Online appendix to:

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

* This appendix contains supplementary material.

** email: Conor Donaldson (conor.donaldson@bis.org) at 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) at the Bank for International Settlements (BIS).

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

Governance

Table 8

Authority	Governance
APRA	An APRA-regulated entity's outsourcing governance framework should outline decision-making and oversight responsibilities with respect to outsourcing, including the use of cloud computing services. The appropriate **governance authority** (board, senior management and any delegations resting with a specific governance body or individuals) should form a view as to the adequacy of the risk and control frameworks to manage the arrangement in line with the Board risk appetite. This would generally include undertaking sufficient due diligence and thorough analysis of the risks involved to understand the consequences if the risks are realised and the adequacy of the mitigants in place. It is important that the appropriate governance authority is informed of all material initiatives involving cloud computing arrangements. This includes the receipt of appropriately detailed information at significant stages: **Once a firm proposal has been identified:** ▪ how the proposal aligns with strategy, the business case, alternative options considered and rationale for the selected solution (including justification for additional risk exposures); ▪ IT assets in scope, categorised by sensitivity and criticality; ▪ materiality assessment, including impact on business processes, systems architecture, organisation and operating model; ▪ high-level risk and control assessments, risk profiles, plausible worst case scenarios and alignment to risk appetite and tolerances; ▪ services selected, products and parties involved and delivery location(s); and ▪ due diligence undertaken (including assurance obtained). **Once the detailed solution is designed and transition plans are in place:** ▪ governance, project, risk management and assurance frameworks (initial and ongoing); ▪ IT operating model and IT security model to be applied, and associated roles/responsibilities of all parties; ▪ alignment with regulatory standards and guidance; ▪ architectural overview (including transitional states) for hardware, software and data stores; ▪ detailed risk and control assessments, risk profiles and alignment to risk appetite and tolerances; ▪ continuity of service strategy, including high availability, recovery and provider failure considerations; ▪ organisational change management and transition plan; and ▪ project structure and schedule (including key stages, milestones and timeframes). **During the execution phase**, the appropriate governance authority would normally be kept informed, as appropriate, regarding the current status and emerging risks and issues. For initiatives with heightened inherent risk, engagement with APRA would typically occur after the APRA-regulated entity has completed its internal governance processes, and the initiative has been fully risk-assessed and approved by the appropriate governance authority. For cloud initiatives with extreme inherent risk, it would be appropriate for regulated entities to engage with APRA once a firm proposal has been identified, and initial approval to proceed has been given by the appropriate governance authority.

Governance

Table 8

Authority	Governance
ACPR	Commitment to cloud services is sometimes based solely on a decision by the business line using such service, after consultation with the head of information systems. On the contrary, given the significance of the risks, **commitment to this type of service should systematically involve the institution's governing bodies**, in accordance with good governance of the information system. These bodies should make their decision while having the independent view of the head of risk management and the head of information systems security if the latter does not belong to the risk management department.
IRDAI	Wherever application/data/system hosting in a cloud is considered inevitable – for commercial, business, regulatory, legal or other reasons, **approvals should be obtained by the organisation from their respective senior management**.
SAMA	The cyber-security requirements within the outsourcing policy and process should be defined, approved, implemented and communicated within Member Organisation and should be measured and periodically evaluated. The outsourcing process should include: i) the approval from SAMA prior to material outsourcing; ii) the involvement of the cyber-security function; and iii) compliance with the SAMA circular on outsourcing. The **cyber-security controls within the cloud computing policy for hybrid and public cloud services should be defined, approved and implemented and communicated** within Member Organisation and should be periodically measured and evaluated. **Compliance with the cloud computing policy should be monitored.**
MAS	The **board of directors and senior management** should ensure that a sound and robust **technology risk management framework** is established and maintained, and outsourcing IT is part of the technology risk management framework. Institutions are ultimately **responsible and accountable** for maintaining **oversight of cloud services** (CS) and managing the attendant risks of adopting CS, as in any other form of outsourcing arrangements. A risk-based approach should be taken by institutions to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the CS.
FCA	Firms retain **full accountability** for discharging all of their responsibilities under the regulatory system and cannot delegate responsibility to the service provider. At a high level, a firm should: ▪ be clear about the service being provided and where responsibility and accountability between the firm and its service provider(s) begins and ends; ▪ allocate responsibility for the day-to-day and strategic management of the service provider; ▪ ensure staff have sufficient skills and resources to oversee and test the outsourced activities; to identify, monitor and mitigate against the risks arising; and properly manage an exit or transfer from an existing third-party provider; and ▪ verify that suitable arrangements for dispute resolution exist.

Assessment of materiality, criticality or importance

Table 9

Authority	Assessment of materiality, criticality or importance
APRA	APRA recognises that the **risks** associated with the use of **cloud computing** services will depend on the **nature of the usage**. Therefore, for the purposes of this paper, risks are classified into three broad categories: low, heightened and extreme. APRA's expectations of APRA-regulated entities with respect to cloud computing services, and APRA's supervisory approach, will depend on the scale of the associated risks. **Low inherent risk** Arrangements which could, if disrupted (where disruption includes a compromise of confidentiality, integrity or availability of systems and/or data) present a low or negligible impact to business operations and the ability of the regulated entity to meet its obligations. Examples of cloud computing usage with low risk: • applications and data stores with low criticality (a measure of the impact of a loss of availability) and sensitivity (a measure of the impact of a loss of either confidentiality or integrity) as classified by the APRA-regulated entity; • non-production environments (eg test and development) populated with desensitised data; and • websites that deliver publicly available information. **Heightened inherent risk** Arrangements involving critical and/or sensitive IT assets that result in either an increased likelihood of a disruption or where a disruption would result in a significant impact to business operations and the ability of an APRA-regulated entity to meet its obligations. Typically this would involve one or more of the following: • exposure to environments which are available to non-financial industry entities (i.e. "public cloud") – as distinct from financial sector 'community clouds' where tenants have comparable security requirements, risk profiles and risk appetites ; • unproven track record of: i) o the provider; ii) the cloud computing service; iii) the specific usage; iv) the control environment; or v) the APRA-regulated entity in managing an arrangement of comparable size, complexity and/or risk profile: • a high degree of difficulty in transitioning to alternate arrangements; • inability for an APRA-regulated entity to assess the design and ongoing operational effectiveness of the control environment; • jurisdictional, contractual or technical considerations which may inhibit operational oversight or business continuity in the event of a disruption (including impediments to timely access to documentation and data/information); and/or • transition to the arrangement involves a complex, resource intensive and/or time-constrained program of work. **Extreme inherent risk** Heightened inherent risk arrangements which could, if disrupted, result in an extreme impact. Extreme impacts can be financial and reputational, potentially threatening the ongoing ability of the APRA-regulated entity to meet its obligations. Examples of extreme inherent risk include public cloud arrangements involving systems of record which maintain information essential to determining obligations to customers and counterparties, such as current balance, benefits and transaction history. For usage of this nature, APRA would expect that entities can demonstrate that their risk management and mitigation techniques and capabilities are sufficiently strong.

