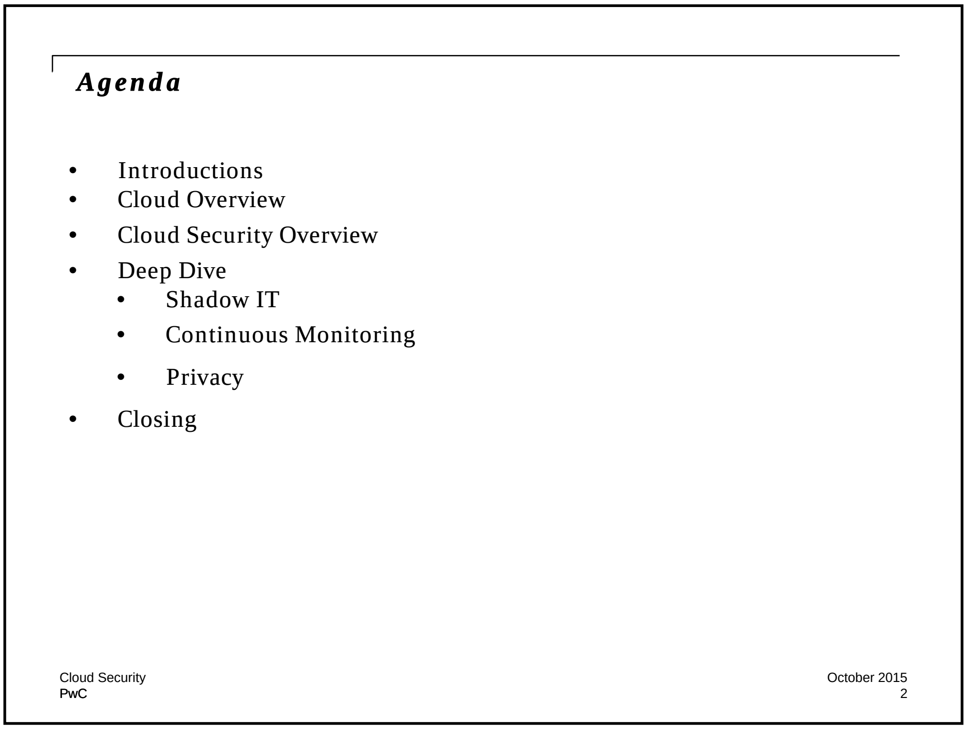
www.pwc.com

Atlanta Regional Compliance & Ethics Conference

Security in the Cloud

October 2015

pwc

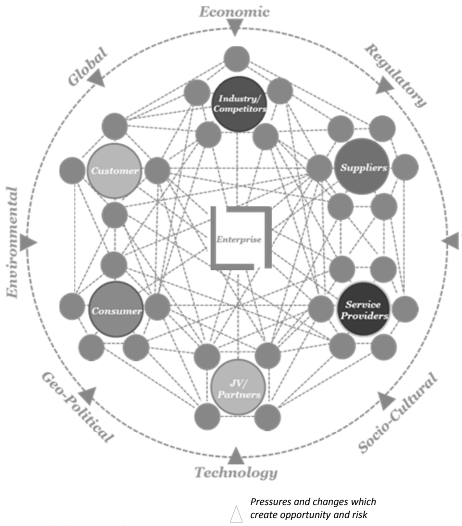


Agenda

- Introductions
- Cloud Overview
- Cloud Security Overview
- Deep Dive
  - Shadow IT
  - Continuous Monitoring
  - Privacy
- Closing

Cloud Overview

The Global Business Ecosystem

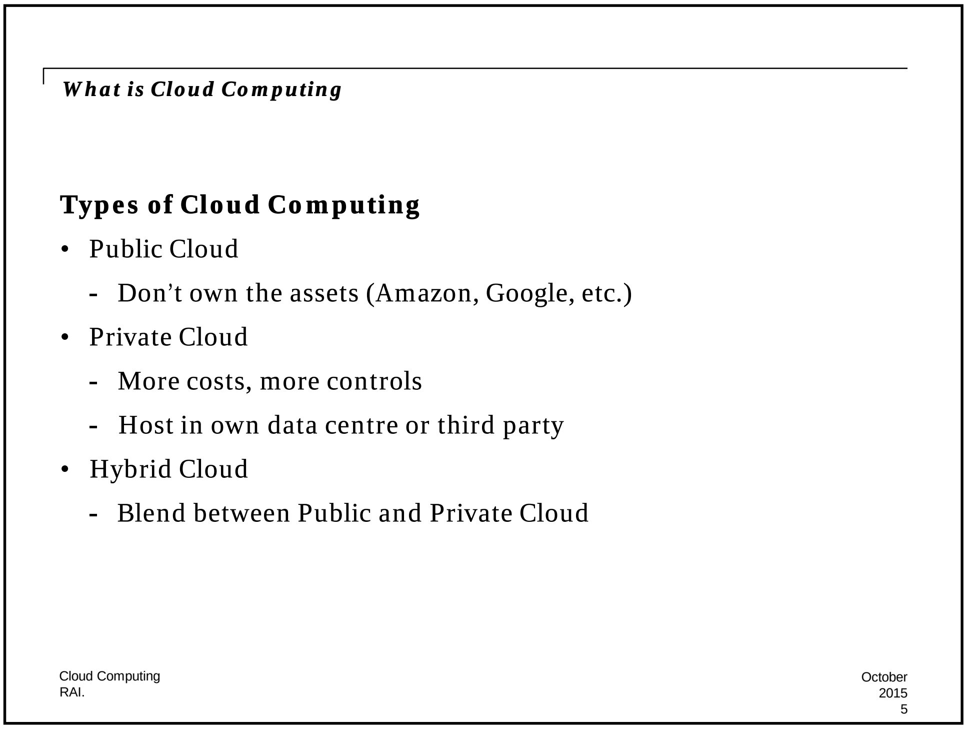


Pressures and changes which create opportunity and risk

Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly interconnected, integrated, and interdependent.

