CAPCO

ARE YOU CLOUD READY ?

PUBLIC CLOUD AND ITS RISK GOVERNANCE

TABLE OF CONTENTS

TABLE OF FIGURES

1. THE CLOUDIFICATION TREND

In the context of the current digitalization efforts, increasing adoption of technology across the enterprise is a tidal wave that must be accompanied at all levels. The current financial industry's average product release time is at least nine months. Business acceleration is a necessity. Today, businesses are increasingly relying on information technology and information sharing. To enhance business value, companies are looking for shorter technology implementation cycles and increased business agility, which can only be achieved by relaxing some of the internal IT constraints. For example, since data must be made readily available to users, the challenge of getting around technical and operational debt mean a substantial array of data types have to be stored within a data lake or a shared big data management framework. Public cloud options tend to make this easier.

Moving to the public cloud is a necessity that businesses will increasingly face for their core activities in years to come. This is best exemplified by the recent partnership IBM has publicized with Bank Of America (partnership to overcome regulatory and risk management constraints for the Financial Industry). While current approaches are mostly performed in a project-by-project fashion, a more thorough attitude to the management of the public cloud adoption becomes necessary. The aim remains to achieve shifting dollars from running the business of IT to growing the (digital) business.

2. THE NEW ROLE OF IT

Technology is integral to almost all business processes. The role of IT has always been to provide the technological means for other departments to function and this role is expanding. However, while technology has progressively been democratized, it remains a challenge for the IT department to propose a hands-off approach to users of its technology.

IT spends a lot of time customizing applications to answer specific needs, fine-tuning architecture and developing new services to better articulate the IT ecosystem. Relying on standardized mass services where a lot of the configuration is at the hand of the users brings a fundamental change.

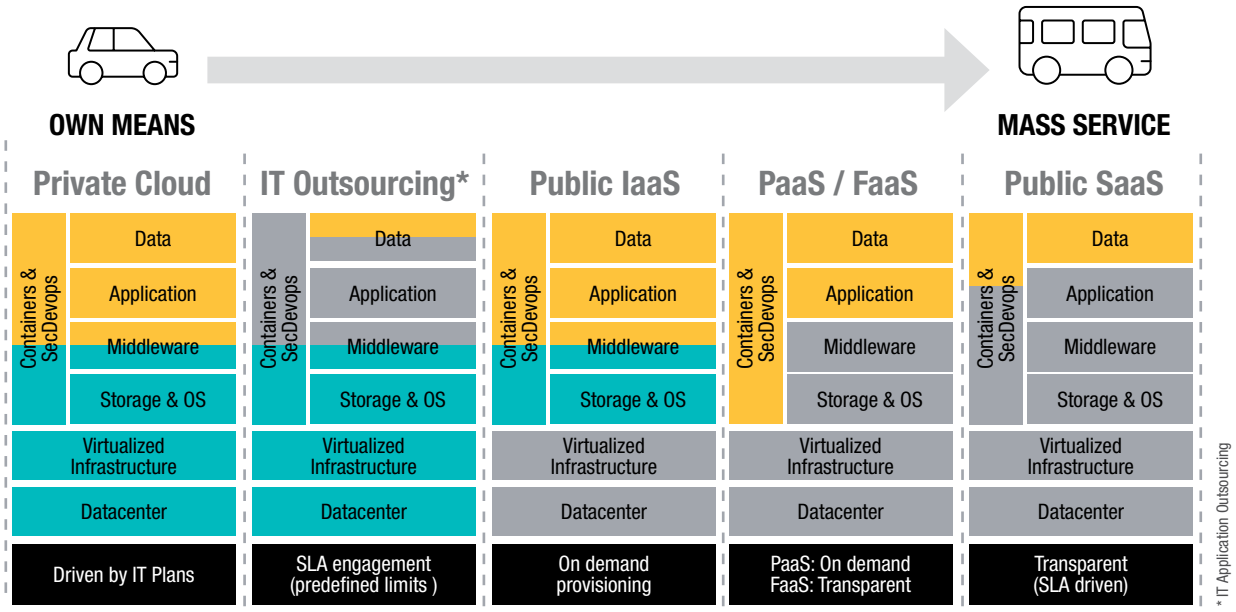
However, from the viewpoint of business departments using the Public Cloud seems often comparable to outsourcing. This does not account for some key differences between the two.

