

# The Key to Success in Choosing a Risk Analytics Cloud Solution

September 8, 2020

# Agenda

1. Introduction to the benefits of SaaS over On-premise
2. Why Cloud adoption is rising in our industry
3. What matters most to customers when evaluating a cloud-based solution?
4. Data protection and Security in SaaS model
5. Common Mistakes and Misconceptions
6. A few guidelines for evaluating a SaaS Vendor

1

Introduction to the benefits  
of SaaS over On-premise

# Benefits of SaaS

## Quality of service

Fast onboarding and environment availability accelerating project kick-off.



Access to affordable compute capacity on-demand



Always up to date on latest version allowing to be current on latest regulations.



Experimenting new features, new regulations in a sandbox environment with no impact on production



High Standard SLA (performance, availability, business continuity) without the high cost.



## Cost of service



No upfront technology investment



No maintenance cost (no team, no monitoring, no redundant system)



No upgrade project and it's associated risk



The vendor can optimized & standardize operation of its software like no other, reducing significantly the cost therefore the price



Deployed & operated in lower cost, efficient Public Cloud infrastructure

2

Why Cloud adoption is  
rising in our industry

# JPMC Exemplifies Cloud Adoption



We were a little slow in adopting the cloud, for which I am partially responsible...we are now full speed ahead.



JPMC Annual Letter to Shareholders

April 2019

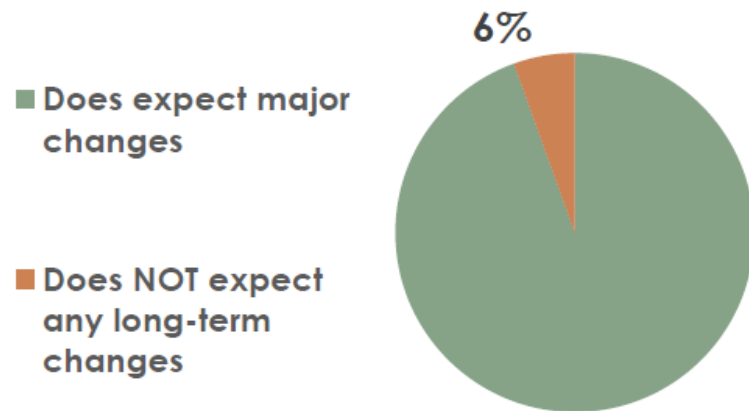
“Cloud give us...elasticity of computing power exponentially beyond our own capacity...

“Cloud...increases developers’ effectiveness by multiples...as well as increasing the speed of delivering new capabilities to our customers and clients

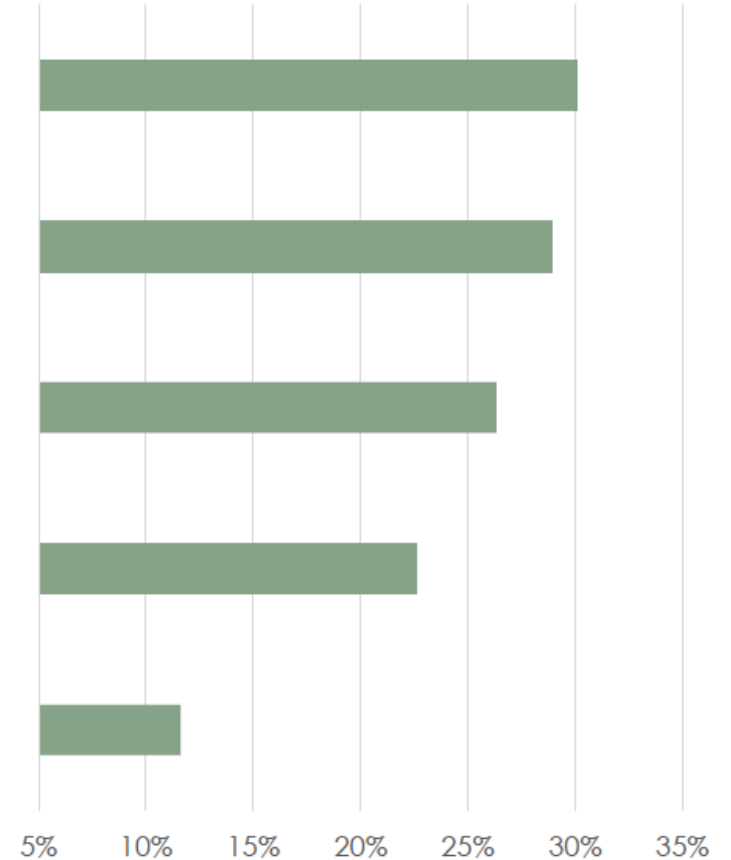
“The cloud has matured to the point where it can meet the high expectations that are set by large enterprises that have fairly intense demands around security, audit procedures, access to systems, cyber security and business resiliency.”