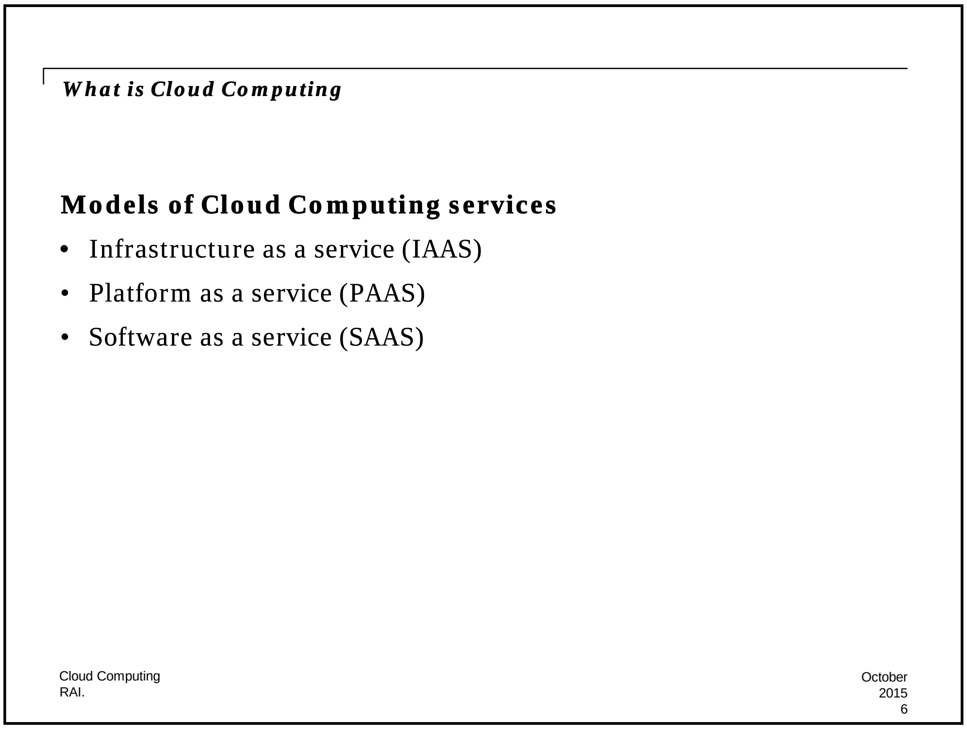
- The ecosystem is **built around a model of open collaboration and trust**—the very attributes being exploited by an increasing number of global adversaries.
- Constant **information flow is the lifeblood of the business ecosystem**. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- **Adversaries are actively targeting critical assets** throughout the ecosystem—significantly increasing the exposure and impact to businesses.

Years of underinvestment in security and privacy has impacted organizations' ability to adapt and respond to evolving, dynamic cyber risks.



Types of Cloud Computing

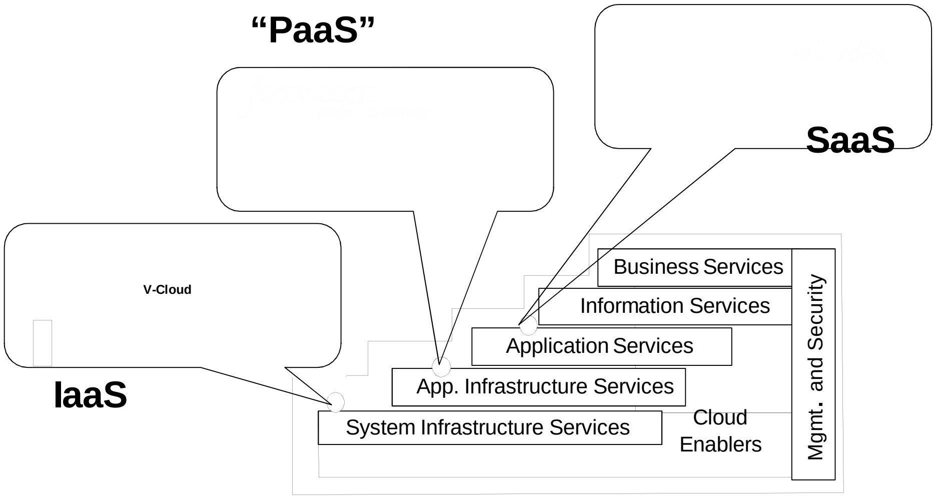
- Public Cloud
  - Don’t own the assets (Amazon, Google, etc.)
- Private Cloud
  - More costs, more controls
  - Host in own data centre or third party
- Hybrid Cloud
  - Blend between Public and Private Cloud



