Governance in the Cloud

Cloud Governance

- Cloud Governance can be defined as the set of policies or principles that act as the guidance for the adoption, use and management of cloud technology services.
- Cloud governance is an ongoing process that must sit on top of existing governance models.

Industry Standards Organizations and Groups associated with Cloud Computing

- These groups have defined various guidelines and best practices to help interoperability and portability of data and applications.
- Some of the well-known organisations are as follows:
  - National Institute of Standards and Technology (NIST), United States.
  - Cloud Security Alliance
  - Open Grid Forum (OGF)
  - The Object Management Group (OMG)
  - Cloud Computing Interoperability Forum (CCIF)
  - Distributed Management Task Force (DMTF)
  - Storage Networking Industry Association (SNIA)
  - Open Cloud Consortium (OCC)

Need for IT governance in cloud computing

- To understand the major issues related to IT resource , security and compliance.
- To make cloud deployment successful IT decision makers come up with some facts which when coupled with right tools and strategies will be beneficial compared to in-house legacy applications.
- By implementing cloud governance, organisations can avoid the following issues:
  - Security and privacy risks
  - Vendor Lock in
  - Cloud sprawl
  - Shadow IT and unwarranted usage of cloud resources
  - Lack of data portability and interoperability

Need for IT governance in cloud computing

- **Security and privacy risks:**

  Which may arise due to unauthorised downloads /installation of software, storage of illegal data and access to restricted sites by users.

- **Vendor lock-in:**

  This clause creates organisations to depend on the cloud service provider (or vendor) for products and services. The clause is usually made part of the agreement, and as a result, it prevents the organisations to bring in another vendor to work on different modules, for a specific period of time. This can be avoided by making changes to the SLA suitably and reduce dependencies on a single vendor, thus ensuring freedom to the organisation.

Need for IT governance in cloud computing

- **Cloud Sprawl:**

  Happens when employees of different departments use different programs and cloud infrastructure from third party providers without involving the IT department and getting necessary approvals. Employees usually utilise free cloud services like Google Drive, Dropbox etc. for many of their official work as it is free and there is not much of approvals required. If not detected and restricted, crowd sprawl may lead to fragmented, redundant, inefficient and unmanaged cloud programs sitting on the enterprise cloud and unnecessarily creating troubles.

