November 28, 2017

Agenda

Committee on Credit Rating Agencies (Committee 6)

5-6 December 2017

Rio de Janeiro, Brazil

Meeting times:	December 5, 2017 – 9.00 am to 5.45 pm December 6, 2017 – 9.00 am to 5.30 pm
Meeting Venue:	Hotel Rio Othon Palace - Av. Atlântica, 3264 - Copacabana, Rio de Janeiro - RJ, 22070-001
Social Event:	TBC

Day 1

Tuesday, December 5, 2017

1. **Opening remarks, adoption of agenda and approval of the key outcomes of the last meeting** *(15 minutes) (9.00am – 9.15am)*

2. **IOSCO General Secretariat update** *(30 minutes) (9.15am – 9.45am)*

   The General Secretariat will inform Committee members about the progress of IOSCO's work and issues of interest for the Committee's work (e.g., work in other Committees).

3. **Tour de Table: Discussion of legislative and regulatory matters in the area of CRAs** *(60 minutes) (9.45pm - 10.45pm)*

   Update by Committee members on recent legislative and regulatory changes and initiatives.

COFFEE BREAK *(10.45am – 11.00am)*

4. **Members only discussion of responses to the Survey on Outsourcing and Cloud Computing** *(90 minutes) (11.00am – 12.30pm)*

   Drafting Working Group will present on responses to the Survey on Outsourcing and Cloud Computing.

LUNCH *(12.30pm -1.30pm)*

5. **External Presentation 1 - Microsoft Azure** – *(90 minutes) (1.30pm –3.00pm)*

   Dave Dadoun, Assistant General Counsel, Robert Dring, Principal PM Manager and Alan Ross, Senior Director, Financial Services Industry will present on the Microsoft model for cloud computing, on contracting for cloud services and will address questions related to cyber security.

COFFEE BREAK *(3.00pm - 3.15pm)*

6. **Members only discussion of external presentation 1 and preparation for other presentations** *(30 minutes) (3.15pm – 3.45pm)*

7. **External Presentation 2 - Banco Central do Brasil** – *(60 minutes) (3.45pm –4.45pm)*

   Carlos André de Melo Alves, Deputy Advisor of Central Bank of Brazil - Department of Financial System Regulation, will present the Brazilian central bank approach to cloud computing.

8. **Members only discussion of external presentation 2 and preparation for other presentations** *(30 minutes) (4.45pm – 5.15pm)*

9. **Members only discussion on IOSCO Board decision about Committee 6** *(30 minutes) (5.15pm – 5.45pm)*

Conclusion of first day (5.45 pm)

Day 2

Wednesday, December 6, 2017

10. **External Presentation 3 - Moody's Presentation** *(60 minutes) (9.00am – 10.00am)*

    Blair Worrall, Neil Acres, Derek Vadala will present on Moody's Investors Service perspective on outsourcing and cloud computing.

11. **Members only discussion of external presentation 3** *(30 minutes) (10.00am – 10.30am)*

COFFEE BREAK *(10.30am – 10.45am)*

12. **External presentation 4 – S&P Presentation** *(60 minutes) (10.45am – 11.45pm)*

    Sherif Khalifa, Global Head – In Business Controls (Operating Office), Kelly Shen, Executive Managing Director and Chief Operating Officer, Laura Deaner, Vice President – Chief Information Security Officer, Christian Mittelberg, Vice President – Global Head of Risk Management and Prasanna Ramaswamy, Vice President – Enterprise Architecture will present on S&P Global Ratings perspective on outsourcing and cloud computing.

13. **Members only discussion of external presentation 4** *(30 minutes) (11.45pm – 12.15pm)*

LUNCH *(12.15pm - 1.15pm)*

14. **External presentation 5 - Fitch presentation** *(60 minutes) (1.15pm - 2.15pm)*

    Jeff Horvath, Global Chief Compliance Officer and Rob Harpel, Chief Technology Officer will present on Fitch Ratings perspective on outsourcing and cloud computing.