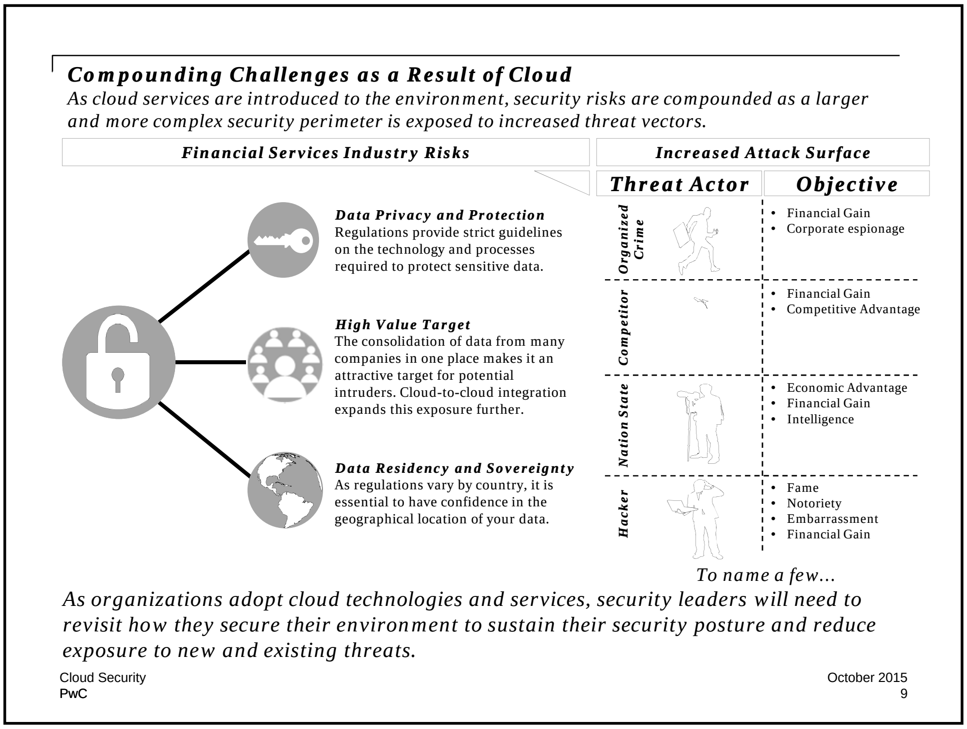
Models of Cloud Computing services

- Infrastructure as a service (IAAS)
- Platform as a service (PAAS)
- Software as a service (SAAS)

What is Cloud Computing



Cloud Security Overview



Compounding Challenges as a Result of Cloud

As cloud services are introduced to the environment, security risks are compounded as a larger and more complex security perimeter is exposed to increased threat vectors.

Financial Services Industry Risks

Data Privacy and Protection
Regulations provide strict guidelines on the technology and processes required to protect sensitive data.

High Value Target
The consolidation of data from many companies in one place makes it an attractive target for potential intruders. Cloud-to-cloud integration expands this exposure further.

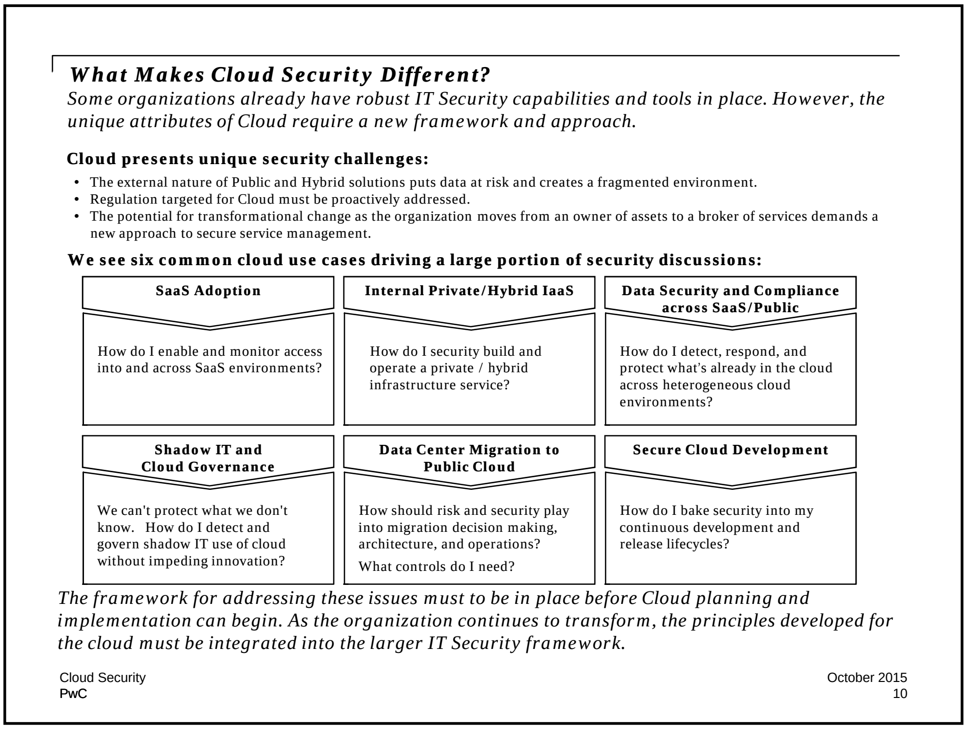
Data Residency and Sovereignty
As regulations vary by country, it is essential to have confidence in the geographical location of your data.

Increased Attack Surface

Threat Actor	Objective
Organized Crime	Financial Gain Corporate espionage
Competitor	Financial Gain Competitive Advantage
Nation State	Economic Advantage Financial Gain Intelligence
Hacker	Fame Notoriety Embarrassment Financial Gain

To name a few...

As organizations adopt cloud technologies and services, security leaders will need to revisit how they secure their environment to sustain their security posture and reduce exposure to new and existing threats.



What Makes Cloud Security Different?

Some organizations already have robust IT Security capabilities and tools in place. However, the unique attributes of Cloud require a new framework and approach.

Cloud presents unique security challenges:

- The external nature of Public and Hybrid solutions puts data at risk and creates a fragmented environment.
- Regulation targeted for Cloud must be proactively addressed.
- The potential for transformational change as the organization moves from an owner of assets to a broker of services demands a new approach to secure service management.

We see six common cloud use cases driving a large portion of security discussions:

SaaS Adoption
How do I enable and monitor access into and across SaaS environments?

Internal Private/Hybrid IaaS
How do I security build and operate a private / hybrid infrastructure service?

Data Security and Compliance across SaaS/Public
How do I detect, respond, and protect what's already in the cloud across heterogeneous cloud environments?