Assessment of materiality, criticality or importance

Table 9

Authority	Assessment of materiality, criticality or importance
ACPR	The use of cloud services will tend to grow, driven by business lines that appreciate the ease of use and speed of implementation; and commitment to this type of service is sometimes based solely on a decision by the business line using such service, after consultation with the head of information systems security. On the contrary, given the significance of the risks, **commitment to this type of service should systematically involve the institution's governing bodies, in accordance with good governance of the information system.** These bodies should make their decision while having the independent view of the head of risk management and the head of information systems security if the latter does not belong to the risk management department. With regard to outsourcing of critical services or other important tasks, it is not obvious that functions considered as "support functions" are not, in practice, to be regarded as critical or important, given the role they play in the realisation of certain services and for business continuity (IT resources in particular).
MAS	"**Material outsourcing arrangement**" means an outsourcing arrangement - • which, **in the event of a service failure or security breach**, has the potential to either materially impact an institution's: o business operations, reputation or profitability; or o ability to manage risk and comply with applicable laws and regulations, or • which **involves customer information** and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on an institution's customers. Outsourcing of all or substantially all of its risk management or internal control functions, including compliance, internal audit, financial accounting and actuarial (other than performing certification activities) is to be considered a material outsourcing arrangement.
FCA	Different requirements apply to different types of firm and may be determined by the type of function being outsourced. Of particular relevance is whether or not the function being outsourced is considered critical or important, whether it is material outsourcing, or for authorised payment institutions and authorised electronic money institutions whether it relates to important operational functions. These are specific terms in respect of outsourcing and are defined in the Handbook or Regulations as follows: ▪ **Critical or important** – an operational function is regarded as critical or important if a defect or failure in its performance would materially impair the continuing compliance of a common platform firm with the conditions and obligations of its authorisation, its other obligations under the regulatory system, its financial performance, or the soundness or continuity of its relevant services and activities (Senior Management Arrangements, Systems and Controls (SYSC 8.1.4R)). ▪ **Material outsourcing** – defined in the FCA Handbook as outsourcing services of such importance that weakness or failure of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Principles for Businesses (PRIN). ▪ **Important operational functions** – under the Electronic Money Regulations 2011 and the Payment Services Regulations 2009, an operational function is important if a defect or failure in its performance would materially impair: (a) the authorised institutions compliance with the Regulations and any requirement of its authorisation; (b) the financial performance of the authorised institution; or (c) the soundness or continuity of the authorised institution.

Due diligence

Table 10

Authority	Due diligence
APRA	The selection of the solution involving cloud computing would typically be conducted in a **systematic** and **considered manner**. This includes ensuring the selected **solution minimises risk** wherever possible, and **complies** with the processes established by the entity for changing the IT environment including security, risk management, IT architecture, procurement and supplier management. **Observed weaknesses**: i) solutions not aligned to the desired enterprise architecture; ii) bypassing established risk management and outsourcing frameworks; and iii) failure to engage with the risk, security, outsourcing and assurance functions at the initiation stage. A **comprehensive due diligence process, including independent assessments,** rather than placing sole reliance on attestations by the provider and customer references, would normally be conducted. The intent would typically be to verify the **maturity, adequacy and appropriateness** of the provider and services selected (including the associated control environment), taking into account the **intended usage** of the cloud computing service. The **depth** of **due diligence** undertaken would normally be **commensurate** with the **criticality and/or sensitivity of the IT assets** involved and the level of reliance the APRA-regulated entity places on the provider to maintain effective security controls. An APRA-regulated entity should consider the benefits of the following factors as ways of reducing inherent risk as part of the solution selection process: ▪ **Australian hosted options**, if available, in the absence of any compelling business rationale to do otherwise. Australian hosting eliminates a number of additional risks which can: impede a regulated entity's ability to meet its obligations; or impede APRA from fulfilling responsibilities considered necessary in its role as prudential regulator; and ▪ cloud computing services only used by parties which have comparable security requirements, risk profiles and risk appetites (such as other financial sector entities). Some cloud computing services offer a high degree of flexibility in how the solution is implemented. In these circumstances, design and architectural considerations would include how to minimise the risk of a loss of confidentiality, integrity and availability. Better practice would be to design the solution and associated control on the assumption that the cloud environment is "untrusted" and therefore could be compromised.
OSFI	Under the self-assessment guide, it is recommended that firms consider cyber-security risk as part of their due diligence process for material outsourcing arrangements and critical IT service providers, including related subcontracting arrangements.
IRDAI	**Prior to engagement, external parties shall be subject to a relationship assessment** (sometimes referred to as due diligence review) which shall cover: • dealing with the said party (eg details of provider history, previous and current business arrangement and dispute information); • contract requirements shall include non-disclosure agreements, subcontracting, roles and responsibilities, and termination clauses and right to inspect/audit by organisation, law enforcement agencies and regulating agencies including IRDAI; and • third party demonstrable level of maturity in relation to information security and their degree of commitment to information security. This is via a self-assessment checklist covering their maturity in the area.
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for the process for adopting cloud services, including **due diligence on the cloud service provider** and its cloud services should be performed.
MAS	The types of risks in CS that confront institutions are not distinct from that of other forms of outsourcing arrangements. Institutions should perform the necessary due diligence in this outsourcing guidelines when subscribing to CS.

Due diligence

Table 10

Authority	Due diligence
FCA	Before acceptance, a firm should, as part of the due diligence exercise, ensure that in entering into an outsource agreement, it does not worsen the firms operational risk. **In conducting its due diligence** on potential third-party providers, and as part of ongoing monitoring of service provision, a firm may wish to take account of the **provider's adherence to international standards** as relevant to the provision of IT services. Assurance obtained from international standards for the delivery of critical or important operational functions or material outsourcing is unlikely to be sufficient on its own. Nevertheless firms should take account of any external assurance that has already been provided when conducting their own due diligence. External **assurance** may be more relevant to a firm's consideration where: ▪ it complies to well-understood standards (such as, for example, the ISO 27000 series) ▪ the part of the service being assessed is relatively stable (such as physical controls in the data centre or staff vetting) ▪ the service is uniform across the customer base (ie not particular or bespoke to the firm outsourcing) The scope of the third-party audit is specific to the service a firm proposes to use (ie the audit is against the data centre you are using – not a similar data centre in another jurisdiction).