- **Lack of data portability and interoperability:**

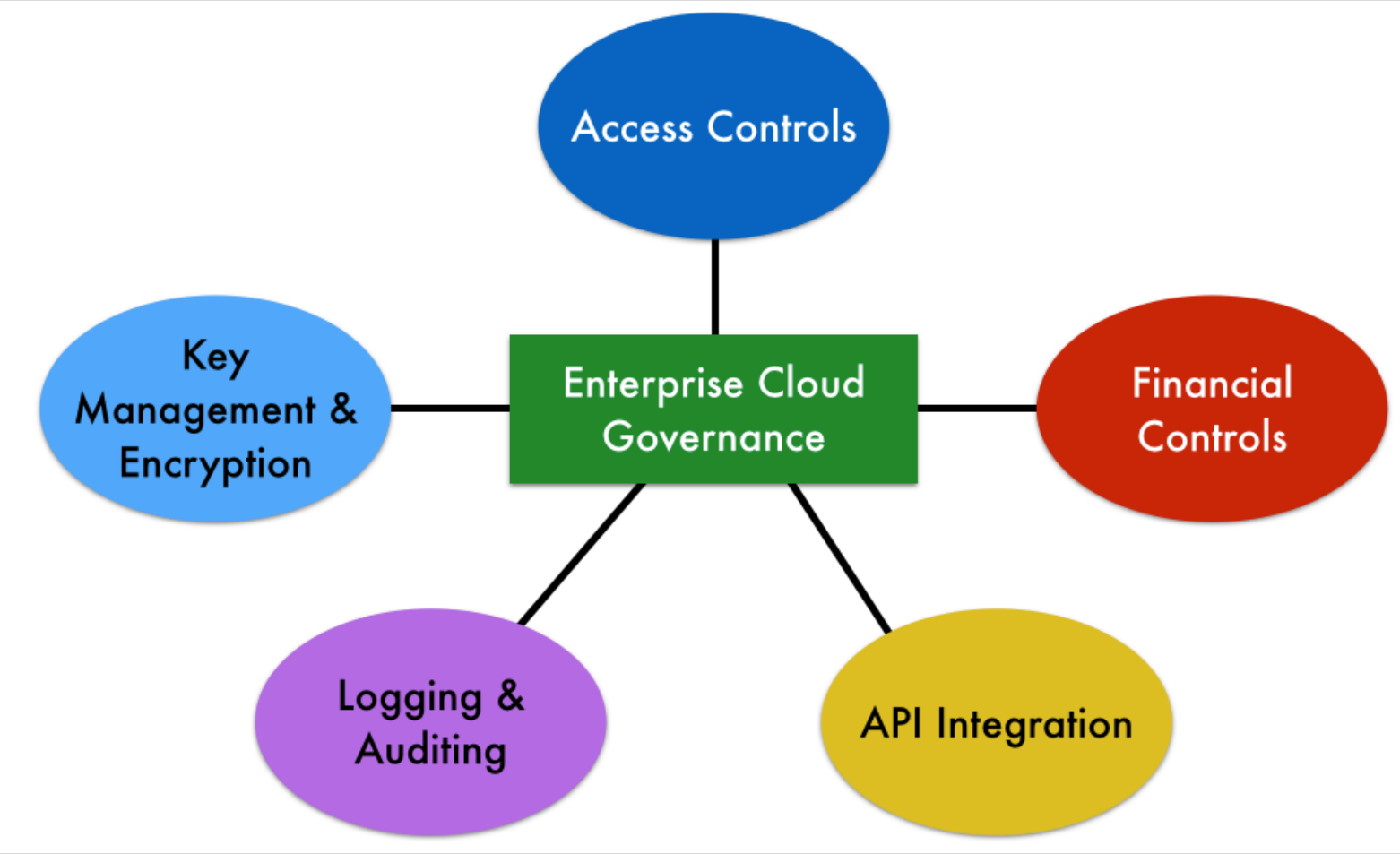
  Happens when the cloud service provider or the inbuilt cloud infrastructure is incapable of connecting well with other software and products outside the organisation. This may also lead to modules not compatible with each other and hence chaos in the cloud due to inefficient system.

Need for IT governance in cloud computing

- **Shadow IT and unwarranted usage of cloud resources:**

  Happens when employees in various departments don't follow the rules and regulations as imposed by the IT department on cloud usage resulting in security breach and fragmented control throughout the organisation. This leads to not getting sufficient results from the cloud in the long run.

Cloud Governance in Enterprise



Cloud Governance in an Enterprise

Access Controls

- it is very essential to avoid multiple employees making changes (or) modifications at the same instance.
- Limit the access to specific people or team instead whole IT deptt.
- Modifications can be done to the application through raising requests to the specific set of individuals.
- Implement role based security model like
  - super-administrators
  - administrators,
  - developers,
  - managers and
  - employees.
- Different roles would have different access levels

Financial Controls

- The Finance team would allocate specific budgets to each cloud based project based on the scope and requirements.
- The finance team has to allocate bigger budgets for the :
  - Cloud application with high Infrastructure and Software requirements
  - high impact projects
  - mission critical projects and
  - projects carried out for premium clients of the organisation
- Multi-national corporations have implemented effective governance measures to track the budgets for each and every project in the cloud
- Effectively control the spending based on periodic reviews on a monthly, quarterly or yearly basis.

API (Application Program Interface) Integration

- It is important when the cloud based application (or) infrastructure is to be shared with other applications developed by third-party developers outside the organisation for various business reasons.
- Necessary protocols and policies are to be communicated while the API is shared with the public.
- Strict regulations have to be implemented to provide restricted access to outsiders.

Logging and Auditing

- Almost all corporations log every activity across the private, public and hybrid clouds.
- Activities like changes to code, changes to database, addition (or) modification (or) edits done to a specific application are all tracked and logged.
- These log files are audited regularly by system administrators and quality assessment professionals to ensure everything is executed as per the Cloud Governance policies.
- Any discrepancies are monitored and necessary corrective measures are taken.