Shadow IT and Cloud Governance
We can't protect what we don't know. How do I detect and govern shadow IT use of cloud without impeding innovation?

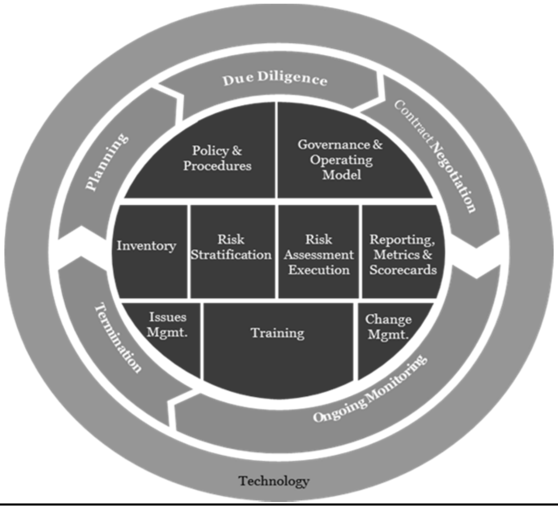
Data Center Migration to Public Cloud
How should risk and security play into migration decision making, architecture, and operations?
What controls do I need?

Secure Cloud Development
How do I bake security into my continuous development and release lifecycles?

The framework for addressing these issues must to be in place before Cloud planning and implementation can begin. As the organization continues to transform, the principles developed for the cloud must be integrated into the larger IT Security framework.

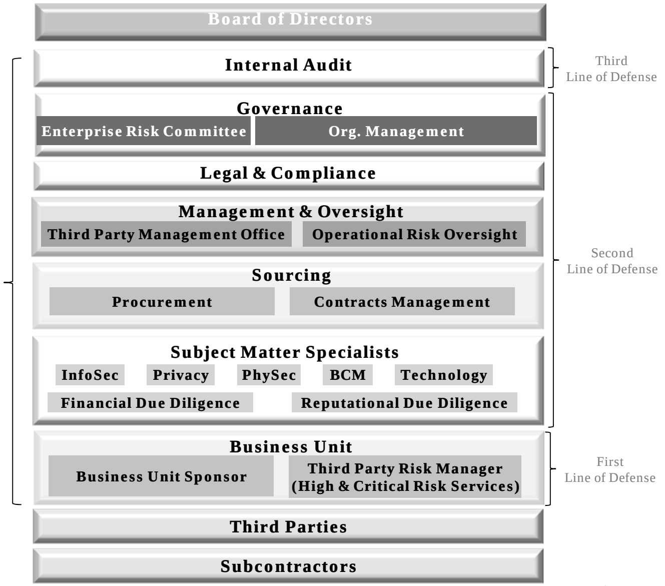
A Framework for Managing Cloud Security Risk

.



A robust Third Party Risk Management program is based on adoption of key building blocks, and successfully linking the program strategy, policies and processes together.

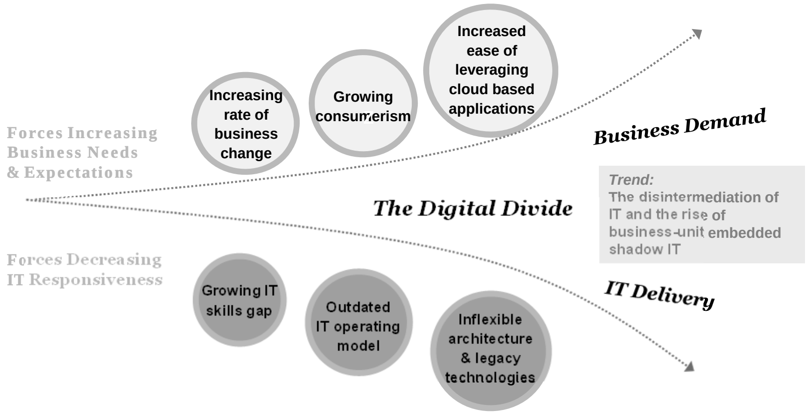
A Framework for Managing Cloud Security Risk.



Third Party Risk Management roles and responsibilities impact each aspect of the three lines of defense model

Deep Dive: Shadow IT

Cloud is a Contributor to the Growing "Digital Divide" Between Business and IT



Increasing rate of business change

Growing consumerism

Increased ease of leveraging cloud based applications

Business Demand

Forces Increasing Business Needs & Expectations

The Digital Divide

Trend:
The disintermediation of IT and the rise of business-unit embedded shadow IT

Forces Decreasing IT Responsiveness

IT Delivery

Growing IT skills gap

Outdated IT operating model

Inflexible architecture & legacy technologies

Forward thinking IT Leaders are challenging traditional assumptions around IT's role in the enterprise and it's operating model

Shadow IT – Security Risks, Impact, and Recommendations

Shadow IT adopts and operates technology services (IaaS, PaaS, SaaS) without consulting and / or leveraging centralized IT skills, standards, and capabilities. This can lead to increased risk exposure for organizations.

#	Risk / Impact	Recommendation / Good Practice
1	***You can't protect what you don't know:*** Lack of awareness of which cloud services are consumed by the organization possess significant risk that those services are not compliant with corporate security policy and pose increased risk of data loss, introduction of malware, etc.	• Assess existing network traffic to detect 3rd party services being used by Shadow IT (tools like those from PAN, CloudLock, CipherCloud, SkyHigh, etc.). • Implement policy and standards / technologies that will incentivize the business to use more controlled services.
2	***Vulnerabilities:*** Systems used / supported by Shadow IT can contain un-detected / managed vulnerabilities as capabilities to do such are often provided / operated at the central IT Security function. Vulnerabilities can include mis-configuration, lack of patching, outdated software, infected systems, etc.	• Consumers should assess 3rd parties with robust vendor risk analysis framework before contracting / using the service. • Organizations should adopt cloud-specific vulnerability scanning and detection solutions (and triage processes) and run them continuously against known cloud systems where possible. • Identified vulnerabilities should be prioritized and remediated.
3	***Regulatory Compliance:*** Shadow IT are often not focused on or aware of all the regulatory requirements the organization must comply (such as Basel II, COBIT, FISMA, HIPAA or PCI DSS) with and how to achieve them. This increases risk of non-compliance and associated penalties.	• Ensure policies require all services to be vetted for compliance requirements and implications before acquisition. • Assess existing cloud services discovered in #1 above for these risks and ways the Shadow IT is controlling / ensuring compliance.