Risk assessment of outsourcing arrangements

Table 11

Authority	Risk assessment of outsourcing arrangements
APRA	Once the solution design is completed, it would be appropriate to conduct a **risk assessment** considering the following: • ability for the APRA-regulated entity to avoid a significant impact on business operations and meet obligations regardless of technology, people, process or service provider failure; • ability to meet performance, capacity, security, high-availability, recoverability and other business requirements; • adequacy of secure design principles and development practices; • adequacy of processes to verify that software operates as intended within the cloud computing service; • critical and/or sensitive IT assets which are accessible from the cloud computing service; • ability to meet legislative and prudential requirements (including the outsourcing standards); and • any impediments which could inhibit APRA's ability to fulfil its duties as a prudential regulator. An APRA-regulated entity would normally conduct initial and periodic security and risk assessment of all material service provision arrangements. Security and risk assessments would typically be conducted whenever a material change to existing arrangements occurs. Comprehensive risk assessments typically include consideration of factors such as: • the **nature** of the **service** (including specific underlying arrangement); • the **provider** and the **location** of the service; • the **criticality** and **sensitivity** of the IT assets involved, • the **transition** process; and • the target **operating model** Risk assessments are generally more effective when the risks are clearly described and at a level of granularity that allows for a meaningful understanding of the actual risk and mitigating controls associated with each risk, including any required remediation actions. **Scenario analysis** of plausible security events, including a loss of availability, is a useful technique to understand risks associated with the arrangement. This includes consideration of the risks to critical and/or sensitive IT assets which are accessible from the cloud computing service. **Observed weaknesses:** i) high-level risk descriptions that lack clarity or describe control weaknesses rather than risks; ii) lack of consideration of critical and/or sensitive IT assets which are accessible from the cloud computing service; iii) inadequate consideration of the sensitivity of data (collectively and at the individual field level) when considering implementation solution options for cloud computing services; iv) cursory risk assessments which fail to consider specific risks and any changes to the risk profile; v) control design and operation, and assurance obtained, do not accurately reflect APRA-regulated entity responsibilities for operating and managing the arrangement; and vi) limited due diligence and assurance activities undertaken, with heavy reliance placed on provider attestations and/or usage by other organisations.
ACPR	As the risks associated with cloud computing are many and new (without sufficient hindsight being available), the **use of cloud services should only ever result from the demonstration that the benefits they bring are worth the risks taken**. The key question of any discussion on the use of cloud computing is the control of information and its degree of sensitivity.

Risk assessment of outsourcing arrangements — Table 11

Authority	Risk assessment of outsourcing arrangements
IRDAI	**Requirements that institutions must meet prior to engagement**: ▪ Risk assessment shall be conducted for determining the risks involved in granting access to third parties to organisation's information or information systems. ▪ The list of security controls shall be determined to be implemented based on the type of engagement and nature of information sharing requirement. ▪ Data should be shared only on "Need to know" basis.
DNB	Supervised institutions must **analyse and sufficiently mitigate** risks. This also applies to operational processes that are (partly) outsourced to a third party. In line with statutory requirements, DNB assumes the supervised institutions are able to produce a coherent risk analysis before they decide to outsource operational (IT) processes. Such a risk analysis should encompass in any case an assessment regarding compliance with current legislation, regarding the mutual understanding about the services offered (the agreement), regarding the stability and reliability of the service provider, regarding the location where the services are to be provided, and regarding the importance of and reliance on the outsourced IT services and/or IT components. **In case of cloud computing, this requires explicit attention to risks associated with, among other things, data integrity, data confidentiality and data availability**. Also, assurance must be obtained as regards the location where the business data are to be processed and stored. In the event of stopping the use of third-party services, the supervised institution must secure all data and verify that all data has been removed from the third party's systems.
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for the process for adopting cloud services, including a **cyber-security risk assessment** on the cloud service provider and its cloud services should be performed.
MAS	The types of risks in CS that confront institutions are not distinct from that of other forms of outsourcing arrangements. Institutions should apply sound governance and risk management practices articulated in this set of guidelines when subscribing to CS.

Risk assessment of outsourcing arrangements

Table 11

Authority	Risk assessment of outsourcing arrangements
FCA	Before acceptance, a firm should: ▪ have a clear and **documented business case or rationale** in support of the decision to use one or more service providers for the delivery of critical or important operational functions or material outsourcing; ▪ ensure the service is **suitable** for the firm and consider any relevant legal or regulatory obligations, including where a firm is looking to change their existing outsourcing requirements; ▪ consider the relative risks of using one type of service over another eg **public versus private 'cloud**;' ▪ know which **jurisdiction** the service provider's business premises are located in and how that affects the firm's outsource arrangements; ▪ assess the **overall operational risks** associated with the regulated service for which the firm is responsible and assign responsibility for managing them; ▪ carry out a **risk assessment to identify relevant risks and identify steps to mitigate** them and document this assessment; ▪ identify current industry good practice, including data and information security management system requirements, cyber risks, as well as the relevant regulator's rules and guidance to then use this to support its decision-making; ▪ carry out a security risk assessment that includes the service provider and the technology assets administered by the firm; ▪ know whether its contract with the service provider is governed by the law and subject to the jurisdiction of the UK. If it is not, it should still ensure effective access to data and business premises for the firm, auditor and relevant regulator; and ▪ consider any additional legal or regulatory obligations and requirements that may arise such as through the General Data Protection Regulation (GDPR)

Data protection and security

Table 12

Authority	Data protection and security
APRA	It is important that the strength of the **control environment** is commensurate with: ▪ the risks involved; ▪ the sensitivity and criticality of the IT assets involved; ▪ the level of trust that will be placed on the cloud computing service environment; and ▪ the shared responsibilities between the service provider and entity. The aspects of the control environment which would typically be managed by an APRA-regulated entity include: maintaining data quality, information security (such as identity and access management, incident detection and response management, data loss prevention, vulnerability management, configuration management, encryption and key management) and the ongoing monitoring of control effectiveness. An understanding of the nature and strength of controls required is typically achieved through initial and periodic (or on material change) assessments of **Observed weaknesses:** Inadequate consideration of the following: i) controls to prevent, detect and respond in a timely manner to unauthorised access and changes to the APRA-regulated entity's environment by internal staff and service provider staff, service accounts, other customers or third parties, including any changes to the environment which may weaken preventative controls (eg configuration changes to the entity's environment or platform); ii) access rights, ensuring they are limited to those required for the assigned role – for example, a Platform as a Service (PaaS) provider requires access to maintain the platforms supporting the customer's environment but not the ability to access the virtual assets within that environment; iii) controls relating to administration console system access and encryption key management; iv) controls to ensure appropriate isolation from third parties to protect against intentional or inadvertent security incidents; v) protection of sensitive data, both in transit and storage, through cryptographic techniques; v) controls to protect critical and/or sensitive IT assets which are accessible from the cloud computing service; ; vi) protection (eg using desensitisation) of sensitive data in non-production environments (eg development and test); and vii) alignment of the disaster recovery environment with the security requirements of the production systems. System administrator capabilities enable the execution of high impact activities and potentially provide unauthorised access to sensitive IT assets. Consequently, system administrator access entitlements would normally be subject to stronger controls, commensurate with the heightened risks involved. **Additional controls relating to system administrator capabilities** could include: ▪ administration tools, systems, consoles and other related software restricted to only those authorised; ▪ access restricted to the minimum time and capability required to perform an authorised activity; ▪ system administrators restricted from accessing sensitive IT assets through the use of cryptographic, authentication and other techniques; ▪ four-eyes principle (also know as two-person rule) applied to high impact activities (eg deletion of an entire environment); ▪ restrictions on the location and number of authorised system administrators (an APRA-regulated entity should have visibility of system administrators which could impact the entity's environment) ; ▪ multi-factor authentication for system administrator access and activities; ▪ logging and other detective controls for monitoring system administrator activities; and ▪ backup and log data protected through segregation of administrator duties and environments.

