



Cloud Computing and Security

ISACA Big 4 Information Security Forum

May 20, 2010

Arun Perinkolam, Manager

Deloitte & Touche LLP



Table of contents

• Key Messages	2
• Overview, trends and adoption	5
• Security and Risk management concerns	10
• Audit considerations	26
• Key Takeaways	36
• Food for Thought	37

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

Cloud: Key Messages



Key messages

Business models are shaping cloud adoption	Business models are evolving to partnerships and networks of companies, forming a product or service delivery chain to the end customer
Traditional IT is being challenged	Executives are demanding increased agility and highly collaborative IT architectures, challenging traditional IT and resulting in increased demand for cloud computing
Security & Privacy challenges are real, but not insurmountable	Many traditional risk assessment approaches apply, but new thinking may be required on risk acceptance
Many different cloud deployment models	With corresponding differences in risk and control requirements
Cloud deployment will further accelerate de-perimeterization	Highly collaborative, services oriented architecture required

Key messages (cont.)

Low risk applications with standardized workloads form the first wave	Examples of workloads being deployed include collaboration, high performance computing, development & test environments, integration with specific SAAS applications, etc.
Cloud providers are listening to their customers	And beginning to build industry specific solutions that will account for regulatory & compliance requirements (e.g. PCI Compliance, Email Retention and Archival, etc.)
Cloud Strategy and business case approach is the first step in the path to adoption	Option Analysis should be conducted to develop a decision on the optimal cloud model, vendor, cost, service quality, etc. TCO must factor in the cost of risk and compliance requirements.

Cloud Overview, Trends and Adoption



Definition of cloud computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.

Essential Characteristics:

1. On-demand self-service.
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured Service

Deployment Models:

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

Service Models:

1. Cloud Software as a Service (SaaS)
2. Cloud Platform as a Service (PaaS)
3. Cloud Infrastructure as a Service (IaaS)

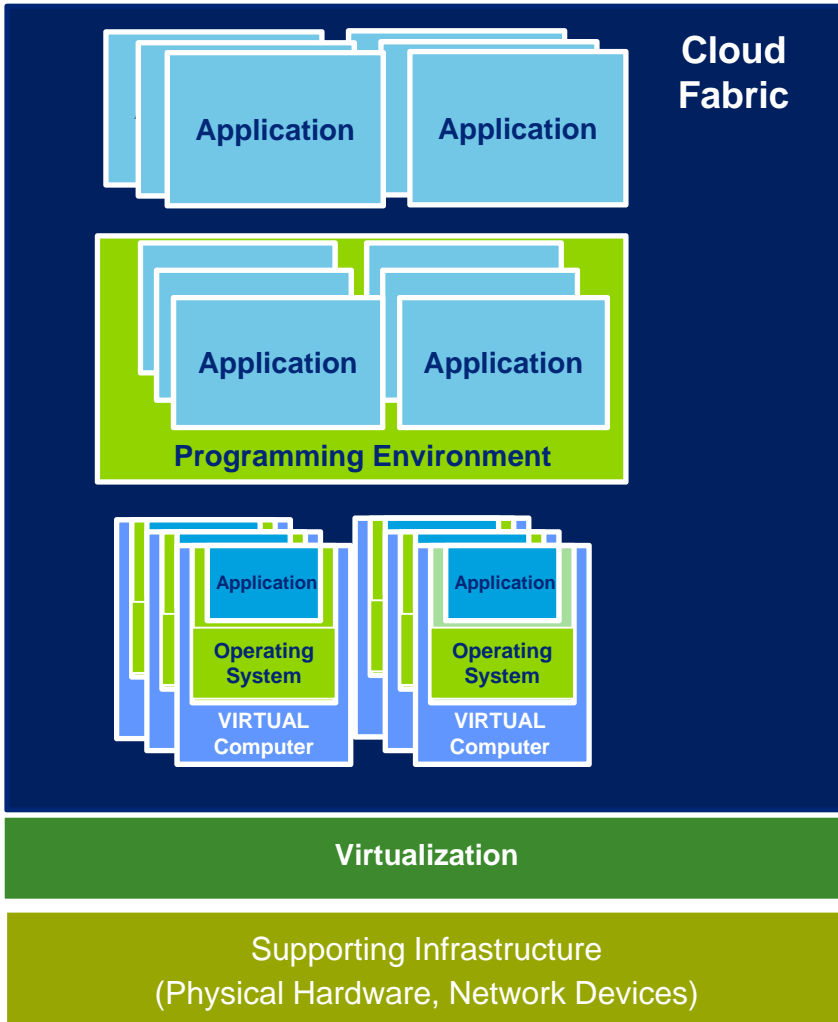
Source: <http://csrc.nist.gov/groups/SNS/cloud-computing/>