15. **Members only discussion of external presentation 5** *(30 minutes) (2.15pm - 2.45pm)*

COFFEE BREAK *(2.45pm - 3.00pm)*

16. **External presentation 6 – Banco Itau** *(60 minutes) (3.00pm – 4.00pm)*

    Roberto Figueira Santos Filho, Executive IT Architect, Annette Martinelli de Mattos Pereira, Senior Special Lawyer and Bruno Henrique Barros de Moura, Head of Global Wealth Management and Services Legal Division will present on Banco Itau's experience with outsourcing and cloud computing

17. **Members only discussion of external presentation 6** *(30 minutes) (4.00pm – 4.30pm)*

18. **Members only discussion of the structure of the Consultation Report** *(45 minutes) (4.30pm – 5.15pm)*

19. **AOB & next meetings** *(15 minutes) (5.15pm – 5.30pm)*

2018:

(Committee 6 meetings for 2018 tbd)

21 & 22 February 2018:	IOSCO Board, Madrid, Spain
7-11 May 2018:	IOSCO annual meeting & conference, Budapest, Hungary
17 & 18 October 2018:	IOSCO Board, Madrid, Spain

Conclusion of second day (5.30 pm)

SPEAKERS' BIOS

Dave Dadoun is the lead lawyer for Microsoft's Financial Services Industry team and is the architect of Microsoft's regulatory strategy in the financial services industry globally. He is responsible for driving Microsoft's engagement with financial services regulators, and to help financial institutions meet their regulatory compliance needs. Working with engineering, sales and legal teams worldwide, he has helped craft a unique compliance program exclusively for financial institutions to help meet the appropriate level of supervision needed for financial institutions. He also has developed unique commercial terms to meet regulatory requirements for financial services customers and provide examination rights to regulators. Prior to his current role, he served as general counsel for Microsoft's Small Midmarket Solutions and Partner organization, and from 2001-2010 served as competition counsel, working on the U.S. Department of Justice antitrust case and follow-on European Commission case. During that time, he was appointed to serve as the compliance officer under a federally mandated consent decree from 2002-2006, and then led antitrust counseling and defended the company in numerous competition investigations in Europe, residing in Paris, France from 2006-2010.

Carlos André de Melo Alves is a Deputy Advisor of Central Bank of Brazil - Department of Financial System Regulation. He joined Central Bank in 1998 and has held several positions within the entity working in an array of issues including information technology, payment systems and financial regulation. He also is a teacher at Business Administration Department – University of Brasilia (UnB). He holds degree in Data Processing from State University Julio de Mesquita Filho – São Paulo (UNESP - SP), Master in Business Administration from Federal University of Paraná (UFPR) and PhD in Business Administration from University of São Paulo (USP).

Robert Dring owns Microsoft's global programs that enable financial services customers to meet their regulatory obligations for risk assessment and audit. Robert meets regularly with financial services regulators to enable their understanding of the Microsoft Cloud and resolve their concerns with product features and contracts. Robert has staff on three continents who work closely with the largest banks and insurance companies in the world and support them in realizing the benefits of the cloud. As part of the Office 365 engineering organization, Robert's team provides the deepest technical knowledge of the features and security of Office 365, helps Microsoft's field organization respond to customer questions, manages our Financial Services Compliance Program which provides customer audit rights for all Microsoft's Online Services, and ensures customer feedback is included in product development planning.

Robert joined what is now the Office 365 team eleven years ago when Microsoft had one customer of its original enterprise cloud service. His team is responsible for championing many improvements in our product features, documentation, and contracts based on direct feedback from customers worldwide. Robert has been personally involved in negotiating key contract issues with our largest customers including American Airlines, A.P. Møller – Mærsk, AT&T, Bank of Nova Scotia, The Coca Cola Company, Dow Chemical, DuPont, Hyatt Hotels, KBC Bank, Novartis, Philips Electronics, Royal Mail Group, and 19 of the global systemically important financial institutions.

Robert is a 22-year Microsoft veteran, starting as a messaging consultant in New England helping customers such as Fidelity Investments deploy Microsoft Exchange. His last role before joining the Office 365 team was in Microsoft Services worldwide headquarters

managing a team of over 100 developing repeatable "QuickStart" consulting solutions that helped more than 1,000 customers deploy Microsoft products. Prior to joining Microsoft, Robert spent 10 years in IT operations at companies such as Staples, The Office Superstore in the USA, and the leading private Lloyds of London insurance broker in England. Robert was born and raised in England and now lives with his family in Foxboro, Massachusetts.

