitrust perspective, there is a possibility of the creation of new barriers to entry in some market segments/lines of business due to the necessary investment in technology to achieve a viable business case. The latter might not be achievable for smaller insurers (although less complex blockchain solutions seem to be more accessible also for SMEs).

For smart contracts[7], the issues related to oracles, including dependency on and reliability of oracles[8], are also a major concern. The smart contract itself depends on input data for its execution, often including external data. These external oracles could introduce dependencies and may, in

[6] (IMF (2022), Blockchain Consensus Mechanisms: A Primer for Supervisors, available at https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx

[7] These are programs on a blockchain that automatically execute, control or document events and actions when predetermined conditions are met.

[8] Oracles are systems that connect data from the outside world with the blockchain.

some cases, lead to heavily centralised contract execution.[9] This could also invite questions on who determines which oracles are necessary in smart contracts, how to guarantee their reliability (eg should they possibly be validated before use in order to secure their reliability) and who is ultimately accountable in the case of inaccurate information. Related to that, change and governance of smart contracts could also be seen as an issue, including governance of the chain and ownership of data.

From a broader supervisory perspective, it is unclear who and how to oversee the correct and legitimate functioning of the complex structures of blockchain and smart contracts. The lack of a central authority could lead to potential systemic risks. For example an erroneous transaction, activated automatically, could settle numerous contracts simultaneously and lead to sudden market movements.

3.4.2 Data privacy concerns

DLT solutions could heighten data privacy concerns and compliance risk due to the need to abide by applicable data protection requirements in each jurisdictions (eg General Data Protection Regulation (GDPR) in the European Union, Personal Data Protection Act (PDPA) in Singapore).

As highlighted in the European Insurance and Occupational Pensions Authority's (EIOPA's) recent discussion paper,[10] records on the blockchain are largely tamper-resistant and immutable. Data protection requirements such as the right to be forgotten and data erasure requirements under GDPR in the EU, or the requirements for an organisation to cease the retention of personal data when no longer required under PDPA in Singapore, need to be taken into account by insurers so as to ensure compliance with these requirements.

In addition, as the blockchain could hold large amounts of data, insurers may also run the risk that sensitive data is used indirectly in areas that are not permissible by law.

3.4.3 Cyber risks

DLT has the potential to strengthen resilience and reliability, as it reduces risks from a single-point-of-failure. However, the distributed nature of DLT solutions, with the use of multiple ledgers and nodes, create additional points of entry for potential malicious acts.[11]

Cyber risk could be further exacerbated if there is weak governance structure in these DLT solutions, where they cannot react in a timely manner to emerging security issues and threats. As with other technology implementation, the integration of DLT into existing systems or transition to DLT solutions could also generate new areas of potential security breaches.

The use of smart contracts, while enhancing operational efficiency, could also invite hacking and heighten cyber risks for insurers.

3.4.4 Money Laundering/Terrorism Financing Risks

As highlighted in EIOPA's recent discussion paper, the use of DLT solutions could also heighten the money laundering/terrorism financing risks that insures could be exposed to.

---

[9] See eg https://www.coindesk.com/the-flash-loan-attacks-explained-for-everybody and https://blog.coinbase.com/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in-1289f7f77137.

[10] EIOPA, Discussion Paper on Blockchain and Smart Contracts in Insurance, 2021.

[11] Bank for International Settlements: Distributed ledger technology in payment, clearing and settlement, 2017.

While the information stored on the ledger itself is meant to be visible and transparent to the participants of the system, data protection laws (such as GDPR) and similar types of requirements may require the anonymisation of data and thus limit the identification of real identities.

3.4.5 Legal, Regulatory and Reputational Risks

More broadly, there are the legal, regulatory and reputational risks that could be elevated in the use of DLT solutions and smart contracts.

For instance, when DLT solutions are used to enhance operational processes, such as claims processing or disclosures, they should have the same level of service standards and transparency with consumers. Otherwise, insurers may lose their credibility and suffer from reputational risks.