# Cloud Tops List of Planned Changes to Long-Term IT strategy

How do you think that your organization's **long-term IT strategy** will be affected by the COVID-19 crisis? [Choose all that apply]

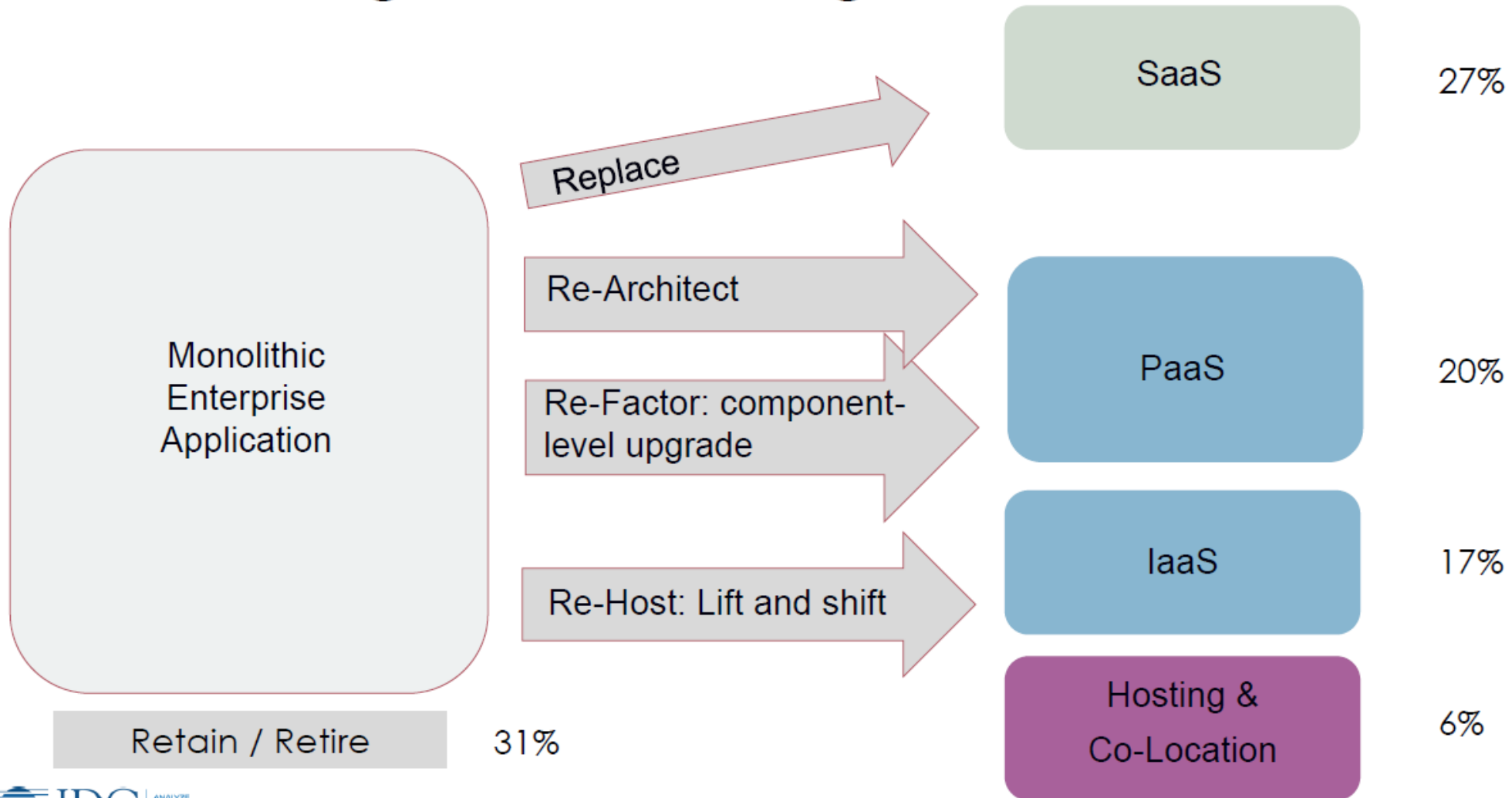


- More aggressive cloud move
- More IT spending towards remote working (inc. Mobile devices and apps)
- More investment in risk management (DR, security)
- More investment in automation and real time insights
- More outsourcing



