Principles on Outsourcing

Final Report

The Board
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR07/2021	**OCTOBER 2021**

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org

© *International Organization of Securities Commissions 2021. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

Contents

Chapter 1 - Executive Summary

IOSCO has undertaken work to gain a better understanding of recent developments in outsourcing by market participants in the securities markets and to update the existing IOSCO Principles on Outsourcing to address these developments. Committee 2 on Secondary Markets (C2), Committee 3 on the Regulation of Financial Intermediaries (C3), Committee 6 on Credit Rating Agencies (C6), and Committee 7 on Derivatives (C7) participated in this joint project.

Based on this work, IOSCO has developed a common set of outsourcing principles. These principles are based on the earlier 2005 Outsourcing Principles for Market Intermediaries and the 2009 Outsourcing Principles for Markets, but their application is expanded to trading venues, market intermediaries, market participants acting on a proprietary basis, and credit rating agencies. Their application may also be considered by financial market infrastructures.

The revised outsourcing principles comprise a set of fundamental precepts and seven principles (the "Principles on Outsourcing" or "these Principles"). The fundamental precepts cover issues such as the definition of outsourcing, the assessment of materiality and criticality, affiliates, sub-outsourcing and outsourcing on a cross-border basis. The seven principles (each a "Principle") set out expectations for regulated entities that outsource tasks, along with guidance for implementation.

This report ("Report") also contains sections on particular sectors and issues and Annex A provides a report on outsourcing among credit rating agencies, including the use of cloud computing. The Report also briefly addresses the impact of COVID-19 on outsourcing and operational resilience.

The Principles on Outsourcing

Principle 1: A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.

Principle 2: A regulated entity should enter into a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.

Principle 3: A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.

Principle 4: A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients, from intentional or inadvertent unauthorised disclosure to third parties.

Principle 5: A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

Principle 6: A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.

Principle 7: A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.

Chapter 2 - Background

Introduction

In many jurisdictions, the complexity of the global financial markets and the wider trading landscape has grown as securities markets become faster and more competitive. These developments, coupled with increasing automation, are incentivising businesses to reduce costs and improve efficiency, in some cases, by outsourcing certain tasks to service providers. Work by IOSCO shows that some market intermediaries and market participants, trading venues, and credit rating agencies, as well as market infrastructures may rely to a significant extent on service providers for outsourced tasks.

The increasing use of outsourcing by many regulated entities is of growing importance to a number of IOSCO Committees. Given that markets have undergone technological and other developments in recent years, including an increased reliance on a few concentrated service providers, the IOSCO Board agreed in October 2018 to undertake a joint project on outsourcing with the participation of:

- Committee 2 on Secondary Markets (C2);
- Committee 3 on the Regulation of Financial Intermediaries (C3);
- Committee 6 on Credit Rating Agencies (C6); and
- Committee 7 on Derivatives (C7) (collectively, the "Committees").

The purpose of this review was to assess whether the existing principles remained suitable and to update them where appropriate. Additionally, C6 and C7 wished to consider principles for outsourcing for credit rating agencies and in the area of derivatives, respectively. C6 conducted work to establish the use of cloud computing for outsourcing; their findings are included as Annex A.

Context

In September 2005, IOSCO published a report on Principles on Outsourcing of Financial Services for Market Intermediaries[1] ("2005 Principles"). This report sets out principles that are designed to assist market intermediaries in determining the steps they should take when considering outsourcing tasks. The report also contains some broad principles to assist regulators in addressing outsourcing in their regular risk reviews of entities.

In July 2009, IOSCO published a report on Principles on Outsourcing by Markets[2] ("2009 Principles") to address the risks relevant to outsourcing and the use of third parties in the context of secondary trading in securities markets. For example, the 2009 Principles highlight the issues of due diligence in selecting a provider, contract terms and termination, business continuity, security and confidentiality of information and ensuring the regulators' prompt access to relevant information.

---

[1] See PD187 Principles on Outsourcing of Financial Services for Market Intermediaries, Report of the Board of IOSCO, February 2005 available at:

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

[2] See PD299 Principles on Outsourcing of Financial Services by Markets, Report of the Board of IOSCO, February 2009 available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD299.pdf

However, in the last ten years, the trading landscape for firms and markets has changed considerably. Regulatory reforms, technology developments, increased connectivity among market participants and increased levels of electronic trading and process automation have heightened the complexity of markets and the financial infrastructure and increased focus on operational efficiency.

A wide range of tasks are outsourced by regulated entities to service providers. These commonly outsourced tasks include information technology (IT), operation/support of exchanges and trading platforms, regulatory reporting, and other control functions such as real-time trade monitoring and audits. Other examples include joint ventures and strategic alliances aimed at facilitating trading (e.g., the shared use of analytical, legal, compliance, internal controls, IT, and other support functions for critical tasks within a group of entities). In the over-the-counter (OTC) derivatives sector, outsourced post trade tasks typically include trade matching and confirmation, portfolio reconciliation and compression, collateral management, trade reporting, credit limit checks, and custody of assets.

It is increasingly commonplace for regulated entities to use third-party service providers to carry out, or otherwise support, some of their regulated business activities. The benefits of outsourcing include lowering costs, increasing automation to speed up tasks and reduce the need for manual intervention, and providing flexibility to allow regulated entities to rapidly adjust both to the scope and scale of their activities. However, while outsourcing can deliver benefits, it may also raise concerns about risk management and compliance when such tasks are outsourced to entities that are not regulated and/or are based in different jurisdictions. In particular, it can diminish regulators' ability to regulate or supervise certain functions within firms or other regulated entities.

Members of the Committees participating in this work surveyed or consulted industry participants in their respective jurisdictions and sectors for information regarding current outsourcing practices and how they have been impacted by recent changes. After their information gathering exercises, some IOSCO members reported that outsourced tasks are, in parts of some markets, concentrated in a small number of highly specialised, often IT-based companies. Consequently, some IOSCO members are concerned that disruption to the functioning of these companies could constitute a source of risk in the areas they serve. Therefore, although outsourcing may bring substantial benefits to markets and their participants, it poses a number of important and evolving challenges and may have an impact on the effectiveness and integrity of markets.

Based on their information gathering exercises, the Committees concluded that much of the content of the 2005 Principles and the 2009 Principles reports is still valid and gives helpful guidance to regulated entities on outsourcing. Accordingly, the Committees have merged the 2005 and 2009 Principles into the Principles on Outsourcing set out in this Report. These Principles on Outsourcing retain the principles in prior reports whilst adapting and updating them and expanding their scope as appropriate.

These Principles on Outsourcing are intended to be technology-neutral and provide regulated entities with sufficient flexibility to implement them according to the nature and size of their business model.

Impact of COVID-19 on Outsourcing and Operational Resilience[3]

During the COVID-19 pandemic, outsourcing activity generally proved to be resilient and outsourcing may have enhanced operational resilience at some financial institutions, especially in cases where the financial institutions were located in areas with less developed IT infrastructure. However, the shift to a remote working environment also highlighted vulnerabilities, for example, from cyber threats, as well as practical challenges such as auditing and obtaining information when onsite audits, inspections and face-to-face meetings were restricted. More generally, the location of a service provider also became a more relevant factor during the COVID-19 pandemic.

The COVID-19 pandemic has also had a broader impact than simply the move to remote working. In particular, it has led to the increased use of technology, restricted the ability to conduct onsite meetings and visits, and some service providers experienced significant increases in volumes whilst simultaneously responding to lockdown measures, increased absenteeism and the challenges of working from home. Moreover, the asynchronous impact of COVID-19 means that regulated entities and service providers in different jurisdictions may be subject to different pressures and constraints.

This event and the greater reliance on outsourcing serve as a useful reminder to increase attention to operational resilience issues. Regulated entities should consider the Principles on Outsourcing when thinking about how to maintain and improve resilience.

The COVID-19 pandemic highlighted certain aspects of the Principles on Outsourcing. In particular, regulated entities should consider:

- With regard to Principles 1 and 2, the service level provisions that apply to the service providers depending on whether the staff are working onsite or remotely, and whether service providers and regulated entities have identified their dependencies and taken steps to mitigate the associated risks.
- With respect to Principle 3 on cyber security and resilience issues, the challenges posed by a remote working environment, the increased use of technology and the evolving threat landscape.
- With regard to Principle 3, testing that uses severe but plausible scenarios which encapsulate multiple concurrent events.
- Regarding Principles 3 and 4, the continuity and quality of outsourced tasks where the regulated entities' and third-party service providers' work forces are working remotely. This could include considering additional capabilities to safeguard the security and the accessibility of the remote network connection used by staff, as well as setting procedures in business continuity plans and performing adequate testing to validate this capability.
- With respect to Principle 5 on concentration risk (as well as the assessment of materiality and criticality) measurement, assessment and understanding of outsourcing

[3] IOSCO has developed an Operational Resilience Group to consider and report on issues raised by the COVID-19 pandemic relating to operational resilience, business continuity planning, cyber security-risks and moves to remote working environment for trading venues and market intermediaries.

from a technology and infrastructure perspective (e.g., cloud service providers) as well as the physical location of the service provider.

- With respect to Principle 6, the possibility of obtaining information regarding a third-party service provider from the regulated entity's or service provider's home country regulator, where there are difficulties arranging on-site inspections or otherwise obtaining information from the regulated entity itself.
- With regard to Principle 7, contingency planning processes and incorporating appropriate exit strategies.

Chapter 3 – Glossary

In this report, the following definitions apply:

"affiliate"	any entity that, directly or indirectly through one or more parties, is controlled by, or is under common control with, the regulated entity.
"cloud service provider"	a service provider of cloud computing, that is, a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
"community cloud"	cloud infrastructure that is provisioned for the exclusive use of a specific community of consumers from organizations that have shared concerns. It may exist on or off the clients' premises.
"credit rating agency" or "CRA"	an entity that is in the business of issuing credit ratings. "Credit rating" or "rating" means an assessment regarding the creditworthiness of an entity or obligation, expressed using an established and defined ranking system.
"critical task"	a task that is critical to the functioning of the regulated entity or the integrity of financial markets. A critical task may be a task that is small in scale but without which the regulated entity is unable to conduct its activities such that the regulated entity is unable to meet its own obligations to its clients or to comply with applicable regulation.
"hybrid cloud"	cloud infrastructure that is composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.
"Infrastructure as a Service" ("IaaS")	a cloud service provider offers clients pay-as-you-go access to storage, networks, and other fundamental computing resources in the cloud.
"market intermediaries" and "market participants"	refers as appropriate in the context of jurisdictional differences in regulatory scope and generally refers to those regulated entities, other than those that are trading venues, that are in the business of some or all of the following: • executing orders in, or distributing, securities or derivatives; • proprietary trading or dealing on own account; • receiving and transmitting orders from or to third parties; • providing advice regarding securities or derivatives or the advisability of purchasing or selling securities or derivatives; and • underwriting of new issues or products.