Roberto Figueira Santos Filho is an Executive IT Architect of Itaú Unibanco with focus on bigdata, advanced analytics and high performance computing. He joined Itaú Unibanco in 2006 in the data warehouse team. Today he is a member of a team working on application modernization and cloud migration. Prior to joining Itaú Unibanco he worked at Itautec Philco S.A., an industrial member of the Itausa Group, focused on banking and retail automation systems, and hardware (servers and microcomputers) manufacturer. Roberto holds a Bachelor's degree in Computer Sciences from Universidade de São Paulo (USP) and a MSc and PhD in database systems from Universidade de São Paulo (USP), with a research internship at Carnegie Mellon University (CMU).

Annette Martinelli de Mattos Pereira is a Senior Specialist Lawyer of Itaú Unibanco with focus on data protection, digital law, credit card and retail banking business. She joined Itaú Unibanco in 2004 and has held several positions within the bank working in an array of matters including social and environmental law, intellectual property, data protection, digital law and third sector law. Prior to joining Itaú Unibanco she has worked at a Brazilian law firm focusing on Contracts, Corporate Law, M&A and Litigation. She holds Bachelor's degree in Law from the Law School of the Pontifícia Universidade Católica de São Paulo (PUC-SP), an Specialization Degree in Litigation from Pontifícia Universidade Católica de São Paulo (PUC-SP) and Specialization Degree in Intellectual Property – Contracts and Litigation from Fundação Getúlio Vargas (FGV-SP).

Bruno Henrique Barros de Moura is the head of Global Wealth Management and Services Legal Division. He joined Itaú Unibanco in 2008, from Hewlett Packard Mexico, where he worked as in-house counsel in the international legal department. At Itaú, he has held several positions working mainly with Corporate and Capital Markets Law both in Brazil and abroad. He holds a LL.B in Law from the Law School of the Federal University of Pernambuco, a Certificate on Financial Management from INSPER – SP and a LL.M degree from Duke University School of Law (USA) and is admitted to practice Law in Brazil and in the New York State.

Participants List

IOSCO Committee on Credit Rating Agencies
Meeting 5 & 6 December 2017
Rio de Janeiro, Brazil

30 November 2017

Chair: Ms. Rita Bolger, SEC, United States of America

Vice-Chair: Ms. Maya Marinov-Shiffer, ISA, Israel

General Secretariat: Mr. Tim Pinkowski

Members:

Australia	ASIC	Ms. Anna Zajkowski Senior Analyst
Brazil	CVM	Mr. Daniel Walter Maeda Bernardo Head of the Institutional Investors Division
China	CSRC	*Not attending*
France	AMF	*Not attending*
Germany	BaFin	Mr. Henning Schultetus Senior Supervision Officer / Investment Recommendations – Users of Ratings and CRA Policy
Hong Kong	SFC	Ms. Irene Tsao Director
Israel	ISA	Ms. Maya Marinov-Shiffer *(Committee Vice Chair)* Head of Investments / International Affairs Department
Japan	FSA	*Not attending*
Korea	FSC/FSS	Mr. Jeongdoo Lee Head
Mexico	CNBV	*Not attending*
Ontario	OSC	Mr. Michael *(via telephone on day 1)* Senior Legal Counsel / Corporate Finance

Poland	KNF	*Not attending*
Russia	BoR	Ms. Elena Chaykovskaya Director of the Financial Markets Development Department
Spain	CNMV	Ms. Elisa Arias Palomero Senior Officer / Primary Markets Department
Chinese Taipei	FSC	Mr. Chih-Wei Li Officer
		Mr. Huang Chun Tseng Auditor
Turkey	CMB	Ms. Inci Kilickaya Senior Expert
		Mr. Özkan Tekneci Expert / Enforcement Department
UK	FCA	Mr. Jamie Black Team Leader / Policy Lead
US	SEC	Ms. Rita Bolger *(Committee Chair)* Assistant Director / Office of Credit Ratings
		Mr. Franco Destro International Counsel / Office of Credit Ratings