Key Management and Encryption

- Corporations implemented a unique security architecture enforces separation of roles through sophisticated algorithms running independently.
- These independent algorithms guards all the security keys and credentials across the cloud based applications.
- They don't essentially run on the same servers where actual applications are hosted and hence, they have no access to confidential data.
- That means, the servers and storage capacity of such corporations contain all the confidential and non-confidential data in an encrypted format and encryption keys are operated and managed by independent algorithms available outside these servers.

DATA PRIVACY AND SECURITY ISSUES

- With a third party organisation managing the infrastructure in the cloud, the responsibility to maintain privacy of all personal data is enhanced.
- Personal details of employees, customer data and company secrets must be protected against the potential risks of theft and leakage.
- Different elements that needs to be considered and made available in contracts and agreements while moving to the cloud are:
  - Privacy and Data Protection
  - Data Controllers and Data Processors
  - Data Protection Issues in the Cloud
  - Data Protection Laws

Privacy and Data Protection

- According to a research by IDC (International Data Corporation),
  - for 71% of enterprises preventing the exposure of confidential data is a big challenge.
  - company's financial and customer information, intellectual properties and personal information of employees are the most vulnerable data.
- Companies must look for cloud service providers that offer sufficient protection to such sensitive information.
- To start with, when third party data has to be moved to the cloud, the existence of any contracts or obligations against such action must be checked for.
- Following this, depending upon the location of the cloud service provider and industry specific laws of privacy such as Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA) stringent privacy measures must be applied.

Data Controllers and Data Processors

- In order to regulate the use of personal data, the Data Protection Act was established.
- Under this act, the data controller implies to an entity that determines the purpose of holding personal data and the data processor “processes” the data on behalf of the controller.
- The data controller takes the ultimate responsibility of complying with the Data Protection Act in case of any discrepancies.
- Though the cloud service provider is often the data processor, there are some cases where it takes the role of a data controller too.
- The precise role of the cloud service provider must be evaluated in each case and the obligation for data protection must be assigned to the right entity.

Data Protection Issues in the Cloud

- With the role of the data controller and data processor defined and the level of obligation stated, cloud customers must now evaluate the technical aspects of the provider and learn how they promise to deliver services within the established expectations of protection.
- Failing this, the following data protection issues can be expected in the cloud environment:
  - Lack of interoperability and data portability
  - Lack of integrity that arises from sharing of resources
  - Inability to ensure data compliance measures
  - Lack of proper data isolation in the multitenant environment
- Data protection risks are further amplified when the cloud service provider involves multiple tiers of sub-processors/ sub-contractors and data transfer happens between different countries.

Data Protection Laws

- Prior to 2011, the Indian judiciary system did not provide space for clear - cut laws pertaining to data protection.
- However with the enhancement of the data protection laws in the European Union, Information Technology Rules 2011 came into place.
- Under this act, corporate bodies, Indian government and information providers were subjected to sensible security practices.
- In addition to this, there are other laws within the Indian Penal Code (IPC) that can assist in practising a reasonable level of security while handling data in the cloud

Laws that Protect Data in India

Law/Act/Rights	Explanation
The Information Technology Act(Section 43A)	When a corporate body causes a "wrongful loss or wrongful gain" due to its negligence in maintaining a fair level of security of data, then it is liable to the compensation to the person affected.
The Information Technology Act(Section 72 A)	Privacy breach which may result in imprisonment for up to 3 years and penalty that may extend up to five lakhs.
Right to Privacy (Article 19 and 21)	Right to privacy (applicable to data privacy as well)

DATA PRIVACY AND SECURITY ISSUES

- U.S. Data Breach Notification Requirements
- U.S. Federal Law Compliance
- International Data Privacy Compliance
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
- Australia Privacy Act.