	Some jurisdictions may regulate an entity as a market intermediary that simply provides advice regarding the value of securities or derivatives or the advisability of investing in, purchasing or selling such instruments[4].
"management body"	a regulated entity's body or bodies, which are appointed in accordance with the jurisdiction's law, which are empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making and include the persons who effectively direct the business of the regulated entity and persons responsible for the management of the regulated entity.
"material task"	a task that comprises or affects a significant proportion of the activities, operations, client or market relationships and would introduce a material or unacceptable level of risk to the entity if the tasks were to fail.
"outsourcing"	a business practice in which a regulated entity uses a service provider to perform tasks, functions, processes, services or activities (collectively, "tasks") that would otherwise be undertaken by the regulated entity itself.
"Platform as a Service ("PaaS")	a model of cloud services where a cloud service provider offers access to a cloud-based environment in which users can deploy consumer-created or acquired applications. The service provider supplies the underlying infrastructure.
"pooled audit"	audits organized jointly with other clients of the same service provider, and performed by them and these clients or by a third-party appointed by them.
"private cloud"	cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third-party, or some combination of them, and it may exist on or off premises
"public cloud"	cloud infrastructure that is for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the cloud provider's premises.
"regulated entities"	trading venues, market intermediaries and market participants acting on a proprietary basis, and credit rating agencies that are regulated under the relevant legal regime of a jurisdiction.
"securities markets"	are used, where the context permits, to refer compendiously to the various market sectors. In particular, where the context permits, they should be understood to include reference to the derivatives

[4] For the purposes of this report, the term intermediary includes broker-dealers but not investment advisers in the U.S. securities sector.

	markets. The same applies to the use of the term "securities regulation".
"service provider"	both third-party and affiliate service providers, regulated (whether or not by the same regulator with authority over the regulated entity) or unregulated.
"Software as a Service" ("SaaS")	a model of cloud service where a cloud service provider offers clients the use of the provider's software and applications running on a cloud infrastructure.
"sub-outsourcing"	means a situation where the service provider under an outsourcing arrangement further transfers an outsourced task (or a part of that task) to another service provider (the sub-contractor).
"tasks"	see definition of "outsourcing".
"third-party certifications"	independent third-party reports and certifications certifying against the particular audit requirements with respect to the service provider and provided by a certification body to the regulated entity.
"trading venues"	exchanges or other multilateral trading systems including for example, alternative trading systems (ATSs) and multilateral trading facilities (MTFs). It also refers to the operator or a particular trading venue. IOSCO recognizes that the concept of a "trading venue" differs among IOSCO member jurisdictions and the concept may, at the discretion of individual members and for their jurisdictions only also include other types of trading venues referred to by alternative nomenclatures.
"virtual inspections"	inspections that utilize electronic technology rather than in-person visits.
"written contracts"	in this Report, written contracts include contracts, arrangements and agreements concluded by electronic means or electronic contracts stored in a durable, recordable and readable form, where permitted under the relevant law.

Chapter 4 - Fundamental Precepts

A. Scope of Application

These Principles on Outsourcing apply to a wide range of regulated entities participating in the securities markets. Those regulated entities will vary in size, sophistication, products and services, and activities. The extent that they use outsourcing will differ. Accordingly, it is important that the Principles on Outsourcing are read in conjunction with the explanatory text and accompanying notes.

The Principles on Outsourcing should apply to those regulated entities that are within the scope of the IOSCO Committees 2, 3, 6, and 7; namely, trading venues, market intermediaries and market participants acting on a proprietary basis, and credit rating agencies that are regulated under the relevant legal regime of a jurisdiction.

These Principles are not addressed to financial market infrastructures within the scope of the CPMI-IOSCO *Principles for Financial Market Infrastructures*.[5] Nonetheless financial market infrastructures may decide to apply some or all of the Principles set out in this Report to themselves, or those parts of their infrastructure not formally covered by these Principles, in particular with respect to areas that are recent developments or not otherwise covered by existing material.

The application and implementation of these Principles should be proportional to the size, complexity and risk posed by the outsourcing.

Regulated entities should also consider whether they should clarify or renegotiate contracts with service providers to gain reasonable assurance that their outsourcing arrangements reflect/adhere to the Principles on Outsourcing in an informed and proportionate manner. Neither IOSCO nor the Committees expect the issuance of updated Principles on Outsourcing to lead to an automatic renegotiation of contracts if existing arrangements are sufficient. When circumstances change or, on a periodic basis, regulated entities should assess and consider the adequacy of their existing contracts; for example, when they fall due for review or renewal, or when the regulatory framework for outsourcing has evolved, or the nature of a firm's business activities or client base has changed.

B. Outsourcing

In this Report "outsourcing" is considered to be a business practice in which a regulated entity uses a service provider to perform tasks, functions, processes, services or activities (collectively, "tasks") that would otherwise be undertaken by the regulated entity itself. This may also be referred to as onshoring, offshoring, near-shoring or right-shoring, depending on the organisational context and the relationship with affiliates and service providers.

Outsourcing may include tasks that the regulated entity has not previously performed, where those tasks would reasonably be expected to be initiated by the regulated entity if they had not been outsourced to a third-party. Outsourcing may also include tasks that the regulated entity does not have the capacity or resources to perform or does not want to perform. This may occur

[5] CPMI-IOSCO Principles for Financial Market Infrastructures, April 2012, available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD377-PFMI.pdf

in particular when a new regulated entity is established, or when an existing regulated entity enters a new area of business or becomes subject to a new regulatory requirement.

In determining whether an arrangement falls under the definition of outsourcing, regulated entities may consider the nature of the task, the totality of the facts and circumstances of the activity, and the relationship with the service provider. Consideration should be given to whether the function:

- is performed on a recurrent or an ongoing basis by the service provider; and
- whether this function would normally fall within the scope of functions that would or could realistically be performed by the regulated entity.

Generally, the following are considered not to be indicative of outsourcing under the Principles:

- a function that is legally required to be performed by a service provider, e.g., statutory audit;
- market information services;
- global network infrastructures;
- clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;
- global financial messaging infrastructures that are subject to oversight by relevant authorities;
- correspondent banking services;
- the acquisition of services that would otherwise not be undertaken by the regulated entity (e.g. advice from an architect, providing legal opinion and representation from outside lawyers, cleaning, gardening and maintenance, etc. of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services, clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g., plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g., electricity, gas, water, telephone line).[6]

For the purposes of these Principles, further transfers of an outsourced task (or a part of that task) from one service provider to another is referred to as "sub-outsourcing". In some jurisdictions, the initial outsourcing by the regulated entity may be referred to as sub-outsourcing. For the purposes of this Report, the difference between outsourcing and sub-outsourcing is explained in Fundamental Precept H on Sub-outsourcing.

A CRA assesses the creditworthiness of an entity that is usually called an obligor or issuer. Obligors include entities such as corporations, financial institutions, insurance companies, or municipalities. Many CRAs are paid by the obligors they rate or by the issuers of the securities they rate. Some CRAs are, in addition, also paid by subscribers to their ratings services, which are usually investors. In either case, CRAs generally do not use the terms "customers" or "clients" to refer to issuers, obligors, subscribers, or investors. However, in the context of these Principles, reference to the term customer or client also applies to these parties.

[6] This list of functions and tasks is non exhaustive.

C. Responsibility for Outsourcing

The regulated entity retains full responsibility, legal liability, and accountability to the regulator for all tasks that it may outsource to a service provider to the same extent as if the service were provided in-house. The regulatory responsibilities of the regulated entity and its management cannot be outsourced unless permitted under the regulatory requirements of the regulated entity's jurisdiction. Moreover, outsourcing should not be permitted to impair the regulator's ability to perform its functions, including the proper supervision and examination of a regulated entity.

Consistent with jurisdictions' laws and regulations, a regulator may impose sanctions and penalties on a regulated entity for the regulated entity's violations of statutory or regulatory requirements that have resulted in whole or in part from the failure of a service provider (whether it is regulated or unregulated).

Management and the governing body of the regulated entity should assess these Principles and, where necessary, develop and implement appropriate policies and procedures reasonably designed to achieve the objectives of these Principles, to periodically review the effectiveness of those policies and procedures, and to address any identified outsourcing risks in an effective and timely manner.

Regulated entities should also be aware of and comply with mechanisms within their jurisdiction that may have been put in place to implement these Principles on Outsourcing. Such mechanisms may take the form of government regulation, guidelines, codes, or practices imposed by non-government statutory regulators, or some combination of these items.

Outsourcing may pose important challenges to the integrity and effectiveness of jurisdictions' financial services regulatory regimes. Where outsourcing is undertaken by regulated entities, absent a credible supervisory structure within the regulated entity to supervise the outsourced activity, that entity's control over the people and processes dealing with the outsourced tasks may decrease. In some jurisdictions, regulators may impose restrictions on the outsourcing of certain tasks where they believe the outsourcing introduces an unacceptable risk or is critical to the functioning of a regulated entity.

Regulators expect to have prompt and complete physical or electronic, or remote access to data concerning a regulated entity's activities, whether such data are stored with or held by the regulated entity's service provider or otherwise.

D. Potential Risks and Challenges

Outsourcing poses a number of challenges and risks, both for regulated entities that outsource and for their regulators.

Control: When a regulated entity uses a third-party to perform a task, it may have a detrimental impact on the regulated entity's understanding of how the task is performed, with a consequential loss of control over that task.

A regulated entity may lack control over some outsourced tasks, hindering its ability to protect the confidentiality of its own and client information. This may present risks that a service provider or its staff could misappropriate information, or that an external party could gain unauthorized access to information held by the service provider. These risks may have increased in recent years, as many tasks are being digitalised and/or based on algorithms, and data and information are stored in cloud environments, i.e., stored on remote servers and

accessed from the internet. However, it is also common industry practice to use privacy agreements when outsourcing tasks to safeguard data and information, as well as implementation of cyber defences, such as encryption.

Data and Technology: It is generally recognised that the number of cyber incidents and data leaks is increasing. Further, the inappropriate selection of a service provider may lead to a business disruption, with negative consequences for the regulated entity's clients and, in certain instances, the potential for spill-over effects and systemic risk to the market as a whole. Outsourcing to, and storing of, data in a cloud may increase certain risks, such as the risk of cyber incidents. This could make the monitoring of, and reliance on, outsourced tasks more difficult due to the uncertainty of the physical location of data, a possible lack of understanding of cloud technology risks on the part of the regulated entity, and the rapid development and changing nature of cloud technology.

However, the adoption of cloud technology by regulated entities may have a mitigating impact on these risks; cloud service providers may be more aware of cyber-security issues and have more sophisticated systems to detect and prevent cyber-incidents than local data centre providers or the regulated entities themselves. Regulated entities may outsource tasks that use artificial intelligence and machine learning techniques to third-party service providers; the issues raised here are addressed in the IOSCO report on The use of artificial intelligence and machine learning by market intermediaries and asset managers (2021)[7].

Operational resilience: Operational disruptions to the services that a regulated entity provides have the potential to harm consumers and market participants, threaten the viability of regulated entities, and cause instability in the financial system. Operational resilience generally refers to how well an organisation can continue to deliver critical operations when faced with a sudden shock or disruption to its normal operating environment and is addressed in a number of other IOSCO Reports[8].

There are numerous challenges to ensuring that the businesses of regulated entities are resilient to operational disruption and additional challenges may occur where regulated entities outsource a significant level of tasks to third parties and operate internationally.

Finally, given the increasing interconnectedness of international markets, the development of common principles on outsourcing helps ensure that operational resilience is not adversely affected by the location of the regulated entity's service providers and can facilitate regulatory cooperation in the supervision of regulated entities that operate internationally.