Source: IDC European IT Buyer Sentiment Survey — Wave 3, 20-27 April 2020 WEIGHTED – IT respondents only (N = 218) –Grouped and averaged answers

# Cloud Migration Strategies



Source: IDC's Covid-19 Impact Survey, Wave 5, May 25, Europe N=730 © IDC

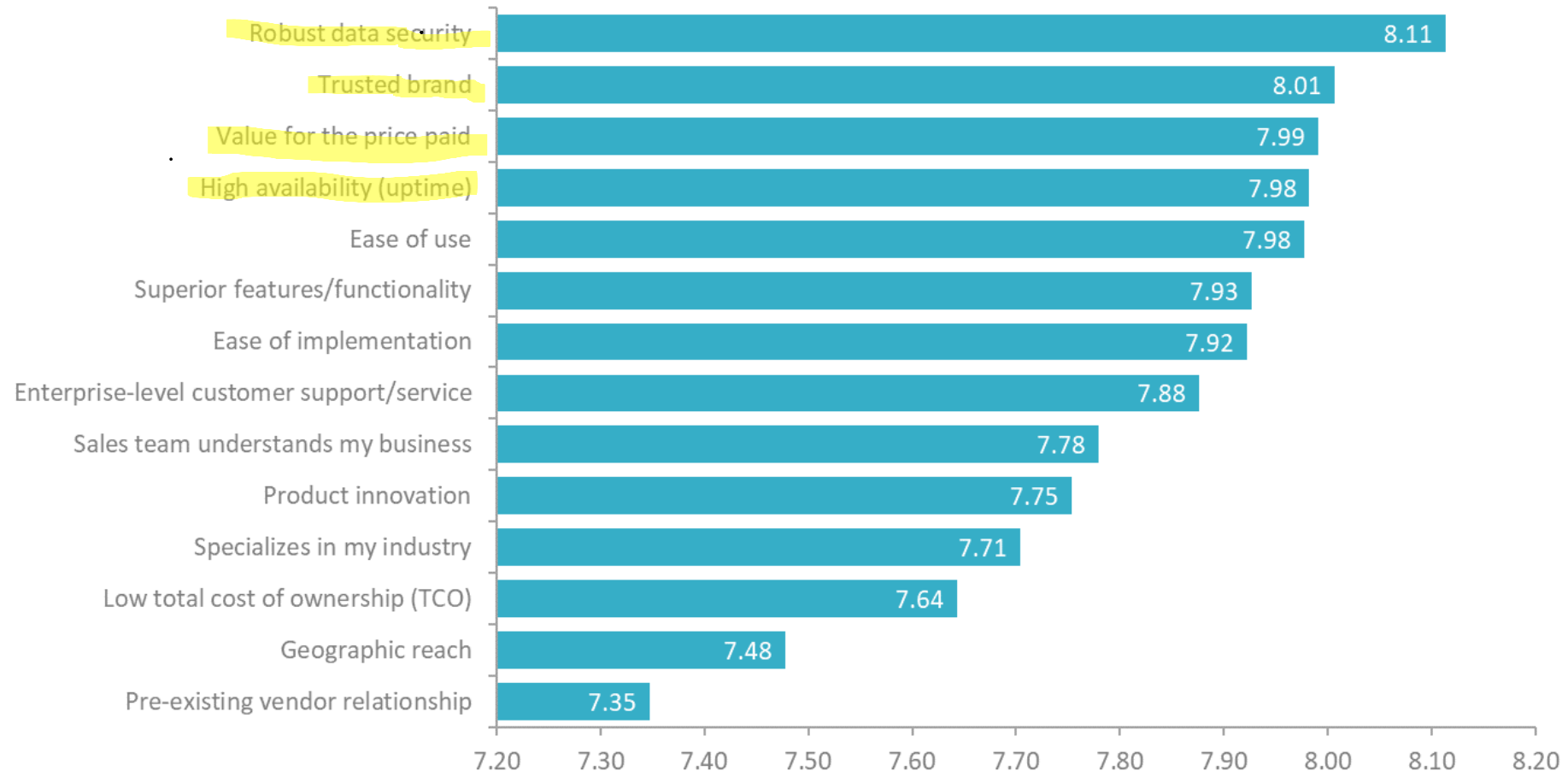


3

What matters most to customers when evaluating a cloud based solution?

# Importance of SaaS Provider Attributes

Q11. Rate how important the following attributes are when you evaluate a SaaS provider? Please rate on a scale from 0-10 where 0 is 'Not at all important' and 10 is 'Extremely important'.



