Financial Stability Institute

FSI Insights

on policy implementation

No 13

Regulating and supervising the clouds: emerging prudential approaches for insurance companies

By Juan Carlos Crisanto, Conor Donaldson,
Denise Garcia Ocampo and Jermy Prenio

December 2018

JEL classification: G22, M15, O33
Keywords: Cloud computing, insurance, operational risk, outsourcing

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-198-4 (print)

ISSN 2522-249X (online)
ISBN 978-92-9259-199-1 (online)

Contents

* These Annexes are available as an online appendix and can be found on the BIS website at: www.bis.org/fsi/publ/insights13_appendix.pdf

Regulating and supervising the clouds: emerging prudential approaches for insurance companies[2]

Executive summary

Insurers have made increasing use of cloud computing in recent years. Cloud services were initially applied to business support functions, such as customer management or collaboration applications. Currently, cloud computing is being used in core business functions, such as product development, distribution, underwriting or claims administration.

Cloud computing brings a number of benefits to the insurance industry. It lets insurers share available-on-demand networks, servers, storage, application and services that can be rapidly scaled up or down, and accessed anytime and anywhere. In this way, cloud computing allows insurers to quickly launch new products and services, make business processes more efficient and reduce information technology (IT) costs.

The use of third-party cloud computing services may pose risks that are different from traditional outsourcing arrangements. Besides the operational risks of any outsourcing activity, cloud computing may pose additional risks to the insurance sector, given (i) shared computing resources in some cloud deployment models; (ii) the type of information that is stored and processed; (iii) the different geographical location of computing resources and providers; as well as (iv) the small number of global cloud providers, resulting in market concentration that could have systemic implications. The cross-border nature of cloud services complicates the effective oversight of all these risks.

This paper outlines the emerging regulatory and supervisory approaches in selected jurisdictions to cloud computing activities in the insurance sector. Using publicly available information and interviews with relevant officials, we analyse the regulatory and supervisory approaches of 14 authorities worldwide and present key insights on the emerging prudential treatment of cloud computing in the insurance industry.

Authorities apply their frameworks for general outsourcing and for governance, risk management and information security to cloud computing. Some authorities include cloud-specific sections in these frameworks. Other authorities have issued cloud-specific recommendations or supervisory expectations. Regardless of the approach taken, cloud computing arrangements are subject to regulatory requirements only if they are deemed as material. However, the criteria for deciding whether such arrangements are material vary across jurisdictions.

Regulatory frameworks have a number of common requirements and expectations for cloud computing. Authorities generally focus on (i) the adequacy of information security and data confidentiality; (ii) the strength of IT and cyber-security capabilities at cloud service providers; (iii) the effectiveness of recovery and resumption capabilities; and (iv) the adequacy of audit rights (ie the supervisory authority's access to documentation and information, and ability to conduct on-site inspections at the provider). Also, authorities are generally using non-binding guidance through principles

[2] Conor Donaldson (Conor.Donaldson@bis.org) from the International Association of Insurance Supervisors (IAIS) and Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org), Denise Garcia Ocampo (Denise.GarciaOcampo@bis.org) and Jermy Prenio (Jermy.Prenio@bis.org) from the Bank for International Settlements (BIS).

The authors are grateful to Todd Coslow, Yoshihiro Kawai, Greg Sutton and to the representatives from the organisations interviewed in Annex 1. We are grateful to Bettina Müller for her valuable support with this paper. The views expressed in this paper are those of the authors and not necessarily those of the BIS, the Basel-based standard setters or the interviewed organisations mentioned in Annex 1.

and recommendations and adopting a proportionate approach (ie tailored to reflect the size, complexity or risk profile of financial institutions or outsourced service).

Cloud computing outsourcing arrangements are generally supervised as part of the oversight of operational risks. Authorities usually assess cloud computing practices as part of insurance companies' off-site and on-site reviews of operational risk, following a risk-based approach. Before an insurer enters into a cloud servicing agreement, some authorities require notification, while others prescribe a consultation or approval process: the approaches to this communication vary widely. At the very least, most authorities expect informal communication from insurers on their material cloud computing plans.

Authorities are increasingly using thematic reviews and informal contacts with cloud providers to complement their oversight of the cloud computing business. Targeted reviews on the use of cloud services in the financial/insurance industry or on closely related areas such as information security risks are helping authorities to gain an industry-wide perspective on cloud computing. In addition, some authorities have established a dialogue with cloud service providers with the aim of better understanding the cloud services business and, in particular, its evolution over time. This helps supervisors to evaluate how insurers are managing cloud-related risks.

This study yields some useful insights on the emerging regulatory and supervisory approaches for cloud computing in the insurance sector. Some key specific considerations for insurance authorities include:

- **There is value in clarifying regulatory/supervisory expectations on insurers' use of cloud computing services.** The usefulness of this approach is to address the unique risks posed by cloud computing and to provide a reasonable level of regulatory certainty with respect to the use of cloud services by the financial industry.
- **Developing a supervisory framework to assess concentration risk in cloud computing is work in progress.** While authorities generally acknowledge that reliance on a relatively small number of providers may result in systemic risk for insurers, very few perform industry reviews of the concentration risks arising from cloud service providers.
- **Enhancing cross-border cooperation, particularly in terms of information-sharing, is essential for the effective supervision of the cloud computing business.** Users and providers of cloud services may be located in different jurisdictions. Even if they are physically in the same place, data storage could be elsewhere. Therefore, international cooperation between different national authorities, in particular by sharing relevant information on cloud service providers, is especially important when it comes to ensuring effective oversight of cloud activities.

Section 1 – Introduction

1. **Digital technologies are changing the way insurance is designed, underwritten, priced, distributed, settled and paid**. Emerging technologies such as the internet of things (IoT) and advanced analytics (AA) are providing real-time information and extensive insights into customer needs, preferences and risk behaviour. These resources help insurers tailor their products and prices to specific customer profiles. Other applications of technologies like machine learning (ML) and artificial intelligence (AI) such as chatbots, robo-advisors or virtual claim adjusters let insurers automate distribution, marketing, underwriting and claims management processes, while distributed ledger technology (DLT) is being used to raise efficiency, reduce costs and lessen the need for intermediation.

2. **New products and business models are being developed in response to evolving customer requirements and expectations**. Continuous connectivity, real-time transactions and customised attention are shaping consumer expectations for financial services, and insurance is no exception. Convenience, speed, transparency, attractive pricing and user-friendliness are all expected of new insurance products. Digital technology is also being harnessed to meet the requirements of the sharing and gig economies,[3] in the shape of on-demand[4] or usage-based insurance.[5] Other models such as peer-to-peer insurance[6] are emerging on new digital platforms that provide consumers with an alternative to traditional insurance policies.

3. **Cloud computing is a model that may enable the application of digital technologies under an efficient, scalable and flexible scheme.** Insurers[7] can offer products and services based on data collected by IoT, processed by AA, ML, AI or structured via DLT, using available-on-demand shared networks, servers, storage, applications and services that can be rapidly scaled up or down and accessed anytime and anywhere. Cloud computing may help insurers to rapidly respond to customer needs and flexibly adapt to market and technological change.

4. **The use of cloud computing is increasing in the insurance sector.** Insurance value chain activities' and key functions' operational processes are becoming predominantly supported by digital technologies. Dataset management and algorithms processing of insurance applications based in IoT, AA, ML, AI and DLT require significant computing power and IT resources, which could be built in-house and/or outsourced to a third-party provider. As more insurance products and processes become more digitalised, there may be even greater demand for computing power.

5. **Cloud computing services are being used directly by insurers and indirectly by some of their third-party service providers.** Cloud computing is being used by (i) insurers, both incumbents and licensed fintech/insurtech startups, to outsource IT resources; and (ii) third-party service providers, including fintech/insurtech startups acting as service providers, to which insurers outsource critical or

[3] As defined by Cambridge Dictionary, a sharing economy is "an economic system that is based on people sharing possessions and services, either for free or for payment, usually using the internet to organise this" and gig economy "a way of working that is based on people having temporary jobs or doing separate pieces of work, each paid separately, rather than working for an employer".

[4] Insurance that covers only the risks of specific items and events faced at a certain moment (IAIS Draft Issues Paper on the Increasing Use of Digital Technology in Insurance and its Potential Impact on Consumer Outcomes).

[5] Insurance that aligns behaviours with premium rates (IAIS Draft Issues Paper on the Increasing Use of Digital Technology in Insurance and its Potential Impact on Consumer Outcomes).

[6] Business model that allows insureds to pool their capital, self-organise and self-administer their own insurance. (IAIS Draft Issues Paper on the Increasing Use of Digital Technology in Insurance and its Potential Impact on Consumer Outcomes).

[7] For the purpose of this paper, the term insurer includes insurance and reinsurance companies.

important activities or functions (eg a third party that provides an insurer with automatic claims processing services, which in turn may use cloud services to run its AI algorithms).[8]

6. **Cloud computing may pose additional operational[9] and reputational risks.** Besides the traditional risks connected with outsourcing, the use of cloud computing expands the sources of operational and reputational risks that could impact insurers' business operations including data security and privacy, system availability, continuity of operations, interoperability, auditability and compliance with legal requirements. The impact may vary depending on the service and deployment model, type of IT assets that are stored, processed and transmitted as well as the particular usage in the business operation.

7. **Given the small number of cloud service providers, concentration risk is an issue.** At the end of 2017, more than 60% of the world's cloud computing services were provided by just five companies.[10] Due to this concentration of service providers, as well as their interconnection across the financial system, a failure of any one provider could have a potentially adverse systemic impact on the financial system. Business continuity and operational resilience may be compromised if those few providers experience a failure; or a shared environment experiences a breach and data become unavailable or is stolen; or insurers and their supervisory authorities are restricted from accessing, auditing and making on-site examinations to cloud providers located in different jurisdictions.