For example, when a data leak occurs for an outsourced service, the provider is often responsible by contract for failing to comply with the company's policies. It is the one responsible to take proportionate measures to answer or avoid such events in compliance with provided security policies. Using a public cloud service means that there is limited oversight on operational controls, the burden to manage appropriate prevention and recovery means is to be taken by the cloud customer (usually using a provided toolset). For example, Office 365 offers tools and recommendations for GDPR Compliance. You can for example setup the GDPR Dashboard in the Office Compliance Center (with steps to follow of Discover/ Govern/ Protect/ Monitor/ Respond).

For non-core business processes, it is possible to use the services of BPO companies that leverage cloud technology to provide BPaaS (Business Process As A Service). BPaaS provides the benefits of covering services end-to-end, driven by agreed outcome indicators, and where technology responsibility is shifted together with business responsibility. The fact is that as long as technology users are associated with a company, the control of their identification, behavior, and data must be performed internally.

OUTSOURCING SERVICES	CLOUD SERVICES
For outsourcing services, you specify the risks and responsibilities you want to transfer to the Service Provider in the contract	For cloud services, you agree to share risks and responsibilities with the Cloud Provider on standardized terms

Figure 1 : Main types of technology service models



LEXICON

IaaS	PaaS	FaaS	SaaS
Infrastructure As A Service	(Software) Platform As A Service	(Serverless) Function As A Service	Software As A Service

3. IMPACT OF CLOUD SERVICE MODELS ON RISKS

As technology services increasingly move to the public cloud, the types of risks faced by businesses are changing. It is important to understand the evolving nature of these risks especially when using a public infrastructure that is accessible anywhere in the world 24/7.

The most important change is that an always-on vigilance increasingly means the impossibility of infallibility. The level of trust granted is to be individually tuned for each technology service may it be to developers or to final users. The multiplicity of source of risks means a switch from giant walls (network firewalls) to a multiplicity of smaller walls. This forms the basis of Zero Trust Architecture. Some of the new major cloud risks are:

- **Data and regulatory risks**
  - Access control (including for cloud management tools)
  - Data transfers, public APIs and public databases

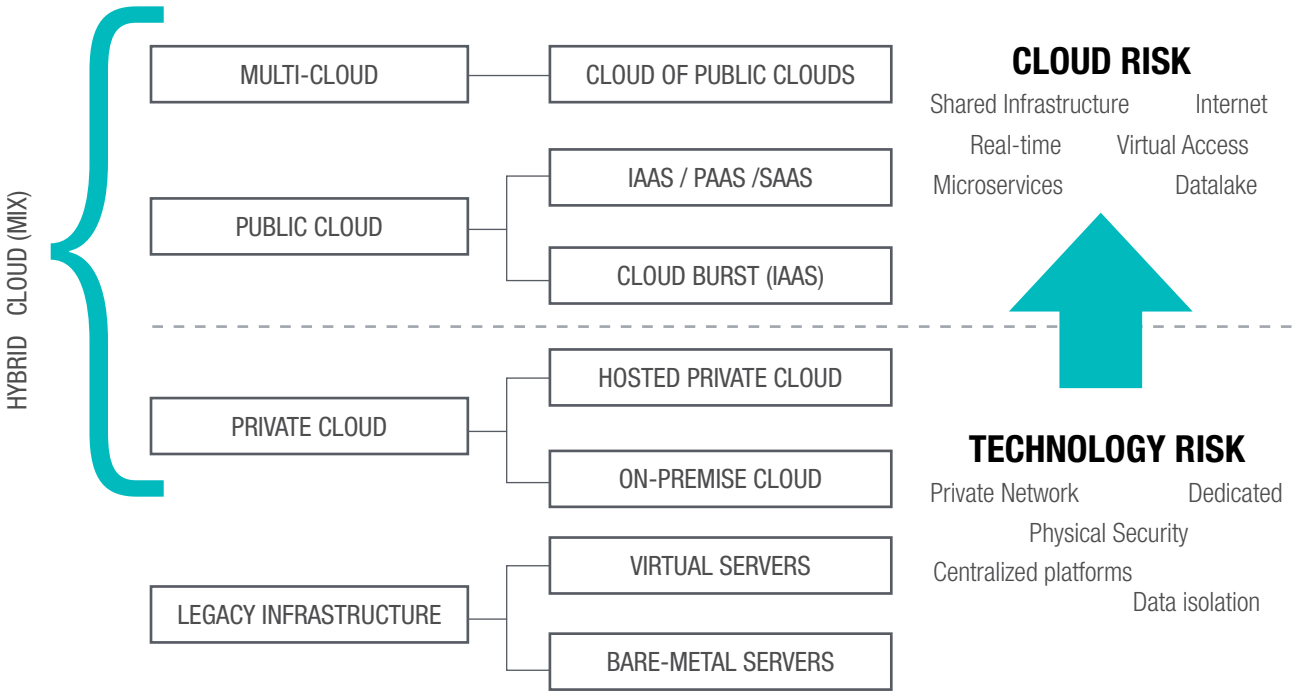
- Data leak from a malicious or non-intentional insider (including while teleworking)
- Data leak across shared infrastructure or misconfiguration (isolation issues)
- Lack of flexibility for encryption, data control
- Lack of visibility into cloud operations and the ability to monitor for compliance
- Unauthorized data access by the service provider
- Dependence on a service provider to ensure adequate internal controls