Concentration: Service providers have become more specialised in recent years, leading to situations where only a few entities offer certain (often IT-dependent) services. As a result, concentration in the number and/or materiality of the services that are outsourced may have increased. This concentration may reduce competitive pressures on service providers, potentially reducing their incentives to improve service and resilience levels or to price competitively. In addition, the potential lack of competition may lead to under-investment in

---

[7] ***The Use of Artificial Intelligence and Machine Learning by Market Intermediaries and Asset Managers,*** September 2021: available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf.

[8] Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (2015) and Market Intermediary Business Continuity and Recovery Planning (2015). IOSCO has developed an Operational Resilience Group to consider and report on issues raised by the COVID-19 pandemic relating to operational resilience, business continuity planning, cyber security-risks and moves to remote working environment for trading venues and market intermediaries.

risk management, systems, and operational innovation, which may ultimately reduce the resilience and efficiency of the overall market.

There were different views on the issues raised by concentration. For example, although they reported limited competition in some post-trade services, some regulated entities viewed concentration of service providers as beneficial to the market. They expressed concern that regulatory action, such as reducing barriers to entry, may cause some established firms in markets that tend to concentrate (e.g., those with significant economies of scale or network effects) to leave those markets. This would then have negative consequences for users.

Other regulated entities reported that service providers with a "market-controlling" position often refuse to agree on contractual provisions that are necessary for the regulated entity to comply with jurisdictions' regulatory requirements or to agree to contractual inspection rights for regulated entities and their regulators.

Possible operational and systemic risks also may arise if multiple regulated entities use a common service provider.

Supervisory: Outsourcing may pose important challenges to the integrity and effectiveness of financial services regulatory and supervisory regimes and systems. A regulated entity may lose some control over the people and processes dealing with the outsourced tasks. Nonetheless, regulators may require that the regulated entity including its board of directors and senior management, remain fully responsible (to clients and regulatory authorities) for the outsourced task as if the service was being performed in-house. In some jurisdictions, regulators may prohibit or impose restrictions or notification requirements on the outsourcing of certain tasks where the jurisdictions have determined that outsourcing introduces an unacceptable risk or is critical to the functioning of a regulated entity or the integrity of the market.

E. Assessment of Materiality and Criticality

The Principles on Outsourcing set out IOSCO's expectations of regulated entities. They are written to help ensure they apply to outsourced tasks that pose risks to regulated entities and regulatory objectives.

These Principles should be applied according to the degree of materiality or criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations. In understanding and applying the Principles on Outsourcing, the regulated entity should develop a process for determining the materiality or criticality of the tasks it is seeking to outsource.

In simple terms, a material task is one that comprises or affects a significant proportion of the activities, operations, clients or market relationships and would introduce a material or unacceptable level of risk to the entity if they were to fail.

An outsourced task is critical if it is critical to the functioning of the regulated entity or the integrity of financial markets. A critical task may be a task that is small in scale but without which the regulated entity is unable to conduct its activities such that the regulated entity is unable to meet its own obligations to its clients or to comply with applicable regulations.

Even where the task is not material or critical, the regulated entity should consider the appropriateness of applying these Principles as a matter of good practice.

The assessment of what is material or critical is often subjective and depends on the circumstances of the regulated entity in question. Regulated entities should consider individual

factors to determine if an outsourced task is material, critical or both. Factors to be considered by the regulated entity may include, but are not limited to the:

- Potential risks to the regulatory objectives of maintaining fair, orderly, and transparent markets;
- Potential impact on price formation;
- Potential negative impacts on investor protection or directly on clients;
- Potential threats to relevant clearing and settlement systems;
- Whether the regulated entity would be unable to deliver core services to its clients without the relevant outsourced service;
- Financial, reputational, and operational impact on the regulated entity of the failure of a service provider to perform certain tasks;
- Potential impact of a deterioration of the quality of services provided by a service provider on the regulated entity's clients;
- Potential impact on the quality of credit ratings as well as the quality of the credit rating process;
- Sensitivity of the outsourced task, such that failure to recover within a specific timeframe may pose contagion risk to the broader market;
- Potential monetary losses and other harms to a regulated entity's clients resulting from the failure of a service provider to perform;
- Impact of outsourcing the task on the ability and capacity of the regulated entity to comply with regulatory requirements and changes in requirements;
- Impact on a regulated entity's control functions and risk management;
- Involvement of critical (including price-sensitive or client-confidential) information;
- Impact of outsourcing on the data security and data integrity of the regulated entity and its clients;
- Degree of difficulty and time required to select an alternative service provider or to bring the task in-house;

For the purposes of CRAs in the context of these Principles, "material" or "critical" tasks may include, for example, the shared use by entities within a CRA network of analytical, legal, compliance, internal controls, IT, and potential other tasks.

These examples are illustrative only, and should not be regarded as determinative in all circumstances as to whether a factor is material or critical.

Regulated entities should consider the totality of all factors relevant to an outsourced task. The combination of a number of factors, which are minimal in isolation may determine that the outsourced task to which they are related is material or critical when they are considered in aggregate.

Some factors, such as the degree of difficulty and time required to select an alternative service provider or to bring the task in-house could be considered to be both material and critical, depending on the task that they relate to.

F. Affiliates

The Principles on Outsourcing apply whether the outsourced tasks are performed by an affiliated entity within the corporate group of the regulated entity or by an entity that is external to the corporate group.

In the case of CRAs, the Principles on Outsourcing should be applied equally to all tasks within the entire network of rating affiliates and non-rating affiliates, as well as entities unaffiliated with a credit rating agency, or joint ventures and strategic alliances with other credit rating agencies.

While the Principles on Outsourcing should be applied to affiliated entities, their application should take into account the organisation and control structures and arrangements between the regulated entity and its affiliates. The risks associated with outsourcing tasks to an affiliated service provider may be different to those encountered in outsourcing to an unaffiliated external service provider.

Risks may, in certain cases, not be as pronounced within an affiliated group. For example, the regulated entity may have the ability to control or influence the actions of the affiliated service provider, and the regulated entity may be more familiar with the affiliated service provider's business attributes. These factors might reduce certain risks involved in outsourcing compared to outsourcing to an unaffiliated service provider.

However, intra-group outsourcing may potentially increase risk in certain instances: for example, the relationship may be less than arms-length, and the regulated entity and its clients may have different interests from those of the affiliated service provider. In some cases, the intra-group relationship may restrict the ability of the regulated entity to control or influence the service provider, and, by extension, of the regulator to effectively supervise the regulated entity. Additionally, the provision of tasks between affiliates may not be the subject of an executed contract, or the affiliates may choose not to enforce its provisions with rigour.

Therefore, while the Principles on Outsourcing should be applied to affiliated entities where relevant, it may also be appropriate to assess and apply them with some modification.

G. Outsourcing on a cross-border basis

The Principles on Outsourcing apply to tasks that a regulated entity outsources both within the jurisdiction in which it maintains a presence and on a cross-border basis.

Additional risks may arise when outsourcing is on a cross-border basis compared to those that arise when the service provider is in the same jurisdiction as that of the regulated entity. These risks may include the following:

- The jurisdictions of the regulated entity and service provider may have different or conflicting requirements on the use and provision of outsourcing;
- The jurisdictions of the regulated entity and service provider may have different legal systems, in particular with respect to the treatment of contracts between the regulated entity and service providers in relation to bankruptcy and rights to assets/collateral;
- In an emergency or business continuity situation, it may be more difficult to monitor and control the task that was outsourced or to implement appropriate responses in a timely fashion;

- The use of a cross-border service provider may require an analysis by the regulated entity of any economic, social, or political conditions that might adversely impact the service provider's ability to perform effectively for the regulated entity;
- A regulated entity should give special consideration to the use of a cross-border service provider if the books, records, or other material are maintained in a foreign jurisdiction and ensure prompt access to, and translation of, such data when necessary; and
- Where confidential information and/or client data are subject to outsourcing, the regulated entity should assess the regulatory environment for data security and protection and, if necessary, consider additional precautionary measures such as introducing enhanced encryption.

Taken together, regulated entities should consider the additional risks arising from outsourcing on a cross-border basis which may require enhanced attention during the due diligence process and contract negotiations.

H. Sub-outsourcing

Service providers may use the services of a sub-contractor to perform the outsourced tasks, but the regulated entity should take appropriate steps to ensure that the service provider provides the regulated entity notice including relevant details, which may include but are not limited to, the names of any sub-contractors, where the sub-outsourcing service will be performed and, if applicable, the location (i.e. country or region) where the data will be stored. However, regulated entities should take appropriate measures if the sub-outsourcing could have material adverse effects on the outsourcing arrangement of a critical or material function or would lead to a material increase of risk. Such measures may include objecting to the sub-outsourcing, and/or terminating the contract. Regulated entities should take appropriate measures if they identify shortcomings in the provision of the outsourced function as a consequence of any sub-outsourcing.

I. Concentration of outsourcing tasks

Where multiple regulated entities use a common service provider, operational risks are correspondingly concentrated, and may increase to the extent that they present a systemic risk. Examples of these operational risks include:

- If the service provider suddenly and unexpectedly becomes unable to perform services that are material or critical to the business of a significant number of regulated entities, each entity will be similarly disabled;
- A latent flaw in the design of a product or service that multiple regulated entities rely upon may affect all these users;
- A vulnerability in application software that multiple regulated entities rely upon may permit an intruder to disable or corrupt the systems or data of some or all users;
- If multiple regulated entities depend upon the same provider of business continuity services (e.g., a common disaster recovery site), a disruption that affects a large number of those entities may reduce the capacity of the business continuity service.

Each of these scenarios may have knock-on effects on other sectors or on public confidence in markets.

Chapter 5 – Outsourcing Principles

Due diligence in the selection and monitoring of a service provider and the service provider's performance

Principle 1: ***A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.***

It is important that regulated entities exercise due care, skill, and diligence in the selection of service providers. The regulated entity should be satisfied that the service provider has the ability and capacity to undertake the provision of the outsourced task effectively at all times.

The regulated entity should also establish appropriate processes and procedures for monitoring the performance of the service provider on an ongoing basis to ensure that it retains the ability and capacity to continue to provide the outsourced task. In determining the appropriate level of monitoring, the regulated entity should consider the materiality and criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations (see Fundamental Precept E on assessment of materiality and criticality).

Implementation

Regulated entities should take appropriate steps to ensure they select suitable service providers and that service providers are appropriately monitored, having regard to the services they provide. The following are examples of steps that could be taken:

- The regulated entity should implement documented processes and procedures that enable it to assess, prior to selection and on an ongoing basis, the service provider's ability and capacity to perform the outsourced tasks effectively, reliably, continuously, and to a high standard. This should include consideration of the service provider's technical, financial, and human resources capacity, together with any specific risk factors associated with using a service provider.
- The regulated entity should take appropriate steps to ensure the selection, assessment, and monitoring of a service provider is undertaken by competent staff who are able and empowered to evaluate the ability of the service provider to perform the outsourced tasks. This may require the participation of different internal areas within the regulated entity, such as the staff who are familiar with the tasks to be outsourced, IT and information security, risk management, as well as the legal and finance functions.
- The regulated entity should take appropriate steps to identify any potential or actual conflicts of interest between the regulated entity and the service provider (including any of the service provider's affiliated entities and sub-contractors) and take appropriate steps to ensure policies and procedures are in place to mitigate and manage any potential conflicts of interest that have been identified or could arise.
- Subject to the availability of information, the regulated entity should determine, document and implement procedures that enable it to assess, prior to selection, the impact of a sudden interruption of service and the availability on a timely basis of an alternative service provider capable of meeting the expected standards.