Shadow IT – Security Risks, Impact, and Recommendations cont'd

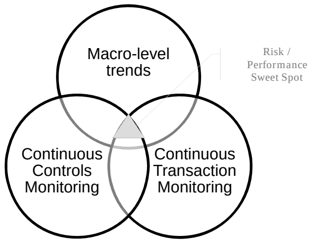
#	Risk / Impact	Recommendation / Good Practice
4	***Data Loss****:* Shadow IT increases risk of data loss, exposure, alteration, interruption of business services, etc. as leading-practice controls are not implemented or operated. Implementing such controls are viewed as costly and complex.	Strong policy for data protection should exist to give guidance to business and shadow IT on protecting data. Flexible, easy to use, "emphasis on detection" - data protection controls should exist that enable the innovation the business and IT demand.
5	***Loss of Financial Leverage****:* Shadow IT increases risk of duplicate and or overlapping relationships with vendors → this reduces the organizations negotiating leverage.	Establishing SLAs and contracts to find providers will help quickly assess similar cloud solutions.
6	***Security Controls****:* Shadow IT can lack the expertise, systems, and processes to apply proper security controls – such as identity and access management, monitoring and incident response, etc.	Define flexible, cloud-native, "as a service" solutions with built-in integration for the Shadow IT services most in-demand. Establish flexible, nimble, enterprise security controls standards and services to enable and product cloud-adoption.

Deep Dive: Continuous Monitoring & Threat Intelligence

Continuous Monitoring – Overview

- Continuous Monitoring (CM) is a feedback mechanism used by management to ensure that controls operate as designed and transactions are processed as prescribed.
- New architectures, revised process and data flows, and dis-integrated consumption of Cloud adoption are making intelligent detection and response to risks more challenging.
- Continuous monitoring for cloud includes:
  - *Coordinated and multi-dimension approach:* including security controls and configurations, transactions, and business context
  - *Risk-based:* priority on higher risk data, systems, transactions
  - *Integration with Security Incident and Event Monitoring*
  - *Big-data enabled:* Due to increased volume of unstructured log data from across 3rd party and internal services – organizations are adopting big-data analytics engines to identify risks across a broader landscape
  - *Business-centric:* While response to technical anomalies is important, organizations must define and seek actionable intelligence from their cloud use
  - *Increased sophistication*: e.g anomaly detection against access usage patterns, etc.

Continuous Monitoring Framework

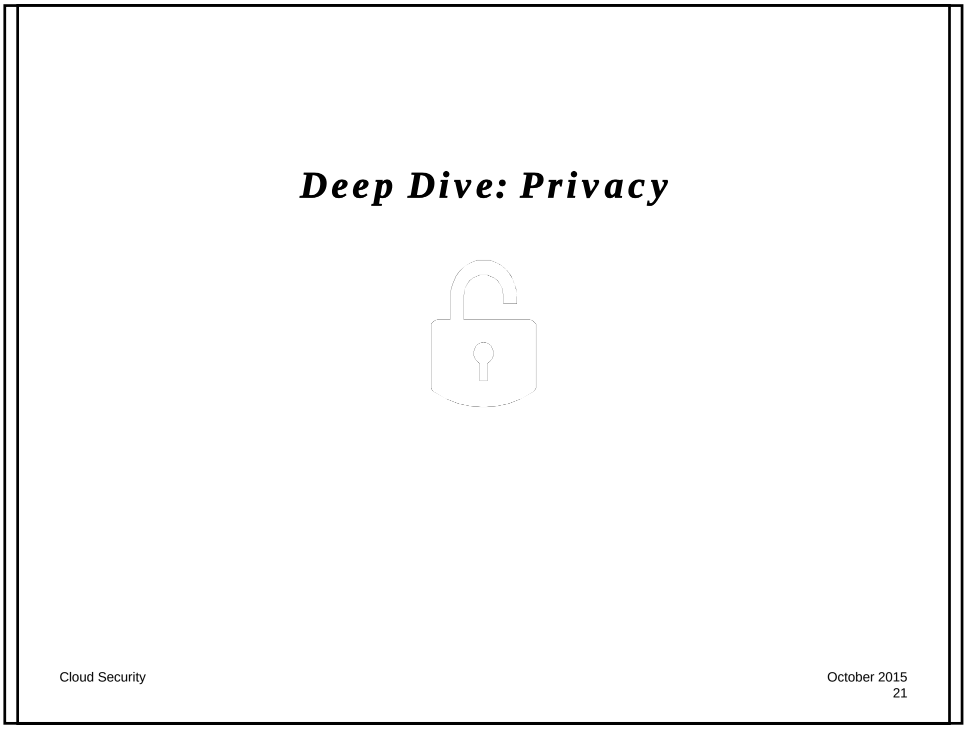

Macro-level trends
Risk / Performance Sweet Spot
Continuous Controls Monitoring
Continuous Transaction Monitoring

