Negotiating Cloud Services Agreements:
Perspectives from Providers and Customers

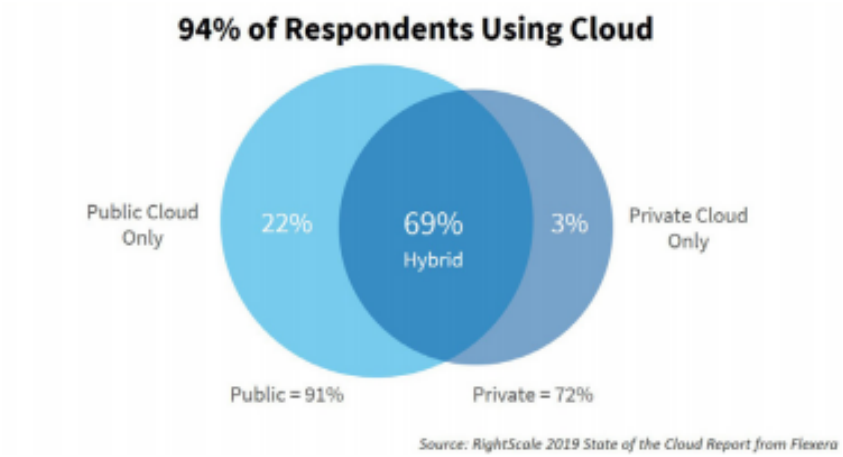
Suzanne K. Gainey
Susan Linnstaedter
Todd C. Taylor

September 4, 2019

CLOUD SERVICES OVERVIEW

Overview of Cloud Services

- In Jan. 2019, RightScale conducted a survey of approx. 800 technical professionals about the use of cloud computing by their organizations:



- According to estimates by Gartner, Inc. , the worldwide public cloud services market is expected to grow 17.5% in 2019 to almost $215 billion.

Types of Cloud Services

- Public Cloud – services and infrastructure are provided via the Internet to multiple entities.
- Private Cloud – services and infrastructure are maintained on a private network (can be onsite or offsite) for single entity.
- Hybrid Cloud – integrated cloud service combining elements of both Public and Private Cloud.
- IaaS – Infrastructure as a Service.
- PaaS – Platform as a Service.
- SaaS – Software as a Service.