- Carrying out due diligence to allow the regulated entity to assess at an entity-level how many tasks are outsourced to the same service provider and assess possible over-reliance risk. Regulated entities could also consider choosing a different service provider for different outsourced services to reduce dependencies and reduce the risk of becoming locked into a specific provider's technological or operational configuration.
- Implementing processes and procedures to monitor the service provider's performance in accordance with its contractual obligations which could include:
  - Establishing and documenting clearly defined metrics which will be used by the regulated entity to measure the service level, and specify what service levels are required including with respect to emergency procedures and disaster recovery and contingency plans, as addressed under Principle 3 regarding business resilience, continuity and disaster recovery; Enabling the regulated entity to assess and report to its responsible management the quality of tasks performed by the service provider on an ongoing basis;
  - An agreement with the service provider on the type and frequency of service delivery reports to monitor the performance of the outsourced tasks;
  - Measures for the service provider to identify, record, and remediate instances of failure to meet contractual obligations or unsatisfactory performance and to report such instances to the regulated entity on a timely basis;
  - The use of internal and/or external auditors to monitor, assess, and report to the regulated entity on performance;
  - The use of written service level agreements or the inclusion of specific service level provisions in contracts for service to achieve clarity of performance targets and measurements for service providers; and
  - The regulated entity assessing the control over confidential information or client data, particularly when outsourcing to a cloud function or a technology provider, especially when based in a different jurisdiction where different regulation will be applicable.
- Implementing processes and procedures intended to ensure:
  - The service provider complies with applicable laws and regulatory requirements in its jurisdiction;
  - Where the service provider fails to perform tasks required by statute or regulation, the regulated entity is able to report the failure as soon as possible to its regulator, where it is required to do so. This requirement is generally consistent with regulations in many IOSCO jurisdictions requiring a regulated entity to notify its regulator with respect to any breaches that may have occurred; and
  - The regulated entity takes corrective actions immediately on the detection of a failure by a service provider to perform its obligations to ensure those obligations required by statute or regulation are met.
- When outsourcing is undertaken on a cross-border basis, the regulated entity should consider conducting enhanced due diligence that focuses on particular risks, including the ability to:
  - Effectively monitor the foreign service provider;
  - Maintain the confidentiality of entity and client information; and

- Execute contingency plans and exit strategies with minimal impact on the continuity of the regulated entity's operations.

The regulated entity should also determine whether any laws in the service provider's jurisdiction would obstruct or frustrate the ability of it or its regulator to obtain prompt access to data.

- Documenting processes and procedures that allow the regulated entity to re-assess an outsourcing arrangement, including its materiality or criticality, where there is a significant change in the volume or the nature of its business or the tasks outsourced. Where an arrangement is re-assessed as material or critical, (consistent with Fundamental Precept E on assessment of materiality and criticality) consideration should be given to all aspects of the Principles on Outsourcing and whether changes are required either immediately or when the outsourcing contract is substantively amended, renewed, or extended.
- No matter how much outsourcing is carried out, regulated entities should conduct adequate due diligence on service providers, consistent with their jurisdictions' laws and regulations.
- The regulated entity should maintain a minimum operational and managerial capability, including technical and human resources appropriate for its business model, the size of the entity, and the nature of the services provided to clients. Key tasks and personnel should, in general, be retained within the regulated entity. This could include senior management, key function holders such as control functions, in particular personnel responsible for the compliance and risk management function, and other personnel necessary to credibly supervise the outsourced activity on behalf of the regulated entity.
- A regulated entity should periodically assess whether it is outsourcing extensively (including key tasks) and should avoid the risk of becoming an "empty shell" at any time. A regulated entity should also periodically consider whether to bring the outsourced tasks back "in-house".
- The regulated entity should also periodically assess whether its internal controls are adequate to oversee the outsourced tasks, including the fulfilment of all contractual terms by the service provider.
- To facilitate this assessment and ongoing oversight, the regulated entity may consider appointing an individual, central function or committee tasked with the oversight of its outsourcing arrangements. Such a person or body should ensure that a holistic view is taken by the regulated entity of the extent of its outsourcing and the associated risks. Such a view should be maintained on an ongoing basis to ensure that any evolution in the nature of risks, activities or markets is considered.

The contract with a service provider

Principle 2: ***A regulated entity should enter into a legally binding written contract[9] with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.***

A legally binding written contract between a regulated entity and a service provider is the critical element underpinning the relationship between the regulated entity and the service provider. Contractual provisions can reduce the risks of non-performance or aid the resolution of disagreements about the scope, nature, and quality of the service to be provided. A written contract will assist the monitoring of the outsourced tasks by the regulated entity and/or by regulators.

The level of detail of the written contract should reflect the level of monitoring, assessment, inspection and auditing required, as well as the risks, size and complexity of the outsourced services involved. In determining the nature and detail of the written contract, the regulated entity should consider the materiality and criticality of the outsourced task to the ongoing business of the regulated entity and to its regulatory obligations, as discussed in the section on assessment of materiality and criticality, above.

Where different regulatory requirements may apply for the regulated entity and the service provider due to the cross-border nature of the service, the service provider should recognise and accommodate the requirements of each jurisdiction in which it operates, as appropriate, and ensure it acts in a manner that is consistent with the regulated entity's regulatory obligations.

Implementation

A regulated entity should have a written and legally binding contract with the service provider, appropriate to the materiality and criticality (consistent with Fundamental Precept E on assessment of materiality and criticality) of the outsourced task to the ongoing business of the regulated entity. The contract should define the rights and obligations of both parties and may include, as applicable, provisions dealing with:

- Responsibilities of the regulated entity and the responsibilities of the service provider and subcontractors, if any, including specific service level provisions, and how such responsibilities will be monitored;
- Limitations or conditions, if any, on the service provider's ability to sub-outsource, and, to the extent sub-outsourcing is permitted, obligations in connection therewith;
- Framework to amend existing arrangements with the service provider if there are changes in regulatory requirements;
- Confidentiality of information of the regulated entity and of its clients, including adequate restrictions on onward sharing of such confidential information;

[9] References to written contracts in this Report include contracts concluded by electronic means or electronic contracts stored in a durable, recordable and readable form, where permitted under the relevant law.

- Levels of staffing and competency (including education, certifications or qualifications, skill sets, language proficiency, experience and training) appropriate to meet the needs of the outsourced task;
- Responsibilities relating to IT security, including cyber security;
- Payment arrangements;
- Liability of the service provider to the regulated entity for unsatisfactory performance or other breach of the agreement;
- Guarantees, indemnities, and appropriate types and levels of insurance cover;
- Obligations of the service provider to ensure, upon request, prompt access to records and information, premises, IT systems and personnel and to provide assistance concerning outsourced tasks to the regulated entity, its auditors and/or its regulators and possible consequences in case of failure or refusal of the service provider to do so;
- Prohibitions on the service provider deleting or discarding or otherwise making records unavailable to the regulated entity, including in the event of non-payment by the regulated entity, in a manner that is inconsistent with the record retention requirements applicable to the regulated entity;
- Mechanisms to resolve disputes that might arise under the outsourcing arrangement;
- Business continuity provisions and disaster recovery;
- When outsourcing on a cross-border basis, choice of law and/or choice of court provisions; and
- Termination of the contract, transfer and/or deletion of information and exit strategies, including any wind down plans for the outsourced tasks to ensure that post-termination no confidential data or information remains with the service provider other than that required to meet its own legal obligations, and no ongoing operational and technological dependency on the service provider remains.

Information security, business resilience, continuity and disaster recovery

Principle 3: ***A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.***

Effective, secure and resilient information technology systems are fundamental to the markets. Cyber vulnerabilities may arise through connections to unsecure vendors and the exploitation of information and communication platforms.

Security breaches and cyber incidents can undermine investors' privacy and/or entities' confidentiality interests and have a damaging effect on a regulated entity's reputation, which may ultimately cause a loss of market confidence and adversely impact the overall operational risk profile of the regulated entity.

In particular, robust IT security is important where details of trade data and client assets, or the assets themselves, might be vulnerable to unauthorised access or theft. Accordingly, regulated entities should take appropriate steps to ensure that service providers maintain appropriate IT security, cyber-resilience, and disaster recovery capabilities and business continuity plans. As part of its reviews of these matters, a regulated entity should also take into account whether additional issues are raised when the outsourcing is performed on a cross-border basis.

Implementation

Regulated entities should take appropriate steps to ensure, consistent with precept E on assessment of materiality and criticality, that service providers have in place a comprehensive IT security, cyber-resilience, disaster recovery and business continuity program. These steps may include the insertion of provisions in the contract with the service provider to address such issues as:

- Specification of the security requirements of automated systems to be used by the service provider, including the technical and organisational measures that will be taken to protect entity and client-related data, and market sensitive data. Appropriate care should be exercised to ensure that IT and cyber security measures in place protect the privacy of the regulated entity's clients to the extent mandated by law; this may be particularly relevant when outsourcing to cloud service providers.
- Requirements that the service provider has put in place and maintains effective measures and protocols for cyber security and to protect against cyber incidents. This should cover all software used by, or made available to the regulated entity, including any software developed by the service provider for the use of the regulated entity.
- Requirements that the service provider conducts regular tests to measure the effectiveness of cyber security measures; regulated entities could also decide to require service providers to undergo a regular security assessment by another third-party to ensure that security requirements are met.
- Specification of the rights of each party to change or require changes to security procedures and requirements and of the circumstances under which such changes might occur.