# 4

## Data protection and Security in SaaS model

# Data Protection and Security in a SaaS model

Achieved jointly by articulating a transparent **Shared Responsibility Model** between the Customer, the SaaS vendor and the underlying Public Cloud Provider

Retain full control of the outsourced activity

<b>Customer</b>	<b>Authorizations</b> (user identity, encryption key ownership)
	<b>Governance</b> (periodic service review, audit check)

Retain full control of who can access the SaaS application with no dependency to the SaaS vendor.  
Control the encryption key life cycle independently from the SaaS vendor.  
Has access to transparent service KPI and various Audit reports to ensure the effectiveness of the security and the availability.

Responsibility for Security “in” the Cloud

<b>Moody's</b>	<b>Applications</b> (availability, SLA., access control)
	<b>Customer Data Protection</b> (encryption, network traffic control)
	<b>Governance &amp; Incident Mgmt.</b> (monitoring, cyber security)

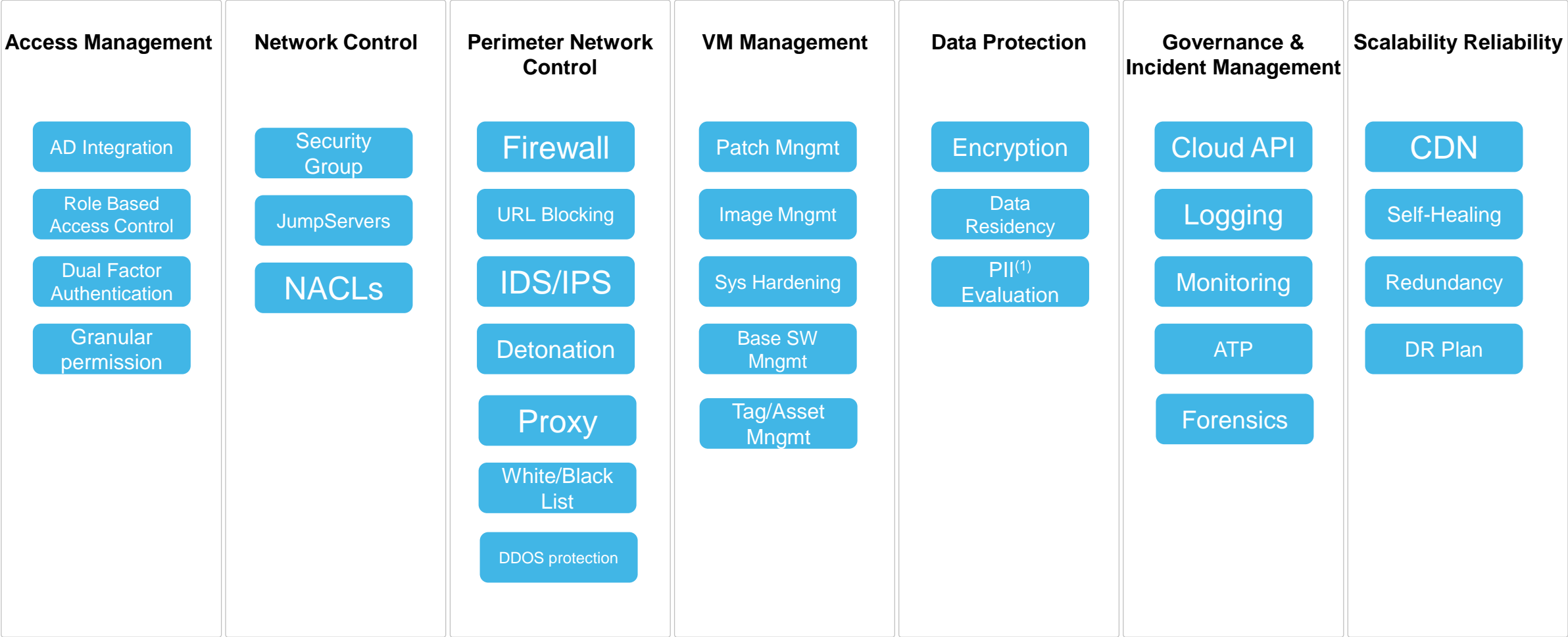
Implement end-to-end and monitor the security to protect the customer data.  
Manage the compute capacity to achieve on the SLAs (perf. availability, etc ...)  
Govern and monitor the use of the public cloud infrastructure

Responsibility for Security “of” the Cloud

<b>AWS</b>	<b>Managed Services</b> (database, monitoring, encryption)
	<b>Infrastructure</b> (compute, storage, network)
	<b>Data Centers</b> (availability, physical integrity)

Physical access to AWS data centers is strictly controlled. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors are required to present identification and are signed in and continually escorted by authorized staff.