- **U.S. Data Breach Notification Requirements:**

  Data breach: it is a loss of unencrypted electronically stored personal information. server compromised, loss of a thumb drive, or theft of a laptop or cell phone

- Avoid it as it will effect both cloud providers and users of cloud services.
- User's viewpoint: risk of identity theft, credit or debit card fraud.
- Provider's viewpoint: financial harm, potential for lawsuits, Federal Trade Commission (FTC) investigations, loss of customers, and damage to reputation
- Almost all 50 states in the United States now require company notification of affected persons and require details of when their information had been compromised or upon the occurrence of a data breach.
- Because of these laws business customers have expanded their contract of obligations and have shifted the risk of harm towards providers.

- **U.S. Federal Law Compliance:**

1. GrammLeachBliley Act: Financial Privacy Rule.(GLB Act)

- This act requires financial institutions implement procedures to ensure the confidentiality of personal information and to protect against unauthorized access to the information.
- The cloud provider under this act must ensure:

  (1) comply with the relevant portions of GLB by demonstrating how it prevents unauthorized access to information,

  (2) contractually agree to prevent unauthorized access, or

  (3) both of the above.

2. The Role of the FTC: Safeguards Rule and Red Flags Rule.

- The Federal Trade Commission Act has been given authority to protect consumers and their personal information.
- The Safeguards Rule mandated by GLB and enforced by the FTC requires that all businesses significantly involved in the provision of financial services and products have a written security plan to protect customer information.
- The plan must include the following elements
  - Designation of one or more employees to coordinate its information security program;
  - Identification and assessment of the risks to customer information in each relevant area of the company's operation, and evaluation of the effectiveness of the current safeguards for controlling these risks;
  - Designing and implementing a safeguards program, and regularly monitoring and testing it;
  - Selection of service providers that can maintain appropriate safeguards;
  - Evaluation and adjustment of the program in light of relevant circumstances, including (a) changes in the firm's business or operations or (b) the results of security testing and monitoring.

3. Red Flag Rules:

- These rules are intended to curb identity theft by having financial institutions identify potential “red flags” for activities conducted through the organization’s systems that could lead to identity theft.
- The rules apply to financial institutions or those that hold credit accounts.
- The organizations covered by these rules must have a written identity theft program to detect specific activities that could indicate identity theft.

4. Health Insurance Portability and Accountability Act & HITECH Act.

- The Health Information Technology for Economic and Clinical Health Act (HITECH ACT) requires notification of a breach of unencrypted health records for all covered entitites that are required to comply with the Health insurance Portability and Accountability Act of 1996 (HIPAA)

5. USA PATRIOT Act

- United States Congress passed the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act” (USA PATRIOT Act) of 2001 which has significant implications for the cloud provider seeking to maintain the privacy of data it holds.
- For example, the Act allows the installation of devices to record all routing ,addressing, and signalling information kept by a computer.

International Data Privacy Compliance:

- European Union Data Privacy Directive. In 1995, the European Union (EU) passed the "European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Movement of Such Data Privacy Directive" (Directive).
- The Directive says:
  - Countries part of EU pass law that covers business and consumer data of government and private.
  - covers written, oral, electronic, and Internet-based data that reside in the EU.
  - EU personal data is sent anywhere must have an adequate level of data protection as measured by EU standards.
  - Data controller implement appropriate technical and organizational controls to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.
  - There should be written contract between a data controller and a data processor
  - Data cannot leave the EU unless it goes to a country that ensures an "adequate level of protection."

- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).
- PIPEDA is intended to "support and promote electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances. . ." .
- Canada, taken an organization-to-organization approach to privacy.
- In essence, organizations are held accountable for the protection of personal information it transfers to third parties, whether such parties are inside or outside of Canada.
- The law is enforced through contractual arrangements between entities, regardless of their geographic location.

- Australia Privacy Act.
- Australia's Privacy Act is based on

  (a) "Information Privacy Principles" that apply to the public sector and

  (b) "National Privacy Principles" that apply to the private sector.

- These principles address public and private sector use, disclosure, and management of personal data, among other things.
- The Office of the Privacy Commissioner expects that Australian organizations will ensure:

  (1) take steps to ensure that the personal information it holds is accurate, up-to-date, and secure and

  (2) protect personal information that it transfers outside Australia.