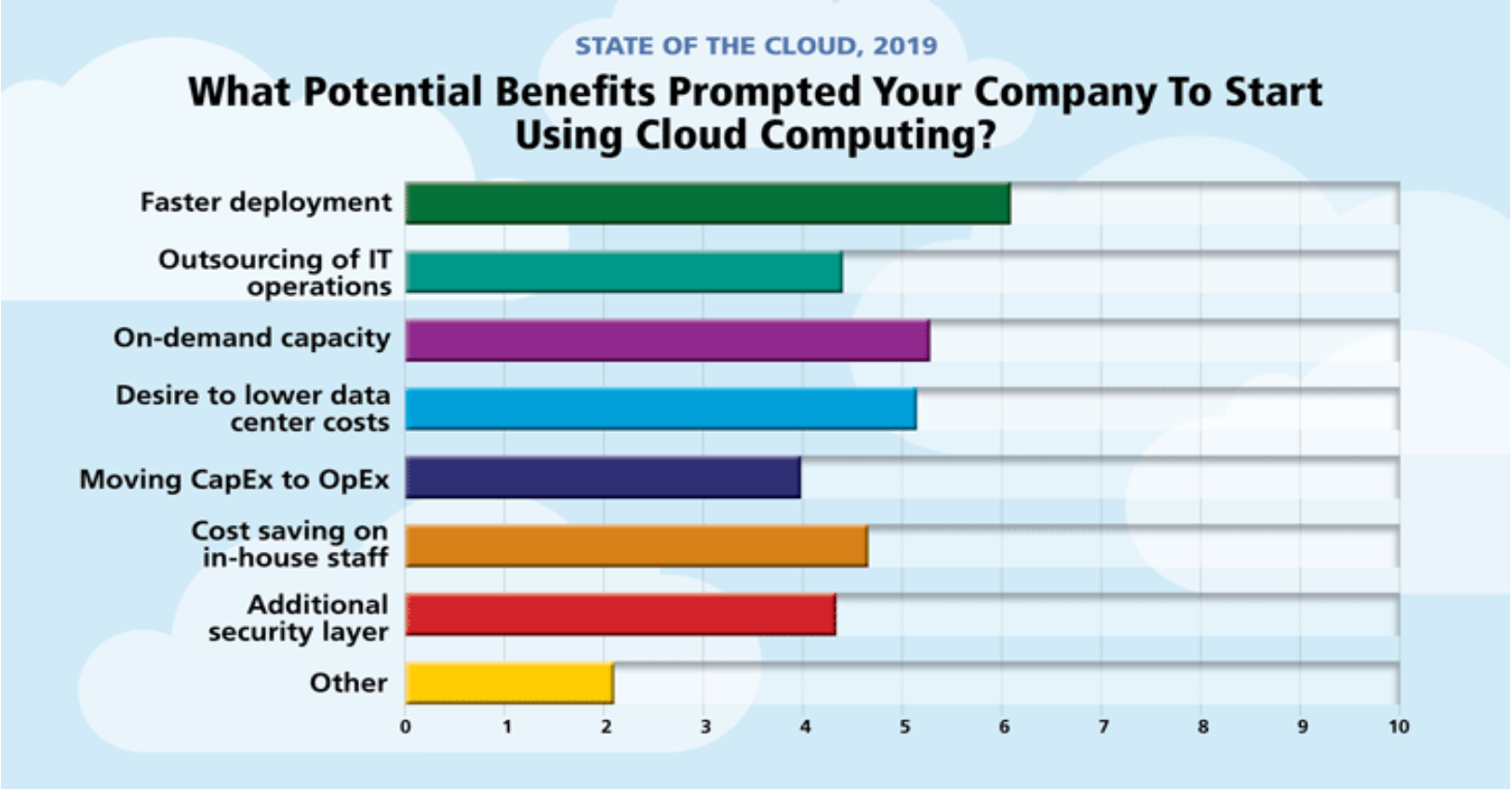
On-Prem vs SaaS

	On-Prem	SaaS
Fees	One-time license fee + maintenance fees	Typically bundled monthly or annual subscription fees
Accounting Treatment	Capital expenditure	Operating expenditure
Updates	Maintenance contract required	Typically included in subscription
Customizations	Generally customizable at a cost	Generally standardized, but may be configurable
Security	Licensee responsibility	Shared responsibility
Business Continuity	Licensee responsibility	Shared responsibility