Data protection and security

Table 12

Authority	Data protection and security

Implementation of controls: The nature of cloud computing services necessitates the allocation of responsibility for the implementation of controls between the provider and the client. This is commonly referred to as the shared responsibility model. Due to the myriad of cloud computing service offerings that can be consumed, it would be prudent for APRA-regulated entities to carefully consider the differing levels of responsibility for operating and managing these arrangements. Accordingly, an APRA-regulated entity's responsibilities would typically reflect both the combination of controls implemented and assurance obtained from the provider.

An APRA-regulated entity would normally have the capability to evaluate the design and operating effectiveness of controls within the shared responsibility model (both provider and APRA-regulated entity), with a level of assessment commensurate with the impact on the APRA-regulated entity if the service is compromised.

This normally involves evaluations initiated by the APRA-regulated entity (resourced internally and via independent expertise) as well as the leveraging of audit reports initiated by the service provider, conducted by an independent third party. Common examples include Service Organisation Control reports (SOC 1/2/3) and ISO27001/2, ISO 27017, CSA STAR, NIST Cyber Security Framework. It is important, however, that the APRA-regulated entity considers the adequacy of audit reports initiated by the service provider for this purpose and supplement these where considered deficient.

Common areas of responsibility for the different cloud computing models:

Areas of responsibility	Infrastructure as a Service (IaaS)	Platform as a Service (Paas)	Software as a Service (SaaS)
Ongoing monitoring for control effectiveness	Customer	Customer	Customer
Customer side information security	Customer	Customer	Customer
Data quality	Customer	Customer	Customer
Application management	Customer	Customer	Provider
Virtual machines and networks	Customer	Provider	Provider
Cloud infrastructure	Provider	Provider	Provider

An important control objective is the timely detection of unauthorised access and usage of the APRA-regulated entity's environment by the service provider's staff, service accounts, other customers or third parties. This includes any changes to the environment which may weaken preventative controls (eg configuration changes to the entity's environment or platform). An APRA-regulated entity would normally have controls for responding in a timely manner to these alerts.

Observed weaknesses: Inadequate consideration of the following: i) roles and accountabilities under the shared responsibility model; ii) controls for which the APRA-regulated entity is responsible for under the shared responsibility model. Examples include identity and access management, incident detection and response management, data loss prevention, vulnerability management, configuration management, encryption and key management; and iii) scope and coverage of audits initiated by the service provider for sufficiency.

OSFI

Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on confidentiality, security and separation of property. Under the self-assessment guide, it is recommended that:

- Contracts for all material outsourcing arrangements and critical IT service providers include the provision for safeguarding the firm's information.
- Firms have processes in place to ensure the timely notification of a cyber incident from service providers with whom the firm has one or more material outsourcing arrangements, or critical IT service providers.

Data protection and security

Table 12

Authority	Data protection and security
ACPR	The peculiarities of cloud computing concern the criteria of information security in particular: • **Data privacy**: the protection of sensitive and personal data, as well as compliance with banking secrecy, are particularly difficult within pooled infrastructures that can potentially be accessed by local regulatory bodies. This risk is accentuated by the lack of visibility in terms of the location of data and therefore the applicable regulations and the number of stakeholders in a cloud computing solution. The question of data privacy is also an issue in terms of ensuring their effective destruction when the service is terminated, including backups in sites that may be geographically dispersed. • **Availability of data and processes**: the dispersal of data and the multiplicity of parties involved undermine the company's ability to ensure these criteria. The asymmetric relationship that links the supplier to its customer, characterised in particular by the difficulty of including binding commitments (penalty clauses) on a minimum level of availability, may enhance this risk. • **Data integrity**: the use of a cloud computing service creates a risk to the overall integrity of the information system owing to the loss of technical expertise or even dependency on the supplier. More specifically, management by the customer organisation of cloud computing services is more remote and restricted than in other cases of outsourcing, resulting over the long term in a significant risk of dependency: loss of knowledge of the information system and the associated expertise and being tied to the supplier's specific technology may prevent reversibility of the service. Where they concern core (and/or confidential) activities, the implementation of cloud services must be accompanied by suitable risk management measures: ▪ **Legal**: the contractual framework of the service is mandatory. The measures for data protection implemented by the service provider must be assessed before subscription to the service. Concerning the protection of personal data, the service must comply with EU regulations on data protection and more broadly with the rules of protection of intellectual property. Some elements transferred to the cloud are likely to become part of the company's intellectual property capital and must be the subject of a contractual clause. Moreover, any change in the nature of the service must be controlled, including changes to software versions. The corporate customer using a cloud solution must establish a form of ongoing contractual management, relying on penalty clauses to be applied in the event of shortcomings in the service rendered by the service provider. ▪ **Technical**: in the absence of anonymisation, confidential data entrusted to the service provider must be encrypted during transport and during storage. The encryption solution must be controlled by the owner of the data (which implies that key management is performed by the company subject to the supervision of the ACP), and particular attention must be paid to the segregation of environments between customer companies and to the management of access rights.

Data protection and security

Table 12

Authority	Data protection and security
IRDAI	To ensure that information processed, transmitted and stored on the cloud architecture is secure, procedures & guidelines shall be framed to provide direction for **hosting the type of information, its criticality and the level of security controls to be adopted**, on cloud or on any external hosting infrastructure: ▪ With reference to the **electronic maintenance of core business records, records shall be hosted within India**. ▪ The **selection of cloud hosting model** shall **depend** on the **criticality** of the information being hosted. ▪ **Business justification** for considering inevitable to host the data and system in Cloud. An appropriate **service level agreement (SLA)** shall be in place to address: ▪ security control measures to prevent, detect and react to breaches including data leakage and demonstration of the same; ▪ unilateral contract termination/exit clause; and ▪ right to audit for IRDAI /Law enforcement agencies and Cert-fin to access information / log. Service Provider's contract shall include clauses to ensure confidentiality, integrity, availability and privacy of the data collected, processed, stored and disposed through cloud services. **Contracts with service provider** shall include but not limited to following in addition to the other contractual requirement: i) SLA; ii) compliance to applicable laws & regulations; iii) data ownership; iv) authentication controls; v) log retrievals; vi) patch management; vii) configuration management; viii) application/system security testing; ix) data recovery plan; and x) data deletion at separation or expiry of contract. **Cloud Access Control:** appropriate access control mechanism shall be implemented with reliable authentication mechanism to ensure: a) data is not shared accidentally with other customers on the cloud; b) cloud service provider/application service provider/any third-party personnel controls are in place to provide a logical segregation of duties; and c) logging and monitoring of privilege access shall be carried out. **Cloud Data Security** should cover: • controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS, DB, Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements on cloud; • data-in-transition cloud shall be in encrypted form, as appropriate to the information classification; • encryption techniques shall be implemented for cloud data hosting like Data in Transit and Data-at-rest for PII; • it is recommended to use appropriate Data Loss Prevention (DLP) solution to identify, monitor and protect sensitive data and manage the data risk for the organisation; • data retention and destruction schedules should be defined by the organisation and service provider should be made responsible to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures and on the media. The company should audit this practice, wherever applicable; and • data retention controls should also ensure that the multiple copies of the data stored in different locations are also destroyed post the retention timeframe.