8. **Financial regulators, including insurance supervisors, worldwide are paying increased attention to cloud computing.** When assessing the supervisory and regulatory issues raised by the application of digital technologies to financial services, the FSB identified[11] managing operational risks from third-party service providers, including cloud computing providers, as one of 10 issues that merit authorities' attention and one of three issues seen as a priority for international collaboration.[12] Likewise, the IAIS identifies cloud computing as one of the challenges that insurance supervisors are facing in the increasing digitalisation of the insurance business.[13]

9. **This paper seeks to provide an overview of the emerging approaches that selected authorities are taking to deal with the regulation and supervision of cloud computing activities in the insurance business.** As of yet, no comparison has been made about how cloud use by insurers is regulated and supervised in different jurisdictions. This paper aims to provide an overview of the regulatory and supervisory approaches relevant to cloud computing. It is based on interviews and publicly available information relating to 14 financial authorities worldwide (as listed in Annex 1). Section 2 presents the main characteristics of cloud computing technology, its use in the insurance industry and its benefits and risks. Section 3 describes the insurance regulations that are relevant to cloud computing activities, and compares the requirements for general outsourcing with those for cloud computing. Section 4 outlines the range of emerging supervisory practices vis-à-vis insurers' cloud computing activities. Section 5 concludes.

[8] For example, the company Medin Tec, www.medin-tec.com/solutions/about.

[9] As defined by the IAIS Glossary, operational risk refers to "the risk arising from the inadequacy or failure of internal systems, personnel, procedures or controls leading to financial loss".

[10] See Synergy Research Group (2018).

[11] See FSB (2017).

[12] Furthermore, the FSB highlighted that the assessment of current oversight frameworks for important third-party service providers as well as greater global coordination between different authorities (eg financial, IT, data protection) are areas where international bodies and national authorities should seek to develop their micro- and macroprudential regulatory frameworks.

[13] See IAIS (2018).

Section 2 – Outsourcing to cloud service providers

Outsourcing of information system services

10. **Outsourcing is an arrangement between an insurer and a service provider**[14] **whereby the latter performs a process, service or activity, or parts thereof, which would otherwise be performed by the insurer itself.**[15] Some examples of activities and functions that insurers outsource include:[16]

- Marketing and research (eg product development, advertising);
- Policy administration (eg premium collection, invoicing, endorsements);
- Claims administration (eg loss reporting, adjusting);
- Investment management;
- Professional services related to the insurers' business activities (eg actuarial, risk management, accounting, compliance, internal audit);
- Human resources and back office management;
- Documents and application processing; and
- Information system services.

11. **Outsourcing to cloud service providers is generally classified as a type of information system**[17] **service outsourcing.** Information system services usually include:

- Management and maintenance services (eg data entry and processing, data centres, data centre facilities management, end-user support, local area networks management, help desks, IT security operations).
- Hosting services, which refer to IT resources and capabilities (eg software, hardware) offered by a service provider (eg cloud service provider).

Overview of cloud computing

12. **In common terms, cloud computing could be defined as a model that enables on-demand network access to a shared pool of configurable computing resources.** The US National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg networks, servers, storage, applications, and services) that can be rapidly provisioned and released with

[14] The service provider could be a supervised or non-supervised entity, and part of or not part of the insurer's financial group.

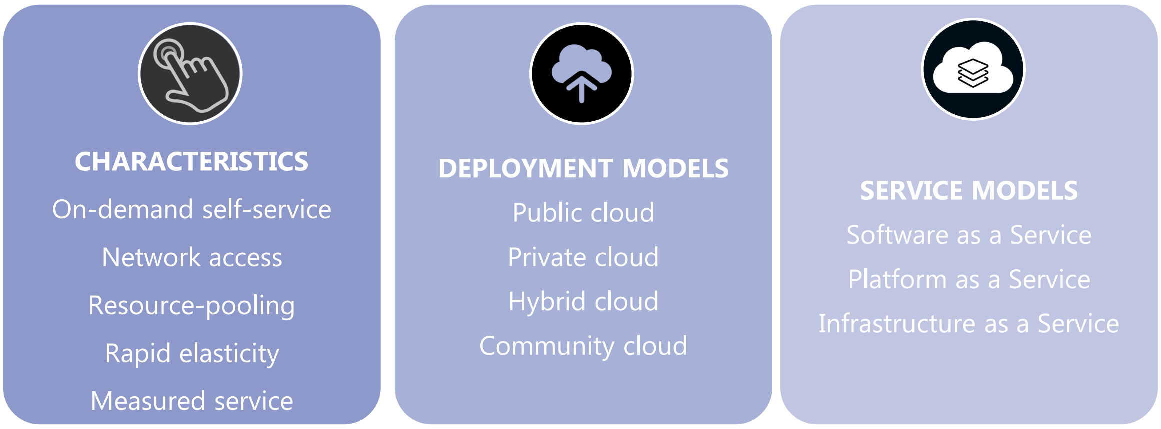
[15] A process, service or activity is generally not considered to be outsourced if it is not expected to be performed internally by the insurer (eg banking, legal, market information, courier, maintenance services; medical examinations).

[16] Which activities and functions insurers are permitted to outsource depends on each jurisdiction's regulations.

[17] According to NIST, information systems (IS) and information technology (IT) are often considered synonymous but are not. IS represents a discrete set of information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. IT is a subset of IS, defined as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Source: NIST Online glossary, https://csrc.nist.gov/glossary.

minimal management effort or service provider interaction".[18] According to NIST, cloud computing has five essential characteristics, three service models and four deployment models, as described in Figure 1.

Figure 1: Cloud computing characteristics, deployment and service models



CHARACTERISTICS

On-demand self-service

Network access

Resource-pooling

Rapid elasticity

Measured service

DEPLOYMENT MODELS

Public cloud

Private cloud

Hybrid cloud

Community cloud

SERVICE MODELS

Software as a Service

Platform as a Service

Infrastructure as a Service

13. **The main characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.**

- **On-demand self-service:** Users are able to access computing resources without any human interaction with the service provider.
- **Broad network access:** Computing resources are accessible over the network, supporting heterogeneous client platforms (eg mobile devices and workstations).
- **Resource-pooling:** The provider's computing resources are pooled to serve multiple users under a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand.
- **Rapid elasticity (scalability):** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward, commensurately with demand.
- **Measured service:** Cloud systems optimise resource use by leveraging and metering their capabilities appropriately according to the type of service. Resource usage can be monitored, measured, controlled and reported, providing transparency for the provider and user (pay-by-use).

14. **Service models refer to the type of computing resource that is offered.** There are three main types of service model: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

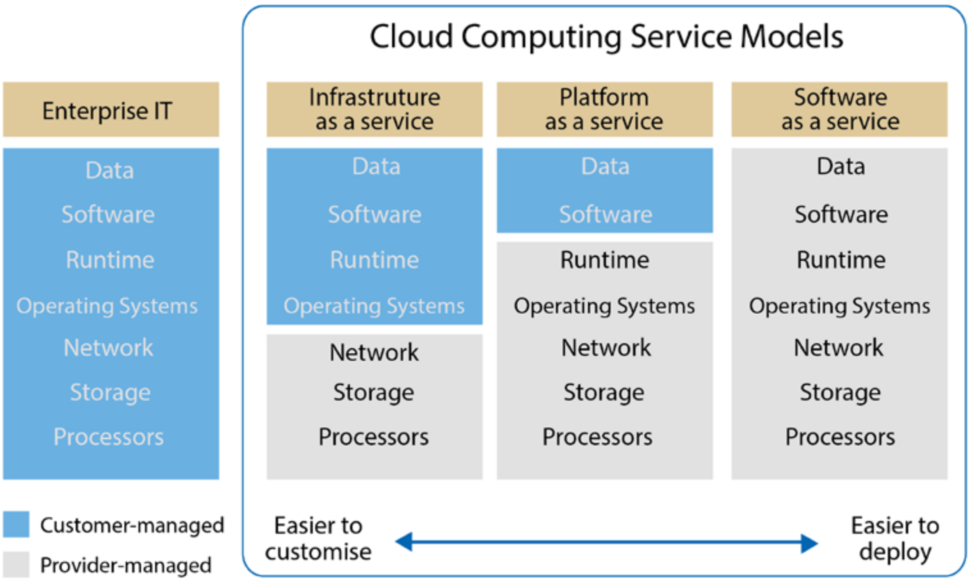
- **Infrastructure as a Service (IaaS).** Providers offer access to computer infrastructure resources as processing power, storage, servers, networks and other resources where users are able to run an operating system with applications of their choice on it. Virtualisation allows many users to share one physical server. Users have control over storage levels, operating system and specific network components.
- **Platform as a Service (PaaS).** Providers offer a computing platform where users can run and develop their own applications using libraries, languages, databases, tools and other providers' resources. This option provides users with tools for developing new online applications. Users

[18] See NIST (2011).

have control only of their own applications that run on the platform plus the platform's configuration settings.

- **Software as a Service (SaaS).** Providers offer access to application software from any device with an internet connection and web browser. Off-the-shelf applications are free or paid via a subscription, accessed over the internet from any device, facilitating collaborative working. Users have control only of configuration settings specific to the application.

Figure 2: Main types of service model



Source: US Department of the Treasury, *A financial system that creates economic opportunities.*

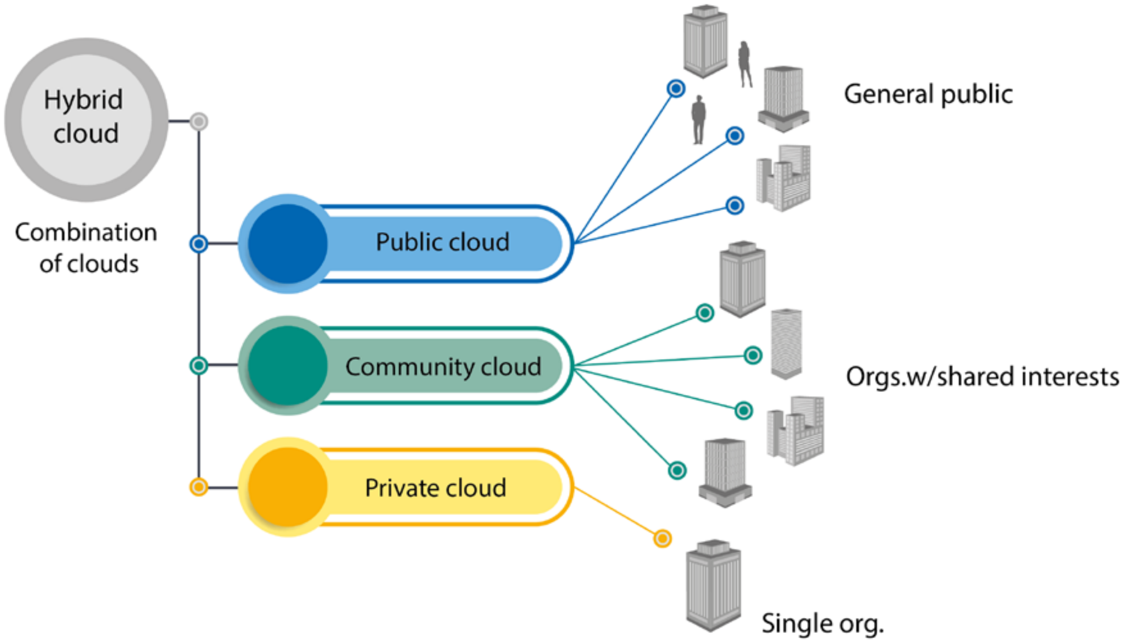
15. **Cloud computing services are constantly evolving.** As emerging technologies evolve and are applied to different use cases, new services are being offered, such as Business Process as a Service (BPaaS), Cloud Management as a Service (CMaaS), Blockchain as a Service (BaaS) or the recently launched Quantum Cloud Services.[19]

16. **Cloud computing can be deployed in different models according to the type of use.** There are four types of deployment model: private, public, community and hybrid (Figure 3). The main differences between these deployment models relate to the availability of the cloud infrastructure:

- **Public cloud**: Available for open use by the general public.
- **Community cloud**: Available for the exclusive use by a specific community of users from organisations that have shared interests.
- **Private cloud**: Available for the exclusive use of a single organisation.
- **Hybrid cloud**: Composition of two or more distinct deployment models that retain unique infrastructures but are interconnected.