Network & Data Center Outsourcing vs. IaaS

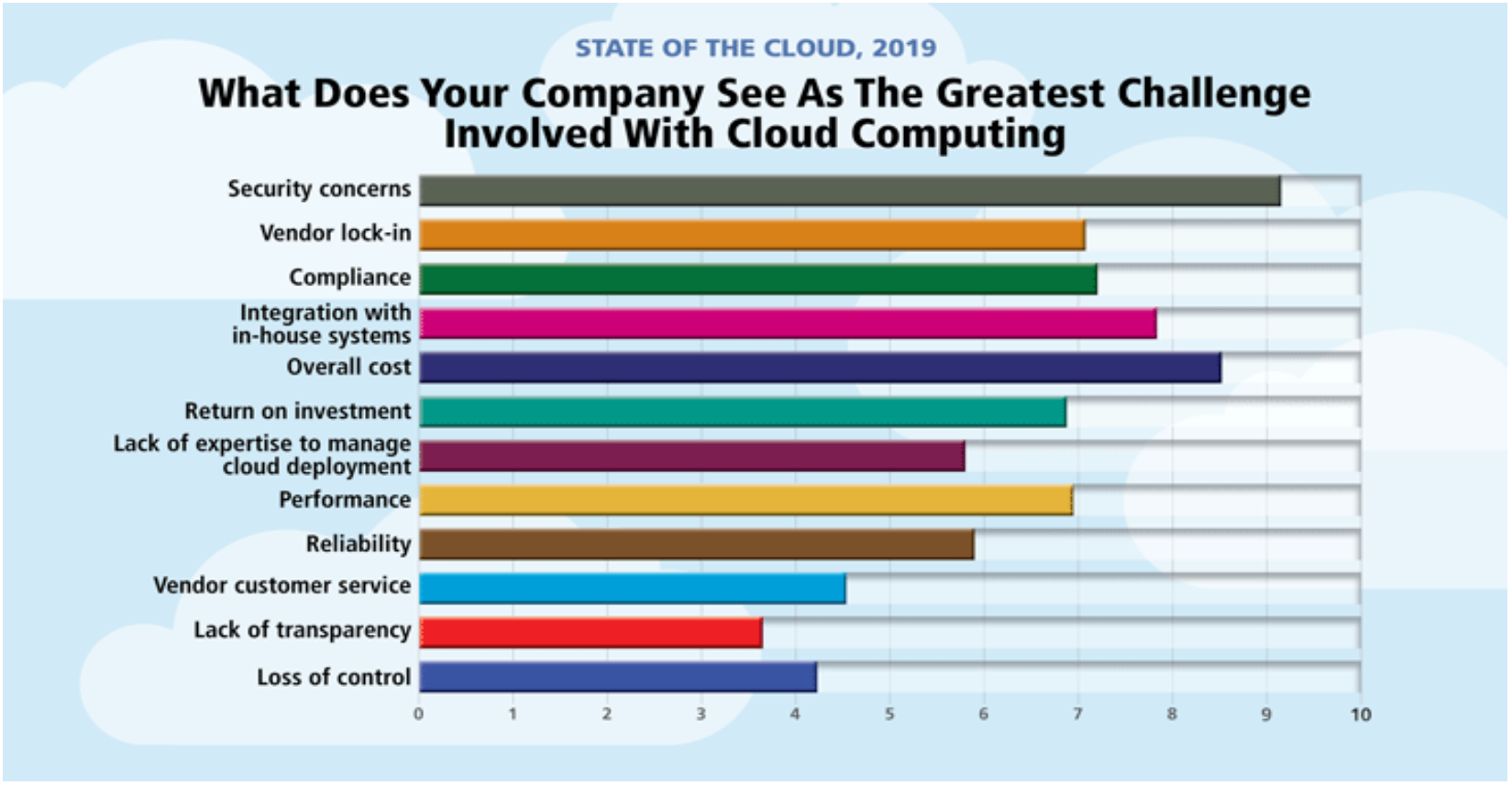
	Network & Data Center Outsourcing	IaaS
Contracting	Often on Customer's paper	Almost always on Provider's paper
Level of Control	Customer can maintain high degree of oversight and control	Shared control within the framework established by Provider
Managing Capacity	Can be time consuming and expensive to add or reduce capacity	Capacity can be added or removed fairly quickly
Security	Customer can often dictate type of security controls and frameworks used by Provider	Provider controls overall security framework, but frequently provides Customer tools to manage security within framework
Audit Rights	Often broad	Often limited to third party reports
Business Continuity	Shared responsibility	Shared responsibility
Transition Services	Customer can frequently obtain extended transition services period	Ability to obtain extended transition services can be more limited, though leverage helps

Cloud Services: The Good



- Source – Datamation, *2019 State of the Cloud Survey*.

Cloud Services: The Bad



- Source – Datamation, *2019 State of the Cloud Survey*.

Cloud Services: The Ugly

The New York Times

Capital One Data Breach Compromises Data of Over 100 Million

GeekWire NEWS JOBS EVENTS RESOURCES ABOUT Search

Amazon and Capital One face legal backlash after massive hack affects 106M customers

BY NAT LEVY on August 9, 2019 at 12:16 pm

RELEVANT LAWS, RULES, REGULATIONS, GUIDANCE AND INDUSTRY STANDARDS

Examples of U.S. Federal Data Privacy/Security Laws

- **The Federal Information Security Management Act**, 44 USC §3551 *et. seq.* ("FISMA") – Covers federal agencies and federal contractors who access federal agency databases or information.

- **Gramm-Leach-Bliley Act**, 15 USC §6801-09 ("GLBA")/ **Interagency Guidelines Establishing Information Security Standards** – Requires financial institutions to protect the security and confidentiality of their customers' non-public personal information.

- **The Health Insurance Portability and Accountability Act**, Pub. Law 104-191 ("HIPAA") & **the HITECH Act**, 42 USC §§300jj *et. seq.* & 17901 *et. seq.* – Sets out privacy and security obligations of "covered entities" (*i.e.*, health plans, health care clearinghouses and health care providers).