- Provisions that address the service provider's emergency procedures and disaster recovery and contingency plans as well as any particular issues that may need to be addressed where the regulated entity is utilising a service provider in another jurisdiction. Where relevant, this may include the service provider's responsibility for backing up and otherwise protecting program and data files, as well as regulatory reporting; this may also include requirements for service providers to have a backup in the jurisdiction of the regulated entity.
- Where appropriate, terms and conditions relevant to the use of subcontractors with respect to IT security should also apply to open-source resources, and appropriate steps to minimise the risks arising out of such sub-outsourcing and the use of open-source resources.
- Where appropriate, requirements for testing by the service provider of the processes, systems and back-up facilities critical to their business on a periodic basis in order to review the ability of the service provider to perform adequately even under unusual physical and/or market conditions at the regulated entity, the service provider, or both, and to determine whether sufficient capacity exists under all relevant conditions.
- Requirements for disclosure by the service provider of breaches in security resulting in unauthorised intrusions (whether deliberate or inadvertent, and whether confirmed or not) that may affect the regulated entity or its clients, including a report of corrective action taken. The report by the service provider could include the following matters:
  - An explanation of the kind of breach experienced;
  - A statement of when the breach was discovered, how it was discovered and how long it had existed before being discovered and reported;
  - The time to correct the issue;
  - A clear statement of the data content that has been exposed, and whether any part of the data relates to clients of the regulated entity;
  - An explanation of how the security breach was resolved, and the controls that were implemented to achieve this; and
  - An explanation of the measures that will be undertaken by the service provider to prevent recurrence of the security breach or the data loss.
- Provisions in the regulated entity's own contingency plans that address circumstances in which one or more of its service providers fail to adequately perform their contractual obligations or where the provision of the service is disrupted or the service cannot be continued due to changes in the technological or regulatory environment. Where relevant, this may include reporting by the regulated entity to its regulator. The regulated entity should consider contractually requiring information from the service provider to fulfil this obligation.
- Provisions to ensure the continuity and quality of outsourced tasks or services in the event of termination of the outsourcing, either by transferring the outsourced tasks or services to another service provider or by the regulated entity performing them itself.
- Regulated entities should take appropriate steps to ensure that third parties have in place a comprehensive cyber security and resilience program. To avoid overlap or duplication, the regulated entities should look to and implement existing cyber frameworks to address these risks. The Core Standards that may be applied include:

- CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures;[10]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework;[11]
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 family of standards;[12]
- G7 fundamental elements for third-party cyber risk management in the financial sector.[13]

➢ Technology tools and solutions relevant to IT security and business continuity in the context of outsourcing may include, but are not limited to:

- assessment of the benefits and appropriateness of a multi-cloud/multi-vendor strategy;
- technology solutions and tools to facilitate the switching and portability of data and applications as part of exit planning, stressed exits testing and business continuity planning;
- consideration of open source standards as a foundation for portability and interoperability and assessing their providers' adherence to these standards as additional selection criteria;
- Application Programming Interfaces (APIs) or other solutions which allow for the extraction of data directly from the providers and standardised protocols and common data formats to allow data migration features from one provider to another; and
- relevant industry codes and standards.

➢ Regulated entities adopting APIs in connection with outsourced tasks should adopt prevailing best practices in their design, implementation and maintenance.

Confidentiality Issues

Principle 4: ***A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients from intentional or inadvertent unauthorised disclosure to third parties.***

---

[10] CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

[11] National Institute of Standards and Technology (NIST) Cybersecurity Framework, U.S. National Institute of Standards and Technology (NIST) at https://www.nist.gov/cyberframework/critical-infrastructure-resources

NIST in 2018 updated to Version 1.1 of its popular framework, commonly known at the NIST Cybersecurity Framework, including updates to authentication and identity; self-assessing cybersecurity risk; managing cybersecurity with supply chain; and vulnerability disclosure. Available at https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurityframework

[12] See: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_E.zi.

[13] See G7 fundamental elements for third-party cyber risk management in the financial sector available at https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf

Unauthorised disclosure of confidential regulated entity or client information could have a number of negative consequences, including harm to clients and investors, damage to the regulated entity's reputation, financial losses, and the loss of or risk to proprietary information (including the regulated entity's trade secrets).

In addition, unauthorised disclosure or unauthorised access to this information could result in the intentional or inadvertent disclosure of private and sensitive information about individuals who have a reasonable expectation of privacy or a right to privacy pursuant to applicable legal provisions, and might also result in a material financial loss to an entity's clients.

In addition to the potential harm and material financial loss to a regulated entity's clients, an unauthorised disclosure could also result in the regulated entity having financial liability to its clients and/or its regulators, possibly affecting the entity's solvency.

As noted above in the discussion of concepts of outsourcing, CRAs generally do not use the terms "customers" or "clients" to refer to issuers, obligors, subscribers or investors. In the context of these Principles, for CRA's, confidential information should be understood to not just include information related to the CRA itself, but to any issuer, obligor, subscriber or investor–related information and/or software.

Implementation

- Regulated entities that engage in outsourcing should take appropriate steps to confirm that their confidential information and client information is not misused, misappropriated, or unlawfully or inadvertently disclosed to others. Such steps may include insertion of provisions in the contract with the service provider that:
  - Prohibit the service provider and its agents or sub-contractors from using or disclosing the regulated entity's proprietary information or that of the regulated entity's clients or members, except as necessary to provide the contracted services;
  - Consider both physical and electronic information;
  - Where appropriate, govern the use of subcontractors and their obligations with respect to entity, member and client confidentiality; and
  - Require the service provider and its agents to safely dispose of any confidential data and information relating to the entity and its clients when the relationship ends. Such requirements should be consistent with any record keeping requirements that apply to the regulated entity.
- Regulated entities should also consider whether it is appropriate to notify clients that client data may be transmitted to a service provider, taking into account any regulatory or statutory provisions that may be applicable, including in a cross-border context.
- Where confidential information and/or client data is permitted to be outsourced and is subject to outsourcing, the regulatory environment for data security and data protection should be assessed and, if necessary, additional precautionary measures such as enhanced encryption should be considered.
- Regulated entities should consider the use of encryption, in particular, the protection of encryption keys and their availability to the regulator in addition to regulator access to

hardware holding records and the encryption of data at rest and in transit (in accordance with the data classification).

- Regulated entities should comply with applicable laws regarding records management including, but not limited to, how records should be stored and how long data should be retained.

Concentration of outsourcing arrangements

Principle 5: ***A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.***

Concentration risks may arise when one regulated entity relies extensively on one service provider or when many regulated entities rely on one or very few service providers.

Where multiple regulated entities use a common service provider, operational risks are correspondingly concentrated, and may pose a threat of systemic risk.

- For example, if the service provider suddenly and unexpectedly becomes unable to perform services that are material or critical to the business of a significant number of regulated entities, each of the regulated entities will be similarly disabled.
- Alternatively, if multiple regulated entities depend upon the same provider of business continuity services (e.g., a common disaster recovery site), a disruption that affects a large number of those entities may result in a lack of capacity for the business continuity services.

Either of these scenarios may result in negative effects on markets that depend on participation by the impacted regulated entities, or more generally on public confidence in the functioning of financial markets.

Similarly, where a regulated entity is significantly dependent on a single service provider for the provision of outsourced tasks, a concentration risk exists. This may result in business continuity concerns, should an interruption to the provision of tasks occur. Where the regulated entity is critical to a particular market, service or asset class this may also increase systemic risk. Sub-outsourcing can complicate the effective identification of concentration risks, particularly where the parties to the sub-outsourcing chain are spread across different physical and geographical locations.

Although a regulated entity should assess concentration pursuant to this principle, it is recognised that a single regulated entity, despite using best endeavours, may not be aware of, or have enough information or otherwise be able to assess, concentration risks where multiple regulated entities use a common service provider. The application of this Principle and the means of implementation below should therefore apply to the extent that the regulated entity is aware or should be aware of concentration risks from many regulated entities' reliance on one or very few service providers.

Implementation

- Where regulated entities are faced with a concentration risk of service providers, they should carry out an appropriately thorough due diligence assessment before entering into contractual relations with such service providers. They should consider different measures to mitigate the risk, for example entering into a shorter duration contract or implementing business continuity and insourcing plans.

- Regulated entities could also consider, where suitable competition exists, choosing a different service provider for different tasks or parts of tasks that are outsourced. This may reduce dependency on a single service provider and could avoid becoming locked into a specific provider's technological or operational configuration. A regulated entity may also designate a primary and secondary provider. The secondary provider should have the capacity to assume the primary provider's services should an interruption occur.
- Where a regulated entity, during its due diligence process and based on available information, has identified a possible concentration risk, it should consider taking steps to ensure that, to the degree practicable, the service provider has adequate capacity to meet the needs of all regulated entities, both during normal operations as well as unusual circumstances (e.g., unusual market activity, physical disaster).
- Regulated entities should also have procedures for ongoing, periodic reviews of service provider capacity and the regulated entity's own business continuity, disaster recovery and insourcing procedures, and actions as appropriate. Regulated entities should have regard to their assessment of business continuity and disaster recovery arrangements (Principle 3) and ensuring the security and confidentiality of data (Principle 4).
- Regulated entities should identify and monitor sub-outsourcing, intra-group concentration and group dependency in their outsourcing assessments.

Access to data, premises, personnel and associated rights of inspection.

Principle 6: ***A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.***

Regulated entities should ensure that their regulator has prompt and comprehensive access to information concerning outsourced tasks, to enable the regulator to carry out its inspection, investigation and monitoring powers over the activities for which they are regulated. Generally, the scope of supervision should not be impacted by a regulated entity's decision to engage a service provider. The regulated entity retains full responsibility, legal liability and accountability to the regulator for all tasks that the regulated entity may outsource to a service provider to the same extent as if the service were provided in-house.

Regulated entities should ensure that their regulators should also be able, upon request, to obtain promptly any data relating to or generated by the outsourced task, irrespective of whether the data is in the possession of the regulated entity or the service provider and to obtain any additional relevant information concerning the tasks performed by the service provider for the regulated entity.

A regulator's access to such data may be achieved in different ways (depending on regulatory requirements). A regulated entity may first be contacted by the regulator and should deliver information to the regulator based on information obtained via the regulated entity's requests to the service provider. Regulated entities can ensure access to relevant data and information through provisions for clear access and data ownership rights in its contract with the service provider. The regulated entity may also consider the protection of encryption keys and their availability to the regulator and access rights to the data and information, and may consider the use of pooled audits and reliance on relevant third-party certificates.

In some cases, the regulated entity may be required by its regulator to ensure that data is maintained in the regulator's jurisdiction, such as through a locally stored back-up of relevant data, or that the service provider will provide originals or copies of the data to the regulator's jurisdiction upon request (referred to as data localisation when requirements require original copies, or data mirroring when requirements require local copies). In that respect, regulated entities may be required to make provision in their arrangements with service providers for prompt access by regulators to relevant premises that relate to the provision of services to the regulated entity, and to key personnel who manage and oversee the outsourced services. Where data localisation or mirroring is required, arrangements between regulated entities and service providers should seek to ensure that the regulated entities, and their auditors and regulators have appropriate prompt access to the premises, personnel, and data and other information where it is held. Neither data localisation nor mirroring are required for consistency with this Principle, as regulated entities may provide access to relevant data and information in alternative ways.

Access to data should be in a form that is acceptable to the regulator. This should be considered in terms of both the format in which information is made available (e.g., electronic versus paper) and the language in which the material is provided, particularly where the outsourced task is performed in a jurisdiction other than that of the regulated entity.

Implementation:

Regulated entities should consider that jurisdictions and regulators have requirements to ensure prompt access by the regulator to books, records and information of the service provider about the performance of outsourced tasks. These measures may include:

- Requiring the regulated entity to provide promptly, upon request, any data relating to or generated by the outsourced task, irrespective of whether the data is in the possession of the regulated entity or the service provider. The regulated entity should deliver information to the regulator based on information obtained via the regulated entity's requests to the service provider.
- Imposing specific requirements concerning access to data that are held by a service provider and which are necessary for the authority to perform its oversight and supervisory functions with respect to regulated entities in its jurisdiction. These may include requiring that records be maintained in the regulator's jurisdiction (where relevant, in a locally stored back-up of relevant data), allowing for a right of inspection, or requiring that the service provider agrees to send originals or copies of the data to the regulator's jurisdiction upon request.
- Where appropriate, taking action against regulated entities for the failure to provide data required in that jurisdiction, without regard to whether the regulated entity has transferred possession of required data to one or more of its service providers.
- In the case of outsourcing to a regulated service provider, establishing a cooperation and information sharing arrangement with the regulator of the regulated service provider.