3.5 Conclusion and next steps

As DLT technology is still evolving, several challenges are emerging. The potential benefits of deploying DLT solutions need to be weighed carefully against the risks. As more DLT solutions are developed across the insurance value chain and other DLT-related business models emerge, it is important for supervisors to keep monitoring these developments.

One development that has attracted much attention is the rise of DeFi services. DeFi relies on publicly distributed ledgers and automated digital (smart) contracts to provide financial services without requiring the presence of intermediary agents. Certain DeFi applications have begun to offer protection coverages in the DeFi space including:

- Dollar peg stability for stablecoins;
- Smart contract failures;
- Exchange and custodial wallet hacks or halted withdrawals; and
- Deposited fund protection.

It is not yet clear if these products are defined as “insurance” products or what the best or appropriate regulatory approach is for these applications. The FinTech Forum will continue to research these issues to understand the marketplace and the products offered. This includes the analysis of specific use cases, to assess specific benefits, risks and threats.

4 Artificial intelligence and machine learning

4.1 Introduction

This section presents the outcomes of the deep-dive exercise performed in 2021-2022 aimed at identifying any material risks of financial loss, or to the fair treatment or inclusion of customers, introduced by the application of AI/ML models, or the use of data analytics by insurers. Three areas were the focus of this risk assessment study: model risk management, data usage and ethical issues (including discriminatory biases). The outcomes presented below reflect preliminary observations of a small subset of IAIS member jurisdictions and are supplemented by a member survey.

4.2 Model Risk Management and Governance

The assessment focused on the following questions:

- The extent to which oversight and control exercised by insurers over their ML models enables them to maintain performance and reduce the risk of financial loss; and
- Whether senior management has sufficient information to understand potentially opaque and complex predictive or decision-making models.

4.2.1 The principle of proportionality and explainability

In general, the principle of proportionality is well-established in the insurance sector, also with regards to AI. There are a range of AI use cases across the value chain, and not all present the same risks for consumers and insurers. As a result, the governance measures required to ensure ethical and reliable AI differ between use cases; they should be proportionate to the characteristics and impact of the specific application.

Explainability of an AI/ML model is a multidimensional question as the answer depends on the intended recipient of an explanation. Each stakeholder (consumers, technical experts, domain experts, auditors) will have different requirements regarding the interpretability of insurance models based on AI. Distinct AI use cases may also require different explanations; for higher impact use cases, the need for explanation is arguably greater.

In practice, some insurers require full auditability of any pricing model they put into production, including, for example, an audit trail of all manual overrides that have been implemented. Full auditability can significantly reduce model risk, especially insofar as it is very difficult to satisfactorily back-test an insurance pricing model due to, for example, the anti-selection risk arising from noise in the input data for sparse subdomains.

4.2.2 Supervisory approaches and governance measures

Three possible supervisory approaches of Model Risk Management (MRM), of increasing complexity and different levels of AI/ML deployment, are:

- A top-down approach that establishes cross-sectional AI regulations or extends existing MRM principles/guidelines;
- A bottom-up approach that ensures that business trials of innovative services are thoroughly reviewed and approved with a set of self-regulatory guidance for each successful case; and
- Standard measures targeting governance and control mechanisms considering that technical innovation, such as AI/ML, are at a proof-of-concept stage and complement, rather than replace, conventional analytics.

Some jurisdictions have prioritised MRM and published model governance principles accompanied by initial guidelines. Some jurisdictions have also addressed consumer-focused use cases (eg by publishing a directive on online insurance sales). Many jurisdictions that do not have explicit MRM standards, or are in the process of developing regulations or guidelines, are supervising AI/ML-related model risk through other policy angles such as:

- Actuarial standards;
- Risk management guidance and standards;
- Third party outsourcing standards;
- Technical risk standards;
- Guidelines on cyber security;
- Existing governance (via the Chief Risk Officer and three lines of defence);
- Controls and compliance standards, eg ICP 8 (Risk Management and Internal Controls); and/or
- Monitoring model outputs/consumer impact through market conduct oversight.