The CLOUD Act

- The Clarifying Lawful Overseas Use of Data ("CLOUD") Act provides that U.S. law enforcement orders issued under the Stored Communications Act may reach certain data stored in other countries.
- Also allows foreign governments that have entered into a bilateral agreement with the U.S. to make law enforcement requests directly to U.S. service providers (not the government).
- The CLOUD Act was originally introduced as a stand-alone bill, but was later added to the $1.3 trillion bill to fund the government.
- Many organizations have voiced concerns regarding the CLOUD Act, and the expansion of executive power.

Litigation Concerns with Cloud Storage

- Under Rule 34 of Federal Rules of Civil Procedure, a party to litigation can be required to produce documents ***and electronically stored information*** in a party's possession, custody, or ***control***.

- Similar rules exist at the state level as well.

U.S. State Data Privacy/Security Laws

- **Data Breach Notification Laws**
  - Typically protect a name in combination with other data (*e.g.*, social security number, financial account numbers – sometimes in combination with passcode), if not publicly available.
  - Notice to affected individuals (and/or governmental agencies) is typically triggered when an entity reasonably believes there has been unauthorized disclosure or access to personal information.
  - A large majority of states do ***not*** require notice where there is no "risk of harm" to affected individuals.
- **Data Security Laws**
  - Generally require an entity that collects personal information to implement and maintain reasonable security procedures and practices to protect such information from unauthorized access, destruction, use, modification or disclosure.

General Data Protection Regulation (GDPR)

- If an entity is directly subject to the GDPR, it must:
  - implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing personal data;
  - impose certain obligations on any of its vendors/subcontractors that have access to personal data (*i.e.*, Article 28 requirements);
  - provide notices to supervisory authorities and data subjects after discovering a personal data breach;
  - provide to data subjects notice of its practices relating to its processing of personal data; and
  - comply with data subject requests.

EBA Guidelines on Outsourcing Arrangements

- Finalized in February 2019.
- Goes into effect on September 30, 2019.
- Addresses the use of Cloud Providers, with a focus on data security.

Industry Data Security Standards

- ISO/IEC 27000 – a series of information security standards promulgated by the International Organization for Standardization and the International Electrotechnical Commission.

- NIST 800-53 – a set of security controls promulgated for U.S. federal information systems and their third party service providers by the National Institute of Standards and Technology.

- COBIT 5 – a framework for the governance and management of enterprise IT created by a global task force and development team from ISACA (formerly the Information Systems Audit and Control Association).

- FedRAMP -- a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

PREPARING FOR CLOUD SERVICES

Understanding the Cloud Service and Issues Presented

- Is the proposed offering a SaaS, IaaS or PaaS offering?
- Have solutions been compared (*i.e.*, have RFIs and RFPs been undertaken)?
- Are there unique legal or regulatory concerns that will impact the use of the Cloud Service?
- Are their implementation or migration concerns (*e.g.*, interoperability with existing concerns, licensing concerns with existing software, timelines)?

Can Risks be Addressed Outside of the Contract?

Cyber/Data Breach Insurance can include coverage for:

- third party claims (including, in some cases regulatory and PCI fines);
- initial forensic response;
- repair of network damages;
- notification of breach victims;
- lost revenues;
- business interruption;
- cyber extortion; and
- reputational damages.

CONTRACTING STRUCTURE & MATERIAL TERMS IN CLOUD SERVICES ARRANGEMENTS

The Agreement Structure

- Frequently Cloud Providers use one or more written agreements (*e.g.*, a Master Agreement, Order Form) for a set of Cloud Services.
- One or more sets of electronic terms will also apply (*e.g.*, use rights, online service terms).
- Cloud Providers may use special addenda to address unique regulatory issues (*e.g.*, data protection terms, financial service terms).
- Pay attention to:
  - Online linked terms -- do the links work and are they accessible?
  - How are terms amended?
  - Order of precedence?

Basic Privacy/Information Security Terms

- What types of data does the Agreement address?
  - "Your Content"/"Customer Data" vs. Data Pertaining to Customer.
- How does the Agreement address confidentiality/information sharing?
  - Does the Agreement permit third party sharing/use for purposes other than providing the services?
- Does the Agreement address information security?
  - Does the Agreement address physical, technical, administrative and organizational measures to protect data?
  - Does the Agreement reference any industry security standards?
  - Encryption?
  - Data Segregation?