- **Technology risks**
  - Limitations on customization of service offerings
  - Compatibility with other cloud providers/reversibility (lock-in)
  - Cyber Security (Denial of Service, Viruses, Malware, Phishing, Network intrusions, Code injection, Infrastructure damage, Mobile devices)
  - Limited choice of technology and related tools
  - SecDevOps Management
  - Cloud underperformance
  - Cloud implementation discrepancies (from project to project)
  - Need for always-on controls
  - Shadow IT and unregistered IT assets
  - Cloud projects performed with no IT or architecture support (shadow IT)
  - Errors/incidents

- **Financial risks**
  - Contract modification or cancellation fees
  - Runaway costs from poor planning and lack of periodic monitoring
  - Additional overhead of managing the service providers (with more frequent cascading contracts)

- **Legal risks**
  - Jurisdiction and data sovereignty issues

Figure 2 : Change in the risk typology with cloud models



4. ADDRESSING THE CLOUD RISK: WHERE IS MY CLOUD?

The first challenge when it comes to understanding the cloud risk is to know all applications, services, APIs that are using Public cloud Infrastructure. With the increased use of microservices architecture, employee devices (BYOD) and online applications, it is necessary to keep the usage of public clouds in the company up to date. This includes:

1) IaaS / PaaS / FaaS applications like force.com, Microsoft PowerApps, SAP Cloud, AWS, Google Cloud, Azure, Openshift Online, CloudFoundry, Heroku, Domino Data Lab

2) SaaS applications used like Salesforce, Office 365, G Suite, EverNote, Slack, Trello, GitHub, GitLab, MailChimp, TalentSoft, Dropbox, Paypal, Expensify, LinkedIn Recruiter, Youtube

3) Open APIs, Backend Microservices and SecDevOps pipeline services hosted on different platforms: Google Maps, Google Apps, Yahoo Finance, IBM Watson, Microsoft Computer Vision, Facebook, LinkedIn, Twilio, Dropbox, Twitter, Government and Institutions Open Data Banks, eap.bloomberg.com, FactSet REST API, Markit Data API, triReduce API, Global Trade Repositories, Online Testing Tools

To facilitate the management of this heterogeneity of usage, it is increasingly possible to centralize the oversight of these services by relying on some of the following technologies:

Figure 3: Cloud Oversight Options

Technologies for cloud oversight

Technology	Examples	Pros	Cons
HYBRID CLOUD PLATFORMS	Red Hat Openshift, Ms Azure Arc, VMWare	Manage containers across multiple clouds	Only for usage 1)
CASB Cloud Security Broker	Cloudlock, Netskope, CloudFlare, CipherCloud	Can control all usages of multiple clouds	Focus on security (limited financial and technical management)
MULTI-CLOUD MANAGEMENT	ServiceNow, Embotics, Morpheus, Flexera, ScalR	Manage and control cloud resources including some policy enforcement (DevOps)	Mostly for usage 1)

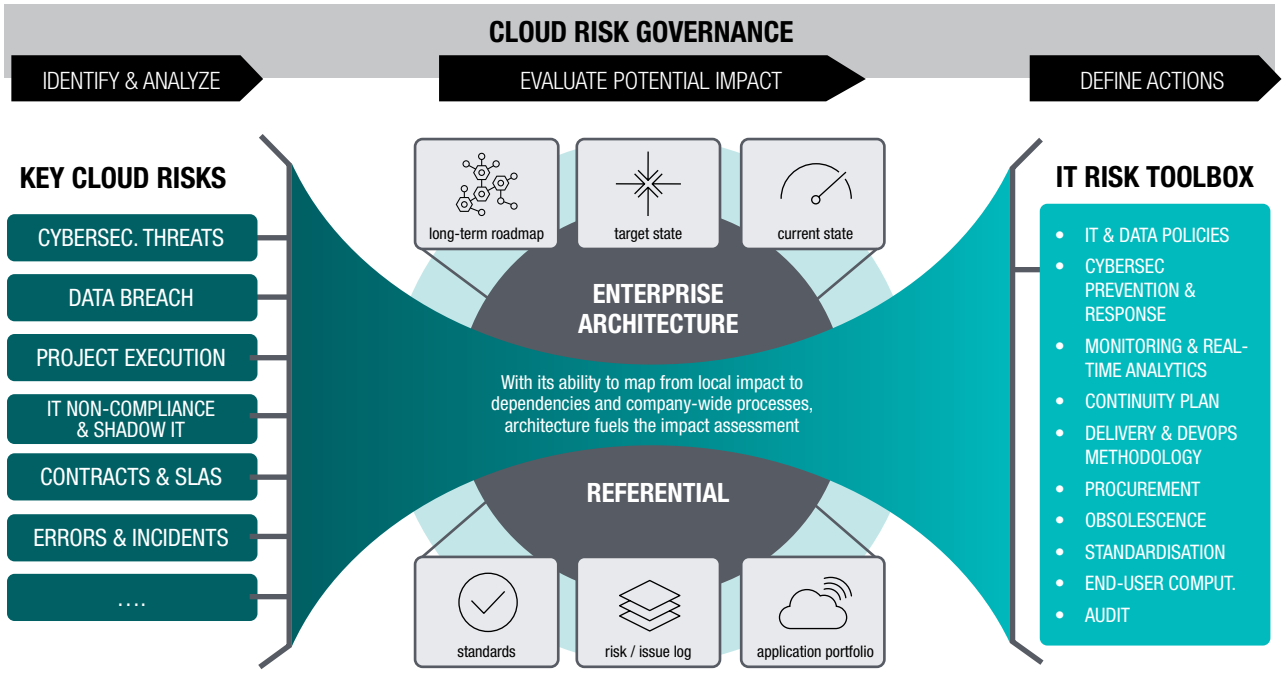
Many incidents like the attack that affected Canva (data for 139 million user accounts / May 2019) show that data leaks and security risks can be posed even by non-critical applications like a diagramming tool. This can be trickier to assess than attacks on primary applications like the one that occurred to Capital One in March and April (data with 100 million credit card applications).

