Moody's Analytics

Better Faster Decisions

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

JPMC Annual Letter to Shareholders

April 2019

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

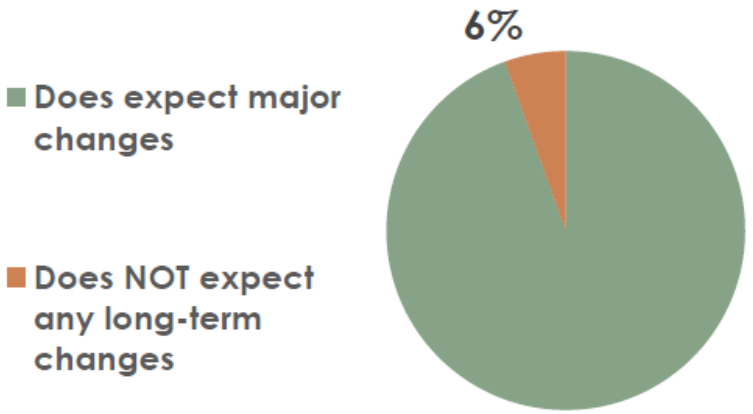
"Cloud give us…elasticity of computing power exponentially beyond our own capacity…

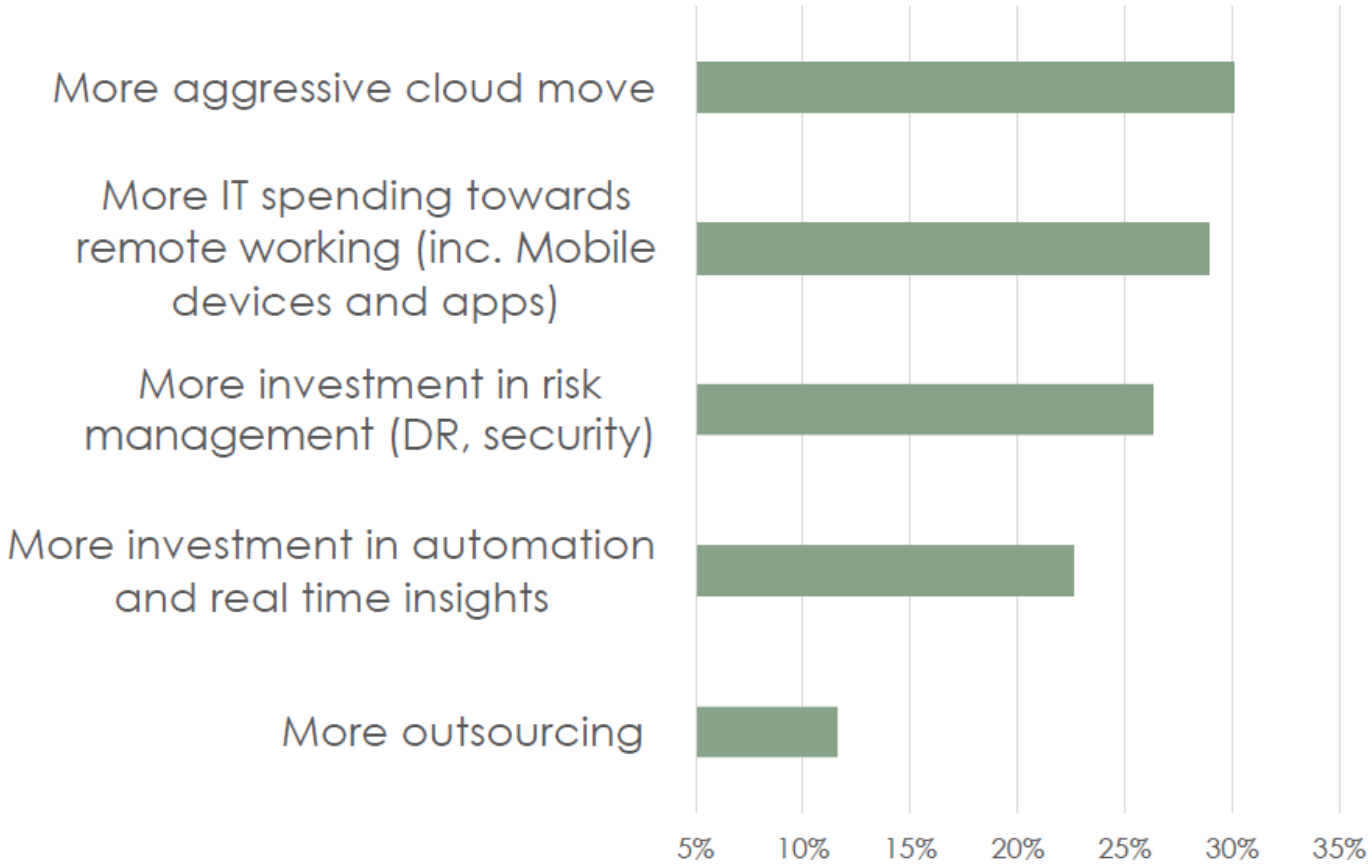
"Cloud…increases developers' effectiveness by multiples…as well as increasing the speed of delivering new capabilities to our customers and clients