Observers:

European Union	ESMA	Mr. Eduardo-Javier Moral-Prieto Senior Policy Officer / Credit Rating Agencies
	European Commission	*Not attending*

IOSCO General Secretariat:

Mr. Tim Pinkowski
Policy Advisor

Guests:

Microsoft – *for item 5*

- Mr. Dave Dadoun, Assistant General Counsel
- Mr. Alan Ross, Senior Director, Financial Services Industry
- Mr. Robert Dring, Principal PM Manager

Central Bank of Brazil – *for item 7*

- Mr. Carlos Andre de Melo Alves, Deputy Advisor

Moodys – *for item 10*

- Mr. Neil Acres, Managing Director Moody's Shared Services
- Mr. Blair Worrall, Senior Vice President, Ratings Delivery and Data
- Mr. Joseph Gimigliano, Managing Director Infrastructure Services *by phone*
- Mr. Derek Vadala, Managing Director, Chief Information Security Officer *by phone*

S&P – *for item 12*

- Mr. Sherif Khalifa, Global Head – In Business Controls (Operating Office)
- Ms. Anna Rego, Associate General Counsel and Head of Legal and Regulatory Affairs for Latin America
- Ms. Allison Reid, Associate General Counsel, Legal & Regulatory Affairs
- Ms. Kelly Shen, Executive Managing Director and Chief Operating Officer *by phone*
- Ms. Laura Deaner, Vice President – Chief Information Security Officer *by phone*
- Ms. Mary McCann, Global Head of Regulatory Affairs *by phone*
- Mr. Christian Mittelberg, Vice President – Global Head of Risk Management *by phone*
- Ms. Prasanna Ramaswamy, Vice President – Enterprise Architecture *by phone*

Fitch – *for item 14*

- Mr. Jeff Horvath, Global Chief Compliance Officer
- Mr. Rob Harpel, Chief Technology Officer *by phone*

Itau – *for item 16*

- Mr. Roberto Figueira Santos Filho, Executive IT Architect
- Ms. Annette Martinelli de Mattos Pereira, Senior Special Lawyer
- Mr. Bruno Henrique Barros de Moura, Head of Global Wealth Management and Services Legal Division

Outsourcing- Process and Functions

IOSCO COMMITTEE 6

Outsourcing Process

- In certain CRAs, determination with respect to the functions and members involved in outsourcing decision making is made on a **case by case basis** depending on the nature of the outsourced functions.
- In certain CRAs a need for outsourcing is being identified and initiates the process for evaluating and choosing the third party provider.
- Then, relevant functions of the CRA get involved in the process

General

- **22** CRAs responded to the questionnaires
- **7** CRAs specifically mentioned that they **do not** outsource any part of the rating process.
- **6** CRAs specifically mentioned that they do not use outsourcing at all.
- **The large CRAs** (Moody's, S&P) that do outsource part of the rating process, described policies which detail the process of outsourcing

Functions Involved in Outsourcing Decision Making- an Aggregated List

- Relevant department regarding the functions to be outsourced
- Planning Department
- Finance
- IT
- Compliance
- Credit Risk
- Risk Management
- Legal
- Internal Audit
- Top management of the CRA
- CEO
- President
- BOD

Outsourcing Process–Large CRAs

- **S&P and Moody's** have very detailed and structured policies and processes for outsourcing.
- The process involves the participation of many functions (**S&P**– also from the parent company level)
- **Moody's**– there is a difference in the outsourcing process between "all outsourced functions" and "important operational functions" (IOF).

Moody's IOF

- Moody's IOF– any activity for which a defect or failure in its performance would materially impair the soundness or continuity of credit rating activities or a CRA's ability to comply with legal or regulatory requirements relating to its credit rating activities.

Factors for Determining Analytical Function

- **13** CRAs specifically mentioned that they **do not** outsource any part of the rating process/do not outsource at all.
- 1 small CRA stated that analytical function is anything that demands or leads to a **critical judgment of rating related information**
- 1 small CRA stated that analytical factors are activities that may have **an impact on the rating process** and on the **methodology**.
- 1 small CRA stated that an analytical function is comprised by employees who participate in determining, approving and monitoring **credit ratings** or for developing reviewing and approving **methodologies**.