# The bare minimum security framework you need



(1) Personal Identifiable Information (including GDPR)

# 5

## Common Mistakes and Misconceptions

# Common Mistakes and Misconceptions #1



## *Data must reside in my country?*

### **EBA**

- data must remain in a EU country (we support Dublin, Frankfurt as of now)
- All EU local supervisors are aligned with the EBA guidances (few have additional reqs).
- AWS has no data center in each EU country

### **Non EBA in Europe**

- For non EBA (ex: Switzerland), they are already coping with this problem by anonymizing the data when data are exchanged across EU.

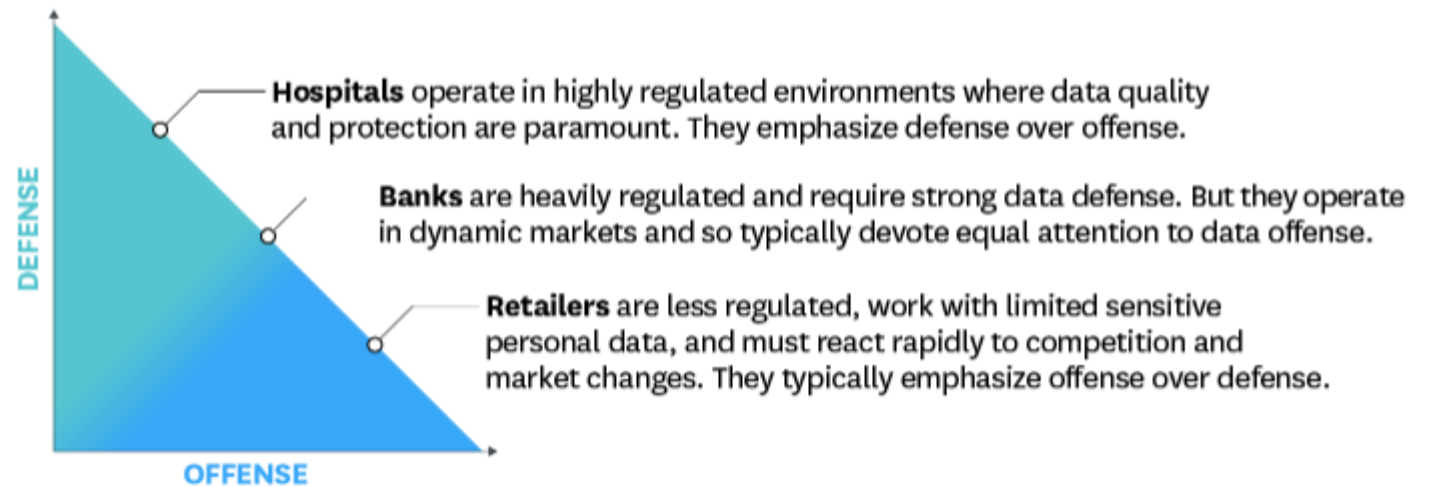
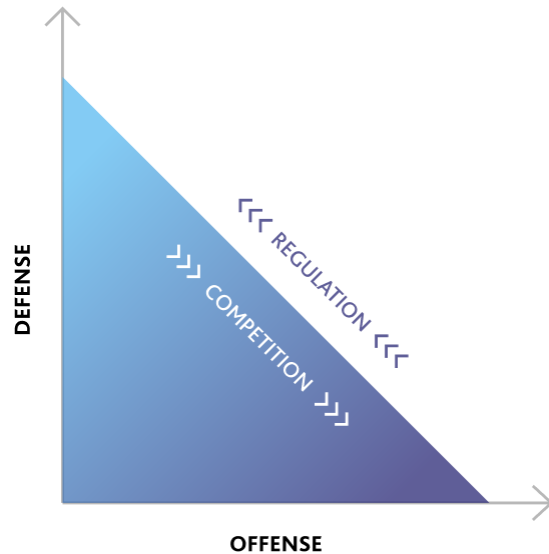
### **Rest of the world**

- Case by case but often it must reside in the country.
- All major countries have their own AWS data centers.

# Common Mistakes and Misconceptions #2



## ***Banks are not ready for the cloud?***



\* WHAT'S YOUR DATA STRATEGY?" BY LEANDRO DALLEMULE AND THOMAS H. DAVENPORT, MAY-JUNE 2017



# Common Mistakes and Misconceptions #3



## *How secure is multitenancy?*

### **Multi-Tenant Architecture**

- A single application & Infrastructure shared across all customers
- **But a dedicated storage & processing resources for each Tenant**
- High-Availability is achieved by distribution across several datacenters
- When resources are not used, they are either released to AWS (Elasticity) or reused for another workload
- Updates & upgrades rolled once and available to all customers
- Cloud Ops effort remains monitoring a single application on a standardized infrastructure type.
- Cost is compressed to the minimum thanks to sharing & elasticity

# Common Mistakes and Misconceptions #4



***My cloud provider is not approved by the local regulator?***

- Regulators are agnostic when it comes to choosing a specific cloud provider.
- There is no certification or approval process for specific cloud providers.
- Not a single regulator has stated a preference for specific cloud provider(s).
- Frequently banks rely on two or more leading cloud providers.
- Mind the “Concentration Risk” recommendation of EBA of using a single leading cloud provider.