Some insurers have built automation into their models but often retain a human-in-the-loop for review and sign-off of new models. Notwithstanding the combination of governance measures used, explainability is an important factor for insurers to remain accountable for the AI systems they use within their organisations, as well as for consumers to have access to effective redress mechanisms (eg to provide consumers with meaningful explanations when their claims are rejected).

4.2.3 Dedicated structures and flexibility in guidance

From an organisational perspective, many supervisors have set up dedicated structures (typically FinTech innovation hubs) and, in some cases, infrastructure (such as a regulatory sandboxes) that are dedicated to experimental projects and analyses on digital innovation in the sector. Interestingly, this is analogous to market practices, whereby jurisdictions have observed that some financial actors leverage existing governance structures (such as transverse risk committees) whereas other actors have set up dedicated committees. Many jurisdictions underscore the need for flexibility in any guidance provided to the market in order to accommodate new, unanticipated, risks stemming from increased digitalisation.

4.3 Data usage and management

Questions examined on this topic included whether insurers are able to source sufficient, high-quality structured and unstructured data to support their AI/ML applications; or if they are facing IT or operational barriers that can impede access to (and secure usage of) new data sources.

4.3.1 Data provenance

The provenance of the data used in AI-based insurance pricing models is a mix of internal, vendor, and open data. Several insurers reported being limited in how they leverage multiple sources of internal data, because it can be challenging to draw upon heterogeneous datasets that are stored within databases as part of legacy systems.

4.3.2 Data hosting

Some insurers (especially large insurers and bank insurers) are hesitant to host their AI-based systems in a public cloud, due to the re-identification risks that arise in the event of a data leak, even though no personal identifying information (PII) is present in the data. However, overall there is a clear trend to increased use of cloud services for data storage as well as for outsourced AI applications from cloud service providers. Most InsurTechs offer an ISO-27001 compliant solution.

4.4 Ethics, Bias and Discrimination

Regarding the potential for biases, unfair discrimination and financial exclusion, insurers in some jurisdictions have taken into consideration these ethical principles and have put in place measures to address such risks.

4.4.1 Nascent stage of AI fairness

Many supervisors consider that the topic of biased datasets should be addressed. Bias assessment and mitigation is deemed important to supervisors, insurers and consumers. Some observed that biased datasets are not the exclusivity of AI/ML and were already a risk for models using traditional techniques. Others stressed the importance of proxy variables to define and detect discriminatory biases. Due to the relative lack of maturity of most jurisdictions on the subject of discriminatory biases

and the lack of consensus on appropriate fairness metrics or even objectives adopted by supervisors, continued research and monitoring of any associated developments may be useful.

For the implementation of fair AI systems, sustainable solutions may depend largely on the context and desired notion of fairness. For high-impact AI applications, insurers could select the definition/metric of fairness that best suits their concrete AI use case in order to measure outcomes. Techniques can be explored to go beyond the desired metric for a given application, to introduce into the AI system relevant constraints/guardrails that would prevent the undesired effect on protected groups, in some sense fair by design. However, although these investigations are promising, such solutions are at an early stage.

4.4.2 Ethical governance standards

To ensure ethical and trustworthy AI systems, a lack of explainability could be compensated with other governance measures such as an enhanced level of human oversight (human-in-the-loop) and data management throughout the AI model lifecycle. if automated model building and deployment with limited human oversight is used, it is important to adopt AI systems with greater model explainability, subject to the principle of proportionality. Alternatively, the use of black-box AI systems could be limited.

Processes, including training, may facilitate a corporate culture that fosters ethical values, including awareness of AI activities and their challenges and potential pitfalls. All actors should respect the rules in place throughout the AI life cycle, specifically those on data usage to discriminate against protected classes, which may fall under data privacy and anti-discrimination laws in various jurisdictions. Consistent with the risk-based principles of insurance, AI actors should proactively engage in responsible stewardship of trustworthy AI for the benefit of consumer outcomes and to avoid proxy discrimination.