A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks and, if applicable, sub-outsourced task. These steps may include the following:

- Contractual provisions by which the regulated entity (including its auditor) has access to, and a right of inspection of, the service provider dealing with outsourced tasks, and similar access to subcontractors providing material or critical services related to the outsourced task. Where appropriate, these may include physical inspections at the premises of the service provider, where appropriate on short or with no prior notice (e.g., in an emergency or a crisis situation), delivery of data or copies of data to the regulated entity or its auditor, or inspections that utilise electronic technology (e.g. "virtual inspections"). These may also include relevant systems information such as infrastructure diagrams and setups.
- Access may be also necessary to systems, hardware, software, algorithms, procedures, manuals, and the staff at the service provider responsible for maintaining them.
- The regulated entity may also consider the protection of encryption keys and their availability to the regulator and access rights to the data and information relating to or generated by the outsourced task, irrespective of whether the data is in the possession of the regulated entity or the service provider.
- Considering the use of pooled audits or assurance statements to obtain confirmation that their requirements and associated regulatory expectations are being met. Consideration should be given to ensuring that appropriate access to these statements is permitted to

regulators. When utilising third-party certifications or pooled audits, the regulated entity should confirm that:

- The certification or audit adequately covers the relevant scope of the outsourced tasks;
- The certification or audit is up to date and takes account of all relevant legal and regulatory requirements;
- The third-party commissioned to conduct this review has the appropriate skills and expertise; and
- The regulated entity has the appropriate skills and expertise to review, challenge and make informed decisions as to the quality and outcomes of the review.

- Having in place contractual provisions by which the service provider is required to make books, records, and other information about outsourced tasks by the service provider available to the regulator upon request. Such contractual provisions may include the requirement to store electronic data in a format that is easily accessible by regulators. In addition, the service provider may be required to comply with any requirements in the regulated entity's jurisdiction to provide periodic reports to the regulator.
- Having appropriate plans for continued access by the regulator to books, records and appropriate personnel and systems in the event of the termination of the contract. Such plans may be dealt with by transfer of information, repatriation of books and records to the regulated entity, and exit strategies, including any wind down plans for the outsourced tasks to ensure that post-termination no ongoing regulatory, operational or technological dependency on the service provider remains.
- Regulated entities may require contractual provisions which prohibit the service provider from deleting, discarding, or otherwise making unavailable, the records of the regulated entity in a manner that is not consistent with the record retention requirements applicable to the regulated entity, including in the event of non-payment of fees and charges by the regulated entity.

Termination of outsourcing arrangements

Principle 7: ***A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.***

Where a task is outsourced, there is an increased risk that the continuity of the particular task in terms of daily management and control of that task, related information and data, staff training, and knowledge management, is dependent on the service provider continuing in that role and performing that task. This risk should be addressed by an agreement between the entity and the service provider, taking into account factors such as when an outsourcing arrangement can be terminated, what will occur on termination and strategies for managing the transfer of the task back to the entity or to another party.

There should be clarity on who owns the relevant data, and whether the service provider has any retention rights.

The written contract and exit strategies should be viewed as separate concepts, though there may be aspects of an exit strategy included in a written contract e.g., an undertaking that the service provider cooperates with the firm to manage the exit when the firm decides to leave the service provider.

Regulated entities should be aware that in practice implementing an exit plan can be complex, time-consuming, and that the exercise of termination arrangements may be difficult. Moreover, termination of external and intragroup processes differ and exit strategies should therefore take appropriate account of affiliate outsourcing; for example, the termination of an outsourcing agreement between a regulated entity and an affiliate providing intragroup services may be more challenging and require a more rigorous exit strategy.

Implementation:

Regulated entities should take appropriate steps to manage termination of outsourcing arrangements. These steps may include provisions in contracts with service providers such as the following:

- Termination rights, e.g., in case of insolvency, liquidation or receivership, change in ownership, failure to comply with regulatory requirements, poor performance (including poor performance resulting from technical problems), breach of confidentiality, vulnerability to cyber intrusions through the service provider or, where permitted, its subcontractor(s), and in other circumstances.
- Minimum periods before a termination can take effect to allow an orderly transition to another provider or to the entity itself, and to provide for the return of all client-related data, the entity-related data of the regulated entity, and any other resources.
- The clear delineation of ownership of intellectual property following the contract's termination, and specifications relating to the transfer of information back to the regulated entity, including confirmation of deletion of records, and confirmation of effective transfer of information.

- The obligation of the service provider to assist and provide full support for a successful and complete transition.

However, there may be areas relating to how an exit strategy is managed in practice that may not be suitable for a written contract, and/or may not be relevant to the particular service provider, but are relevant to how the regulated entity approaches its exit strategy. These matters should be considered by the regulated entity to manage its exit strategy e.g., internal planning for exit and or engagement with alternative suppliers once a decision to exit is taken.

Annex A - Outsourcing and Cloud Computing

This work by IOSCO Committee 6 was finalised on 22 May 2019

Section 1 – Executive Summary

Pursuant to its mandate on *Outsourcing and Cloud Computing*, Committee 6 on Credit Rating Agencies ("C6") conducted a fact-finding exercise by surveying the credit rating agency ("CRA") industry and analysing information from academics, legal experts, and the leading providers of cloud computing services. In addition to this fact-finding exercise, C6 was tasked with evaluating whether certain IOSCO documents should be clarified to address aspects of the fact-finding.

C6 observed that functions being outsourced[14] in the CRA industry are trending towards more central aspects of the credit rating process, particularly where the function is outsourced to an affiliated entity, rather than types of uses associated with traditional back-office responsibilities. Cloud computing is an outsourcing relationship that is complex and is reshaping the financial services industry's information technology profile. The basic approaches to outsourcing and cloud computing are not limited to the CRA sector; they span the financial services industry. For the reasons discussed in this report, C6 recommends that existing IOSCO documents that specifically relate to the CRA industry should not be amended at this time.

Section 2 – Introduction and Background

In May 2017, the IOSCO Board approved a project specification on *Outsourcing and Cloud Computing* ("Project Specification") proposed by C6 to conduct a survey to obtain a better understanding of how outsourcing integrates with cloud computing, and how outsourcing and cloud computing are used by CRAs and incorporated in their organisational strategies and structures. The Project Specification was intended to shed light on how outsourcing and cloud computing are used within the global network of CRA affiliates and non-CRA affiliates, as well as unaffiliated entities of the CRAs, to issue traditional credit ratings and other CRA products.

---

[14] For the purposes of its fact-finding exercise, C6 considered the term "outsourcing" to include any onshoring, offshoring, nearshoring and right-shoring, that takes place, where applicable, within the entire network of rating affiliates and non-rating affiliates, as well as unaffiliated entities of a credit rating agency or other joint ventures and strategic alliances with other credit rating agencies. The objective of such outsourcing is to issue credit ratings or other credit rating agencies' products and includes, for example, the shared use by entities within such network of analytical, legal, compliance, internal controls, IT, and any other support functions.

This definition was informed by the following sources: The Joint Forum, Basel Committee on Banking Supervision, ***Outsourcing in Financial Services***, (Feb. 2005), available at:

https://www.bis.org/publ/joint12.pdf;

IOSCO Technical Committee, ***Principles on Outsourcing of Financial Services for Market Intermediaries***, (Feb. 2005), available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf;

IOSCO Technical Committee, Principles on Outsourcing by Markets, (July 2009), available at:

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD299.pdf.

The Project Specification also was intended to evaluate whether outsourcing and cloud computing align with the following IOSCO documents: (a) the 2005 IOSCO Intermediaries Outsourcing Principles,[15] as appropriate; (b) the Principles Regarding the Activities of CRAs ("IOSCO CRA Principles");[16] and (c) IOSCO's Code of Conduct Fundamentals for CRAs ("IOSCO CRA Code"),[17] or whether a specific set of principles on outsourcing should be considered for CRAs, and/or whether any of the IOSCO principles or the IOSCO CRA Code should be clarified to address outsourcing and cloud computing. As part of its process, C6 also evaluated IOSCO's Principles on Outsourcing by Markets ("2009 IOSCO Market Outsourcing Principles").[18]

During the course of 2017, C6 distributed a survey to 46 CRAs on outsourcing and cloud computing and received 23 responses. C6 met with academics, legal experts, and leading cloud service providers to discuss: the risks associated with cloud computing and outsourcing; how these risks are addressed; and how responsibility for risk mitigation is apportioned among multiple parties. C6 also discussed with academics, legal experts, and leading cloud service providers how outsourcing has evolved over the last ten years and how cloud computing is affecting the financial services industry. Several CRAs provided C6 with presentations on their approaches to outsourcing and cloud computing, including identifying whether they outsourced portions of the rating process.

Section 3 – Outsourcing among CRAs

Functions currently outsourced by CRAs

Of the 23 CRAs that responded to the survey, six stated that they do not use outsourcing at all. Eight other CRAs responded that they do not outsource any part of the credit rating process. Outsourcing for these eight CRAs is limited to administrative and ancillary services. Among the remaining survey respondents that do use outsourcing to some degree, functions are outsourced to global credit rating affiliates, non-credit rating affiliates, and unaffiliated entities.

While C6 used a broad definition of outsourcing that reflected the expanded use beyond traditional outsourcing relationships and included functions performed by global credit rating affiliates, certain CRAs stated that they did not consider this type of arrangement to be outsourcing. For example, one CRA stated that, while certain aspects of the credit rating process may be performed by another global credit rating affiliate, the firm operates as a cohesive global network and, therefore, it would not classify those activities as being outsourced. C6 evaluated the responses of the CRAs based on their conduct rather than based on the CRAs' own internal classifications.

---

[15] See IOSCO Technical Committee, *Principles on Outsourcing of Financial Services for Market Intermediaries*, (Feb. 2005), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf.

[16] See IOSCO Technical Committee, *Statement of Principles Regarding the Activities of Credit Rating Agencies*, (Sept. 2003), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD151.pdf.

[17] See IOSCO Technical Committee, *Code of Conduct Fundamentals for Credit Rating Agencies*, (rev. March 2015), available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD482.pdf.

[18] See IOSCO Technical Committee, *Principles on Outsourcing by Markets*, (July 2009), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD299.pdf.

Several CRAs commented that, in deciding whether to outsource, a threshold concern is that the proposed outsourcing relationship should not materially impact the quality of ratings, quality of internal controls, and compliance with codes, policies, and regulatory requirements.

Functions outsourced to *affiliated* entities included, but were not limited to:

- Analytical support (from credit rating affiliates);
- Updating and validating financial data;
- Updating portions of the ratings analysis;
- Contributing to preliminary research and drafting commentaries;
- Technology support services;
- Data and analytics support services for structured finance;
- Customised macroeconomic reports;
- Support in the dissemination of ratings data; and
- Various other shared services (including finance, business development, legal, compliance, audit, human resources, and IT).

Functions outsourced to *unaffiliated* entities included, but were not limited to:

- Data transcription services which feed data into a CRA's internal financial performance database;
- Data and IT support;
- Data management and business consulting services;
- Delivery of ratings announcements to media outlets;
- Software to support commercial activities;
- Cloud computing services;
- Next generation cloud-based services (including research and development on artificial intelligence, machine learning, and database technologies);
- Testing and migration of applications and systems;
- Data centre hosting;
- Helpdesk services;
- Disaster recovery services; and
- Translation services.