"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]*

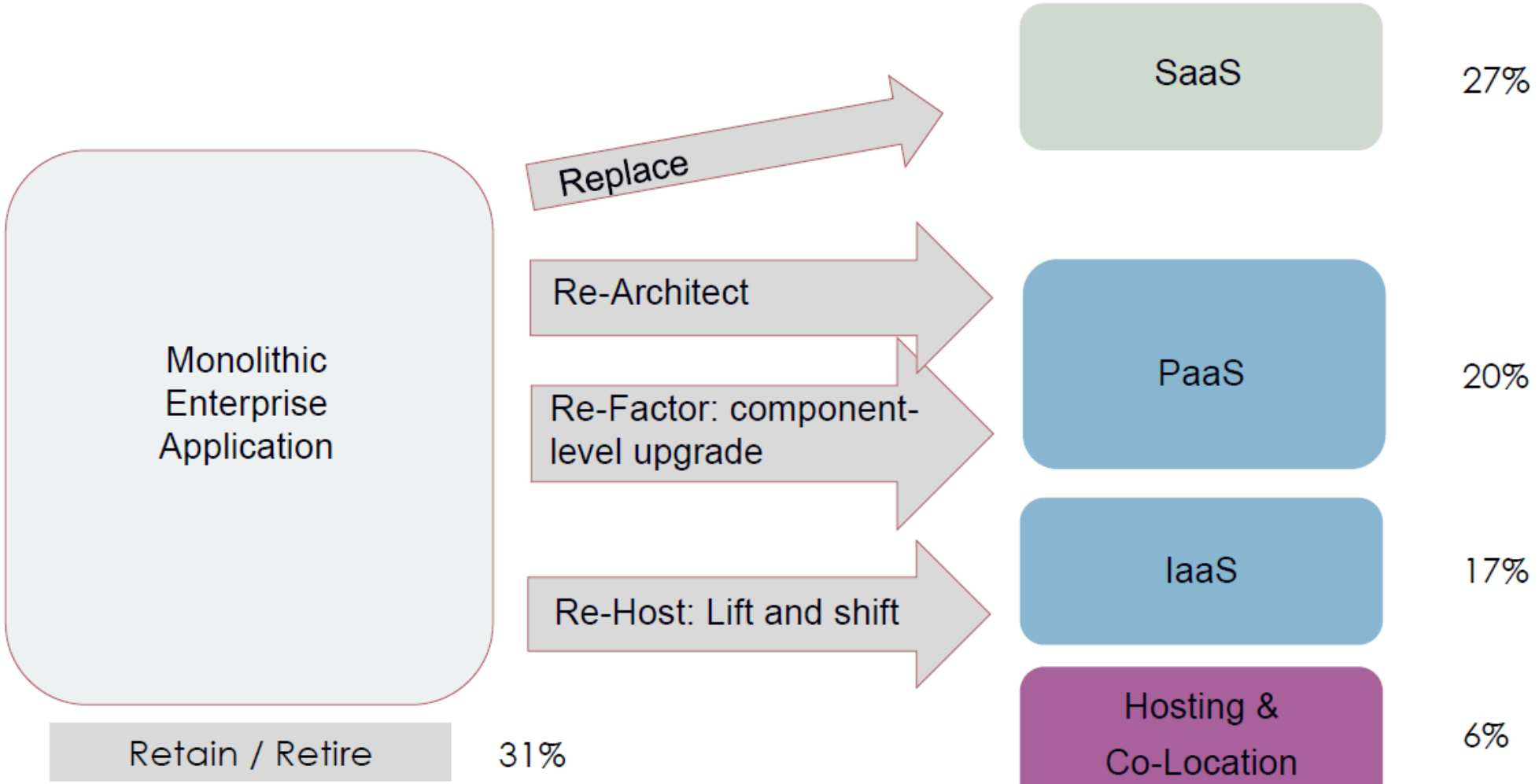




IDC ANALYZE THE FUTURE

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