# 6

A few guidelines for  
evaluating a SaaS Vendor

# Roles and Concerns

## Roles

## Key Concerns

### Risk/Finance

Features & functionality  
Reputation  
Peer validation User Experience  
Efficiencies

### Procurement/Vendor Management/Data Sourcing/Contracting

Pricing/Total Spend  
Contract clauses – termination/caps/YOY upticks/More modules/License structure  
Subsidiaries/Affiliates  
Cloud outsourcing aligned with local regulations

### IT

**Ease of Implementation**  
**Choice of cloud provider**  
**Objection to cloud (e.g. maintain control of environments and security)**  
Technology stack  
Resource demand-FTE  
Documentation

### Information Security

**Cybersecurity/Data Breaches**  
**Disaster Recovery/Backups**  
**SOC Audits & other certifications**

### CIO/CTO

Contractual terms (e.g. liability);  
Budget (signatory);  
Hitting implementation deadlines

# New areas of scrutiny

Outsourcing to a SaaS vendor requires an extensive assessment of the risks and the vendor compliance profile

## Security Assessment

- » Perimeter & Network Security
- » Data Isolation
- » Data Residency
- » Encryption
- » User Access Control
- » Reliability
- » Disaster Recovery
- » Cyber Security

## Vendor Compliance

- » Information security policies, awareness/training materials for employees and contractors
- » Human Resources Security
- » IT Asset Management & Physical Security
- » Access Control Policy
- » Business Continuity / Incident Response Policy
- » Data Protection
- » Compliance Reports (ex: SOC2, GDPR)

## Contractual Terms

- » SLAs
- » Security Plan
- » EBA Financial Service Audit Rights
- » Special terms per jurisdiction

# Risk and Compliance assessment

## Objectives:

- » Verify that the SaaS vendor security policies meet the bank expectations and any gaps is acceptable
- » Verify that Moody's SaaS offering & AWS have a compliance framework aligned with the bank expectations
- » Verify the contractual terms are aligned and support the bank expectations
- » Verify the EBA & Local PRA/FCA requirements are met
- » Adjust the contractual terms to specific bank expectations

## BUT It is not:

### A full Audit

- » Moody's contract with independent auditors to produce reports (ex: SOC2 Reports) in order to demonstrate controls are effective and confidential evidences have been demonstrated
- » We encourage our customers to rely and trust such independent reports



### A technical deep dive

- » First security rule is to keep the architecture confidential in order not to disclose sensitive information to cyber criminals.
- » However, a more advanced technical review can be performed with a reduced audience of Security Officers (CISO office for example).

# EBA - guidelines on Cloud Outsourcing

EBA has issued a revised guidelines on outsourcing arrangement in Feb 2019 (circular EBA/GL/2019/02) with a focus on cloud outsourcing

- » Guidelines enter into force on 30 September 2019
- » Define materiality, our Regulatory SaaS offering is considered as material for banks
- » A risk assessment and a due diligence must be performed and documented
- » An assessment of operational risk & cost benefits must be performed (and highly supportive)
- » An Audit Rights (system & data centers) must be given to the bank and the supervisors
- » Exit Strategy & termination of the service must be contractually agreed ahead and documented
- » The contractual agreement must reflect these points
- » Board Approval is required

# PRA and FCA - guidelines on Cloud Outsourcing



Consultation Paper | CP30/19

## Outsourcing and third party risk management

December 2019

Takes into account recently finalised guidelines on ICT and security risk management issued by the EBA as well as EIOPA's draft cloud outsourcing guidelines as they were at the time and addresses the following risks:

- » Cyber risk data protection
- » Oversight of sub-contracting arrangements
- » Business continuity
- » Consolidation risk
- » Data retention



MOODY'S  
ANALYTICS

Better  
Faster  
Decisions



[moodysanalytics.com](http://moodysanalytics.com)

© 2020 Moody's Corporation, Moody's Investors Service, Inc., Moody's Analytics, Inc. and/or their licensors and affiliates (collectively, "MOODY'S"). All rights reserved.