5. ADDRESSING THE CLOUD RISK: A GOVERNANCE FRAMEWORK

Building a governance framework specialized for the cloud sounds like a nice-to-have since it seems covered within existing enterprise risk governance (through technology risks or outsourcing risks). However, experience shows that consistency is a critical requirement to ensure weaknesses are always addressed across the rising complexity and variety of cloud usage. An example of this has been the failure to patch all web development tools at Equifax in 2017 which led to one of the largest data breach in history with 147,9 millions of personal information on their US consumers and prospects. With an augmenting exposed surface and rising interconnection of provided services, global compliance with company policies is challenging to monitor. Weaknesses can even come from unused/not actively used assets as was the case in the 2014 data leak that occurred at JP Morgan Chase where a server from their past acquisition of "Bank One" had been easy to exploit by relatively unsophisticated hackers.

It is also important to ensure that users of the cloud are increasingly aware of the risks. Tools to mitigate the risks come first by having all users (from sales to managers to developers) understand the logic for policies. It also requires some efforts to provide options for end-users to work efficiently (i.e. more abilities to automate tasks, share data, etc. to facilitate the use of vetted standardized services at the hand of users instead of providing calibrated services that tend to require complex configurations and still not satisfy a large number of end users)

Figure 4: Cloud Risk Governance Framework



Here are the 3 steps of a typical cloud governance model:

1) Identify and analyze cloud risks

The public cloud threats is to be assessed in occurrence likelihood and analyzed with known vulnerabilities across the cloud and related assets. The banks and capital markets infrastructure attract a lot of attention due to the substantial value of money flows and the political connotation of finance. They are generally more exposed to cybersecurity threats and require a good level of trust to operate, making them an ideal prey. The key to properly identify these risks is first and foremost to have a consolidated and updated view of cloud assets.

2) Evaluate potential impact

The vulnerabilities that might affect certain assets (from physical hardware to application code and data) will usually impact a larger number of applications and business processes in case of incident. A well-maintained architecture referential allows assessing the expected impact of any compromise and the precise list of similar assets potentially affected by the vulnerabilities.

3) Define actions

Each risk materialization has its own characteristics and thus requires 2 types of actions in proportion of the assessed potential impact it would have:

- **Prevention and mitigation actions**
  - i) The general idea for information security experts is to have a maximum number of sensors and traps in place to prevent or detect intrusions. These include firewalls, API managers, microservice control planes (service mesh), behavior analysis, network traffic analysis, application log analysis, database log analysis, exploit checkers, honeypots, etc. with ideally all data collected centrally in a SIEM (Security information and event management). Public clouds can provide most of these services as options but will let you configure them with your own experts.
  - ii) The next lot of actions are related to SecDevOps best practices including real-time application monitoring and alerting, code analytics, strong identification and authentication practices and tools. There is good reason here to roll out the new passwordless authentication solutions using means like biometrics, voice, geolocation, mobile device ownership proofs or physical security keys.
  - iii) For new projects and regular deployments, it is necessary to ensure that policies are enforced, and architecture is valid (or that exceptions are acknowledged). Ideally, projects are run through SAFe Release Trains to ensure best practices at each project stage.
  - iv) Part of data controls/compliance is enforcing data encryption for communication and storage, archiving or anonymizing historical contents and ensuring control of the dissemination of data.
  - v) End-user computing must be able to provide the right solutions for the mobile worker to ensure compliance is workable for 100% of personnel.
  - vi) Cost management monitoring and audits should allow keeping spending under control.

- **Standard response actions**
  - i) Continuity plans and Disaster Recovery Plans must allow the switch to safe environments to continue operations unaffected
  - ii) Procurement can help prevent financial risks like contracts with the ability to scale up but restricted ability to scale down, etc.
  - iii) Obsolescence of technologies in use is also necessary on the cloud (end of life for products, issues with quality, etc.) All these actions are best enforced using automated controls and responses which is key to ensuring consistency across multiple cloud platforms. Cloud risks require real-time continuous compliance checks and fast response times. The risk governance framework should in effect accompany the agility and speed provided by the move to a public cloud. Inheriting all legacy rules and policies not always adapted or specific enough for the public cloud would typically challenge this search for agility. This is why setting up a separate Cloud Risk Governance focused on cloud rules and policies becomes more and more appropriate.

6. THE PARALLEL EVOLUTION OF ENTERPRISE ARCHITECTURE

With the ascent of agile/lean practices and SAFe to scale across the enterprise, the perceived ivory tower role of the Enterprise Architecture has evolved towards a collaborative view that can accompany decisions made on projects and transformations.