[19] For example, the company Rigetti, www.rigetti.com/about.

Figure 3: Types of deployment model



17. **As new service models emerge, the use of cloud infrastructure is also evolving.** At the initial stage of cloud computing adoption, users placed their workloads on a single cloud (public or private). Some years later, the hybrid cloud emerged to offer users the benefits of both public and private models, usually with single cloud providers for each model. Recently, a new pattern of use referred to as "multicloud" has emerged. Under this approach, users have multiple cloud service providers and hence avoid depending on a single provider.

Cloud computing adoption

18. **Investment in public cloud infrastructure and services is expected to reach $160 billion in 2018.** According to the International Data Corporation (IDC),[20] worldwide spending on public cloud services and infrastructure is forecast to increase by 23.2% more than investments in 2017. The industries expected to spend the most on public cloud services in 2018 are discrete manufacturing ($19.7 billion), professional services ($18.1 billion) and banking ($16.7 billion). Software as a Service is expected to be the largest cloud computing category, representing almost two thirds of all public cloud spending in 2018. The United States is expected to be the largest country market for public cloud services in 2018, followed by the United Kingdom, Germany, Japan and China.

19. **Historically, adoption of cloud services by the insurance industry has been slower than that of other industries, focusing initially mainly on non-core applications.** Gartner (2012) reported that the insurance industry used cloud services for non-core office and business support functions such as project planning management, human resources, email, collaboration tools, web conferencing and customer relationship management.

[20] See IDC (2018).

Industry use of cloud computing, 2012

Table 1

Industry	Adopting	Maturity
Media	Content management, distribution and analytics	🟩
Education	Email, collaborative and back office SaaS and IaaS	🟦
Banking	Private cloud – SaaS and IaaS	🟥
Government	Private cloud, email and some SaaS	
Insurance	Non-core applications, limited SaaS for vertical solutions	
Manufacturing	Mostly SaaS	🟨
Retails	SaaS, IaaS and PaaS	

Advanced	🟩	Heavy	🟦	Moderate	🟥	Measured	🟨

Source: Industries aim to extend cloud computing beyond support functions to more strategic uses; Gartner (2012).

20. **In recent years, some insurers have changed their approach and are now using cloud based infrastructure to support their core functions.**[21] Public, private and hybrid cloud infrastructures are being adopted to support key business functions such as:

- Product development, for introducing new business models based on digital applications.
- Policy and underwriting administration, for capturing real-time information on customers risk profiles, quote creation, auto-generated policy documents, endorsements, cancellations and renewals.
- Claims management, for automation of loss and claims valuation, adjustments and reports.
- Billing and receivable systems, for automation of premium billing, reimbursement, reports and connection with accounting systems.
- Actuarial and financial models, for providing scalable computing resources according to workload.

21. **Most of the global systemically important insurers (G-SIIs)**[22] **listed in 2016 are using cloud computing services and infrastructures.**[23] These insurers have adopted cloud computing as part of their digital transformation, with the aim of meeting changing customer needs, supporting innovation and making efficiency gains.

Benefits and risks of cloud computing

22. **How far users can benefit from cloud computing depends on how it is used and the deployment and service model that is implemented.** In general, the potential benefits of cloud computing can include savings in IT costs, access to qualified talent and capabilities, flexibility (scaling on-demand), faster deployment cycles and faster innovation. Some specific advantages that have been identified for each deployment model are shown in Table 2.[24]

[21] See Lambert (2014).

[22] According to the FSB, the 2016 list of global systemically important insurers include Aegon, Allianz, American International Group, Aviva, AXA, Metlife, Ping An Insurance Company, Prudential Financial, and Prudential.

[23] See Ratcliff.

[24] See Maletski (2018).

Examples of cloud computing benefits by deployment model Table 2

Public cloud	Community cloud	Private cloud	Hybrid cloud
Cost-saving: organisations pay only for the services they use	Cost-effectiveness: organisations share costs of a private cloud model for specific community needs.	Increased flexibility: computing resources are customised according to the organisation's IT requirements	Cost-effectiveness: organisations pay for extra computing resources only when necessary
Virtually unlimited scalability: computing resources are available according to demand	High scalability: computing resources are available according to demand	High scalability: computing resources are available according to demand	Flexibility: additional resources of the public cloud may be available on demand
High reliability: business continuity supported by vast network of servers	Tailored security: security levels according to community needs.	High and tailored security: high control and security levels since resources are not shared	Control and security: organisations can maintain a private cloud for sensitive assets
Agility and availability: reduced time-to-market and fast implementation		Risk-averse: provides data preservation during an outage	Risk-averse: provides data preservation during an outage

Source: FSI staff.

23. **Given its particular nature, cloud computing may pose specific risks that may vary according to the use and type of deployment and service model.** According to the European Union Agency for Network and Information Security (ENISA), some of the main risks[25] that cloud computing services pose to organisations are shown in Table 3.

[25] See ENISA (2012).

Examples of cloud computing security risks

Table 3

Policy and organisational	
Lock-in	Clients that rely strongly on the services of one cloud provider may experience severe difficulties if migrating to another provider or back to an in-house IT environment.
Loss of governance	Control is ceded by the client to the cloud provider regarding cloud infrastructure and other issues that may affect security.
Supply chain failure	If a cloud provider outsources parts of its production chain to third parties, or uses services of another cloud provider, potential for cascading failures may be created.
Technical	
Isolation failure	Failures, errors or attacks in shared environments may lead to situations where one tenant has access to another tenant's resources or data.
Malicious insider	Various kinds of damage may be caused to a consumer's assets if an insider at the cloud provider abuses a high-privilege role.
Management interface compromise	To manage and interact with cloud services, clients use application programming interfaces (APIs) that are internet-accessible, which may increase their exposure to attacks.
Insecure or ineffective deletion of data	Given the clients' reduced visibility of the physical location of data, as well as reduced ability to verify complete data deletion, a client's information may not be completely deleted from all cloud providers' resources.
Legal	
Data protection	Clients may experience difficulties in checking compliance of cloud providers to data protection legislation since data may be processed and stored in different locations and even between different clouds.

Source: ENISA.

24. **Specific risks posed by cloud computing may increase the operational and reputational risks of insurance companies.** Operational risks caused by failures in data security and privacy, system availability, continuity of operations, interoperability, auditability and compliance with legal requirements may be increased by cloud computing activities, impacting insurers' business operations and their financial situation. The impact may vary depending on the service and deployment model, type of IT assets that are stored, processed and transmitted as well as the particular usage in the business operation. Nonetheless, as a result of those cloud computing failures, it is possible to foresee reputational risks[26] emerging from, for example, unauthorised access to sensitive or restricted information or impossibility to access information due to disruption in the cloud provider operations.[27]

25. **Information security risks related to cloud computing, in particular cyber-risks, are a particular concern to financial sector authorities.** Business continuity of financial firms may be impacted by cyber-attacks and outages[28] of a small number of cloud providers, which are not regulated under the same prudential principles as the financial sector. In the past decade, there have been various outages of Microsoft, Amazon, Google, Verizon and Salesforce. Their clients were affected in various ways, ranging

[26] The Reputation Institute defines reputational risk as the likelihood of negative events, as well as public opinions and perceptions, adversely impacting an entity's income, brand, support, and public image. See: https://www.reputationinstitute.com/blog/what-reputational-risk.

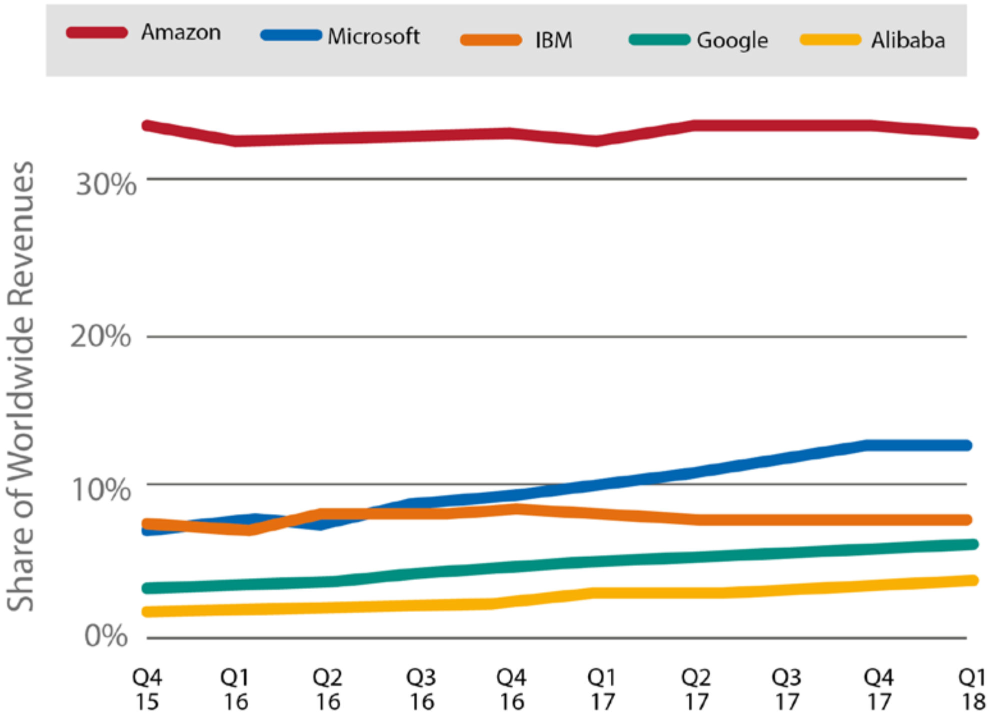
[27] See Morris (2018).