**CREDIT RATINGS ISSUED BY MOODY'S INVESTORS SERVICE, INC. AND/OR ITS CREDIT RATINGS AFFILIATES ARE MOODY'S CURRENT OPINIONS OF THE RELATIVE FUTURE CREDIT RISK OF ENTITIES, CREDIT COMMITMENTS, OR DEBT OR DEBT-LIKE SECURITIES, AND MATERIALS, PRODUCTS, SERVICES AND INFORMATION PUBLISHED BY MOODY'S (COLLECTIVELY, "PUBLICATIONS") MAY INCLUDE SUCH CURRENT OPINIONS. MOODY'S INVESTORS SERVICE DEFINES CREDIT RISK AS THE RISK THAT AN ENTITY MAY NOT MEET ITS CONTRACTUAL FINANCIAL OBLIGATIONS AS THEY COME DUE AND ANY ESTIMATED FINANCIAL LOSS IN THE EVENT OF DEFAULT OR IMPAIRMENT. SEE MOODY'S RATING SYMBOLS AND DEFINITIONS PUBLICATION FOR INFORMATION ON THE TYPES OF CONTRACTUAL FINANCIAL OBLIGATIONS ADDRESSED BY MOODY'S INVESTORS SERVICE CREDIT RATINGS. CREDIT RATINGS DO NOT ADDRESS ANY OTHER RISK, INCLUDING BUT NOT LIMITED TO: LIQUIDITY RISK, MARKET VALUE RISK, OR PRICE VOLATILITY. CREDIT RATINGS, NON-CREDIT ASSESSMENTS ("ASSESSMENTS"), AND OTHER OPINIONS INCLUDED IN MOODY'S PUBLICATIONS ARE NOT STATEMENTS OF CURRENT OR HISTORICAL FACT. MOODY'S PUBLICATIONS MAY ALSO INCLUDE QUANTITATIVE MODEL-BASED ESTIMATES OF CREDIT RISK AND RELATED OPINIONS OR COMMENTARY PUBLISHED BY MOODY'S ANALYTICS, INC. AND/OR ITS AFFILIATES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT CONSTITUTE OR PROVIDE INVESTMENT OR FINANCIAL ADVICE, AND MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT AND DO NOT PROVIDE RECOMMENDATIONS TO PURCHASE, SELL, OR HOLD PARTICULAR SECURITIES. MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS DO NOT COMMENT ON THE SUITABILITY OF AN INVESTMENT FOR ANY PARTICULAR INVESTOR. MOODY'S ISSUES ITS CREDIT RATINGS, ASSESSMENTS AND OTHER OPINIONS AND PUBLISHES ITS PUBLICATIONS WITH THE EXPECTATION AND UNDERSTANDING THAT EACH INVESTOR WILL, WITH DUE CARE, MAKE ITS OWN STUDY AND EVALUATION OF EACH SECURITY THAT IS UNDER CONSIDERATION FOR PURCHASE, HOLDING, OR SALE.**

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS, AND PUBLICATIONS ARE NOT INTENDED FOR USE BY RETAIL INVESTORS AND IT WOULD BE RECKLESS AND INAPPROPRIATE FOR RETAIL INVESTORS TO USE MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS OR PUBLICATIONS WHEN MAKING AN INVESTMENT DECISION. IF IN DOUBT YOU SHOULD CONTACT YOUR FINANCIAL OR OTHER PROFESSIONAL ADVISER.

ALL INFORMATION CONTAINED HEREIN IS PROTECTED BY LAW, INCLUDING BUT NOT LIMITED TO, COPYRIGHT LAW, AND NONE OF SUCH INFORMATION MAY BE COPIED OR OTHERWISE REPRODUCED, REPACKAGED, FURTHER TRANSMITTED, TRANSFERRED, DISSEMINATED, REDISTRIBUTED OR RESOLD, OR STORED FOR SUBSEQUENT USE FOR ANY SUCH PURPOSE, IN WHOLE OR IN PART, IN ANY FORM OR MANNER OR BY ANY MEANS WHATSOEVER, BY ANY PERSON WITHOUT MOODY'S PRIOR WRITTEN CONSENT.

MOODY'S CREDIT RATINGS, ASSESSMENTS, OTHER OPINIONS AND PUBLICATIONS ARE NOT INTENDED FOR USE BY ANY PERSON AS A BENCHMARK AS THAT TERM IS DEFINED FOR REGULATORY PURPOSES AND MUST NOT BE USED IN ANY WAY THAT COULD RESULT IN THEM BEING CONSIDERED A BENCHMARK.