Continuous Monitoring – Key Issues, Risks, and Recommendations

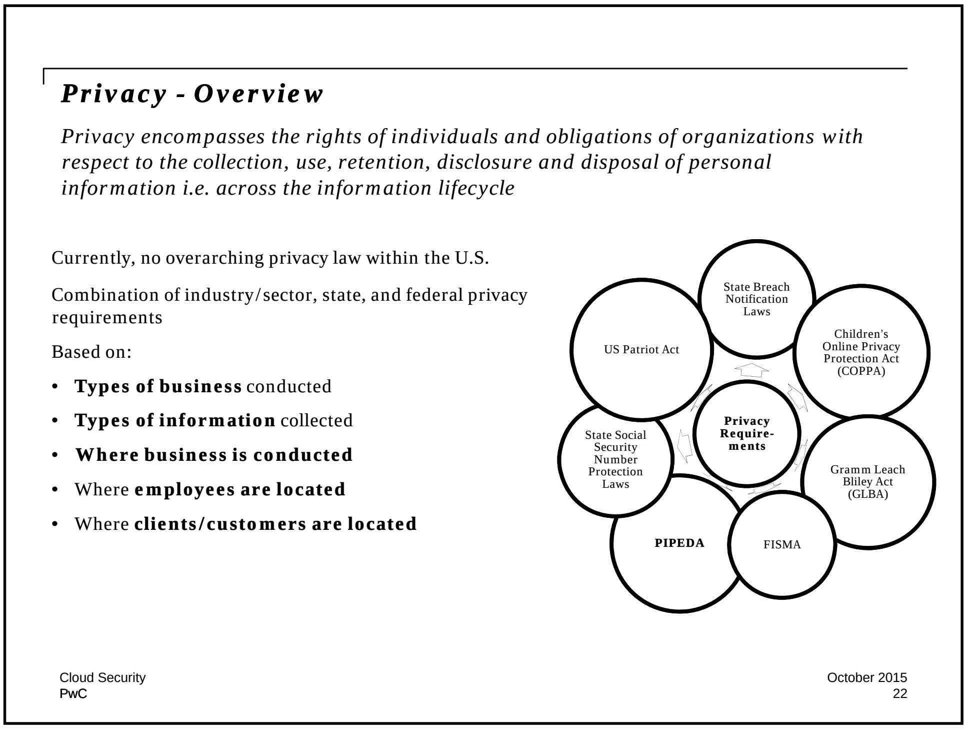
#	Risk / Impact	Recommendation / Good Practice
1	***One-dimensional view of cloud risks are limiting:*** Myopic logging and monitoring (e.g. only controls, only transactions, etc.) leaves the organization exposed to significant risks.	A multidimensional approach to continuous monitoring including • *Controls & Configuration Monitoring:* Establish configuration baselines for cloud environments and monitor for changes. Monitor and co-relate logs from key controls - i.e. private access, failed log-in attempts, etc. • *Transaction Monitoring*: Create rules and run tests against the actual flow of transactions, identify exceptions, anomalous patterns and trends, or other outliers contrary to KPIs • *Macro-level trends:* Incorporate external threat intelligence into monitoring environments. Tune monitoring to reflect business processes and objectives / context.
2	***Manual processes and log / event review times are insufficient:*** The rate of change, volume of log events, and decentralized nature of cloud use makes manual monitoring techniques wholly under-suited for risk-management in a cloud world. Furthermore, if data isn't reviewed / monitored on a timely basis – the log information diminishes in value.	Organizations should adopt an automated tooling-based approach for continuous monitoring (coupled with revised processes, and people as necessary). Key tooling requirements should provide: • *Support for multiple sources*: Pull information from a variety of sources, support open specifications such as the Security Content Automation Protocol (SCAP), • *Interoperability:* Offer interoperability with other products such as SIEM, help desk, inventory management, configuration management, and incident response solutions • *Compliance:* Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines • *Reporting and Metrics:* Provide reporting with the ability to tailor output and drill down from high-level, aggregate metrics to system-level metrics

Continuous Monitoring – Key Issues, Risks, and Recommendations Cont'd

#	Risk / Impact	Recommendation / Good Practice
3	***In-secure and uncompliant log retention***: Lack of prioritization of application log data and log data retention policies violates regulatory and risk management good practices.	• Define and apply security and retention policy to cloud logs and log environments. • Classify log data based on the system value (low, med, high impact). Consider the following risk-based log analysis guidance: low impact systems → every 1 to 7 days; moderate impact systems → every 12 to 24 hrs; high impact systems → six times a day.
4	***Failure to integrate continuous monitoring with Enterprise Risk Management:*** Financial, Regulatory, Fraud, and Operational risks will increase if ISCM is not linked with Enterprise Risk Management (ERM).	• Integrate continuous monitoring with ERM program. • ERM program to define what to monitor, how to monitor, and at what frequency to monitor • Includes exception-based remediation and control improvement program to identify exceptions or areas for improvement, communicate and correct them, and enhance processes.
5	***Cloud-to-Cloud interactions***: Organizations are increasingly facing scenarios where their data is transacting across multiple cloud environments (and not just the enterprise to a single cloud provider). Continuous monitoring must accommodate and include services, data, and transactions that occur across cloud environments.	• Assess cloud architectures, features, and contracts to ensure cloud to cloud monitoring is available. • Where feasible, implement logging and monitoring tools and processes to address these gaps.



Deep Dive: Privacy



Privacy - Overview

Privacy encompasses the rights of individuals and obligations of organizations with respect to the collection, use, retention, disclosure and disposal of personal information i.e. across the information lifecycle

Currently, no overarching privacy law within the U.S.