CLOUD CONTRACTING MODELS

While engaging with cloud service providers, there are few models that are available in the industry - that an organisation can assess and adopt. They are:

- Standard Contract
- Negotiated Contract
- Time-bound Contract

Standard Contract

- It contains the most common terms and conditions listed in the agreement.
- It talks about
  - The security and data protection standards followed by the cloud service providers
  - Capacity allocation and scalability terms
  - Location of the datacenters
  - Lock-in period (which talks about how long the client would sign up for)
  - Pricing structure and payments terms
  - Periodic audits and updates
- This model is also referred to as Click-Through Agreement - as the client just needs to review the contract and sign off with minimal or no changes.
- Both the client and the service provider know about all the agreement terms prevalent in the industry.

Negotiated Contract

- It talks about specific terms and conditions in the agreement as per the unique requirements of the organisation.
- Usually, organisations which serve business customers negotiate strict terms and conditions and they would insist the cloud service provider to abide to it.
- The additional terms that are negotiated includes
  - Key Management and Encryption requests
  - Specific policies and procedures
  - Standard data transmission protocols as per the sector
  - API Integration and related set of guidelines
  - Contingency measures and action plan
  - Administrative roles and responsibilities etc.
- The more sensitive the data being handled, stricter the terms and conditions would be.

Time-bound Contract

- This is either a standard contract (or) a negotiated contract whole validity is for a specific period.
- This ensures efficiency in services provided and move to the better ones if in case there are issues with existing vendors.
- This holds true for cloud service providers as well. If the organisation is happy with a specific cloud service provider whom they have trusted their data with, then they would renew it after the time frame in the contract gets over.
- If they are unhappy (or) if they found any discrepancies with the existing cloud service provider, then they would change them after a certain period.
- Some of the multinational corporations are known to levy heavy penalties for their vendors who don't comply with the contracts. The industrial term for such activity is “Contract Deviation”.
- If the cloud service provider is said to deviate from the contracts, then they might end up paying heavy penalties and in some cases, also face law suits. In such cases, the contract is terminated immediately and the data is moved to other third party service providers.

CLOUD CONTRACTING MODELS

1. Licensing Agreements Versus Services Agreements

Summary of Terms of a License Agreement.

a. A traditional software license agreement is used when a licensor is providing a copy of software to a licensee for its use
b. This copy is not being sold or transferred to the licensee, but a physical copy is being conveyed to the licensee.
c. The software license is important because it sets forth the terms under which the software may be used by the licensee.
d. It also provides a mechanism for the licensor of the software to retrieve the copy it provided to the licensee
e. In the case of infringement the license agreement provides a mechanism for the licensor to repair, replace, or remove the software from the licensee's possession

Summary of Terms of a Service Agreement

a. It is primarily designed to provide the terms under which a service can be accessed or used by a customer.

b. The service agreement may also set forth quality parameters around which the service will be provided to the users.

Value of Using a Service Agreement in Cloud Arrangements

a. In each of the three permutations of cloud computing (SaaS, PaaS, and IaaS), the access to the cloud-based technology is provided as a service to the cloud user.

b. A service agreement covers all the basic terms and conditions that provide adequate protection to the cloud user without committing the cloud provider to risk and liability attendant with the licensing of the software.

2. On-Line Agreements Versus Standard Contracts

a. There are two contracting models under which a cloud provider will grant access to its services.

b. The first, the on-line agreement, is a click wrap agreement with which a cloud user will be presented before initially accessing the service.

c. There is complete inequality in bargaining power in click wrap agreements because there is no ability to negotiate them.

d. The click wrap is currently the most commonly used contracting model.

e. The second model, the standard, negotiated, signature-based contract.

f. As larger companies move to the cloud (especially the public cloud),or more mission-critical applications or data move to the cloud, the cloud user will most likely require the option or a more robust and user-friendly agreement.