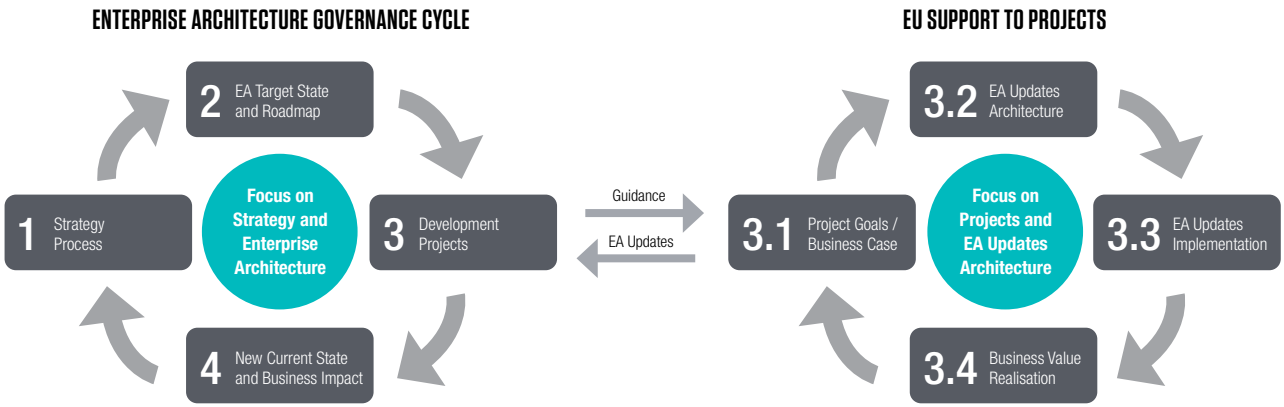
The governance of IT requires the tools and guidance of Enterprise Architecture, especially when it comes to:

- Application portfolio
- Technology portfolio
- Process repository
- Data model repository
- SecDevOps best practices and synchronization of emerging and innovative practices and technology

It is to be noted that the management of cloud and technology risks will often require the setup of architecture policies and standards. However, instead of planning complex roadmaps to move to these new standards, more pragmatical means of achieving the same objectives can be considered. The tendency being for architecture products to be “just enough” to allow room for iterations and feedbacks.

Enterprise architecture is a major enabler of cloud risk governance and is necessary to support it. While a cloud implementation can occur with minimal IT intervention it should not happen without some interaction with EnterpriseArchitecture.

Figure 5 : The 2 pillars of Enterprise Architecture



(cf. BT Standard www.managebt.org)

7. IN SUMMARY

Using the public cloud is a challenge that can test the maturity and agility of the risk governance; therefore, we recommend the setup of a separate Cloud Risk Governance. We believe that as the roles of IT evolves with the use of the cloud, the risk governance framework is a piece of the management of technology that can only grow in importance. The need for an always-on availability of this capacity means greater automation of risk governance is a necessity. The setup of a dedicated Cloud Risk Governance Framework is a necessary force to accompany the increasing use of public clouds.

REFERENCES

MODERNIZED ENTERPRISE ARCHITECTURE

1. SAFe 5.0 /
2. Business-Technology-Standard Section 2 /
3. TOGAF Post : The future Enterprise Architect /

MODERNIZED INFRASTRUCTURE WITH THE CLOUD

4. Mc Kinsey Digital : Unlocking business acceleration in a hybrid cloud world /
5. IBM turned Wall Street's public cloud fears into an opportunity to work with Bank of America /

MODERNIZED TECHNOLOGY RISK MANAGEMENT

6. Technology Risk Management, a new approach /

AUTHOR

François Bourcier, Principal Consultant

CONTACTS

Gilbert Swinkels, Partner
gilbert.swinkels@capco.com

François Bourcier, Principal Consultant
francois.bourcier@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO

© 2019 Capco – SAS The Capital Markets Company | 121, avenue de Malakoff, 75116 Paris | All rights reserved.