Data protection and security

Table 12

Authority	Data protection and security
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for: ▪ **data use limitations**, including that the cloud service provider should not use the Member Organisation's data for secondary purposes; ▪ **security**, including that the cloud service provider should implement and monitor the cyber-security controls as determined in the risk assessment for protecting the confidentiality, integrity and availability of the Member Organisation's data; ▪ **data segregation**, including that the Member Organisation's data is logically segregated from other data held by the cloud service provider, including that the cloud service provider should be able to identify the Member Organisation's data and at all times should be able to distinguish it from other data.
MAS	Institutions should be aware of CS' typical characteristics such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, institutions should take active steps to address the risks associated with **data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing**. In particular, institutions should ensure that the **service provider** possesses the ability to clearly **identify** and **segregate** customer data using strong physical or logical **controls**. The service provider should have in place robust access controls to protect customer information and such access controls should survive the tenure of the contract of the CS.
FCA	Regarding **data security**, a firm should: ▪ agree a **data residency policy** with the provider upon commencing a relationship with them, which sets out the jurisdictions in which the firm's data can be stored, processed and managed. This policy should be reviewed periodically. ▪ understand the **provider's data loss** and **breach notification processes** and ensure they are aligned with the firm's risk appetite and legal or regulatory obligations ▪ consider how data will be **segregated** (if using a public cloud) ▪ take appropriate steps to **mitigate** security risks so that the firm's overall security exposure is acceptable ▪ consider data **sensitivity** and how the data are transmitted, stored and encrypted, where necessary. Regarding **data protection**, a firm should comply with the GDPR and any associated guidance. Data protection requirements are separate from FCA Handbook requirements and each must be met separately. Firms should require **prompt** and appropriately **detailed notification** of any **breaches** or other relevant events arising including the invocation of business recovery arrangements and ensure the contract(s) provide for the remediation of breaches and other adverse events.

Location

Table 13

Authority	Location
APRA	Regulated entities are required to **consult with APRA** prior to entering into an outsourcing arrangement involving a **material** business activity where **offshoring** is involved. When the proposed use of **cloud computing services** involves **heightened or extreme inherent risks**, APRA encourages **consultation prior to entering into any arrangement**, regardless of whether offshoring is involved. The intent is to ensure that the APRA-regulated entity understands and has the capability to manage these risks.
OSFI	Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on **location** of **records.**
IRDAI	Regarding cloud security, with reference to the **electronic maintenance of core business records**, **records** shall be **hosted** within **India**.
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for **data location**, including that in principle **only cloud services** should be used that are **located** in **Saudi Arabia**, or when cloud services are to be used **outside** Saudi Arabia that the Member Organisation should obtain explicit **approval** from SAMA.
MAS	The resiliency and robustness of critical systems which are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links. To minimise impact on business operations in the event of a disruption (eg due to earthquake), the FI should ensure that **cross-border network redundancy**, with strategies such as engagement of different network service providers and alternate network paths, is instituted.
FCA	Before acceptance, firms should review whether the legal and regulatory risks differ if the **customers**, **firms** and **employees** involved in providing or using the services are in **different geographic** or **jurisdictional locations** eg UK, EEA or non-EEA.

Subcontracting

Table 14

Authority	Subcontracting
OSFI	Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on subcontracting.
ACPR	The contractual framework must also make it possible to obtain **visibility** into the service provider's organisation, particularly in terms of any subcontracting.
FCA	**Before** acceptance, forms should **identify**, where these are related to the regulated activity being provided, **all** the **service providers** in the **supply chain** and **ensure** that the **requirements** on the firm can be complied with throughout the supply chain. Similarly, where **multiple providers** form part of an overall arrangement (as distinct from a chain) the requirements should be complied with across the arrangement. **Relationship between service providers**: ▪ If the regulated firm does not directly contract with the outsource provider, it should review subcontracting arrangements relevant to the provision of the regulated activity to determine whether these enable the regulated firm to continue to comply with its regulatory requirements. Firms should consider, for example, security requirements and effective access to data and business premises. The regulated firm must be able to comply with these regulatory requirements even if it does not directly contract with the outsource provider. ▪ The Contracts (Rights of Third Parties) Act 1999 may be relevant to these considerations. ▪ The regulated firm should consider how service providers work together. For example will the firm or one service provider take the lead systems integration role? Firms should consider how easily a service provider's services will interface with a firm's internal systems or other third-party systems (such as agency banking arrangements for payments).

Business continuity and exit strategies

Table 15

Authority	Business continuity and exit strategies
APRA	APRA-regulated entities must develop **contingency plans** that allow for the cloud computing service to be provided through alternate means if required (eg an alternative service provider or brought in-house). This would typically be achieved through: ▪ the development and periodic validation of **exit strategies** to be enacted on contract expiry (or otherwise), including consideration of the contractual and technical ability to isolate and clearly identify IT assets for transition to another arrangement (or in-house); and ▪ **consideration of the removal** of **sensitive IT assets** from the incumbent provider's environment (including from backups and other copies). The intent of these contingency plans is to enable an orderly transition, if needed, while continuing to meet obligations. **Business disruption**: APRA expects that an APRA-regulated entity would continue to meet its obligations regardless of disruptions resulting from a failure of technology, people, process or service providers. To this end, APRA-regulated entities have taken advantage of the high-availability solutions inherent in many of the cloud computing offerings. However, it is important to distinguish between high-availability and recovery capability when considering the use of cloud computing services. **High-availability** refers to techniques which reduce the likelihood of IT assets becoming unavailable in the event of failure of individual components. **Recovery** refers to techniques to restore IT assets to a known state following a compromise of integrity or availability, thereby reducing the impact of a business disruption. Both high-availability and recovery capability aim to ensure that the business can continue to meet objectives in the event of disruption to IT assets. APRA-regulated entities need to maintain recovery capability regardless of the level of the level of high-availability in place. In addition, contingency plans are also relevant in the case of provider failure for material arrangements **Observed weaknesses** i) inadequate consideration of how the regulated entity will continue to meet obligations for a variety of scenarios, including provider failure – either technological or financial; ii) inadequate consideration of point-in-time recovery capability with reliance placed upon high-availability solutions; iii) inadequate contingency plans which enable critical business activities to be delivered through alternate means, such as via an alternate provider or reverting to operating in-house; and iv) inadequate segregation between production and the IT assets necessary to enact recovery, such that a single incident could compromise recovery capability. **Recovery planning**, when using cloud computing services, can be informed by a set of plausible **disruption scenarios**. This would generally include consideration of the failure of high-availability mechanisms (both hardware and software), compromise of a management console(s) and logical failure(s) (eg software errors, replication malfunction or a failed change). In addition, the following are important considerations as part of effective recovery capability when using cloud computing services: ▪ **clarity** regarding **roles** and **responsibilities** of the cloud computing service provider, the APRA-regulated entity and other parties in the event of a disruption event (including crisis management, recovery initiation, co-ordination of recovery activities and communication); ▪ **clarity** regarding the **state** to which the cloud computing service will be **recovered** and the **impact** this has on recovery and backup activities of the APRA-regulated entity and other parties. This includes consideration of data, software and software configuration; ▪ **ensuring** that the security control environment of the **alternate site** meets production requirements; ▪ **ensuring** that recovery strategies, when using cloud computing services, are not exposed to the risk of the same event impacting production and recovery environments: and ▪ **testing regime** that verifies that recovery plans and strategies, when using share computing services, are effective, and ensure business requirements (including recovery objectives relating to time, point, capacity and performance) are met in the event of a loss of availability.