Combination of industry/sector, state, and federal privacy requirements

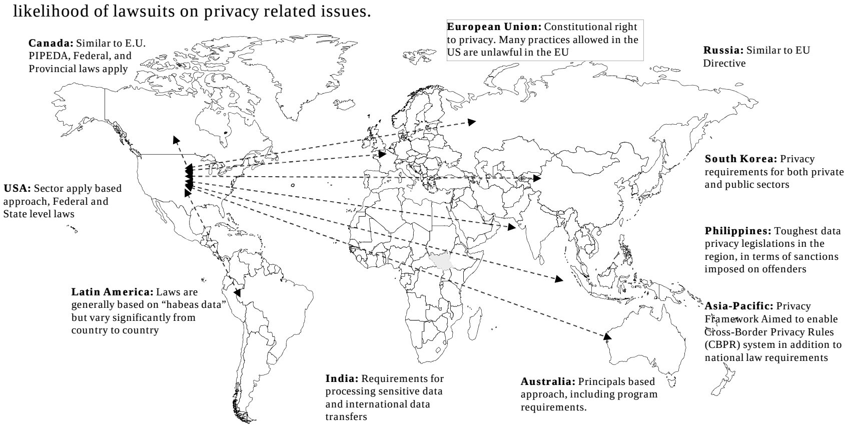
Based on:

- **Types of business** conducted
- **Types of information** collected
- **Where business is conducted**
- Where **employees are located**
- Where **clients/customers are located**

State Breach Notification Laws
Children's Online Privacy Protection Act (COPPA)
US Patriot Act
Privacy Require-ments
State Social Security Number Protection Laws
Gramm Leach Bliley Act (GLBA)
PIPEDA
FISMA

Global legal and regulatory landscape

Conducting business internationally and managing a global workforce becomes more challenging as an increasing numbers of privacy and data protection requirements may apply to the personal data that a global company collects, shares, uses and transmits – particularly where cross-border transfers occur. In addition to legal requirements, regulators have different abilities to enforce laws and areas of focus, which will impact the likelihood of lawsuits on privacy related issues.



European Union: Constitutional right to privacy. Many practices allowed in the US are unlawful in the EU

Canada: Similar to E.U. PIPEDA, Federal, and Provincial laws apply

Russia: Similar to EU Directive

South Korea: Privacy requirements for both private and public sectors

USA: Sector apply based approach, Federal and State level laws

Philippines: Toughest data privacy legislations in the region, in terms of sanctions imposed on offenders

Latin America: Laws are generally based on “habeas data” but vary significantly from country to country

Asia-Pacific: Privacy Framework Aimed to enable Cross-Border Privacy Rules (CBPR) system in addition to national law requirements

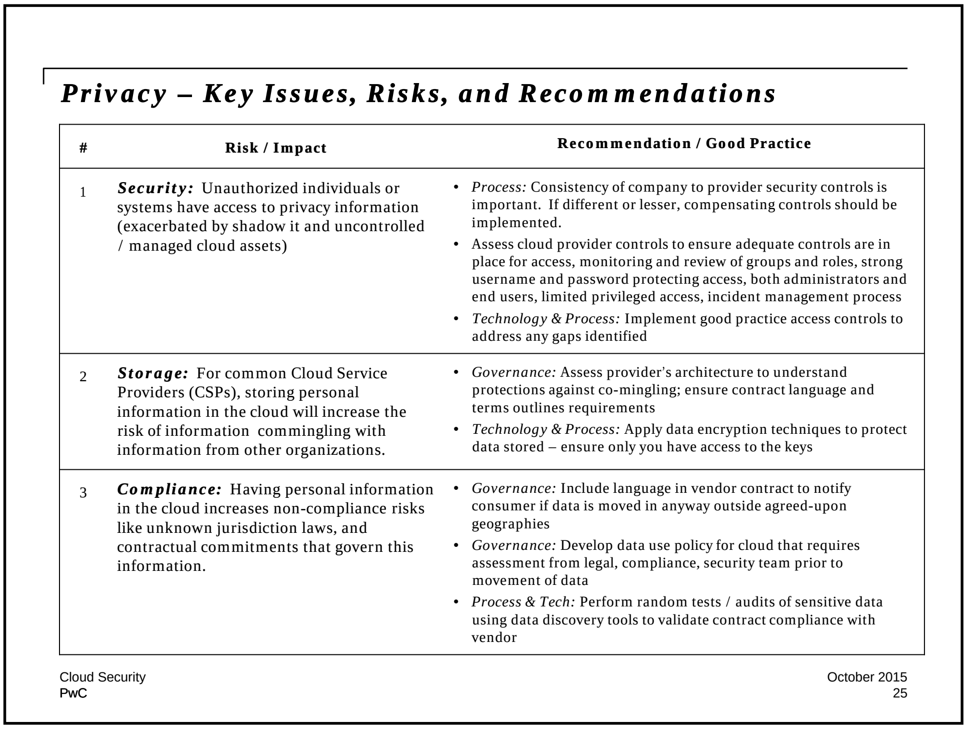
India: Requirements for processing sensitive data and international data transfers

Australia: Principals based approach, including program requirements.