Cloud Migration Strategies



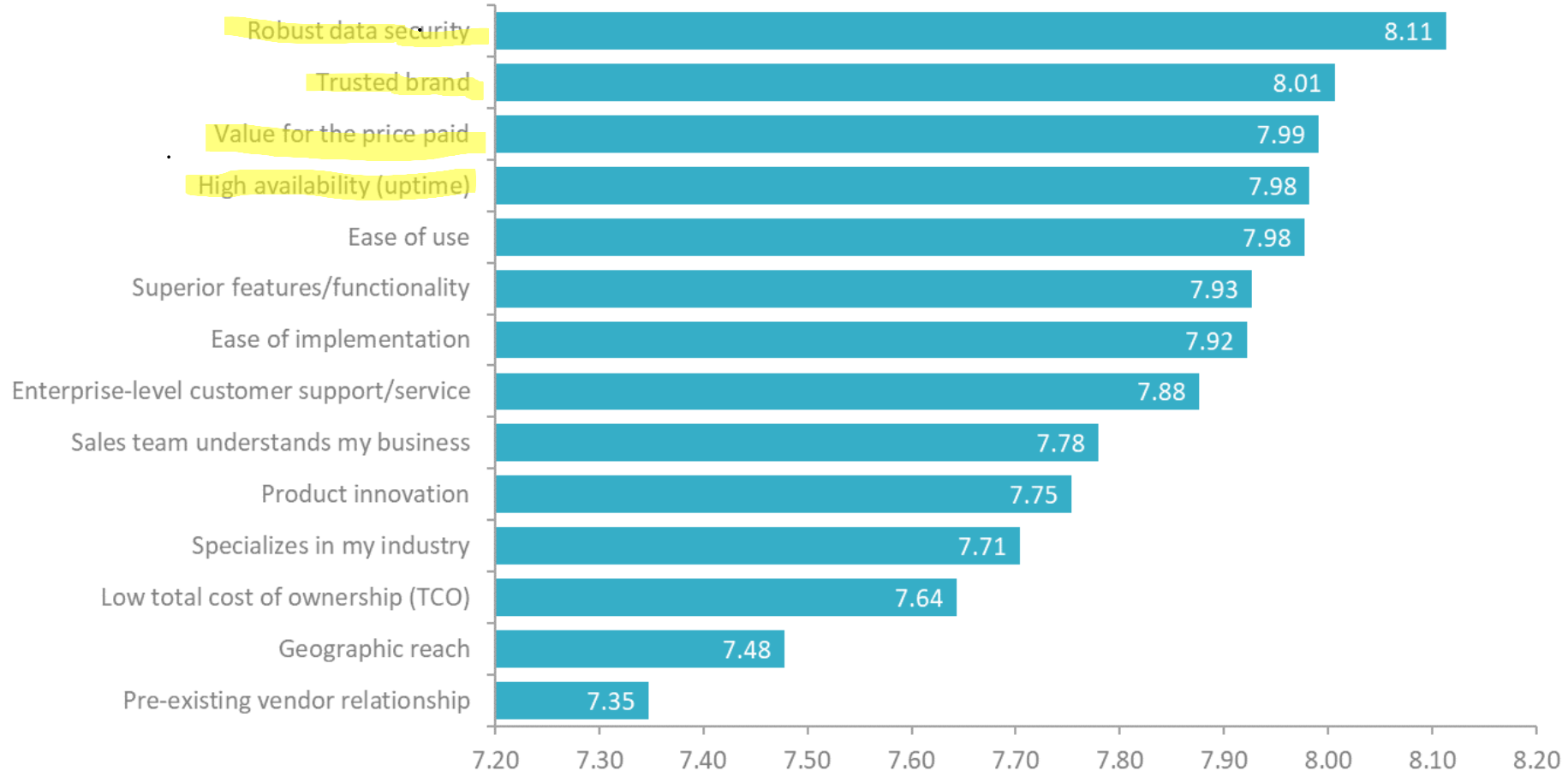
IDC ANALYZE THE FUTURE Source: IDC's Covid-19 Impact Survey, Wave 5, May 25, Europe N=730 © IDC