Business continuity and exit strategies — Table 15

Authority	Business continuity and exit strategies
OSFI	Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on contingency planning.
ACPR	**Continuity** of the service: it is crucial for SLAs to be in place. These make it possible to formalise the expectations of the client company. Specific commitments on the part of the service provider are expected with respect to business continuity (including the maximum duration of downtime and the maximum allowable loss of data). Monitoring of the service must be based on reports on the availability, security incidents and location of the data. **Reversibility of the service**: conditions of reversibility must to be defined when subscribing to the service. Issues of the format of **returned data** and their **destruction** must be covered in the contract between the parties. This ability to withdraw from the service provider also leads to constraints on the side of the customer organisation. The latter must in effect ensure its ability to re-absorb the outsourced activity or to transfer it to another service provider with sufficient reactivity (management of functional, application-based and technical knowledge, ability to position resources and to develop their skills, budget allocation, etc). **Dependence** on the **provider** of the cloud computing solution should be **assessed regularly.**
IRDAI	An appropriate **service level agreement** shall be in place to address **sustainability** (support for fail safe operations) and data retrieval time. SLA should have a **unilateral** contract **termination/exit** clause. A consistent method for **securely handling** the **termination** of relationships with Parties shall be established which shall include: • designating individuals responsible for managing the termination; • revocation of physical and logical access rights to the organisation's information; • return, transfer or secure destruction of assets (eg' back-up media storage' documentation, hardware and data); and • coverage of license agreements and intellectual property rights. **Alternative (contingency) arrangements** shall be established to ensure that the organisation's business processes can continue in the event that the external party is not available (eg due to contract termination or a disaster or a dispute with the external supplier or the entry ceases its operations). This arrangement shall be based on the results of a risk assessment.
DNB	A specific clause in the agreement that, at a minimum, provide for the manner in which the agreement is to be terminated and the guarantee(s) provided to enable the supervised institution to resume performance of the outsourced processes, or to outsource their performance to another third party, upon termination of the agreement.
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for business continuity, including that business continuity requirements are met in **accordance** with the Member Organisation's **business continuity policy**. The cloud computing policy for hybrid and public cloud services should address requirements for exit, including that: • the Member Organisation has **termination rights**; • the cloud service provider has to **return** the Member Organisation's data on termination; and • the cloud service provider has to **irreversibly delete** the Member Organisation's data on termination.
MAS	FI should verify the service provider's ability to recover the outsourced systems and IT services within the stipulated **recovery time objective** ("RTO") prior to contracting with the service provider.

Business continuity and exit strategies

Table 15

Authority	Business continuity and exit strategies
FCA	A firm should have in place appropriate arrangements to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption of the outsourced services. Firms should: ▪ consider the **likelihood** and **impact** of an unexpected disruption to the continuity of its operations; ▪ **document** its **strategy** for maintaining continuity of its operations, including recovery from an event, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy; ▪ regularly **update** and **test arrangements** to ensure their effectiveness; and ▪ put in place arrangements to ensure the **regulator** has **access to data** in the event of **insolvency** or other **disruption**. For exit plan, firms should: ▪ have **exit plans** and **termination arrangements** that are **understood**, **documented** and fully **tested;** ▪ know how it would **transition** to an alternative service provider and maintain business continuity; ▪ have a specific obligation put on the outsourcing provider to **cooperate** fully with both the firm and any new outsource; provider(s) to ensure there is a smooth transition; ▪ know how it would **remove** data from the service provider's systems on exit; and ▪ monitor **concentration risk** and consider what action it would take if the outsource provider failed.

Monitor and control

Table 16

Authority	Monitor and control
APRA	Effective management is typically achieved through the development and maintenance of ongoing **operational** and **strategic oversight mechanisms. These** facilitate **assessment** of **performance** against **agreed service levels**, assessment of the ongoing **viability** of the provider and the service, timely notification of **change** (this includes changes to service location, key personnel, subcontracting arrangements, control environment, relevant policies/standard/procedures and IT assets, either by service provider or other customers, as relevant), and a timely **response** to issues and emerging risks. **Observed weaknesses** Lack of consideration of the framework for ongoing management including operational oversight, risk management and assurance. Ongoing management would generally include monitoring alignment of the APRA-regulated entity's IT environmental requirements to those provided by the cloud computing service. This includes **performance, capacity, security, high-availability and recoverability** requirements. The contract for the cloud computing service agreement would typically address the APRA-regulated entity's access to the service provider's information and personnel under various scenarios. This is both for oversight and assurance purposes as well as in the event of a security incident. The provisions would also allow access by APRA in accordance with the outsourcing standards. An APRA-regulated entity would benefit from developing an engagement model between the internal risk function and that of the service provider to facilitate greater understanding and influence regarding the risk profile and associated control environment. This would typically be facilitated by joint forums and the sharing of risk and control assessments.
OSFI	Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on monitoring the material outsourcing arrangements. Under the self-assessment guide, it is recommended that firms have a process in place to **monitor** the **level** of **cyber risk preparedness** for material outsourcing arrangements and critical IT service providers.
ACPR	The corporate customer using a cloud solution must establish a form of **ongoing contractual management**, relying on **penalty** clauses to be applied in the event of shortcomings in the service rendered by the service provider. The deployment of a suitable **internal control mechanism** is complicated by the difficulties in establishing a balanced contractual relationship, in auditing the service provider (multiplicity of stakeholders, potentially global geographic location, etc) and in identifying the regulatory rules that apply to the data.
SAMA	The cyber-sec**urity controls** regarding the cloud computing policy and process for hybrid and public cloud services should be periodically **measured** and **evaluated**. Additionally compliance with the cloud computing policy should be monitored.
MAS	Institutions are ultimately responsible and accountable for maintaining oversight of CS and managing the attendant risks of adopting CS, as in any other form of outsourcing arrangements. A risk-based approach should be taken by institutions to ensure that the level of oversight and controls are commensurate with the materiality of the risks posed by the CS.
FCA	Firms should maintain an accurate **record of contracts** between the firm and its service provider(s) and should monitor **concentration** risk and consider what action it would take if the outsource provider failed.