Privacy – In the Cloud

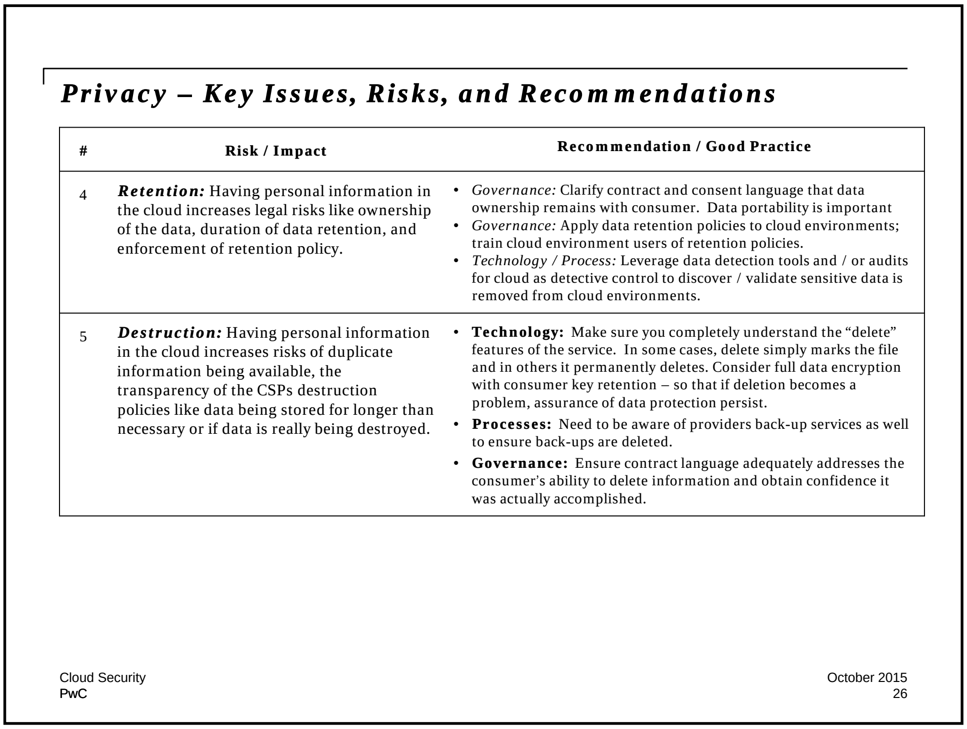
Organizations looking to adopt and transact in the cloud must answer the following:

- Have I **defined and classified** my sensitive/personal data?
- Do I know **how and where** my sensitive data will be collected, transmitted, shared, and stored, etc. across my cloud services and infrastructure?
- What are the **applicable privacy laws** for my business?
- How does my cloud adoption **affect/change my privacy risk**?
- **What must I do** to compensate for the change? What controls, process, procedures, and technology do I need to maintain compliance to privacy laws and risk levels?



Privacy – Key Issues, Risks, and Recommendations

#	Risk / Impact	Recommendation / Good Practice
1	***Security:*** Unauthorized individuals or systems have access to privacy information (exacerbated by shadow it and uncontrolled / managed cloud assets)	• *Process:* Consistency of company to provider security controls is important. If different or lesser, compensating controls should be implemented. • Assess cloud provider controls to ensure adequate controls are in place for access, monitoring and review of groups and roles, strong username and password protecting access, both administrators and end users, limited privileged access, incident management process • *Technology & Process:* Implement good practice access controls to address any gaps identified
2	***Storage:*** For common Cloud Service Providers (CSPs), storing personal information in the cloud will increase the risk of information commingling with information from other organizations.	• *Governance:* Assess provider's architecture to understand protections against co-mingling; ensure contract language and terms outlines requirements • *Technology & Process:* Apply data encryption techniques to protect data stored – ensure only you have access to the keys
3	***Compliance:*** Having personal information in the cloud increases non-compliance risks like unknown jurisdiction laws, and contractual commitments that govern this information.	• *Governance:* Include language in vendor contract to notify consumer if data is moved in anyway outside agreed-upon geographies • *Governance:* Develop data use policy for cloud that requires assessment from legal, compliance, security team prior to movement of data • *Process & Tech:* Perform random tests / audits of sensitive data using data discovery tools to validate contract compliance with vendor



Privacy – Key Issues, Risks, and Recommendations

#	Risk / Impact	Recommendation / Good Practice
4	***Retention:*** Having personal information in the cloud increases legal risks like ownership of the data, duration of data retention, and enforcement of retention policy.	• *Governance:* Clarify contract and consent language that data ownership remains with consumer. Data portability is important • *Governance:* Apply data retention policies to cloud environments; train cloud environment users of retention policies. • *Technology / Process:* Leverage data detection tools and / or audits for cloud as detective control to discover / validate sensitive data is removed from cloud environments.
5	***Destruction:*** Having personal information in the cloud increases risks of duplicate information being available, the transparency of the CSPs destruction policies like data being stored for longer than necessary or if data is really being destroyed.	• **Technology:** Make sure you completely understand the "delete" features of the service. In some cases, delete simply marks the file and in others it permanently deletes. Consider full data encryption with consumer key retention – so that if deletion becomes a problem, assurance of data protection persist. • **Processes:** Need to be aware of providers back-up services as well to ensure back-ups are deleted. • **Governance:** Ensure contract language adequately addresses the consumer's ability to delete information and obtain confidence it was actually accomplished.

Thank you

Aaron Shapiro
Director, Cybersecurity & Privacy
aaron.l.shapiro@us.pwc.com
(717) 542-2269

Toby Spry
Director, Cybersecurity & Privacy
Toby.a.spry@us.pwc.com
(678) 419-1443

PwC Thought Leadership on Cloud

Cloud, a necessary component of data center consolidation and IT agility

Protecting your brand in the cloud: Transparency and trust through enhanced reporting

A shift to cloud computing and its impact on revenue recognition

Leveraging the cloud – the new sourcing alternative

View: Cloud Computing Gets Strategic

Navigating Cloud Management

Navigating Security in the Cloud

Making the move to cloud-based ERP

Technology forecast – Issue 2 2011 – Decoding Innovation's DNA

Clouds in the enterprise: Navigating the path to business advantage

Security Among the Clouds

Global Software Leaders: Key players & market trends

Managing Cloud Migration

View, The real promise of cloud computing

10Minutes in the Cloud: Chief Executive Supplements

Additional Resources:

http://www.pwc.com/us/en/issues/cloud-computing/publications.jhtml

http://www.pwc.com/us/en/10minutes/cloud-computing.jhtml

http://cloudsolution.hosting.pwc.com/SitePages/Home.aspx

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.