Ethical use of AI may be facilitated with an adequate organisational structure and accountability frameworks with mechanisms to allocate and enforce responsibility for AI systems during their development, implementation and use. The design phase of an AI application would comprise the following stage: Approval (A), Consultation (C) and Information (I). It is recommended to involve staff across departments including representatives from the management/executive board, head of IT department, developers of AI systems, data protection officer (DPO), AI/data officer, compliance function, risk management function, audit function; and actuarial function.

4.4.3 Financial inclusion

Mitigating ethical risks that arise from the use of sensitive customer data and excluding factors regarding proxy variables may not be sufficient to guarantee a fair result. This is because AI systems, such as neural networks or deep learning, are capable of finding multi-variable non-linear correlations in the training data and, in a sense, they are able to reconstruct the hidden (protected) information. This is particularly relevant when insurers embrace ‘big data’, and when complex AI systems with limited explainability are being used. Main areas of focus for the supervisor in these cases include the boundary between risk differentiation and unfair discrimination, and a specific application scenario that is the validation of AI-based insurance pricing engines.

To overcome these challenges, other approaches may be required. For example, more concrete, practical guidance could include not only principles but also use cases in insurance, in particular those following a risk-based approach as well as a discussion of how existing regulation is enforced. Clearly communicated expectations on trustworthy AI could encourage robust supervisory practice. In addition, guidance covering the type of skills and resources (especially technical ones) that would

help fill the gap observed in terms of AI audit and bias analysis capability at a number of supervisory authorities could be useful.

4.5 Conclusions and next steps

The use of AI/ML and big data by insurers may lead to supervisory concerns. Across the IAIS membership, several supervisors have issued high-level guidance around various thematic areas, including that of the use of alternative data, model risk management, third-party vendors and/or fair use of data. The role of the IAIS will be to take stock of these initiatives and identify good practices as well as potential gaps.

4.5.1 Analysing existing guidance/providing new guidance

FinTech Forum members expressed the need for clarification on:

- How the current regulatory framework could/could not apply to AI/ML;
- Whether additional clarification may be helpful;
- How policy can best support and further safeguard AI/ML use by taking into account and leveraging on wider and general regulations such as data/information protection and general consumer ethics/conducts outside of insurance regulations; and
- Necessary guidelines or standards on AI/ML needed to explicitly supplement conventional policy frameworks and impact the sustainability of expected future insurance business models, if any.

More concrete, practical guidance on the use of AI/ML that could include not only principles, but also use cases as well as a discussion on how existing regulation is enforced, should be considered.

In addition, any guidance proposed by the IAIS should ideally suggest the type of skills and resources (especially technical ones) needed to put in place such systems, particularly with regards to AI audit and bias analysis capability. Specific areas of interest for possible further exploration include actuarial questions such as the boundary between risk differentiation and unfair discrimination, and more technical ones (eg which methodology is most adequate for validating AI-based insurance engines on pricing/underwriting/investments/claims/valuation reserving and solvency).

4.5.2 Monitoring developments in ethics and fairness

Despite the importance assigned to the topic of discriminatory biases by most members, concrete deliverables by the FinTech Forum, such as a framework for detecting and mitigating such biases, seems premature at this stage. This is due to the relative lack of maturity of most jurisdictions on the subject and the lack of consensus on appropriate fairness metrics or even objectives. The IAIS plans to continue monitoring those questions and observe any associated developments.

4.5.3 Alternative data

The use of alternative data is indeed relevant both to model risk management and to IoT (a major source of such data) which are two key study themes identified for the FinTech Forum. The focus on alternative data may touch on anchoring issues such as model risk and discriminatory biases, and concrete use cases and data sources that are actually fed into live models and align with the objectives of insurance supervisors.