Information Loss and Protection Terms

- Does the Agreement address data retention/ destruction?
  - Does the Agreement set forth a data retention schedule?
  - Is data deleted at the termination or expiration of the Agreement?
  - Can the Provider retain data following termination or expiration?
  - Does the Agreement address data migration/format issues?
  - Does the Provider's solution allow the Customer to control retention/destruction issues?
  - Are recovery point objectives addressed in the contract?

Oversight and Regulatory Terms

- Does the Customer have an audit right?
  - If no audit right, determine if third party audit reports (*e.g.*, SOC 2, Type II reports) can be obtained.
- Are regulatory required provisions addressed?
  - GDPR Article 28?
  - Data transfer mechanisms (*e.g.*, EU/Swiss Privacy Shield/Model Clauses)?
  - Data incident notification?
  - Oversight rights (*e.g.*, Interagency Guidelines, NY DFS Cybersecurity Regulations, EBA Guidelines)?

Modification and Risk Allocation Terms

- How is the Agreement modified?
  - Can the Cloud Provider unilaterally modify the Agreement through website updates?
- Indemnification?
  - Does the Cloud Provider indemnify the Customer against breach of data security obligations?
  - Does the Customer indemnify the Cloud Provider?
- Limitation of Liability clauses?
  - Does the Agreement cap the Cloud Provider's liability?
  - Are there exceptions or special caps for certain liabilities (*e.g.*, confidentiality breaches/data security breaches)?

NEGOTIATION OBJECTIVES

Key Contractual Objectives – Customer

- Limiting the Cloud Provider's use of Customer's data to the provision of the services.
- Ensuring the Agreement includes adequate confidentiality/information security provisions.
- Ensuring continuity of services (*e.g.*, adequate lead time on retirement of services, business continuity/disaster recovery, post-termination of services).
- Ability to obtain information on key issues (*e.g.*, audit rights, third party reports).
- Ability to exit services without unreasonable lengthy commitment.
- Defined service levels and appropriate remedies (*e.g.*, credits, termination right).

Key Contractual Objectives – Cloud Provider

- Flexibility for service to change and adapt.
- Obtaining some level of minimum revenue commitments.
- Avoiding creation of customized environments/requirements for any one customer.
- Avoiding guaranteed legal commitments for extended or indefinite time periods.

Operational Terms vs. Commercial Terms

- Regardless of leverage, it is very difficult to change operational terms in a public cloud services agreement.
- Based on negotiation leverage, commercial terms can be modified.

OPERATIONAL TERMS	COMMERCIAL TERMS
Data Security Processes and Standards	Service Offering/Fees
Contract Modification	Indemnification/Limitation of Liability
Subcontractor Engagement	Termination
Facility Management	Facility Location

Compensating Controls

If a provision cannot be satisfactorily changed are there compensating controls?

- Limitation on the types of data placed in Cloud Services?
- Are lockbox/encryption controls available?
- Limitation on placement of operational critical applications/processes in the Cloud?
- Cyber Insurance?
- Hybrid Cloud arrangement?
- Termination in event of change in contract?
- Source Code escrow for SaaS solution?

Negotiating the Language

"This Cloud Services Agreement (this "CSA") is entered into between Customer and Cloud Provider and is subject to certain additional terms and conditions set forth in the Electronic Service Terms of Use, currently available at http://cloudprovider.com/estu (the "ESTU") and in the Data Handling Addendum, currently available at http://cloudprovider.com/dha (the "DHA"), each of which may be modified from time to time. In the event of any conflict between such documents, such conflict shall be resolved based on the following order of precedence: (1) the ESTU shall take precedence over the DHA and the CSA, and (2) the DHA shall take precedence over the CSA."

"An Affiliate of Customer may use the Services provided under this CSA by entering into a separate Order specifically referencing this CSA."

"Cloud Provider may immediately suspend the Services for Customer's violation of the Acceptable Use Policy."

"Cloud Provider will implement reasonable technical, administrative and physical measures designed to protect the security and confidentiality of Customer Information."

Questions?

TODD C. TAYLOR
Member

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

toddtaylor@mvalaw.com
T: (704) 331-1112 F: (704) 409-5611

SUZANNE K. GAINEY
Associate

100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003

suzannegainey@mvalaw.com
T: (704) 331-3559 F: (704) 378-1959

Susan Linnstaedter
Microsoft Corporation
Corporate and External Legal Affairs
Director, US Financial Services
sulinnst@microsoft.com
+1-980-776-7234
https://www.microsoft.com/