[28] Events when cloud services are unavailable for a period of time, caused by various factors such as environmental (eg flooding of a data centre), adversarial (eg distributed denial of service attack), accidental (eg improperly tested or updated) or structural causes (eg loss of primary, secondary and back-up power systems).

from being unable to access hosted services for between eight hours to five days or even losing recently written data, affecting the business operations of their clients.[29] A recent report published by Lloyd's and AIR Worldwide[30] estimated that a sustained outage of a major cloud provider would leave 12.4 million businesses in the United States with no access to their IT services. Finance and insurance institutions would be in the top five industries most impacted, with estimated losses of $447 million. To support the development of third party cyber risk management in the financial sector, the G-7 developed a set of fundamental elements on governance, risk management, incident response, contingency planning, monitoring for potential systemic risks and cross-sector coordination to mitigate the impact and severity of cyber-attacks. [31]

26. **Reliance on a relatively small number of highly dominant providers may result in systemic risk for cloud users.** Graph 1 shows that, as of Q1 2018, the main global providers of cloud infrastructure services are Amazon, Microsoft, IBM, Google and Alibaba, where Amazon is currently the leader.[32] Under this market structure, some authorities have raised concerns about concentration risks within the insurance and banking sector, as an increasing number of financial institutions are relying on a limited pool of cloud service providers,[33] increasing the threat of contagion in the event of a service failure.[34]

Graph 1: Market share trend of cloud infrastructure services (IaaS, PaaS and Hosted Private Cloud)



Source: Synergy Research Group.

[29] See Lloyd's and AIR (2018).

[30] See Lloyd's and AIR (2018).

[31] See G7 (2018).

[32] See Synergy research group (2018a).

[33] See Lee (2018).

[34] See Byres (2018).

Section 3 – Regulation of insurers' use of cloud computing

27. **Authorities are enhancing their prudential frameworks to oversee insurers' cloud computing activities.** The authorities covered in this paper (hereinafter, we refer to only as "authorities") are enhancing their regulatory framework to (i) ensure that insurers have effective risk management and internal control systems for their cloud computing activities; (ii) obtain the necessary information to conduct effective supervision of insurers; (iii) monitor market behaviour and trends; and (iv) take preventive and corrective measures that are timely, suitable and necessary to achieve the objectives of insurance supervision.

28. **This section discusses the range of approaches that these financial supervisory authorities have adopted to regulate the use of cloud computing by insurance companies**. Their regulatory approaches rely mainly on binding requirements and supervisory recommendations. The latter tend to take the form of sound practices, principles, guidance or supervisory expectations. Insurers' cloud computing activities may also be subject to data protection and information security laws or regulations issued by other authorities. These laws and regulations are not covered in this paper.

29. **A variety of regulatory approaches exist towards insurers' use of cloud computing.** As shown in Table 4, they include the following:

- **Applying the relevant regulations of the general outsourcing framework to cloud computing.** Authorities that follow this approach include APRA, OSFI, HKIA, IRDAI, SAMA, MAS, FINMA and FCA. Cloud computing is either assumed to fall under these regulations, or a specific section is allocated to cloud computing within the regulations (eg MAS). In general, outsourcing frameworks are based on the Joint Forum high-level principles on outsourcing.[35]

- **Applying the relevant regulations of the governance and risk management framework to cloud computing.** Authorities that follow this approach include the ones that apply the EU Solvency II Directive, where outsourcing provisions are part of the governance and risk management framework (EIOPA, ACPR, BaFin, DNB and PRA) as well as other authorities with governance and risk management regulations, such as APRA, HKIA, IRDAI, FINMA and NAIC.

- **Applying the relevant regulations of the information security framework to cloud computing.** Authorities that follow this approach include APRA,[36] OSFI, BaFin, IRDAI, SAMA, MAS and NAIC. While these regulations are generally relevant to the use of cloud computing, IRDAI, SAMA and MAS include specific sections on cloud-specific requirements. Information security regulations are usually based on the G7's *Fundamental elements of cybersecurity for the financial sector*.

- **Cloud-specific recommendations or supervisory expectations.** APRA, OSFI, ACPR, BaFin, DNB and FCA have either provided guidance/recommendations or clarified their regulatory expectations in circulars, memos, sound practices papers and other published materials on the use of cloud computing.

[35] See Joint Forum (2005).

[36] Currently a cross-sectoral information security regulation is under consultation. See APRA (2018a).

Supervisory authority regulations, expectations and statements applying to cloud computing

Table 4

Frameworks	Outsourcing		Governance and risk management		Information security	
	General	Cloud-specific	General	Cloud-specific	General	Cloud-specific
APRA	🟩	🟨	🟩		🟩 *	
OSFI	🟩	🟨			🟩	
EIOPA			🟩			
ACPR			🟩	🟨		
BaFin			🟩	🟨	🟩	
HKIA	🟩		🟩			
IRDAI	🟩		🟩		🟦	🟦
DNB			🟩	🟨		
SAMA	🟩				🟦	🟦
MAS[37]	🟦	🟦			🟦	🟦
FINMA	🟩		🟩			
FCA	🟩	🟨				
PRA			🟩			
NAIC			🟩		🟩	

* Currently under consultation process.

🟩 General framework 🟨 Cloud-specific statement 🟦 General framework with a specific section on cloud

30. **Many authorities apply their cloud computing regulatory framework in a proportionate manner.** Both binding and non-binding requirements are generally applied on a proportionate basis (ie they are envisaged to be tailored to reflect the size, complexity or risk profile of financial institutions or, as relevant, the outsourced service). Regarding the latter, APRA applies different notification and consultation requirements depending on the inherent risk of the cloud computing outsourcing arrangement.[38]

31. **There are a variety of approaches for categorising different types of cloud computing as outsourcing activities**. For DNB, BaFin[39] and the FCA, cloud computing involving third-party services qualifies as a form of outsourcing, regardless of the exact form of the cloud service used. ACPR turns its attention mainly to the pooling of services of public or hybrid cloud models, as well as any external private cloud model in which services provided to an insurer are pooled with those offered to other customers. For APRA, its regulation applies to all arrangements involving the sharing of IT assets with other parties (whether labelled cloud or otherwise), including public cloud, virtual private cloud and community cloud arrangements, but excluding arrangements where IT assets are dedicated to a single APRA-regulated entity (eg private cloud).

[37] MAS Outsourcing and Technology Risk Management Guidelines are not legally binding and are used to set out MAS expectations on financial institutions on a non-mandatory basis.

[38] APRA classifies cloud services risks depending on its usage into three types: low, heightened and extreme. For examples of low, heightened and extreme inherent risks, see APRA (2018b).

[39] BaFin treats outsourcing to the cloud as a form of outsourcing. Nevertheless, not every use of a cloud solution is outsourcing subject to the specific outsourcing control (assessments are done on a case-by-case basis).

Analysis of general and cloud-specific requirements and recommendations

32. **Cloud-specific requirements and recommendations are typically found in regulations on certain topic areas.** These topics are assessment of materiality; governance; due diligence; risk assessment of outsourcing arrangements; data protection and security; location; subcontracting; business continuity and exit strategy; monitoring and control; and audit and access. The analysis below outlines the requirements in these areas, distinguishing between those that are general requirements from those directly related to cloud services.

a) Assessment of materiality, criticality or importance

General

33. **In general, authorities apply their outsourcing regulations to material, critical or important activities that insurers outsource to third parties.**[40] Authorities use different criteria or consider different factors in assessing whether an outsourced activity or function is material, critical or important. Some common factors that authorities consider in making these assessments include the following:

- The potential impact of any failure or disruption of the outsourced activity or function on the risk profile, risk management, financial situation, business operations or reputation of the insurer;
- The insurer's ability to meet its legal and regulatory requirements as a result of any failure or disruption of the outsourced activity or function;
- The cost of outsourcing as a share of net assets and/or total operational costs; and
- The degree of difficulty involved in finding an alternative provider or bringing the activity back in-house.

34. **Use of customer data-specific materiality criteria is not common.** For instance**,** MAS uses this criterion by requiring that all outsourcing arrangements which expose customer information to potential unauthorised access or disclosure, loss or theft are classified as material outsourcing.

Cloud-specific

35. **Generally, the materiality criteria applied to general outsourcing also apply to cloud computing services.** Under MAS regulations, for example, insurers' use of cloud computing that involves the storage in the cloud of customer information would be considered as material outsourcing. APRA and ACPR also recommend that the nature, sensitivity and criticality of customer data are considered in the materiality assessment of the cloud computing arrangement. OSFI, EIOPA, HKIA and SAMA, on the other hand, give examples in which cloud computing may be considered a material or important outsourced function under the classification of information system management outsourcing.

b) Governance

General

36. **All authorities expect their regulated institutions to retain full responsibility and accountability of outsourced services.** These responsibilities and accountabilities cannot be delegated to the service provider. As such, their Board and senior management (and/or other delegated bodies or

[40] Examples of activities and functions considered material are marketing and research, policy administration, claims administration, investment management, professional services related to insurers' business activities, human resources management, information system services etc.

individuals)[41] are ultimately responsible for ensuring that the outsourcing is conducted in a safe and sound manner, in compliance with applicable laws and regulations. This involves Board approval for a written outsourcing policy and, in some cases, the senior management assigning specific responsibilities with regard to the effective implementation of the policy. One authority (PRA) is strengthening its accountability and duty of responsibility regulations, extending requirements of senior managers and certification regimes to insurers, with the aim of promoting clearer accountability for outsourcing, cyber and operational resilience.

Cloud-specific

37. **As with the general outsourcing regulations, authorities typically require the Board and senior management to play a key role with respect to the material use of cloud computing.** In general, authorities require the Board and senior management of supervised institutions[42] to define the technological strategy and corresponding corporate objectives, including those related to material outsourcing to the cloud. In addition, the Board and senior management are generally responsible for (i) allocating responsibility for the day-to-day management of the use of cloud computing; (ii) defining the associated organisational and operational structure to identify, manage, monitor and mitigate cloud computing risks; and (iii) ensuring there are staff with sufficient skills and resources to oversee and control the associated risks.