Access and audit rights

Table 17

Authority	Access and audit rights
APRA	**APRA access and ability to act** The cloud computing agreement should include a clause for APRA-access to both documentation and information, and the right for APRA to conduct on-site visits to the service provider. The **APRA access clause** is an important prudential tool, as it aims to remove legal impediments which could inhibit APRA's ability to fulfil its duties as a prudential regulator. **Observed weaknesses**: impediments placed on APRA-access rights to the service provider (outsourcing standards). Examples include placing caveats on APRA's ability to access documents, information or the service provider.
OSFI	Regarding the general outsourcing requirements, for cloud computing OSFI recommends to have emphasis on access and audit rights.
ACPR	The ability to audit and the right to do so for the authority is an **essential contractual clause** for any provision of cloud computing services. Conducting **regular audits** is expected. Conducting **penetration** and **vulnerability testing** is necessary for supervision of the service as is access to **audit trails** previously identified (the principle of partitioning data between different customers also applies to these trails). Certification of the service provider alone should not be considered as a measure of adequate risk control. It is necessary to maintain **permanently the list of suppliers** of cloud computing as well as the **list of services** that are entrusted to them.
BaFin	Insurance undertakings are also required to ensure through outsourcing contracts the unrestricted rights of information and audit and the ability to monitor of both the company and BaFin. Whether a service relationship is considered to constitute outsourcing to a cloud service provider depends on which functions or insurance activities are intended to be outsourced. **Not only functions** and **insurance activities** that are regarded as **important** but **also other activities** must, pursuant to section 32 (1), (2) and (4) of the VAG, **be subject to supervision**. In accordance with margin no. 255 of the Minimum Requirements under Supervisory Law on the System of Governance of Insurance Undertakings, the requirements of Article 274 of the Delegated Regulation on Solvency II must also be applied to other functions and insurance activities that are not regarded as important to the extent that these requirements are universal in nature. The statements above regarding the restriction of rights of information and audit also apply here. In particular, if an insurance undertaking is contractually obliged to first rely on standardised audit reports made available by the cloud providers, this is usually regarded as a restriction. Phased information and audit procedures do not comply with the supervisory requirements for insurance undertakings. It is also considered a restriction if audits are dependent on the concept of commercial reasonableness. BaFin is currently considering also allowing insurance undertakings to exercise certain rights of audit vis-à-vis cloud service providers through pooled audits together with other insurance companies. Here a distinction must be made between the granting of unrestricted rights of audit, in particular the option to perform on-site inspections, and the design of the audit procedure. Here too, the choice of audit procedure must not result in a restriction of the rights of audit.
IRDAI	An appropriate **service level agreement** shall be in place to address the right to audit for IRDAI /Law enforcement agencies.
DNB	A specific clause in the agreement that, at a minimum, provide for: ▪ the possibility for **supervisors** to perform, directly or by proxy, **examinations** on the **premises** of the third party; ▪ the **mutual exchange of information** and, by request, the provision of relevant information to supervisors; ▪ the power on the part of the supervised institution to **modify** at any time the manner in which the outsourced processes are performed; and ▪ an obligation on the supervised institution to **comply** at all times with all legal requirements.

Access and audit rights

Table 17

Authority	Access and audit rights
SAMA	The cloud computing policy for hybrid and public cloud services should address requirements for audit, review and monitoring, including that the Member Organisation has the right to perform a **cyber-security audit** at the cloud service provider; and the Member Organisation has the right to perform a **cyber-security examination** at the cloud service provider.
FCA	Regarding **access to data**, a firm should: • ensure that notification requirements on accessing data, as agreed with the service provider are reasonable and not overly restrictive; • ensure there are no restrictions on the number of requests the firm, its auditor or the regulator can make to access or receive data (Under the Financial Services and Markets Act 2000, the FCA has certain powers to require information. These requirements compel the disclosure of information or documents from authorised persons or those believed to be in possession of information relevant to an FCA investigation. In some cases, this information could be stored in the cloud. Regardless of the ultimate location of information, a firm or individual in possession of the information will be expected to comply with such a requirement); • advise the service provider that the regulator will not enter into a nondisclosure agreement with the service provider but will treat any information disclosed in accordance with the confidentiality obligation set out in the Financial Services and Markets Act (FSMA), sections 348 to 349; • ensure that, where a firm cannot disclose data for any reason, the contract enables the regulator or the firm's auditor to contact the service provider directly; and • ensure that data are not stored in jurisdictions that may inhibit effective access to data for UK regulators. Considerations should include the wider political and security stability of the jurisdiction; the law in force in the jurisdiction in question (including data protection); and the international obligations of the jurisdiction (For example international co-operation agreements such as the IOSCO Multilateral Memorandum of Understanding). This should include consideration of the law enforcement provisions within a jurisdiction Regarding **access to business premises**, a firm: • Should be able to request an onsite visit to the relevant business premises, in accordance with applicable legal and regulatory requirements. This right should not be restricted. • Can provide reasonable prior written notice of this visit, except when there is an emergency or crisis situation. • A firm may elect its auditor to undertake the visit. Note that this must be the firm's auditor and not an auditor appointed by the outsourcing provider. • The scope of the firm and/or auditor visit can be limited to those services that the firm and the entities in the firm's group are using, as required by applicable legal and regulatory requirements.

Access and audit rights

Table 17

Authority	Access and audit rights
	Regarding **regulator access**: ▪ A regulator visit to an outsource provider's business premises will only take place if the regulator deems it necessary and required under applicable legal and regulatory requirements. Firms should not stipulate further conditions beyond this. ▪ The outsource provider should commit to cooperate with the reasonable requests of the regulator during such a visit. ▪ The regulator can commit to visits occurring during business hours and at a time specified by the outsourcing provider or with reasonable notice, except in an emergency or crisis situation. ▪ There can be no restrictions regarding employees who attend from the regulator. However, regulators can and will provide relevant information about individuals who will attend. ▪ During the visit, the regulator should be permitted to view the provision of services to the regulated firm or any affiliate within the group, as required under applicable financial services legislation. The regulator can commit to minimising disruption to outsourcing providers' operations.