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

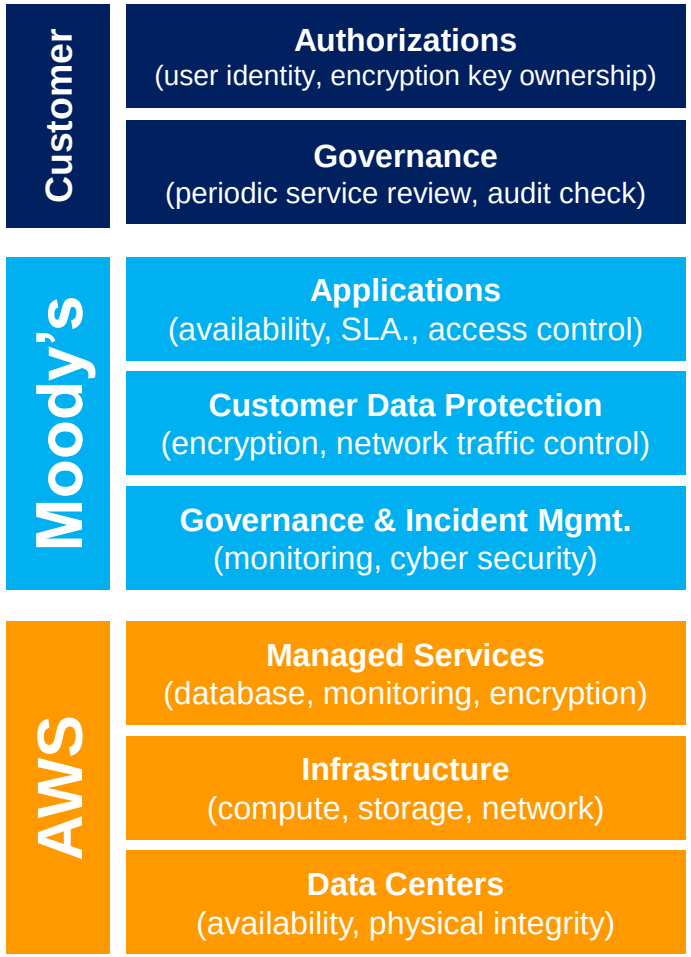
Data Protection and Security in a SaaS model

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

Responsibility for Security “in” the Cloud

Responsibility for Security “of” the Cloud



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.