Factors for Determining Analytical Function

- 1 small CRA stated that analytical functions involve the **application of the methodology** to the inputs required by the methodology to produce credit ratings.

- 1 large CRA (S&P) stated that it uses a defined term to describe the analytical function: "Credit Rating Activities" are an activity engaged in by S&P that leads to or directly supports the **issuance or surveillance of a Credit Rating**.

Factors for Outsourcing

- Availability of skillset needed
- Quality, efficiency, timeliness
- Costs
- Ability to meet regulatory requirements
- Repeatable tasks with standardized processes
- Activities that require scale changes up/down
- Not a core competency
- The outsourcing **will not materially impair** the quality of ratings, quality of internal controls, compliance with code, policies and regulatory commitments.
- Best interest of the CRA

Due Diligence Process

- Explanations of CRAs for **not** performing DD:
  - **Sporadic** use of outsourcing
  - Contracting with **large well known** providers
  - Contracting with partners **within the group**
- 1 small CRA stated that need of more or less profound DD depends on the **type** and **scope** of the outsourced function, its **materiality** for the business continuity of the company, and **availability** of other providers that could quickly replace the current provider if needed.
- 1small CRA stated that decision on DD is done on a **case by case basis.**

Due Diligence Process

- 1 small CRA stated that the Level of DD depends on factors such as: **importance** or **uniqueness** of service, **location** of service provider, **stability, type of information** provider may handle (**confidential, sensitive**).
- If this CRA outsources an **important function** to a lesser known third party, a more comprehensive financial review will be performed (audited financial statements, checking third party sources- credit services)
- Global Technology Department conducts a review of providers that receive **sensitive information** or provide third party data and/or IT services that integrate with CRA's network or internal systems to gain comfort the provider's security measures meet industry and CRAs standards.

Due Diligence Process

- DD process might consist of the following checks:
  - Business stability and organization of provider
  - Market research to assess available solutions
  - Reputation (technical and financial)
  - Financial review (banking and tax information)
  - Qualifications
  - Referrals
  - Anti-social force check
  - Information security standard
  - Technical quality standard
  - Past performance
  - Country risks
  - ISO 27001 Information Security Policy on Outsourcing

Due Diligence Process

- 1 large CRA (Moody's) stated that a risk assessment process is conducted for IOF in accordance with a risk tier allocated to it.
- 1 large CRA (S&P) stated that it adopted a **Vendor Governance Policy** that establishes a **vendor risk framework.**

Functions responsible for DD- an Aggregated List-Small CRAs

Functions responsible for DD process might include the following:

- Financial
- Corporate Management
- Planning
- CEO
- Compliance
- Function using the SERVICES
- Technology
- Legal
- BOD
- Independent audit company (for the service of the CRA audit check on an annual basis)

Designated Outsourcing Department- Large CRAs

- Only **2 CRAs** have a designated outsourcing department.
- These are the large CRAs
- **S&P** specifically stated that it has a **Vendor Management Office** staffed with personnel specifically dedicated to that department.
- **Moody's** stated that its **Procurement and Sourcing Group** leads the sourcing, negotiation and collecting management approval process. **Information Risk and Security Group** is also active in the outsourcing process. **MIS Outsourcing Group** administers the monitoring of outsourced IOFs.

Identification of Potential Risks

- Risk assessment
- Several CRAs (small) stated that they do not perform risk assessment (small portion of non-core business is outsourced) or perform risk assessment if outsourced services are critical for the company.