Based on the survey responses, CRAs use a variety of mechanisms and processes in assessing whether to outsource specific functions or activities. Certain CRAs stated that the determination is made on a case-by-case basis and depends on the nature of the outsourced function. One CRA stated that the decision is made by a combination of the department requesting the service and other internal functions that are necessary to evaluate the request and the service provider. According to the responses, the other internal functions involved in this decision-making process typically include finance; IT; compliance; risk management; legal; internal audit; and senior management (including the CEO, president, and board of directors). C6 observed, based on the survey responses, that larger, more complex CRAs were

more likely to have more formalised governance processes than smaller CRAs when making outsourcing decisions. An example is the use of risk-related score cards.

A larger CRA stated that it identifies opportunities for outsourcing by reviewing activities that have certain characteristics. These characteristics focus on whether each activity:

- Can be optimised in terms of quality, efficiency, or timeliness;
- Involves repeatable tasks, with standardised processes;
- Has a high degree of frequency, requiring low level commodity skill sets;
- Is transactional in nature;
- May require scale change up or down; and
- Is not a core competency.

Other CRAs stated substantially similar factors in determining whether to outsource an activity.

Approach to selecting a service provider

Based on the survey responses, some CRAs have defined criteria for selecting a third-party service provider. These include a requirement not to materially impair the CRA's ability to meet its regulatory obligations (as noted above) and conducting a risk assessment of the provider. CRAs also may consider the following about a third-party service provider:

- Compatibility with their business;
- Resources;
- Geographic coverage;
- Cost;
- Quality;
- Breadth of capabilities;
- Governance;
- Professional references;
- Security profile and track record;
- Length of the engagement;
- Communication capabilities; and
- Responsiveness to employees, management, and board of directors.

Due diligence prior to engagement

Based on the survey responses, the level of due diligence performed on potential third-party service providers varies by the CRAs' size and the depth of their processes. For example, larger CRAs have a comparatively more developed due diligence process compared to smaller CRAs.

Based on the survey responses, the larger CRAs have multifaceted risk frameworks that determine the level of due diligence to conduct and the provider to select. In one instance, the CRA assesses the following risks: data loss; technology; reputational; operational; exit risk;

counterparty risk; country/geopolitical; contractual; access risk; and concentration risk. In high- risk cases, the CRA screens and scores potential providers based on their financial stability, quality, reputation, scalability, ability to meet applicable regulatory and legal requirements, and technical expertise. In another case, the CRA considers the potential impact on its earnings due to outsourcing specific activities, selecting specific providers, the sensitivity of the information to be transmitted, the provider's own policies and procedures, and business continuity planning.

Smaller CRAs generally stated that they decide whether to perform due diligence on a case-by-case basis. The outcome appears to be the result of an informal risk assessment that may include a consideration of the type and scope of the outsourced function, its materiality, and the stability of the service provider.

Finally, certain smaller CRAs stated that they do not perform due diligence prior to engaging a service provider. The reasons given were their sporadic use of outsourcing, contracting with well-known providers, and/or contracting with affiliates. As noted above, certain CRAs did not consider functions performed by credit rating affiliates as outsourcing. C6 used a broad definition of outsourcing and evaluated the survey responses irrespective of the CRAs' characterisations of their outsourcing profile.

CRAs responded that they use the same risk assessment and due diligence procedures for regulated and unregulated service providers.

Risk mitigation

Survey respondents identified risks associated with outsourcing. These risks include a lack of timeliness in delivering services, disclosure of confidential information, the business and financial strength of the provider, quality performance standards, legal liability, data loss, ratings quality, fraud, geopolitical, and exit risk.

The CRAs reported numerous methods for risk mitigation. Such methods include contracting with reputable third-party providers with high market shares, identifying alternative providers in the event of an interruption of service, and ongoing monitoring of quality. Other methods include the CRAs' right to audit a provider on-site and audit its insurance contracts. Many CRAs said they concentrate their mitigation efforts on high-risk outsourced functions. Based on the survey responses, high-risk functions can have an impact on the integrity of credit ratings or involve the transfer of confidential information.

Some CRAs have policies in place to manage potential conflicts of interest between the third-party service provider and the CRA or its employees. These conflicts are addressed in contractual arrangements and policies covering employee ethics, provider conduct, and procurement practices.

Based on the survey responses, CRAs that allow third-party providers to subcontract their obligations generally use contractual clauses that hold providers responsible for their subcontractors' work and require providers to oversee their work and ensure that they adhere to the same standards required of the provider.

Based on the survey responses, some CRAs take steps to address scenarios where the service provider can no longer effectively provide the service. These include engaging multiple providers, enhanced monitoring of high-risk vendors, and maintaining documentation to facilitate transfers between service providers.

Ongoing management of outsourced functions

CRA survey respondents reported a variety of internal functions dedicated to the ongoing management of outsourcing engagements. For example, dedicated "outsourcing departments" at two larger CRAs maintain ongoing oversight of the engagements. Other respondents noted that the internal oversight functions could include a variety of departments, such as IT, the department that requested the outsourcing arrangement, compliance, legal, internal audit, operations, planning, and the involvement of senior management (including the CEO, president, and board of directors).

Some CRA survey respondents require third-party service providers to comply with the CRA's own internal policies in certain cases. The most common circumstance is when a service provider is entrusted with confidential information. In this case, the CRA's confidentiality and information security policies would apply and would be enforced through contractual undertakings.

Some CRAs stated that they provide no training to third-party service providers. In cases where training was provided, it was focused on data transcription policies, confidentiality, compliance, and software development methodologies.

A larger CRA commented that ongoing oversight of outsourced activities is more challenging when third-party service providers are geographically dispersed. The CRA minimises this risk with video and electronic communications, coupled with service and performance metrics. The CRA will also conduct site visits for critical providers to build relationships and increase transparency.

Contingency and exit planning

Several CRAs stated that they periodically assess several factors to determine which functions might be brought back "in-house" in the event of certain contingencies. These factors include the quality of service, cost, results of audits (by compliance and internal audit), adherence to contract obligations, and the CRA's ability to internally perform the function.

One larger CRA stated that its contracts include a clause allowing the CRA to terminate the relationship at will or for cause. There are also contractual clauses requiring the third-party service provider to provide transition services to ensure a smooth changeover between providers.

One smaller CRA stated that it may consult with a limited set of potential providers to address economic and technical considerations related to switching providers. One larger CRA stated that it periodically evaluates business conditions and changes in technology to assess the status of the outsourced function, including whether to terminate providers and bring the function back in-house.

Some CRAs maintain contingency plans for cases where third-party service providers are unable to continue performing services. A larger CRA stated that, for certain functions such as IT, it uses multiple providers. It may use a primary provider and engage a secondary provider who can easily substitute for the primary provider in the event the provider experiences a service disruption. Where the CRA does not maintain multiple providers, it relies on monitoring to identify high risk providers.

Negotiating contract terms

CRAs stated that service contracts are typically negotiated by their legal departments with the input of the business owner of the outsourced function. Based on the survey responses, a common challenge is the asymmetrical bargaining power of large third-party service providers who rarely deviate from standard contracts. Based on the responses, certain providers in other cases do not have experience working with a regulated financial services firm. CRAs indicated that they mitigate this risk in various ways, including contract terms requiring that the provider ensure compliance with the CRAs' regulatory requirements, requiring that the provider cooperate with CRAs' reporting to regulators, and allowing regulators access to providers' books and records.

Section 4 – Cloud Computing and its Use by CRAs

Overview of cloud computing

IT outsourcing is a common practice for firms, and cloud computing solutions are increasingly becoming the preferred IT outsourcing option. The generally accepted definition of cloud computing comes from the National Institute of Standards and Technology ("NIST"). NIST is an agency of the United States Department of Commerce. NIST defines cloud computing as: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources *(*e.g.*,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, four deployment models, and three service models."[19]

The five essential characteristics are:

1. On demand self-service – A consumer can unilaterally access cloud computing capabilities as needed, automatically, without requiring human interaction with each cloud service provider.
2. Broad network access – Capabilities are available over the network and accessed through various platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. Resource pooling – The cloud provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the client generally has no control over or knowledge of the exact physical location of the resources, but may be able to specify location preferences at a high level (e.g., country, state, data centre).
4. Rapid elasticity – Capabilities can be provided elastically, in some cases automatically, to scale rapidly outward and inward commensurate with the client's computing demands.

[19] National Institute of Standards and Technology, U.S. Department of Commerce, *The NIST Definition of Cloud Computing*, (Sept. 2011), available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

5. Measured service – Cloud systems automatically control and optimise resources by leveraging a metering capability (typically on a pay-per-use or charge-per-use basis) at some level appropriate to the type of service.

The four deployment models are:

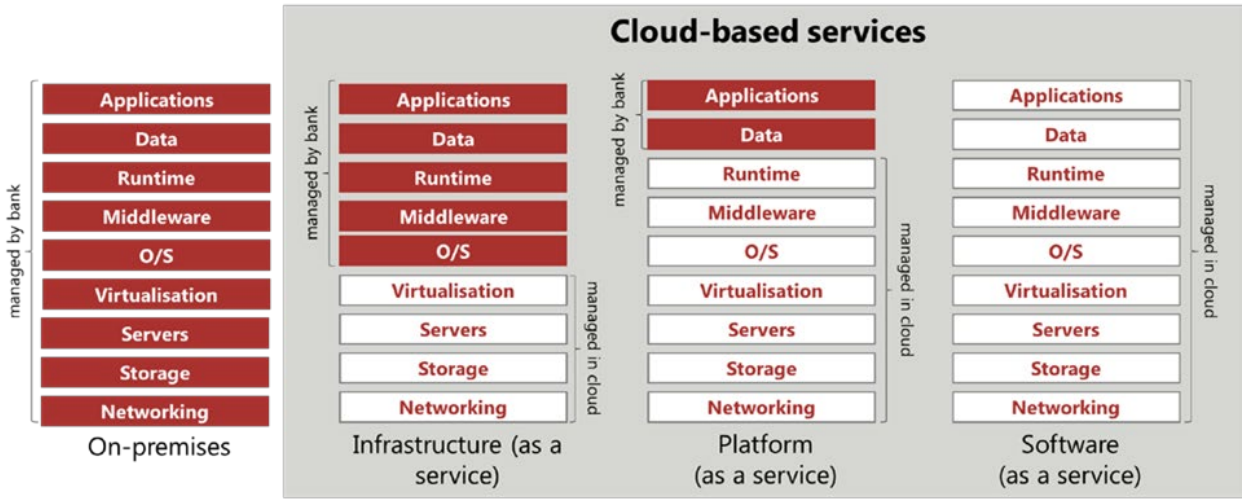
1. Private cloud – This cloud infrastructure is for exclusive use by a single organisation comprised of multiple consumers (e.g., business units). It may exist on or off the clients' premises.
2. Community cloud – This cloud infrastructure is for the exclusive use of a specific community of consumers from organisations that have shared concerns. It may exist on or off the clients' premises.
3. Public cloud – This cloud infrastructure is for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the cloud provider's premises.
4. Hybrid cloud – This cloud infrastructure is composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.