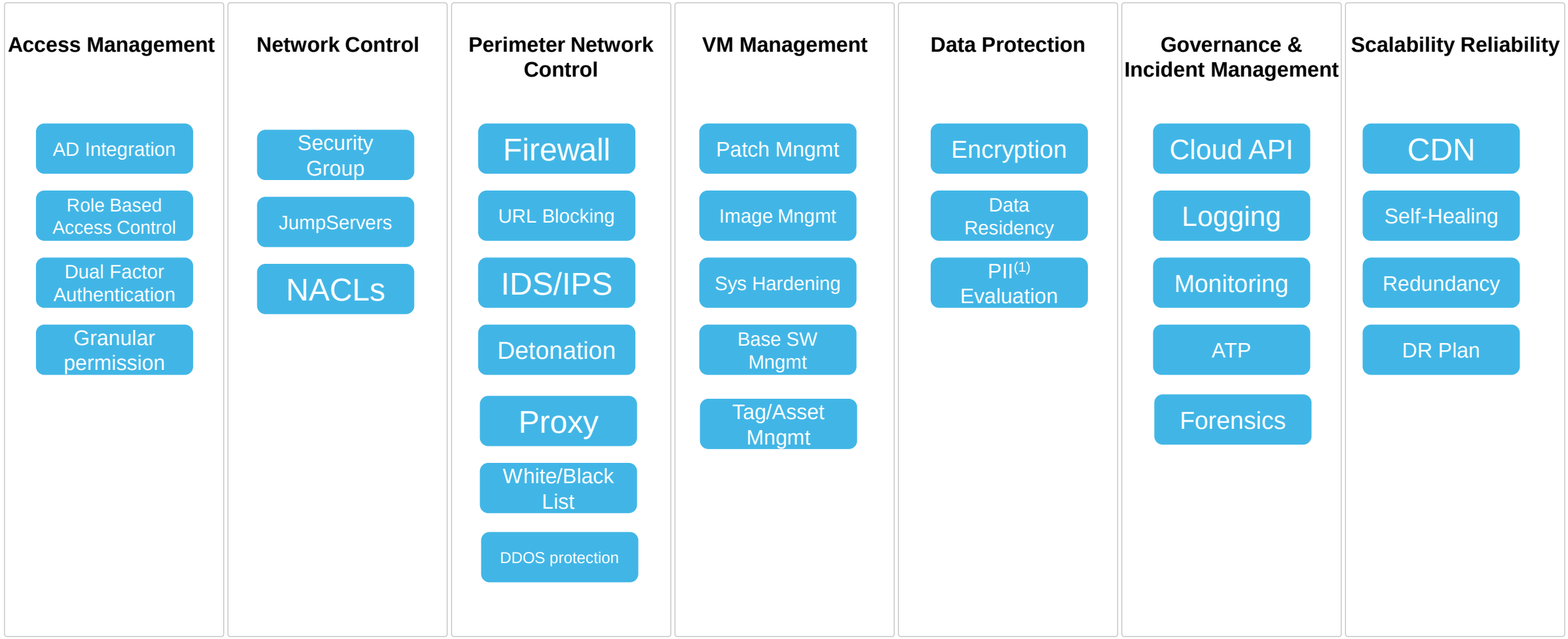
Implement end-to-end and monitor the security to protect the customer data.

Manage the compute capacity to achieve on the SLAs (perf. availability, etc …)

Govern and monitor the use of the public cloud infrastructure

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 Indentifiable Information (including GDPR)

5

Common Mistakes and Misconceptions

Common Mistakes and Misconceptions #1

Data must reside in my country?

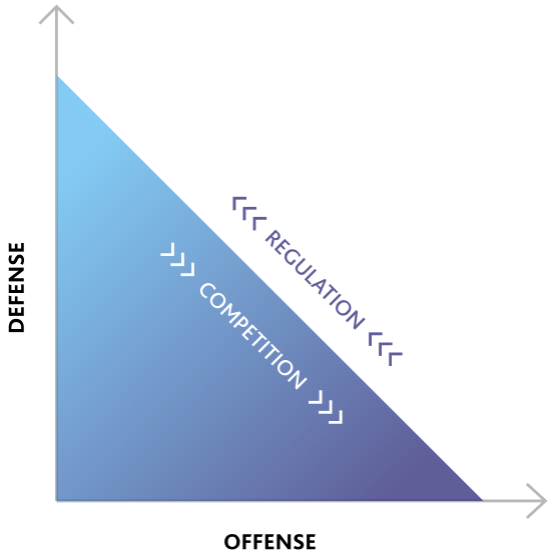
EBA
- data must remain in a EU country (we support Dublin, Frankfurt as of now)
- All EU local supervisors are aligned with the EBA guidances (few have additional reqs).
- AWS has no data center in each EU country