38. **Authorities expect insurers to keep their Boards and senior management appropriately informed of material cloud computing services throughout the key stages of the outsourcing process.** This includes when the cloud computing proposal has been identified, the transition plans are in place and, finally, during the execution phase. APRA, for example, highlights the importance of keeping the governance authority informed regarding the current status and emerging risks and issues related to cloud computing.

c) Due diligence

General

39. **Due diligence requirements already feature in authorities' general outsourcing frameworks.** The most common factors that authorities require insurers to assess are the service provider's knowledge, expertise, staff qualifications and financial capacity, as well as the adequacy of its contingency and business continuity plans.

Cloud-specific

40. **The focus of due diligence requirements for cloud computing services is somewhat different from that for general outsourcing frameworks.** Some authorities that have issued guidance, recommendations or supervisory expectations for cloud computing, focus their due diligence requirements on the adequacy of service providers' risk management and internal control systems, information security capabilities and compliance with data protection and information security legislation (APRA, ACPR, FCA, IRDAI and MAS).

41. **The IT capabilities of service providers are a major focus for a few authorities.** In the FCA guidance, insurance firms are advised to take into account the service providers' adherence to international IT standards (eg ISO 27000 series). Meanwhile, MAS explicitly requires that the insurer conducts an assessment of the service providers' ability to recover outsourced systems and IT services within the stipulated recovery time objective.

[41] For instance, APRA calls it "appropriate governance authority" and the ACPR refers to the "governing bodies".

[42] This includes their delegated bodies and/or individuals.

d) Risk assessment

General

42. **Before any material outsourcing takes place, all authorities require insurers to evaluate the risks associated with an outsourcing agreement.** Insurers are expected to have a framework for risk evaluation that includes (i) identification and understanding of potential risks that might arise from the outsourcing arrangement; (ii) evaluation of the impact on the firm's business strategy, assessment of the firm's financial situation and overall risk profile; (iii) identification of risk mitigation strategies; and (iv) analysis of the benefits of outsourcing against the risks that may arise.

43. **Authorities also typically outline a list of risks that should be included in risk assessments.** Risks that are commonly specified in outsourcing regulations include operational risk, concentration risk, reputational risk, strategic risk and compliance risk.

Cloud-specific

44. **Risk assessment requirements for cloud computing services are narrower and more focused on data-related issues.** Authorities that have issued recommendations or supervisory expectations on cloud computing require firms to focus their risk assessment on risks related to data confidentiality, availability and security. In this context, risk assessments should take into account identification, classification and importance of data stored and processed in the cloud, as well as the institution's legal and regulatory requirements. In some cases, the risk assessment framework also refers to testing security events. For instance, APRA recommends the use of scenario analysis to test the possibility that extreme but plausible security events may compromise the confidentiality, integrity and availability of information located in the cloud.

e) Data protection and security

General

45. **Most authorities require insurers to pay special attention to data protection and security issues in the outsourcing agreement.** APRA, OSFI, BaFin, HKIA, IRDAI, SAMA, MAS, FINMA, FCA and EIOPA require the outsourcing agreement to ensure that the provider protects any confidential information related to the insurer, its policyholders, beneficiaries, employees, contracting parties and all other persons, establishing policies and procedures for disclosing information and monitoring security practices. Additionally, insurers and their providers are expected to comply with data protection and information security laws or regulations issued by other authorities (ie the General Data Protection Regulation for the EU).

46. **Some authorities are more specific with respect to requirements regarding data protection and security clauses.** For example:

- OSFI emphasises ownership and access of all assets (intellectual and physical) related to outsourcing arrangements and also confidentiality, security and separation of property.
- IRDAI emphasises information and asset ownership rights, IT, data security and protection of confidential information and also mentions data retrieval in the event of the arrangement's termination.
- MAS stipulates specific steps that insurers must take to protect the confidentiality and security of customer information.
- NAIC requires insurers to follow certain steps when they learn that a cyber-security event has or may have occurred in a system maintained by a third-party provider.

Cloud-specific

47. **The focus on data protection and security is particularly intense for cloud computing services.** Authorities expect insurers to understand the nature and strength of the cloud service provider's controls to minimise the risk of loss of data confidentiality, integrity and availability. A number of authorities (APRA, ACPR, IRDAI, SAMA and MAS) are explicit in this area and recommend supervised institutions to pay special attention to data classification (according to sensitivity), data segregation (in particular, to clearly identify and segregate customer data), data access, data security (including encryption requirements), data retention and loss prevention, data incident notification and data destruction. A few authorities are emphasising the importance of allocation of responsibilities in sharing environments. For instance, APRA highlights the importance of the control environment and the careful consideration of the allocation of control responsibilities between the provider and the insurer client (commonly referred to as the shared responsibility model).

48. **Some authorities expressly require supervised institutions to ensure that cloud service providers adopt and implement sound cyber-security controls for protecting the confidentiality, integrity and availability of data**. For instance, IRDAI requires insurers to have a contract clause for ensuring data protection and integrity; SAMA requires insurers to ensure that cyber-security requirements established in the outsourcing policy are appropriately addressed before, during and while exiting outsourcing contracts; and OSFI recommends that supervised institutions have processes in place to ensure timely notification of cyber-incidents by cloud service providers.

f) Location

General

49. **When outsourcing outside their jurisdiction (or offshoring[43]), authorities expect insurance companies to pay special attention to the unique risks it brings**. Offshoring, for example, may pose restrictions on the insurers' or their supervisors' rights regarding audit and access to information. Other risks related to offshoring include country risk, compliance and legal risk, contractual risk and counterparty risk. Insurers are expected to assess these risks and adjust their risk management framework accordingly. One authority (FINMA) requires that insurers should maintain in Switzerland all information that could be needed for resolution purposes.

50. **As such, authorities expect insurers to consider specific issues when entering into offshoring.** These include whether or not:

- Contractual provisions are recognised in the foreign jurisdiction and can be enforced in the chosen jurisdiction.
- Data standards in the foreign jurisdiction are in accordance with the laws and regulations in the insurer's jurisdiction.
- Foreign jurisdiction's laws or regulations restrict access to information on outsourced functions or activities and to the service provider's business premises.
- Dispute resolution with the service provider is possible in the insurer's jurisdiction.

[43] In some jurisdictions, offshoring expressly refers to arrangements where the physical location of an outsourced activity is in a foreign jurisdiction, regardless of the location of the service provider. However, in other jurisdictions, offshoring refers to outsourcing to providers located outside the authorities' jurisdiction.

Cloud-specific

51. **Authorities also expect their supervised institutions to pay special attention to data location in relation to cloud computing services**. This means requiring insurers to have a clear understanding of the legal environment of the jurisdictions in which their data will be stored, processed and managed. This is to ensure that there are no restrictions on audit and access rights for the insurer's monitoring activities and compliance with regulations, and for authorities' supervisory functions.

52. **Only a few authorities have imposed data location restrictions on cloud computing.** Only a few authorities currently require that data be hosted locally. For example, IRDAI requires that records including those maintained in electronic mode, pertaining to all the policies issued and claims made in India shall be held in data centres located and maintained in India,[44] as well as the electronic maintenance of core business records.[45] In other cases, authorities require authorisation[46] or previous consultation[47] when cloud services are to be provided outside the jurisdiction. Additionally, FCA recommends that insurers should agree with the service provider on a data residency policy. This sets out the jurisdictions in which the firm's data can be stored, processed and managed. Moreover, APRA recommends that supervised institutions consider the benefits of Australian-hosted options, in the absence of any compelling business rationale to do otherwise, as a way of reducing inherent risks. MAS, meanwhile, highlights the importance of ensuring cross-border network redundancy since the resiliency of critical systems that are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links.

g) Subcontracting

General

53. **Authorities generally require that outsourcing contracts clearly specify that service providers retain full responsibility for and oversight of the services that it has subcontracted.** Three authorities (BaFin, MAS and OSFI) specifically mention that audit and access rights also include subcontracting providers.

Cloud-specific

54. **Authorities that have cloud-specific requirements generally include requirements for the subcontracting of cloud services.** For instance, BaFin and FCA expect supervised institutions to identify all material service providers in the supply chain, review subcontracting agreements and ensure that the requirements on the supervised institution can be complied with throughout the supply chain.

h) Business continuity and exit strategy

General

55. **In general, authorities require supervised institutions to have arrangements in place to maintain their operations if a disruption in the provision of outsourced services occur.** It is expected that these arrangements will include a business continuity plan and an exit strategy. The former typically refers to the service provider's capabilities to recover and resume its services. The latter generally includes the transfer of the services to another provider or the capability to bring those services back in-house.

[44] See IRDAI (2015).

[45] See IRDAI (2017b).

[46] For instance, SAMA.

[47] For example, APRA.

Cloud-specific

56. **Authorities with cloud-specific requirements expect insurers to have strong recovery and resumption capabilities.** Supervised institutions are expected, when considering cloud computing, to assess whether the cloud service provider has adequate plans and resources to ensure the institutions' continuity of operations, including recovery and resumption capabilities. It is also envisaged that the recovery and resumption expectations should be documented, including the plans for communicating and regularly updating and testing the adequacy and effectiveness of those capabilities. Specific business continuity commitments on the part of the cloud provider generally include maximum duration of downtime and maximum allowable loss of data.

57. **Authorities with cloud-specific requirements also expect insurers to have comprehensive and documented exit plans.** Supervised institutions are expected to ensure that they are able to exit cloud outsourcing arrangements, if necessary, without undue disruption to their operations. This requires the development and implementation of exit plans that allow the removal and transfer of existing activities in an orderly, controlled and sufficiently tested manner under robust transitional arrangements. Two key elements of the exit strategy are (i) the complete removal and deletion of data from all locations where it is stored, managed or processed; and (ii) the supervised institution's ability to re-absorb the outsourced activity. Conditions of reversibility are generally defined when subscribing the outsourcing agreement including the format of returned data and their subsequent destruction at the service provider.

i) Monitoring and control

General

58. **Authorities require insurers to have monitoring and control frameworks in place for their outsourcing arrangements.** As part of the general outsourcing requirements, supervised institutions are required to monitor the performance and viability of outsourcing providers and to take corrective measures when required. In general, authorities expect supervised institutions to develop and maintain an oversight framework that facilitates the assessment of performance against agreed service levels as well as the ongoing viability of the provider and the outsourced service. The framework typically captures changes, among others, in the service location, subcontracting agreements and control environment. Finally, the framework also generally allows a timely response to issues and emerging risks.