3. The Importance of Privacy Policies Terms and Conditions

a. The privacy policy of a cloud provider is an important contractual document for the cloud user to read and understand.

b. In its privacy policy the cloud provider will discuss in detail as what it is doing to protect and secure the personal information of a cloud user and its customers.

c. By reviewing the privacy policy a cloud user can analyze that whether the cloud provider is in full compliance with laws or there is a chance of data compromise.

d. On the basis of privacy protection policies a cloud user can differentiate and choose cloud provider.

e. The cloud provider should be explicit in its privacy policy and fully describe what privacy security, safety mechanisms, and safety features it is implementing.

Risk Allocation and Limitations of Liability

a. The limitation of liability in an agreement sets forth the maximum amount the parties will agree to pay one another should there be a reason to bring some sort of legal claim under the agreement.
b. Contractual risk is not distributed evenly between the parties.
c. Some cloud providers disclaim all liability in their agreements, even disclaiming liability if they are at fault or negligent in their performance.
d. Over time, cloud services will be provided under both types of contracts.
e. For mission-critical deployments the cloud provider will likely take on much more significant financial liability and contractual risk as part of the deal.
f. This risk and liability will be reflected in the negotiated contract.
g. The cloud user will pay a fee premium for shifting the liability and contractual risk to the cloud provider

Jurisdictional issues raised by virtualization and data location

- Jurisdiction is defined as a court's authority to judge acts committed in a certain territory.
- The geographical location of the data in a cloud computing environment will have a significant impact on the legal requirements for protection and handling of the data. The various issues are:
  - Virtualization and Multi-tenancy
  - The Issues Associated with the Flexibility of Data-Location
  - Other Jurisdiction Issues like:
    - Confidentiality and Government Access to Data.
    - Subcontracting.
  - International Conflicts of Laws

Virtualization and Multi-tenancy

- **Virtualization:** In this one physical server simulates being several separate servers.
- For example, in an enterprise setting, instead of having a single server dedicated to payroll systems, another one dedicated to sales support systems, and still a third dedicated to asset management systems, virtualization allows one server to handle all of these functions.. Each one of these simulated servers is called a virtual machine.
- Some benefits of virtualization are
  - Need for less hardware
  - Consumption of less power
  - Provides greater utilization and maximization of hardware processing power
  - lower expenses associated with operating a data center.
- Virtualization across a single or multiple data centers makes it difficult for the cloud user or the cloud provider to know what information is housed on various machines at any given time.
- The emphasis in the virtualized environment is on maximizing usage of available resources no matter where they reside.

- **Multi-tenancy :** Multi-tenancy refers to the ability of a cloud provider to deliver software as-a-service solutions to multiple client organizations (or tenants) from a single, shared instance of the software.
- The cloud user's information is virtually, not physically, separated from other users.
- The major benefit of this model is cost-effectiveness for the cloud provider.
- Some risks or issues with the model for the cloud user include

  (a) the potential for one user to be able to access data belonging to another user (b) difficulty to back up and restore data

The Issues Associated with the Flexibility of Data-Location

- One of the benefits of cloud computing
  - From the cloud provider's perspective : to move data among its available data centre resources as necessary to maximize the efficiencies of it overall system.
  - From a technology perspective : this ability to move data is a reasonably good solution to the problem of under utilized machines.
- Data Protection:
  - From a legal perspective, flexibility of data location potentially challenges the governing law provision in the contract.
  - If the law specified in the contract requires a certain treatment of the data, but the law of the jurisdiction where the data resides requires another treatment, there is an inherent conflict that must be resolved.

Other Jurisdiction Issues

- **Confidentiality and Government Access to Data:**
  - In the cloud environment, given the potential movement of data among multiple jurisdictions, the data housed in a jurisdiction is subject to the laws of that jurisdiction, even if its owner resides elsewhere.
  - Given the inconsistency of confidentiality protection in various jurisdictions, a cloud user may find that its sensitive data are not entitled to the protection with which the cloud user may be familiar, or that to which it contractually agreed.
  - A government's ability to access data is also directly connected to the jurisdiction in which the data reside. If the jurisdiction has laws that permit its government to get access to data (with or without notice to the cloud user or the individual or entity that owns the data), that data may be subject to interception by the government.