Annex 2 – Supervisory consultation, notification or authorisation

Supervisory consultation, notification or approval — Table 18

Authority	Supervisory consultation, notification or approval
APRA	**Notification:** • An APRA-regulated institution must **notify** APRA as soon as possible **after entering** into an outsourcing agreement, and in any event no later than 20 business days after execution of the outsourcing agreement. This notification requirement applies to all outsourcing of **material business activities**. When an APRA-regulated institution notifies APRA of a new outsourcing agreement, it must also provide a summary to APRA of the key risks involved in the outsourcing arrangement and the risk mitigation strategies put in place to address these risks. APRA may request additional material where it considers it necessary in order to assess the impact of the outsourcing arrangement on the institution's risk profile. • Where an outsourcing agreement is **terminated**, an APRA-regulated institution must **notify** APRA as soon as practicable and provide a statement about the transition arrangements and future strategies for carrying out the outsourced material business activity **Consultation**: • Regulated entities are required to **consult** with APRA **prior** to entering into an outsourcing arrangement involving a **material business activity** where **offshoring** is involved so that APRA may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the institution's risk management framework. If, in APRA's view, the offshoring agreement involves risks that the APRA regulated institution is not managing appropriately, APRA may require the APRA-regulated institution to make other arrangements for the outsourced activity as soon as practicable. Regulated entities are required to **consult with APRA** prior to entering into an outsourcing arrangement involving a **material** business activity where **offshoring** is involved. When the proposed use of **cloud computing services** involves **heightened or extreme inherent risks**, APRA encourages **consultation prior to entering into any arrangement**, regardless of whether offshoring is involved. The intent is to ensure that the APRA-regulated entity understands and has the capability to manage these risks. For clarity, there is no need for consultation with APRA prior to entering into low inherent risk arrangements. To facilitate the consultation process, regulated entities could provide documentation used to inform the internal governance mechanisms. Regulated entities should be able to demonstrate APRA that risks are understood and managed: ▪ ability to continue operations and meet obligations following a loss of service; ▪ preservation of the quality (including security) of critical and/or sensitive data/information; ▪ compliance with legislative and prudential requirements; and ▪ absence of jurisdictional, contractual or technical considerations which may inhibit APRA's ability to fulfil its duties as prudential regulator (including impediments to timely access to documentation and data/information). The above is relevant whether the cloud computing service is provided directly or through subcontracting / on-sourcing arrangements entered into by the provider, initially or subsequently. This necessitates careful consideration of what is permissible within the agreement and awareness of changes to the way services are provided.

Supervisory consultation, notification or approval

Table 18

Authority	Supervisory consultation, notification or approval
ACPR	**Notification**: Entities should send written notification to ACPR regarding **any** outsourcing of **critical** or **important functions or activities**, The notification should include: ▪ a description of the outsourcing scope; ▪ the reasons for outsourcing; and ▪ the name of the service provider. When outsourcing concerns a key function, the notification also includes the name of the person in charge of the function or activities outsourced to the service provider.
BaFin	**Notification** In accordance with section 47 no. 8 of the VAG, an immediate duty of **notification** with submission of the draft contract applies to the intention to outsource **important functions or insurance activities**. The notification, as well as all documentation to be appended, must generally be submitted in German. The documents can also be submitted in English following consultation with the relevant BaFin division. If necessary, BaFin may request at a later point that the undertaking provide a certified translation. The draft contract must also be submitted together with the signed notification. The notification must state: ▪ •the name of the service provider; ▪ •the address of the service provider; ▪ •a description of the scope of the outsourcing; ▪ •the reasons for the outsourcing; and ▪ •in the event that a key task is being outsourced, in particular one of the four key functions stipulated by statute, the name of the competent person at the service provider side. If a key task is being outsourced, no documentation (eg CV, certificate of good conduct) needs to be submitted in relation to the competent person at the service provider side.

Supervisory consultation, notification or approval — Table 18

Authority	Supervisory consultation, notification or approval
HKIA	**Notification**: **Before entering**: Insurer should notify the HKIA when it is planning to enter into a **new material** outsourcing arrangement or **significantly vary** an existing one. Unless otherwise justifiable by the insurer, the notification should be made at least 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. The insurer should satisfy the HKIA that it has taken into account and properly addressed all the essential issues set out in the Guideline in the planning stage. If considered appropriate, the HKIA may request any additional information, discuss with the insurer on any area of concern on the outsourcing arrangement and require it to take necessary actions to address the concerns. The three-month prior notification period may be extended by the HKIA if the insurer is not able to address the area of concerns to the satisfaction of the HKIA within the period. For overseas material outsourcing, the HKIA may also communicate with the home or host regulator of the insurer and the service provider to seek clarification or confirmation on relevant issues as considered necessary. **After entering** into a **new material** outsourcing arrangement or **significantly varying** an existing one: the insurer should within 30 days submit to the HKIA information relating to the arrangement, including: (a) the service outsourced; (b) the name of the service provider; (c) the location where the outsourced service is performed; (d) the commencement date and expiry or renewal date of the outsourcing agreement; and (e) a copy of the outsourcing agreement. The insurer should notify the HKIA immediately whenever there is any subsequent change to the information submitted and any renewal or termination of the outsourcing arrangement.
DNB	**Notification** Before a supervised institution proceeds to engage in material/critical cloud computing, including important modifications, DNB expects to be informed of this prospective outsourcing arrangement. DNB will ask the supervised institution to submit its risk analysis concerning cloud computing for assessment in the context of risk-based supervision.
SAMA	**Authorisation**: ▪ Insurers and Insurance Service Provides should seek SAMA's **written no objection prior** to undertaking any Material Outsourcing. Proposals for all Material Outsourcing should be submitted to SAMA in writing, at least 30 working days for a domestic Third Party and 60 working days for a foreign Third Party prior to the proposed date of commencement of the Outsourcing Arrangement. The Board of Directors should ensure that senior management has assessed each proposed Outsourcing function qualitatively and quantitatively and classified it as material or non-material prior to submitting to SAMA. ▪ Insurers and Insurance Service Providers may seek SAMA's **guidance** if uncertain whether or not an existing or new arrangement is considered material or non-material. ▪ For cloud services, the Member Organisation should obtain SAMA approval prior to using cloud services or signing the contract with the cloud provider;

Supervisory consultation, notification or approval

Table 18

Authority	Supervisory consultation, notification or approval
MAS	**Modifications**: MAS requires no notification or approval. MAS may require an institution to modify, make alternative arrangements or reintegrate an outsourced service into the institution where one of the following circumstances arises: ▪ An institution fails or is unable to demonstrate a satisfactory level of understanding of the nature and extent of risk arising from the outsourcing arrangement; ▪ An institution fails or is unable to implement adequate measures to address the risks arising from its outsourcing arrangements in a satisfactory and timely manner; ▪ Adverse developments arise from the outsourcing arrangement that could impact an institution; ▪ MAS' supervisory powers over the institution and ability to carry out MAS' supervisory functions in respect of the institution's services are hindered; or ▪ The security and confidentiality of the institution's customer information is lowered due to changes in the control environment of the service provider.
FINMA	**Authorisation** Under Article 4 para. 2 let. J in conjunction with Article 5 para 2 ISA, the outsourcing of significant functions and the partially admissible **outsourcing** of control **functions** are **relevant** to the **business plan** and thus require **authorisation**. For insurance companies: …the outsourcing of significant functions and the partially admissible outsourcing of control functions are relevant to the business plan and thus require authorisation.
PRA	**Notification** A firm should notify the PRA when it intends to enter into a material outsourcing arrangement
FCA	**Notification** A firm should notify the FCA when it intends to enter into a material outsourcing arrangement