Cloud-specific

59. **Authorities with cloud-specific requirements expect insurers to have strong oversight of security aspects relating to cloud computing.** In general, supervised institutions are required to implement oversight mechanisms that are the same as those for general outsourcing. However, some authorities require additional elements for insurers' monitoring and control of their cloud computing activities. This is especially the case when it comes to controls to ensure sound cyber-security practices. SAMA, for example, expects that cyber-security controls in hybrid and public cloud services are periodically measured and evaluated.

j) Audit and access

General

60. **Authorities require the outsourcing contracts to clearly stipulate the audit requirements and access rights.** These audit and access rights refer to those of the insurer, its auditor or appointed

representative and the supervisory authority.[48] As mentioned above, MAS and OSFI specifically mention that audit and access rights should also apply to all significant subcontracting arrangements.

61. **In general, authorities expect to be able to request information from service providers.** These requests are typically made through the supervised institution, and the ability to do so should be specified in the outsourcing contracts.

Cloud-specific

62. **Specific recommendations or supervisory expectations for cloud computing emphasise the importance of granting rights of audit and access to the insurer, its auditors and the authority.** These rights are generally included as a specific clause in the contract. Some authorities have included cyber-specific requirements regarding audit and access rights. For example, SAMA requires that insurers should have the right to perform a cyber-security audit and a cyber-security examination at the cloud service provider while ACPR recommends that insurers require their cloud service providers to conduct penetration and vulnerability tests. The FCA, issued comprehensive guidance for audit and access rights that supervised institutions should consider regarding access to data, access to business premises and regulatory access.

63. **Some authorities are considering the use of pooled audits.** For example, BaFin allows insurers on a case-by-case basis to exercise certain rights of audit vis-à-vis cloud service providers through pooled audits together with other insurance companies, given that the choice of audit procedure must not result in a restriction of the rights of audit.

Areas of emphasis

64. **Regulations and recommendations on cloud computing are most rigorous in specific areas.** These are data protection and security, location, business continuity and exit strategy, monitor and control, and audit and access rights (Table 5).

Areas where cloud computing regulations and recommendations are most rigorous

Table 5

Area	Relevant	Special emphasis
Materiality assessment	✓	
Governance	✓	
Due diligence	✓	
Risk assessment	✓	
Data protection and security		✓
Location		✓
Subcontracting	✓	
Business continuity and exit strategy		✓
Monitor and control	✓	
Audit and access		✓

Source: FSI staff.

[48] Only regarding information related to the functions or activities that are subject of the outsourcing agreement.

Comparison with cloud-specific requirements for banks

65. **Banking regulatory frameworks for cloud computing are very similar to the ones applied by insurance supervisory authorities.** Given that banks are increasingly using cloud computing services, banking authorities have also been enhancing their regulatory frameworks in this area. For instance, in December 2017, the European Banking Authority (EBA) published a set of recommendations with regard to outsourcing to cloud service providers.[49] The recommendations came into force in July 2018. Table 6 compares the main elements of the EBA recommendations with the cloud-specific requirements for insurers, and highlights the overlaps and differences.

Cloud-specific requirements and recommendations

Comparison between EBA recommendations and insurance authorities' regulatory approaches Table 6a

Topic	EBA	Insurance authorities
Materiality assessment	Prior to any outsourcing, institutions should consider criticality and the inherent risk profile of the outsourced activity, impact of outages, confidentiality breaches or failures of data integrity and potential disruptions.	Insurers are subject to the same requirements, except considering the impact of outages, confidentiality breaches or failures of data integrity as part of the materiality assessment. Only one authority includes explicitly the impact of confidentiality breaches or failures of data integrity as a criteria for assessing materiality of cloud computing arrangements.
Security of data and systems:	Written contracts and service level agreements should oblige the cloud service provider to protect data confidentiality and to ensure continuity of services. Institutions should monitor performance of activities and security measures in line with CEBS guidelines	Insurers are subject to very similar requirements. Additionally, one authority emphasises the importance of the allocation of control responsibilities between the provider and the insurer.
Location of data and data processing	Institutions should pay special attention to location considerations, since legal risk, compliance issues and oversight limitations should be assessed regarding the countries where data are provided and stored.	Insurers are subject to the same requirements. However, a few authorities currently require that data be hosted locally. In some cases, authorities require authorisation or previous consultation when cloud services are to be provided outside the jurisdiction.
Chain outsourcing	(i) Institutions should agree that the cloud provider subcontracts part of its service to another provider only if the subcontractors will also fully comply with the same obligations of the cloud service provider. (ii) Agreements should specify types of activity that are excluded from potential subcontracting as well as an obligation for the cloud service provider to inform the institution of any planned significant changes to subcontractors or subcontracted services.	Insurers are subject to the same requirements under (i). Only a few authorities require that insurers comply with the same requirements under (ii).
Contingency plans and exit strategies	Institutions should define and implement arrangements to maintain the continuity of their business in the event that the provider fails or service deteriorates. These arrangements should include contingency planning and an exit strategy.	Insurers are subject to the same requirements.

[49] See EBA (2017).

Cloud-specific requirements and recommendations

Comparison between EBA recommendations and insurance authorities' regulatory approaches Table 6b

Topic	EBA	Insurance authorities
Access and audit rights for both institutions and competent authorities	A written agreement should be in place in which the provider undertakes the obligation to provide full of access to its business premises and to the full range of devices, systems, networks and data used in the outsourcing process, to the institution, its auditor or any third party appointed for this matter. In this area, pooled audits, third-party certifications and third-party or internal audit reports could be considered when the institution does not employ its own audit resources.	Insurers are subject to the same requirements, except pooled audits. Only a few authorities are currently considering the use of pooled audits. Additionally, some authorities require that insurers should have the right to perform a cyber-security audit and examination at the cloud service provider, while others require insurers to conduct penetration and vulnerability tests on providers.
Duty to adequately inform supervisors	Institutions should (i) make available to competent authorities specific information on the cloud service provider, the outsourced activity and the agreements; and (ii) maintain an updated register of information on all their material and non-material activities outsourced to cloud service providers.	Insurers are subject to the same requirements under (i) and (ii). Additionally, some authorities require insurers to submit detailed reports on their outsourcing activities, including cloud computing.

Section 4 – Supervisory practices

66. **Authorities are enhancing their approaches to supervise insurers' cloud computing activities.** These supervisory practices are often risk-based and proportionate, taking into account the nature, scale and complexity of the insurers' operations and the materiality of the cloud computing arrangement service. These practices include formal or informal communication with the supervisor and on-going supervision once the cloud service is in place.

Communication of cloud computing plans

67. **Authorities have different approaches as to how they wish to be informed of their supervised insurers' cloud computing plans.** These range from requiring insurers to provide informal notification to requiring insurers to seek explicit prior authorisation (Table 7). The following describes these different approaches:

- **Notification.** Most authorities in this study require to be informed/notified about any material outsourcing to the cloud (APRA, ACPR, EIOPA, BaFin, HKIA, DNB, FCA and PRA). This notification may take place either ex ante or ex post and involve a variety of formalities, including, for example, a formal communication using pre-defined templates with information regarding name and address of service provider, description of the outsourced service, business rationale for outsourcing, among other relevant information. The HKIA, for example, requires insurers to make the notification three months before the day on which the new outsourcing arrangement is proposed to be entered into or the existing arrangement is proposed to be varied significantly. BaFin requires that all documentation be submitted in German, although it could be submitted in English after prior consultation with the authority.

- **Consultation.** Australian supervised institutions are required to consult with APRA prior to entering into an outsourcing arrangement involving material business activity where offshoring is involved. Regarding cloud computing arrangements, APRA classifies cloud services risks depending on its usage into three types: low, heightened and extreme.[50] APRA encourages prior consultation when the use of cloud computing involves "heightened or extreme inherent risks" regardless of whether offshoring is involved. APRA's objective is to ensure that institutions understand and have the capability to manage these risks. There is no need for consultation with APRA prior to entering into low inherent risk arrangements. For uses involving extreme inherent risk, APRA encourages early engagement. This gives APRA the scope to provide feedback on any areas of potential concern prior to the APRA-regulated entity committing large amounts of resources to the initiative. Proposals with extreme inherent risk will be subject to a greater level of scrutiny by APRA, both initially and as the initiative progresses.
- **Authorisation.** A smaller group of authorities require previous authorisation before outsourcing any material services to the cloud. Within our sample, FINMA and SAMA require their supervised institutions to obtain approval before entering into material outsourcing arrangements. Furthermore, in Saudi Arabia, financial institutions should obtain SAMA's approval before "using cloud services or signing the contract with the cloud provider".
- **Other.** One authority in this study requires neither notification nor authorisation but reserves the right to make modifications to the outsourcing arrangements.

Communicating cloud computing plan to the authority

Table 7

	Notification	Consultation or authorisation
APRA	Yes, for outsourcing arrangements involving cloud low inherent risks.	Consultation, for outsourcing arrangements involving material activities where offshoring is involved and for arrangements involving cloud heightened or extreme inherent risks regardless of whether offshoring is involved.
OSFI	No	No
EIOPA	Yes, for outsourcing arrangements involving critical or important functions.	No
ACPR	Yes, for outsourcing arrangements involving critical or important functions.	No
BaFin	Yes, for outsourcing arrangements involving critical or important functions.	No
HKIA	Yes, for material outsourcing arrangements.	No
IRDAI	No	No
DNB	Yes, for material outsourcing arrangements.	A form of consultation is required.
SAMA	No	Authorisation, for material outsourcing and for any cloud service arrangement.
MAS	No	No
FINMA	No	Authorisation, for outsourcing arrangements involving significant or control functions relevant to the business plan.
FCA	Yes, for material outsourcing arrangements.	No
PRA	Yes, for outsourcing arrangements involving critical or important functions	No
NAIC	No	No

[50] For examples of low, heightened and extreme inherent risks, see APRA (2018b).

68. **Regardless of the communication approach, authorities expect insurers to conduct prior risk assessments and interact with their supervisor on their material cloud computing plans.** Most authorities expect supervised institutions to have performed comprehensive cloud computing risk assessments before entering into the outsourcing arrangements. Also, informal communications and consultations typically take place when a supervised institution is considering material outsourcing arrangements regardless of the above-mentioned approaches.