- Subcontracting :
- A cloud provider's use of a third-party subcontractor to carry out its business may also create jurisdictional issues. The existence or nature of a subcontracting relationship is most likely invisible to the cloud user.
- As a result, the risk associated with the acts of or the locations of the subcontractor are difficult to measure by the cloud user.

International Conflicts of Laws

- The body of law known as “conflict of laws” acknowledges that the laws of different countries may operate in opposition to each other, even as those laws relate to the same subject matter. In such an event, it is necessary to decide which country’s law will be applied.
- Every nation is sovereign within its own territory. That means that the laws of that nation affect all property and people within it, including all contracts made and actions carried out within its borders.
- When there is either

  (1) no statement of the law that governs a contract,

  (2) no discussion of the rules regarding conflicts of laws in the agreement, or

  (3) a public policy in the jurisdiction which mandates that the governing law in the agreement will be ignored, the question of which nation’s law will apply to the transaction will be decided based on a number of factors and circumstances surrounding the transaction.

COMMERCIAL AND BUSINESS CONSIDERATIONS—A CLOUD USER'S VIEWPOINT

- Many of the considerations presented below may manifest in the contractual arrangements between the cloud provider and cloud user:

- Minimizing Risk
- Viability of the Cloud Provider
- Protecting a Cloud User's Access to Its Data

Minimizing Risk

- Maintaining Data Integrity: A cloud user should expect contractual provisions obligating a cloud provider to protect its data, and the user ultimately may be entitled to some sort of contract remedy if data integrity is not maintained.
- Accessibility and Availability of Data/SLAs : The service-level agreement (SLA) is the cloud provider's contractually agreed-to level of performance for certain aspects of the services. The cloud user should get a clear understanding of the cloud provider's performance record regarding accessibility and availability of services and data.
- Disaster Recovery: It is important for both parties to have an understanding of the cloud provider's disaster recovery plan.

Viability of the Cloud Provider

- A potential cloud user should seek to get some understanding about the viability of the cloud provider, particularly early-stage cloud providers.
- A cloud user will make an investment in

  (1) integrating the cloud services into its business processes and

  (2) migrating the data from its environment into the cloud environment.

  The lack of standardization among cloud providers will make it difficult and potentially costly for the cloud user to transition from one cloud provider to the other.

Protecting a Cloud User's Access to Its Data

- This section introduces three scenarios that a cloud user should contemplate when placing its data into the cloud.
- Scenario 1: Cloud Provider Files for Bankruptcy.
- Scenario 2: Cloud Provider Merges or Is Acquired.
- Scenario 3: Cloud Provider Ceases to Do Business.

Scenario 1: Cloud Provider Files for Bankruptcy.

- Data may be consumer-type data, or it may be the business-level transaction data of the bankrupt cloud provider's business customers.
- Regardless of the type of data, the interests of the cloud provider and the cloud user with respect to the data will most likely diverge upon the filing of a bankruptcy.
- The bankrupt cloud provider wants to create as much value in the company as possible to facilitate various exits from the bankruptcy (of which an acquisition may be one).
- Consumer-level data is a valuable asset that might be transferred in a bankruptcy. The cloud user is probably equally concerned about keeping its data (regardless of type) private and out of third-party hands without its consent.
- The cloud user's options are closely tied to the language of the privacy policy of the cloud provider.

Scenario 2: Cloud Provider Merges or Is Acquired.

- Any number of situations could lead to the transfer of the cloud provider's operation and the information associated with it, to a third party.
- The most likely scenarios include the merger or acquisition of the business, or the sale of a business unit or service line.
- Since a cloud user is unlikely to be notified prior to the closing of a transaction, once again the privacy policy is the best place to look to determine what would happen to user data in such an event.

Scenario 3: Cloud Provider Ceases to Do Business.

- If there is an orderly shutdown of a cloud provider as part of its cessation activities, the cloud user may have the ability to retrieve its data as part of the shut-down activities.
- In the event that a cloud provider simply walks away and shuts down the business, cloud users are most likely left with only legal remedies, filing suit, for example, to attempt to get access to its data.