Typical Risks

- Experience
- Lack of timeliness in delivery of service
- Disclosure of confidential information and information security Conflicts of interests
- Business stability
- Financial
- Anti-social force check
- Quality standard, efficiency, quality maintenance and past performance
- Reputational risks
- Operational, regulatory and legal risks
- Data loss
- Technology/Cyber
- Rating quality
- Fraud
- Country
- Concentration
- Exit

Risk Mitigation

- Contracting with previous providers, providers with high market share, highly reputed providers
- Mapping/Contracting alternative (IT) providers (to switch to if the prime vendor discontinues its services)
- Contingency plan
- Ongoing monitoring and oversight
- Assessment of treatment of confidential information (annual plan)

Risk Mitigation

- Having internal back-up solutions
- Conducting crucial functions internally
- NDAs
- Strict SLAs with penalties
- Including appropriate obligations and protections in contracts
- Rights to review and audit, on-site
- Reporting obligations
- Insurance

Most CRAs that responded to this question stated they treat outsourced functions potentially exposed to higher risks differently than those potentially exposed to lower risks

Unacceptable Risks

- Most CRAs did not respond to the question whether they encountered unacceptable risks.
- A few CRAs stated that they did not encountered such risks.
- 1 small CRA stated that unacceptable risks discovered during DD period were resolved through negotiation of protective contractual provisions, or by terminating negotiations and finding an alternate service provider.

Unacceptable Risks

- **1 large CRA (S&P)** stated that its parent company established a Vendor Governance Committee ("VGC") to provide guidance, oversight, and escalation for its Vendor Governance Policy and program.
- Each division of the parent company is represented on the VGC.
- The VGC meets monthly and on an ad hoc basis to review vendors that represent a material risk to the parent company and its division(s).
- Where risks are found to be unacceptable, a decision will be made **not to enter** into an engagement with the subject vendor.

Risks for Non-Regulated Providers

Examples for addressing these type of risks:

- Information security related risks- addressed by checking provider's certification
- Choosing highly reputed providers
- Contractual provisions
- Active global certifications
- Applying same risk assessment processes as for regulated providers

Functions Involved in Overseeing Outsourced Functions

- IT
- Relevant department
- CEO
- BOD
- President
- Planning department
- Compliance
- Operations
- Risk management
- Internal audit
- Legal
- For large CRAs- Outsourcing Group

Training of Third Party Staff

- Several CRAs stated that **no training** is provided to staff of providers
- Several CRAs stated that training is provided with respect to **specific services/areas**:
  - Data transcription
  - Confidentiality
  - Independence
  - Compliance
  - Software development methodologies
- 1 small CRA stated that levels of training is **dependent on type of provider**
- 1 small CRA stated that no training was required as its **relevant staff was transferred** to the provider's employment (IBM)

Process for Outsourced Functions Bring Back/Provider Change

- Several CRAs stated that they continuously/ periodically asses factors such as:
  - **Satisfaction** from service **quality**
  - **Cost**
  - **Problems** with provider
  - **Results of audits** (by compliance and internal audit)
  - **Performance**
  - **Adherence to obligations** under agreement
  - **Type** of services and CRA's ability to perform activities internally
  - **Risk mitigation**
  - **Standing of provider**

Process for Outsourced Functions Bring Back/Provider Change

- Several CRAs stated that their outsourcing contracts include **termination and exit** provisions.
- 1 small CRA stated that it occasionally makes market consultations, to a restrict set of potential suppliers, to address the economic and technical sense of changing to a new supplier.
- 1large CRA stated that it **periodically evaluates business conditions** and changes in **technology** to asses if it would be more efficient and/or of higher quality to bring services in-house.

Confidential

IOSCO Committee 6 Survey on Outsourcing and Cloud Computing

Overview of Responses on Third Party Service Providers

Michael Bennett, Senior Legal Counsel
Ontario Securities Commission

December 5, 2017

Road map

This presentation provides:
- high level overview of responses on third party service providers
- review of sample of responses (S&P, Moody's, Fitch, DBRS)

Question 4A

What criteria does your organization apply in selecting third party service providers?

Responses to Question 4A

Overview

A number of CRAs apply defined criteria when selecting a third party service provider.

S&P

Key factors in deciding whether to outsource any activity: outsourcing must not materially impair:
- quality of credit ratings or credit rating activities
- quality of internal controls
- compliance with code of conduct and policies
- compliance with regulatory commitments.

S&P considers risks presented when selecting third party service providers (e.g., materiality, engagement risk assessment and vendor risk assessment).