On-going supervision

69. **In general, cloud computing is supervised as part of the operational risk reviews that authorities conduct when undertaking a comprehensive risk assessment of an insurer.** Review of cloud computing is part of off-site monitoring and on-site inspections. As for any outsourced activity, cloud computing is subject to the same level of supervision as if that activity were to be performed by the insurer itself.

70. **There are different sources of information that authorities use for supervising insurers' cloud computing activities.** These include:

- Insurers' documentation on materiality determination, risk assessment and due diligence typically prepared before entering into any material outsourcing arrangement, as well as the agreement itself.
- Notification or approval filing, in cases for which this is required by regulation.
- Documents and records located in the insurer's and cloud service provider's premises, as well as information requested from them. Some authorities have required the inclusion of clauses in the cloud services agreements that allow them to request information directly from the service provider, while others have opted to do it through the supervised institution.
- Publicly available information, including solvency and financial condition reports (SFCR), certifications and assurance reports of cloud service providers.
- Information that has to be reported to the authority, including outsourcing policy, outsourcing regulatory reports, and insurers' own risk and solvency assessments (ORSA).

71. **Although authorities generally expect insurers to make available all documents and records related to their outsourcing activities (including cloud computing), a few authorities require detailed reports.** Regarding the latter, for instance, IRDAI, MAS and OSFI require institutions to submit detailed reports on their outsourcing activities either on a regular basis or upon request. These reports should also be made accessible for review by the Board and senior management. The following describes the required reporting by these three authorities.

- **Outsourcing reporting format.** For IRDAI, insurers shall report information on all the outsourcing arrangements "where annual pay-out either per outsourcing service provider or per activity is One Crore rupees or more, every year within 45 days from the close of the financial year".[51] The report includes all outsourcing activities, identifying information of arrangements with related parties or group entities of the insurer or insurance intermediaries and with entities located or operating from outside India. In the report, insurers should send details about (a) description of the outsourced activity; (b) name and address of the service provider; and (c) the amount paid for the reporting and preceding year.
- **Outsourcing arrangements register.** For MAS, institutions should maintain an updated register of all existing outsourcing arrangements (material and non-material), which is to be submitted

[51] See IRDAI (2017a).

to the authority at least annually or upon request. Institutions should ensure that the register is readily accessible for review by the board and senior management of the institution. The register should be updated and form part of the oversight and governance reviews undertaken by the board and senior management of the institution. Examples of the information requested in this register are shown in Box 1.

- **Centralised list of all material outsourcing arrangements.** For OSFI, institutions should maintain a centralised list of all their material outsourcing arrangements. A parent institution may maintain the list on behalf of its subsidiaries. The list should contain information pertaining to the name of the service provider, the country where the service is provided, the expiry or renewal date of the contract or outsourcing agreement and the estimated value (dollar amount) of the contract or outsourcing agreement. The list should be updated on an ongoing basis and should form part of the documentation delivered to the institution's board of directors or the branch's chief agent or principal officer. OSFI should be able to access the list at any time upon request.

Box 1

MAS outsourcing register

Insurers should maintain an updated register of all existing outsourcing arrangements (material and non-material), which is to be submitted to the authority at least annually or upon request. Examples of detailed information that must be included in the register are the following:

- type and description of outsourced service(s) (eg information systems management and maintenance; management of policy issuance and claims operations by managing agents; middle and back office operations);
- name of service provider/material subcontractor;
- country where the service provider/material subcontractor is registered;
- type of outsourcing (eg third-party, intra-group outsourcing);
- support by service provider/material subcontractor (eg for critical business operations or for storing and processing sensitive customer information);
- cities where the service will be carried out and where customer information will be stored or processed;
- service provider substitutability and if alternate service provider has been identified;
- institution's frequency of audit on the service provider/material subcontractor and date of last independent audit on the service provider/material subcontractor; and
- date when service provider/material subcontractor last tested its business continuity plan.

72. **Authorities are increasingly relying on thematic reviews and ongoing contact with cloud providers in order to effectively supervise cloud computing activities**. Annual questionnaires and thematic reviews on operational or IT risks and/or targeted reviews on cloud computing are helping authorities gain an industry-wide perspective to inform their regulatory and supervisory approaches vis-à-vis cloud computing (see Box 2). Also, ongoing dialogue with cloud service providers are helping supervisors to have a better understanding of the service provider's offerings, risk management framework and internal control systems. This dialogue also allows service providers to have a clearer understanding of the regulatory expectations around cloud computing.

Box 2

Examples of thematic reviews

BaFin

Between August and November 2017, BaFin conducted an inquiry on cyber-risks for all German insurance companies and pension funds, which also covered outsourcing. One aim was to identify the typical strengths and weaknesses of insurers in order to focus supervisory attention on the relevant issues. This was also a signal to the industry that BaFin will keep a closer eye on the IT of insurance companies and their IT service providers.

DNB

In 2017, DNB conducted a thematic examination of outsourcing risks for all financial institutions, including insurers, and in July 2018 published a compilation of good practices following the thematic examination with the aim of helping institutions improve their monitoring of material activities.

Regarding the insurance sector, in April 2018, DNB launched a consultation on good practices for controlling outsourcing risks. According to DNB, insurers outsource various activities for various reasons. This could result in risks for an insurer, such as the risk that the continuity and reliability of the insurer's operations might be jeopardised in case of a breach of contract by the service provider, or if the service provider has financial problems or misuses confidential data. Research by DNB has shown that insurers do not always adequately manage such outsourcing risks and therefore the good practices that are being consulted on are intended to rectify this. The main question raised in the DNB's consultation was whether the good practices are sufficiently clear and helpful in meeting the legal requirements around outsourcing. The consultation was closed in May 2018 and the compilation of good practices has recently been published.[52]

FCA

In June 2015, the FCA published a report on "Delegated authority: Outsourcing in the general insurance market" after having conducted a thematic review on the subject. This report sought (i) to understand and fulfil the responsibilities insurers have to customers, where they have outsourced to another party, or where they are the party carrying out these outsourced functions; and (ii) to understand and fulfil the responsibilities they have to customers for related functions they perform under their own regulatory permissions. This report sets out their findings and how they relate to the FCA's rules and guidance.

73. **The information gathered by authorities is used to assess the risks of insurers' cloud computing activities.** Based on the assessment of information gathered, supervisory resources are prioritised. A specific focus on cloud computing may be included in on-site inspections of insurers. In some jurisdictions, the assessment of the outsourcing (including cloud computing) risks is part of regular on-site examinations, while in others it only takes place if the lead supervisory team detects potential issues based on off-site assessments. Besides the analysis made by the lead supervisory team, some authorities involve other teams, such as the operational or IT supervisory team, whose expertise is used in assessing cloud computing arrangements.

74. **Most of the authorities do not directly supervise cloud service providers, even if they have the right to conduct on-site inspections and obtain information.** Supervision of the main cloud service providers in the market is challenging since these are typically large international technology firms. Only one authority mentioned having visited a cloud service provider, which was dominant in a specific insurance business line, with the aim of understanding the outsourcing risks.

75. **A few authorities perform an industry review of concentration risks of cloud service providers.** In one jurisdiction, the authority determines the "top" service providers based on the number

[52] See DNB (2018).

of contracts that such providers have concluded with the industry. Another authority has a database that supports supervisory reviews to assess the concentration risk within the insurance sector or even within the complete financial sector.

76. **Authorities may take a range of supervisory actions based on their assessments.** As with any other supervisory assessments, assessments of cloud computing arrangements could lead to a range of possible supervisory actions – from recommendations to warnings, remediation plans, fines etc. One supervisory agency indicated that it avoids making supervisory recommendations that influence the outsourcing decisions of insurance firms, which are by their nature business decisions. As such, stronger enforcement actions follow only if there are serious regulatory compliance issues. Generally, these supervisory actions are applied to the insurance firm and not to third-party service providers, particularly if the latter are not under the oversight of the supervisory agency.

77. **Authorities are in the process of enhancing their supervisory cooperation frameworks so that they will have scope to exchange information on cloud computing activities, particularly at the international level.** One of the key features of cloud computing is that the provider and the services offered may be located in different jurisdictions, so that the outsourcing arrangement is potentially subject to different sets of laws and regulations. Most authorities have the powers to cooperate and coordinate with foreign authorities with respect to cloud service arrangements. However, the HKIA is one of the few authorities whose framework clearly specifies that it may communicate with the home or host regulators of the insurer and the service provider to seek clarification or confirmation on relevant issues related to material outsourcing overseas. In addition, authorities seem to be turning their attention to reviewing and enhancing their information-sharing agreements with other domestic financial authorities, when relevant, in order to assess the potential vulnerabilities of the entire financial system to cloud computing.

Section 5 – Concluding remarks

78. **Insurers are increasingly using cloud services to support their core functions.** In recent years, cloud services have been adopted by insurers to support innovation and increase the efficiency of product development, marketing and distribution, underwriting and claims management activities, with the aim of meeting changing customer needs and improving customer satisfaction.

79. **Cloud computing offers concrete benefits as well as poses unique risks to the insurance industry.** Savings in IT costs, faster deployment cycles as well as flexibility and on-demand scalability of IT resources are some of the concrete benefits for insurers that use cloud computing. However, cloud computing may pose specific risks to the insurance industry, given (i) the nature of some cloud deployment models where computing resources are shared; (ii) the type of information that is stored and processed; (iii) the cross-border location of computing resources; as well as (iv) the current market structure where a few global cloud providers dominate the market, resulting in a concentration that could have systemic implications. The cross-border nature of cloud services complicates the effective oversight of all these risks.