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

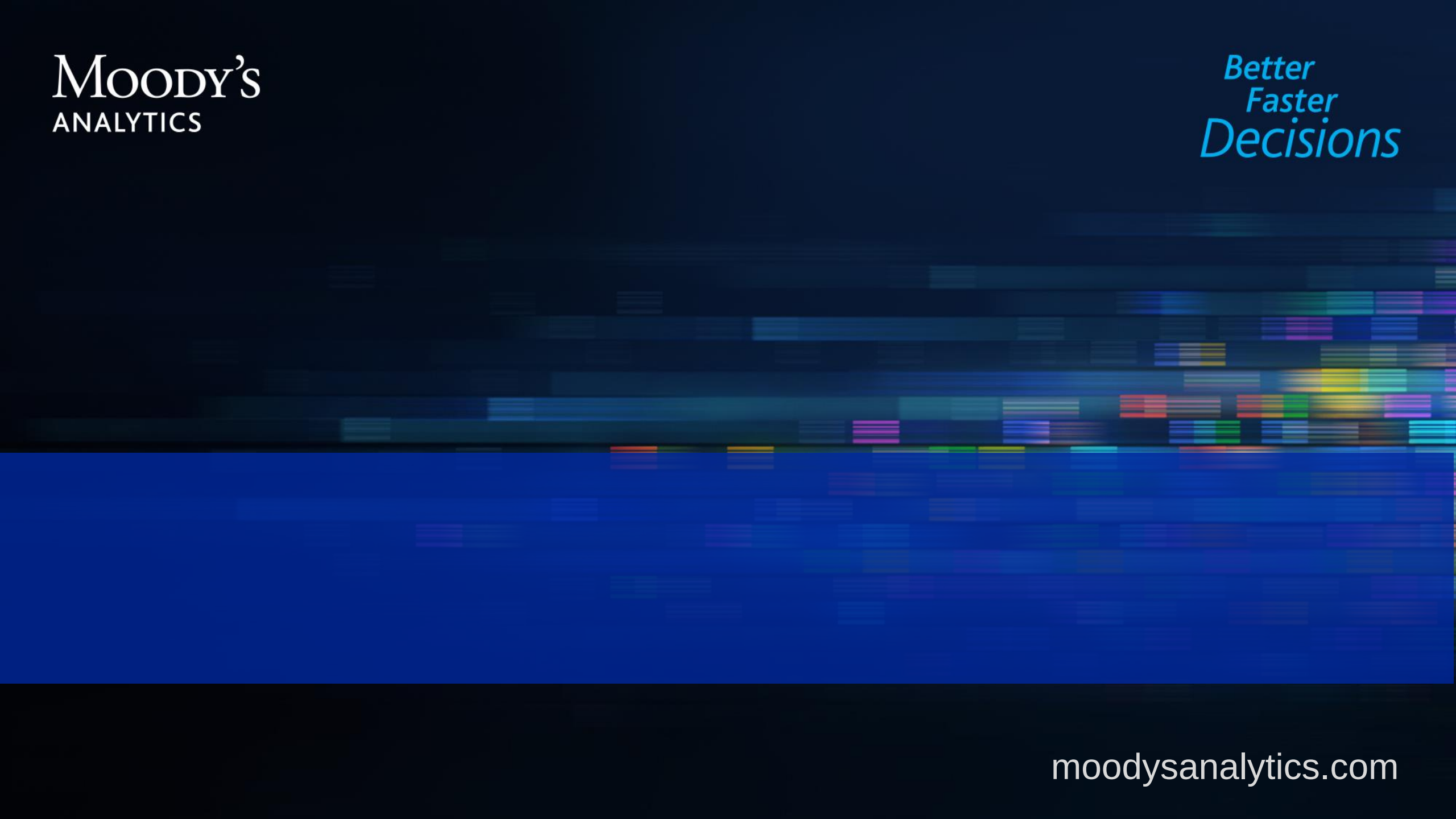
Consultation Paper | CP30/19

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