All information contained herein is obtained by MOODY'S from sources believed by it to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, all information contained herein is provided "AS IS" without warranty of any kind. MOODY'S adopts all necessary measures so that the information it uses in assigning a credit rating is of sufficient quality and from sources MOODY'S considers to be reliable including, when appropriate, independent third-party sources. However, MOODY'S is not an auditor and cannot in every instance independently verify or validate information received in the rating process or in preparing its Publications.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability to any person or entity for any indirect, special, consequential, or incidental losses or damages whatsoever arising from or in connection with the information contained herein or the use of or inability to use any such information, even if MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers is advised in advance of the possibility of such losses or damages, including but not limited to: (a) any loss of present or prospective profits or (b) any loss or damage arising where the relevant financial instrument is not the subject of a particular credit rating assigned by MOODY'S.

To the extent permitted by law, MOODY'S and its directors, officers, employees, agents, representatives, licensors and suppliers disclaim liability for any direct or compensatory losses or damages caused to any person or entity, including but not limited to by any negligence (but excluding fraud, willful misconduct or any other type of liability that, for the avoidance of doubt, by law cannot be excluded) on the part of, or any contingency within or beyond the control of, MOODY'S or any of its directors, officers, employees, agents, representatives, licensors or suppliers, arising from or in connection with the information contained herein or the use of or inability to use any such information.

NO WARRANTY, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY CREDIT RATING, ASSESSMENT, OTHER OPINION OR INFORMATION IS GIVEN OR MADE BY MOODY'S IN ANY FORM OR MANNER WHATSOEVER.

Moody's Investors Service, Inc., a wholly-owned credit rating agency subsidiary of Moody's Corporation ("MCO"), hereby discloses that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by Moody's Investors Service, Inc. have, prior to assignment of any credit rating, agreed to pay to Moody's Investors Service, Inc. for credit ratings opinions and services rendered by it fees ranging from \$1,000 to approximately \$2,700,000. MCO and Moody's investors Service also maintain policies and procedures to address the independence of Moody's Investors Service credit ratings and credit rating processes. Information regarding certain affiliations that may exist between directors of MCO and rated entities, and between entities who hold credit ratings from Moody's Investors Service and have also publicly reported to the SEC an ownership interest in MCO of more than 5%, is posted annually at [www.moody.com](http://www.moody.com) under the heading "Investor Relations — Corporate Governance — Director and Shareholder Affiliation Policy."

Additional terms for Australia only: Any publication into Australia of this document is pursuant to the Australian Financial Services License of MOODY'S affiliate, Moody's Investors Service Pty Limited ABN 61 003 399 657AFSL 336969 and/or Moody's Analytics Australia Pty Ltd ABN 94 105 136 972 AFSL 383569 (as applicable). This document is intended to be provided only to "wholesale clients" within the meaning of section 761G of the Corporations Act 2001. By continuing to access this document from within Australia, you represent to MOODY'S that you are, or are accessing the document as a representative of, a "wholesale client" and that neither you nor the entity you represent will directly or indirectly disseminate this document or its contents to "retail clients" within the meaning of section 761G of the Corporations Act 2001. MOODY'S credit rating is an opinion as to the creditworthiness of a debt obligation of the issuer, not on the equity securities of the issuer or any form of security that is available to retail investors.

Additional terms for Japan only: Moody's Japan K.K. ("MJKK") is a wholly-owned credit rating agency subsidiary of Moody's Group Japan G.K., which is wholly-owned by Moody's Overseas Holdings Inc., a wholly-owned subsidiary of MCO. Moody's SF Japan K.K. ("MSFJ") is a wholly-owned credit rating agency subsidiary of MJKK. MSFJ is not a Nationally Recognized Statistical Rating Organization ("NRSRO"). Therefore, credit ratings assigned by MSFJ are Non-NRSRO Credit Ratings. Non-NRSRO Credit Ratings are assigned by an entity that is not a NRSRO and, consequently, the rated obligation will not qualify for certain types of treatment under U.S. laws. MJKK and MSFJ are credit rating agencies registered with the Japan Financial Services Agency and their registration numbers are FSA Commissioner (Ratings) No. 2 and 3 respectively.

MJKK or MSFJ (as applicable) hereby disclose that most issuers of debt securities (including corporate and municipal bonds, debentures, notes and commercial paper) and preferred stock rated by MJKK or MSFJ (as applicable) have, prior to assignment of any credit rating, agreed to pay to MJKK or MSFJ (as applicable) for credit ratings opinions and services rendered by it fees ranging from JPY125,000 to approximately JPY250,000,000.

MJKK and MSFJ also maintain policies and procedures to address Japanese regulatory requirements.