80. **Although the use of cloud service providers is generally subject to general outsourcing requirements, there is value in clarifying the regulatory expectations on cloud computing**. Most authorities apply their general outsourcing requirements to cloud computing. They also apply other general relevant provisions related to governance, risk management, and information security, under a variety of regulatory approaches. However, some authorities include cloud-specific sections in these regulations or have issued specific supervisory expectations on cloud computing through sound practices, principles or recommendations. The usefulness of this approach is that it addresses the unique risks posed by cloud computing and provides a reasonable level of regulatory certainty with respect to the financial

industry's use of cloud services. The following are some specific considerations that could help insurance authorities in the design of their regulatory frameworks:

- **Many authorities apply their cloud computing regulatory framework in a proportional manner**. Increasingly both binding and non-binding requirements are applied on a proportional basis ie they are envisaged to be tailored to reflect the size, complexity or risk profile of financial institutions or, as relevant, the outsourced service. Regarding the latter, APRA applies different notification and consultation requirements depending on the inherent risk of the cloud computing outsourcing arrangement.
- **Regulatory frameworks related to cloud computing put special emphasis on data confidentiality, security and availability.** When it comes to cloud computing, authorities are focusing on the adequacy of information security and data confidentiality. In particular, insurers are required to ensure that information security and data confidentiality are maintained.
- **Strong IT and cyber-security capabilities at cloud service providers are emerging as key supervisory expectations.** These include requiring insurers to monitor that cyber-security requirements established in the outsourcing policy are appropriately addressed before, during and while exiting outsourcing contracts, assessing the service provider's adherence to international IT standards, or using scenario analysis to test security events.
- **Effective recovery and resumption capabilities appear to be particularly relevant for authorities when insurers use cloud computing services**. Insurers are required to assess the adequacy of the cloud service provider's plans and resources to ensure the institutions' business continuity and to maintain documented and comprehensive exit plans that allow the institution to exit cloud outsourcing arrangements, if necessary, without undue business disruption.
- **The importance of audit rights is consistently highlighted for cloud computing.** Given the geographical dispersion of cloud service locations, insurers are required to ensure that the outsourcing agreements enable them and their respective supervisory authority to have access to documentation and information, and to conduct on-site inspections at the provider.

81. **Supervisory on-site/off-site examinations on cloud computing are generally part of operational risk reviews but authorities are increasingly complementing them with thematic reviews and ongoing contact with cloud providers**. Authorities usually assess cloud computing practices at insurance companies as part of their offsite and onsite reviews of operational risk, following a risk-based approach. There are no common criteria across different supervisory authorities on how supervisors should be involved before an insurer enters into a cloud servicing agreement. The arrangements vary from notification and consultation to formal approval processes. Nonetheless, targeted reviews on the use of cloud services in the financial/insurance sector or on closely related areas such as information security risks are helping authorities to take an industry-wide perspective on cloud computing. In addition, some authorities have established a dialogue with cloud service providers with the aim of better understanding the cloud services business and, in particular, its evolution over time.

82. **Developing a supervisory framework to assess concentration risk in cloud computing is very much work in progress.** While authorities widely recognise that reliance on a relatively small number of providers may result in systemic risk for insurers, very few perform industry-specific reviews of concentration risks arising from cloud service providers. This issue could turn out to be particularly acute because users and providers of cloud services may be overseen by different financial sector authorities. Thus, issues relevant for cloud computing, such as data protection, may be under the remit of other, non-financial authorities. As such, it appears that a supervisory framework to assess potential concentration risks needs to rely on cooperation mechanisms between different domestic cross-sectoral authorities if the potential financial stability risks associated with cloud computing are to be effectively addressed.

83. **Enhancing cross-border cooperation, particularly in terms of information-sharing, is essential for the effective supervision of the cloud computing business.** Users and providers of cloud

services may be located in different jurisdictions. Even if they are physically in the same location, data storage could be placed in another location. Therefore, international cooperation among home and host authorities, in particular through sharing relevant information on cloud service providers, is especially important when it comes to ensuring an effective oversight of cloud computing activities. Among the potential ideas to be considered, for example, is the joint supervision of large cloud service providers by cross-sectoral authorities from different jurisdictions, or the establishment of arrangements similar to supervisory colleges for relevant third-party technology providers.

References

Australian Prudential Regulation Authority (2013): Prudential practice guide PPG 234 on management of security risk in information and information technology, May.

——— (2015): Information paper: Outsourcing involving shared computing services (including cloud), July.

——— (2017): Prudential standard CPS 231 on outsourcing, July.

——— (2018a): Draft Prudential Standard CPS 234 on information security, March.

——— (2018b): Information paper: Outsourcing involving cloud computing services, September.

Autorité de Contrôle Prudentiel (2013): Analyses et syntheses: the risks associated with cloud computing, July.

——— (2015): Notice «Solvabilité II» système de gouvernance, December.

Bank of England (2018): Financial stability report, June.

Byres (2018): Peering into a cloudy future, September.

De Nederlandsche Bank (2006): Decree on prudential rules pursuant to the act on financial supervision, October.

——— (2012): Circulaire cloud computing, January.

——— (2018): Good practice uitbesteding verzekeraars, August.

European Banking Authority (2017): Recommendations on outsourcing to cloud service providers, December.

——— (2018): Draft guidelines on outsourcing arrangements, June.

European Network and Information Security Agency (2012): Cloud computing benefits, risks and recommendations for information security, December.

European Insurance and Occupational Pensions Authority (2013): Guidelines on system of governance.

——— (2013): Explanatory text on the proposal for guidelines on the system of governance, March.

European Parliament and European Union Council (2009), Directive 2009/138/EC on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II), November.

——— (2014): Commission Delegated Regulation (EU) 2015/35 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II), October.

Federal Financial Supervisory Authority (2018a): Circular on minimum requirements under supervisory law on the system of governance of insurance undertakings, January.

——— (2018b): Circular 10/2018 Supervisory Requirements for IT in Insurance Undertakings (Versicherungsaufsichtliche Anforderungen an die IT – VAIT), July.

——— (2018c): Cloud computing, compliance with the supervisory requirements regarding the rights of information and audit and ability to monitor, May.

Financial Conduct Authority (2015): Delegated authority, outsourcing in the general insurance market, June.

——— (2018a): Senior arrangements, systems and controls, Chapter 8 on outsourcing, March.

——— (2018b): Senior arrangements, systems and controls, Chapter 13 on operational risk, systems and controls for insurers, March.

——— (2018c): Senior arrangements, systems and controls, Chapter 14 on risk management and associated systems and controls for insurers, March.

——— (2018d): FG 16/5 Guidance for firms outsourcing to the cloud and other third party IT services, July.

Financial Stability Board (2017): Financial stability implications from Fintech: supervisory and regulatory issues that merit authorities' attention, June.

G7 (2018): Fundamental elements for third party cyber risk management in the financial sector, October.

Gartner (2012): Industries aim to evolve cloud computing beyond support functions to more strategic uses, May.

Insurance Authority (2017a): GL14 Guideline on outsourcing, June.

——— (2017b): GL10 Guideline on the corporate governance of authorized insurers, June.

——— (2017c): GL8 Guideline on the use of Internet for insurance activities, June.

Insurance Regulatory and Development Authority of India (2015): IRDAI Maintenance of Insurance Records Regulations, August.

——— (2016): IRDAI/F&A/GDL/CG/100/05/2016 Guidelines for Corporate Governance for insurers in India, May.

——— (2017a): IRDAI/Reg/5/142/2017 Outsourcing of activities by Indian insurers regulations, April

——— (2017b): IRDAI/IT/GDL/MISC/082/04/2017 Guidelines on information and cybersecurity for insurers, April.

International Association of Insurance Supervisors (2018), Issues paper on the increasing digitalisation in insurance and its potential impact on consumer outcomes, November.

International Data Corporation (2018): Worldwide public cloud services spending forecast to reach $160 billion this year, January.

Joint Forum (2005): Outsourcing in financial services, February.

Lambert, R (2014): Mission critical cloud is on the rise in the insurance industry, May.

Lee, J (2018): Cyber panel flags concentration risk in cloud technology for banks, insurers, October.

Lloyd's and AIR (2018): Cloud down: impacts on the US economy.

Maletski, G (2018): How cloud computing is reshaping the way insurers work, May.

Monetary Authority of Singapore (2013): Technology Risk Management Guidelines, June.

——— (2016): Guidelines on Outsourcing, July.

Morris, S (2018): Cloud computing tops list of emerging risks, September.

National Association of Insurance Commissioner (2012a): Risk Management and Own Risk Solvency Assessment Model Act, October.

——— (2012b): Existing U.S. corporate governance requirements.

——— (2017): Insurance Data Security Model Law, Fourth Quarter.

——— (2018): Financial Condition Examiners Handbook.

National Institute of Standards and Technology (2011): The NIST definition of cloud computing, September.

Office of the Superintendent of Financial Institutions (2009): Guideline B-10, Outsourcing of Business Activities, Functions and Processes, March.

——— (2012): Memorandum on new technology-based outsourcing arrangements, February.

——— (2013): Cyber Security Self-Assessment Guidance, October.

Prudential Regulation Authority (2015): Rulebook: Solvency II firms: Rules on Conditions Governing Business.

——— (2016): Senior managers' regime and senior insurance managers' regimes, March.

Ratcliff, P: The dual agenda of the world's largest insurers, consulted online on 29 August 2018.

Saudi Arabia Monetary Authority (2017a): SAMA Outsourcing Regulations for Insurance and Reinsurance Companies and Insurance Service Providers.

——— (2017b): Cybersecurity Framework, May.

Swiss Financial Market Supervisory Authority (2017): Circular on Corporate Governance 2017/2.

——— (2018): Circular Outsourcing – banks and insurers 2018/3.

Synergy research group (2018a): Cloud growth rate increased again in Q1; Amazon maintains market share dominance, April.

——— (2018b): Cloud revenues continue to grow by 50% as top four providers tighten grip on market, July.

United States Department of the Treasury (2018): A financial system that creates opportunities: nonbank financials, fintech and innovation, July.

Annex – List of authorities

APRA	Australian Prudential Regulation Authority, Australia
OSFI	Office of the Superintendent of Financial Institutions, Canada
EIOPA	European Insurance and Occupational Pensions Authority, European Union
ACPR	Autorité de Contrôle Prudentiel et de Résolution, France
BaFin	Federal Financial Supervisory Authority, Germany
HKIA	Insurance Authority, Hong Kong
IRDAI	Insurance Regulatory and Development Authority of India, India
DNB	De Nederlandsche Bank, Netherlands
SAMA	Saudi Arabian Monetary Authority, Saudi Arabia
MAS	Monetary Authority of Singapore, Singapore
FINMA	Swiss Financial Market Supervisory Authority, Switzerland
FCA	Financial Conduct Authority, United Kingdom
PRA	Prudential Regulation Authority, United Kingdom
NAIC	National Association of Insurance Commissioners, United States

Online Annex 1 – Requirements, recommendations and expectations on cloud-specific issues*

Online Annex 2 – Supervisory consultation, notification or authorisation*

* These Annexes are available as an online appendix and can be found on the BIS website at: www.bis.org/fsi/publ/insights13_appendix.pdf