Question 4A

S&P evaluates marketplace to determine a complete vendor landscape using non-price parameters:
- total cost of ownership
- assurance of supply including resources and geographic coverage of vendor
- core competence of vendor
- innovation/technical profile of vendor
- communication capabilities and responsiveness
- professional references.

Moody's

Conducts sourcing and risk assessment processes.
- Considers suitability of particular service for Moody's, as well as other criteria, including quality, pricing, delivery, service objectives, integration issues, technical expertise, financial stability, organization and management, reputation, computer systems and infrastructure, scalability, communications facilities, insurance coverage, information security measures, ability to meet Moody's regulatory/legal requirements, location of service provider.

Question 4A

Fitch
Key elements in outsourcing decision include:
- service quality
- data/IP ownership
- ability to enhance credit analysis and research
- compatibility with IT systems and network security
- efficiency gains
- compliance with law/regulations
- cost
- conformance to market practices
- business line dependence

DBRS
Criteria varies by outsourced service.
- DBRS evaluates third parties based on its due diligence, as well as criteria such as comfort with service provider's reputation, expertise and experience, management quality, data security capabilities and cost of services.

Question 4B

Does the location of the third party service provider play a role in the selection process, for example, time zone, local laws, geopolitical factors and risk concentration?

Responses to Question 4B
Overview
For some CRAs, location of third party service provider plays a role in selection process.

S&P
Location of third party provider is not by itself dispositive, due to range of factors assessed as part of selection process.
- However, country and concentration risk factor into assessment process.

Moody's
Location of third party service provider is a factor in assessment process.

Question 4B

Fitch
Location is a consideration (e.g., same working hours and language).

DBRS
DBRS considers risks attributable to location, such as geopolitical risk.
- Time zone may be relevant if it's necessary to interact during DBRS business hours or if turning services overnight is desired.

Question 6

What due diligence and ongoing monitoring does your organization conduct on subcontractors of functions or activities to ensure that your organization has effective supervision and oversight of all third party service providers along the supply chain?

Responses to Question 6
Overview
Some CRAs address subcontracting in their standard form agreements for service providers and monitor activities by subcontractors.

S&P
S&P's standard form agreement for service providers contains a provision for subcontractors, which holds vendor responsible for their performance and adherence to policies identified in agreement.
- Ongoing monitoring assesses vendor's performance, which includes any activities by subcontractors.

Question 6

Moody's
Moody's assigns a risk tier to outsourcing project, which determines whether staff should conduct a risk assessment of vendor.
- Risk assessment of vendor includes questions on whether vendor would engage subcontractors to perform services for Moody's and whether vendor has adopted a third party management program.
- Outsourced agreements contain key features to allow Moody's to retain appropriate level of control over outsourced services (including subcontractors).

Fitch
Does not generally permit subcontracting.
- Exception is data management, where subcontractors are managed and held to service level agreements.

Question 6

DBRS
DBRS typically engages with recognized and reputable service providers.
- Those providers remain responsible to DBRS for services provided, including if they subcontract part of services.
- DBRS does not generally seek disclosure of use of subcontractors.

Question 9

Do your organization's internal controls, policies and procedures apply to third party service providers including, by way of example, as they relate to the protection of confidential information, personally identifiable information and material non-public information, document retention, cyber security risks, and securities trading activities of the third party service providers' staff?

Responses to Question 9
Overview
Some CRAs require third party service providers to comply with certain policies and procedures.

S&P
S&P's standard form agreement for service providers includes policies and procedures (including S&P information policy and non-employee service standards) with which vendors are requirement to comply.
- S&P's vendor code of conduct outlines expectations regarding handling of data, security and confidentiality.

Question 9

Moody's
Moody's imposes necessary obligations on third party service providers through contracts.

Fitch
Material third party service providers must enter into a standard form agreement, which requires provider to comply with certain policies and procedures (e.g., security, data protection, confidentiality).

DBRS
DBRS does not currently provided any outsourced service provider with confidential information or access to internal systems.
- Therefore, DBRS does not subject service providers to policies or procedures on those matters.

Question 10

How does your organization address conflicts of interest that may arise with respect to third party service providers? Describe the conflicts of interests that may arise.