The three service models are:

1. Infrastructure as a Service ("IaaS") – A cloud provider offers clients pay-as-you-go access to storage, networks, and other fundamental computing resources in the cloud.
2. Platform as a Service ("Paas") – A cloud provider offers access to a cloud-based environment in which users can deploy consumer-created or acquired applications. The service provider supplies the underlying infrastructure.
3. Software as a Service ("Saas") – A cloud provider offers clients the use of the provider's software and applications running on a cloud infrastructure. Clients access and use the software and applications via the internet.

The distinctions in each of the service models are illustrated in the following graph from a Basel Committee publication in February 2018 on bank adoption of cloud computing.[20]

[20] Basel Committee on Banking Supervision, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors*, (Feb. 2018), available at https://www.bis.org/bcbs/publ/d431.pdf.



Benefits of cloud computing and market adoption

Prior to cloud adoption, organisations would house their data on-premises according to academics, legal experts, and the leading providers of cloud computing services. Under this traditional model, an organisation would have to invest capital by purchasing equipment and maintaining the infrastructure on-site (e.g., power resources, temperature controls, maintenance, and security). Cloud computing is a form of outsourcing as all or parts of this infrastructure are moved to a cloud provider.

Based upon C6's interactions with cloud computing experts, it appears that proponents of cloud-based infrastructures highlight several advantages:

- Improved accessibility – Services are accessible from a wide variety of devices and from any location with network access to the cloud.
- Cost efficiency – Cloud provider resources are pooled to serve multiple clients, which create economies of scale. This reduces the cost of data storage.
- Demand scalability – The cloud provides a flexible platform that can grow and shrink to match the client's needs.
- Always-on availability – Applications running on a cloud infrastructure are rarely off-line and are accessible whenever there is an internet connection.
- Improved security – A key concern of a cloud provider is to carefully monitor the cloud's security, which is more efficient than monitoring a conventional in-house system.

As of the end of 2018, the worldwide cloud infrastructure service market was dominated by a handful of market participants. The largest is Amazon Web Services ("AWS"), which accounted for approximately 32% of the worldwide market in 2018.[21] The next largest

[21] See Canalys, *Cloud Infrastructure Spend Grows 46% in Q4 2018 to Exceed US$80 Billion for Full Year*, (Feb. 2019), available at https://www.canalys.com/static/press_release/2019/pr20190204.pdf.

providers were Microsoft (16.5% of the market), Google (9.5% of the market), and Alibaba (4.2% of the market).[22] Representatives from AWS, Google, and Microsoft presented to C6.

According to the cloud providers, each of them maintains a worldwide network of data centres that house its clients' data. Data can be located anywhere within the cloud provider's network of centres. For example, as of May 2019, AWS maintains data centres in 21 distinct geographic regions.[23] Given concerns regarding data locality requirements, AWS states that it can house data at specific regions at a client's request.[24] AWS also states that it will not move or replicate a client's data outside of the designated region without a change in the client's region specification.[25]

The presenters all stated that adoption of cloud technology in the financial services sector continues to increase. One presenter commented that financial services firms are particularly interested in improving their use of analytics, where cloud technology enables firms to query large datasets. Cloud technology also enables firms to develop their use of artificial intelligence.

Current CRA adoption of cloud computing

Most survey respondents stated that they have adopted cloud technology in varying degrees and for varying purposes. CRAs have adopted three of the four deployment models listed above (private, public, and hybrid) and have used all the service models identified above (IaaS, PaaS, and SaaS).

CRAs stated that they have adopted cloud technology for the following reasons, many of which relate to the five characteristics of cloud computing described above:

- Reduced complexity;
- Higher reliability;
- Increased security;
- Elastic resource capacity;
- Geographic diversity;
- Increased agility and speed;
- Accelerated delivery;
- Cost effectiveness;
- Redundancy;
- Hardware end-of-life concerns;
- Human resourcing constraints; and

---

[22] Id.

[23] See Amazon Web Services, *AWS Global Infrastructure*, available at https://aws.amazon.com/about-aws/global-infrastructure/.

[24] Id.

[25] See Amazon Web Services, Data Privacy FAQ, available at https://aws.amazon.com/compliance/data-privacy-faq/.

- Ability to leverage cloud-based tools, including database technologies and machine learning.

Certain survey respondents maintain on-premises data centres. One CRA stated that it will continue to maintain data centres but anticipates leveraging more cloud-based services and decreasing the number of its data centres. Another CRA stated that it plans to reduce its on-premises data centre footprint and continue migrating more data to the cloud. Another CRA that uses cloud computing on a more limited basis has focused its use on client relationship management and disaster recovery.

Several CRAs stated that they will not migrate certain data to the cloud. One CRA said it will not move employee personal data and other material non-public information. Another CRA stated that it will not migrate data to the cloud when certain conditions exist, including where migration does not enable the CRA to meet regulatory requirements; where applications are targeted for retirement; and where migration would be cost prohibitive. Another CRA said it does not have any such limitations. Two other CRAs said there are no restrictions on data migration other than those imposed by data localisation requirements.

CRA engagements with cloud providers

Similar to the survey responses on outsourcing more broadly, a number of CRAs stated that they apply defined criteria when choosing a cloud provider. CRAs consider some or all of the following factors:

- Security;
- Scalability;
- Availability;
- Reputation/maturity of the provider;
- Geographical constraints;
- Compliance and legal requirements;
- Operational excellence;
- Innovation capabilities; and
- Cost.

Several CRAs give extra consideration to concentration risk. Similar to outsourcing more broadly, one CRA uses a multi-provider strategy to reduce this risk. Another CRA considers the interchangeability with other cloud providers to limit operational risk stemming from provider "lock-in", which hampers the ability to transfer data between cloud providers.

Negotiating cloud contract terms

Similar to outsourcing more broadly, certain CRAs stated that negotiating contract terms with cloud providers can be challenging due to the providers' asymmetrical bargaining power. As noted above, the cloud market is dominated by a few large firms. Several smaller CRAs, in particular, stated that they cannot negotiate contracts with larger cloud providers given their size and the amount of data to be stored versus the greater needs and bargaining power of larger

CRAs. One CRA agreed that cloud providers limit the ability to negotiate terms and conditions, but the firm has had success negotiating terms that meet their security standards.

Survey responses indicate that cloud providers have committed to providing cooperation and assistance to the CRAs' regulators and supervisors. Two CRAs commented that contracts include a regulatory right of access provision that is specifically negotiated to maintain transparency and cooperation with regulators.

One CRA found it difficult to negotiate a requirement granting regulators the right to conduct on-premises inspections of the cloud provider's facilities. Cloud providers believe that allowing multiple clients and regulators to conduct site visits and inspections creates a security risk. A cloud service provider stated that clients can gain comfort around compliance with certain standards through third-party certifications and audits. Examples of third-party certifications include the Cloud Security Alliance's Security Trust Assurance and Risk (STAR) Program[26] and the American Institute of Certified Public Accountants' System and Organization Controls (SOC) certifications.[27]

Several CRAs conduct business in jurisdictions with data localisation requirements. Those CRAs stated that they keep data backed up on physical servers located in those jurisdictions. The cloud providers that presented to C6 stated that they have responded to their regulated clients' concerns and have the ability to place clients' data in specific locations or regions.

CRA cloud policies and procedures

A number of CRA survey respondents stated that they have policies and procedures that address the life cycle of data, that is, from the moment when data is generated and enters their system to when the data is destroyed. One CRA stated that it maintains a records management policy, guidelines, and program to assist with effective record retention, maintenance, and disposition procedures that are consistent with business needs and legal and regulatory requirements. Another CRA stated that it maintains several policies that apply to the life cycle of data rather than one overarching policy. Another CRA stated that it is in the process of developing a policy that addresses the life cycle of data.

Most of the CRAs stated that they treat cloud computing as part of their broader outsourcing strategy and do not maintain separate outsourcing policies and procedures for cloud computing arrangements. One CRA stated that while it does not have separate policies and procedures for cloud-related matters, it places a greater emphasis on technology and information security reviews that include the cloud. Another CRA stated that its cloud computing strategy aligns with its outsourcing policies and that it follows the same processes when assessing cloud computing.

[26] See Cloud Security Alliance, *STAR Registry: Security on the Cloud Verified*, available at https://cloudsecurityalliance.org/star/#_overview.

[27] See American Institute of Certified Public Accounts, *SOC for Service Organizations*, available at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html.

Section 5 – Application of IOSCO Principles

The Project Specification was intended, in part, to evaluate whether outsourcing and cloud computing align with the following IOSCO documents: the 2005 IOSCO Intermediaries Outsourcing Principles, the IOSCO CRA Principles, and the IOSCO CRA Code. C6 also considered the 2009 IOSCO Market Outsourcing Principles.

C6 notes that the 2009 IOSCO Market Outsourcing Principles were intended to complement the 2005 IOSCO Intermediaries Outsourcing Principles. The principles are substantially similar but differ in certain respects. For example, the 2005 IOSCO Intermediaries Outsourcing Principles contain a principle concerning the concentration of outsourced functions.

C6 inquired, through the survey, how CRAs view their use of outsourcing and cloud computing as aligning with the 2005 IOSCO Intermediaries Outsourcing Principles, the IOSCO CRA Principles, and the IOSCO CRA Code. One CRA commented that the IOSCO CRA Principles and the IOSCO CRA Code apply to the credit rating process and are tailored for the determination of credit ratings. Policies and procedures related to outsourcing and cloud computing, therefore, may not implicate these CRA documents as these activities may not directly involve the process by which a CRA determines a credit rating. Several CRAs commented that their policies and procedures on outsourcing and cloud computing are consistent with those described in the 2005 IOSCO Intermediaries Outsourcing Principles.

The IOSCO CRA Code and IOSCO CRA Principles were designed to meet the unique nature of credit rating activities and the credit rating industry. Regulatory concerns regarding outsourcing and cloud computing are broader and span the financial services industry. As such, these topics may be better addressed in principles that apply to a broader set of market participants, including CRAs.

C6 is of the view that the 2005 Intermediaries Outsourcing Principles could apply to CRAs. C6 suggests that any communication broadening the application of these existing principles to CRAs includes language that reflects cloud computing, recent trends and market developments. Many of the 2005 IOSCO Intermediaries Outsourcing Principles are implicated in C6's fact finding process, as discussed in Chapters 3 and 4, for example, the principles concerning contracts with service providers, IT security, client confidentiality, the concentration of outsourcing functions, termination procedures, and access to books and records.

While the use of cloud computing is a form of IT outsourcing and the general principles regarding effective controls for outsourcing apply, there are important specific features of cloud computing and embedded risks that have led many firms to implement different controls to mitigate those risks and ensure compliance with regulatory requirements. In addition, cloud computing offers more standardised services for clients than traditional outsourcing, which was more tailored to clients' needs.

C6 has identified several potentially different challenges and risks posed by the increasing use of cloud computing, such as concentration exposure to cloud providers and lock-in risks, legal uncertainty for the unregulated services provided, data location and data protection rules, where applicable, the unequal negotiating power in contracts, and the challenges derived from restricting access and audit rights to premises, systems and networks which impair regulators' ability to discharge their supervisory tasks.