Responses to Question 10
Overview
Some CRAs have mechanisms to address potential conflicts of interest that may arise in relation to third party service providers.

S&P
S&P's vendor governance policy, vendor code of conduct and employee code of business ethics (COBE) provide guidance on identification, prevention, reporting and handling of conflicts of interest.

COBE provides that a conflict of interest can arise whenever an activity:
- is opposed to best interests of S&P
- creates appearance of impropriety or misconduct
- creates divided loyalty between an employee and S&P.

Question 10

Moody's
Outsourced arrangements with third party services providers are documented in written agreement, including provisions on confidential information.
- By restricting use of confidential information, Moody's seeks to retain appropriate level of control over outsourced services and minimize likelihood that conflicts of interest will arise (e.g., prevent third party service provider from using information from Moody's to obtain an undue advantage).

Fitch
In Fitch's experience, scope for conflicts of interest in relation to third party service providers is limited.

DBRS
Potential conflicts would be identified during procurement process and mitigation plan put in place at that time.
- Potential conflicts could include DBRS employee (who is involved in selection of provider) having an interest in provider that could potentially conflict with DBRS' interest.

Question 12

What contingency plans does your organization have in place with respect to bankruptcy, or other scenarios that might put the third party service provider out of business or lead to financial or legal difficulty?

Responses to Question 12
Overview
Some CRAs have contingency plans in relation to third party service providers not being able to provide the outsourced service.

S&P
Vendors identified as having a high inherent risk rating are subject to increased monitoring.
- For certain outsourced functions such as IT, multiple vendors are maintained across more common skill sets.
- S&P maintains documentation about key processes, systems and tools and therefore typically could bring on new vendors with reasonable knowledge transfer efforts.

Question 12

Moody's
If an event impacts a third party service provider's ability to deliver services, Moody's would either in-source the service or contract it out to another service provider.
- Moody's retains rights to use vendor knowledge that will make it easier to transfer the relevant work to a new vendor or bring it in-house.
- Moody's performs ongoing monitoring of outsourced work to anticipate potential issues that would impact delivery of services.

Fitch
Fitch is well positioned to handle loss (and rapid replacement) of any third party vendor.

DBRS
DBRS has mitigated risk of outsourced services provider outage by leveraging multiple parties to provide the same service.

Question 5B

What criteria does your organization apply in choosing your cloud provider, for example, cost, reputation, location, and negotiability of service agreement?

- *Do you consider concentration risk or the risk of having any of your organization's key functions/activities tied to one single cloud provider as criteria in choosing your cloud provider?*
- *How does your organization determine whether a function or activity outsourced to a cloud provider should be brought back in-house or outsourced to a different cloud provider?*

Responses to Question 5B

Overview

A number of CRAs apply defined criteria when choosing a cloud provider or deciding to bring an outsourced function back in-house.

Question 5B

S&P

Many factors that come into play when choosing a cloud provider, including:

- security, scalability, availability, application characteristics
- cloud provider's reputation/maturity
- geographical constraints/considerations
- cost of providing various services.

S&P considers concentration risk.

- In terms of reconsidering the outsourcing, S&P evaluates cloud provider's ability to meet service level agreements and S&P's effectiveness in achieving its business goals.

Question 5B

Moody's

Moody's considers (1) ability to meet security requirements, (3) ability to meet compliance and legal requirements, (3) innovation capabilities, (4) operational excellence, (5) reputation, and (6) cost.

- Moody's considers concentration risk.
- In terms of reconsidering the outsourcing, Moody's considers above factors, as well as cost of transfer and solution flexibility.

Fitch

Fitch conducted a study to determine feasibility and economic impact of moving applications to AWS.

- A number of factors were considered, including security.
- Fitch does not consider relying on AWS as its sole cloud provider to represent significant risk.

Question 5B

DBRS

Key criteria include:

- company and product reputation
- total cost (including internal integration and on-going support)
- service level agreements
- interchangeability with other competitive providers (to limit operational risk stemming from vendor lock-in).

Functions outsourced to a cloud provider would be brought back in-house or transitioned to a different provider based on the same criteria assessed when adopting the original provider.