Cloud computing delivery models, based on their characteristics and purpose

Cloud computing technology is deployed in different ways, with varying internal or external ownership and technical architectures

Vendor cloud (External)	Cloud computing services from vendors that can be accessed across the Internet or a private network, using one or more data centers, shared among multiple customers, with varying degrees of data privacy control. Sometimes called “public” cloud computing.
Private cloud (Internal)	Computing architectures modeled after vendor clouds, yet built, managed, and used internally by an enterprise; uses a shared services model with variable usage of a common pool of virtualized computing resources. Data is controlled within the enterprise.
Hybrid cloud	A mix of vendor cloud services, internal cloud computing architectures, and classic IT infrastructure, forming a hybrid model that uses the best-of-breed technologies to meet specific needs.
Community cloud	Community clouds are used across organizations that have similar objectives and concerns, allowing for shared infrastructure and services. Community clouds can be deployed using any of the three methods outlined above, simplifying cross-functional IT governance.

Visualizing the differences



Software as a service (SaaS)

SaaS covers the range of application that are licensed for use as services provided to customers on demand typically across the Web.

Platform as a service (PaaS)

The PaaS model makes all of the facilities required to support the complete life cycle of building and delivering Web applications and services entirely available from the Internet.

Infrastructure as a service (IaaS)

IaaS is the delivery of computer infrastructure as a service. Rather than purchasing servers, software, data center space, or network equipment, clients instead buy those resources as a fully outsourced service.

Virtual layer

Common IT Infrastructure

Vendors offer many different services within the three major categories of cloud computing

There is an evolving “ecosystem” of services providers

Infrastructure-as-a-service:

- Amazon web services
 - Provide on-demand cloud computing services (EC2, S3, SQS, etc) using variable-cost model
- Amazon virtual private cloud
 - Provide fully private cloud services model using the Amazon cloud infrastructure
- Mozy.com
 - Provides backup services over the Internet

Platform-as-a-service:

- Google applications engine
 - Allows Web applications to be deployed on Google’s architecture
- Microsoft windows azure
 - Cloud computing architecture that is offered to host.NET applications
- Force.com
 - Multi-tenant platform used by Salesforce
- Cisco
 - WebEx Connect

Software-as-a-service:

- Customer Relationship Management
 - Salesforce.com
 - myERP.com
 - Oracle OnDemand
 - RightNow
- Business intelligence
 - SAS Suite of On-Demand Applications
 - Vitria M3O Suite
- Human resources
 - Oracle Peoplesoft
 - NetSuite ePayroll
 - Workday
- Productivity and collaboration
 - Gmail, Google Apps
 - Zoho.com
 - Apple Mobile Me
 - Cisco WebEx

Cloud Security and Risk Management Concerns



Security and Cloud – Unknowns

Unanswered questions remain on how key security challenges will be addressed in the cloud. New innovative solutions are emerging.

- Understanding security of the virtual machine; how reliable is it, implications of VM compromise are potentially high e.g. “Cloudburst attack” or file system exploitation
- How will applications and data be physically allocated within the cloud fabric? Can risk scores apply, what about policy-based environment management?
- Regulatory risks continue to challenge the move to the cloud. Undefined assurance standards for cloud environment and scramble for the development of standards leading to uncertainty of where to set the bar (solely based on internal risk assessment and current leading practices)
- Managing virtual machine images will become a challenge. Handling their lifecycle, maintenance, and the data and credentials they contain may be difficult. Hard to 'look inside' today.
- New innovations to combat security challenges in the cloud e.g. anti-virus at the virtual layer vs. inter VM. No need to install.
- Vendor lock-in. Not much flexibility and interoperability today.
- Performance management. Management of cloud services necessary to diminish the effectiveness of preventative and detective security controls.

Security considerations for cloud computing

Access Control Issues

- Would you trust placing your directory services in the cloud?
- Given a shared data-tier, how will data-level access be enforced?
- How would you enforce an RBAC model in the cloud?
- How would you provide reduced single-sign-on across cloud services and application?

Vulnerability Management

- How do you provide effective communication to AaaS consumers regarding patch management and security patch management activities (i.e. regression test)?
- How do you perform consistent system hardening across multiple AaaS consumers without affecting application functionality?
- How do you perform routine vulnerability scans within the cloud?

Incident Response

- How do you “image” a system that no longer exists for forensics analysis?
- How do you trace security incidents back to specific cloud services and users?
- How do you support legal chain of custody requirements within the cloud?

Encryption

- How do you manage key management across encryption service providers within the cloud?
- How do you provide consistent encryption services (i.e. key length, algorithms, etc.)?

Privacy and Data Protection

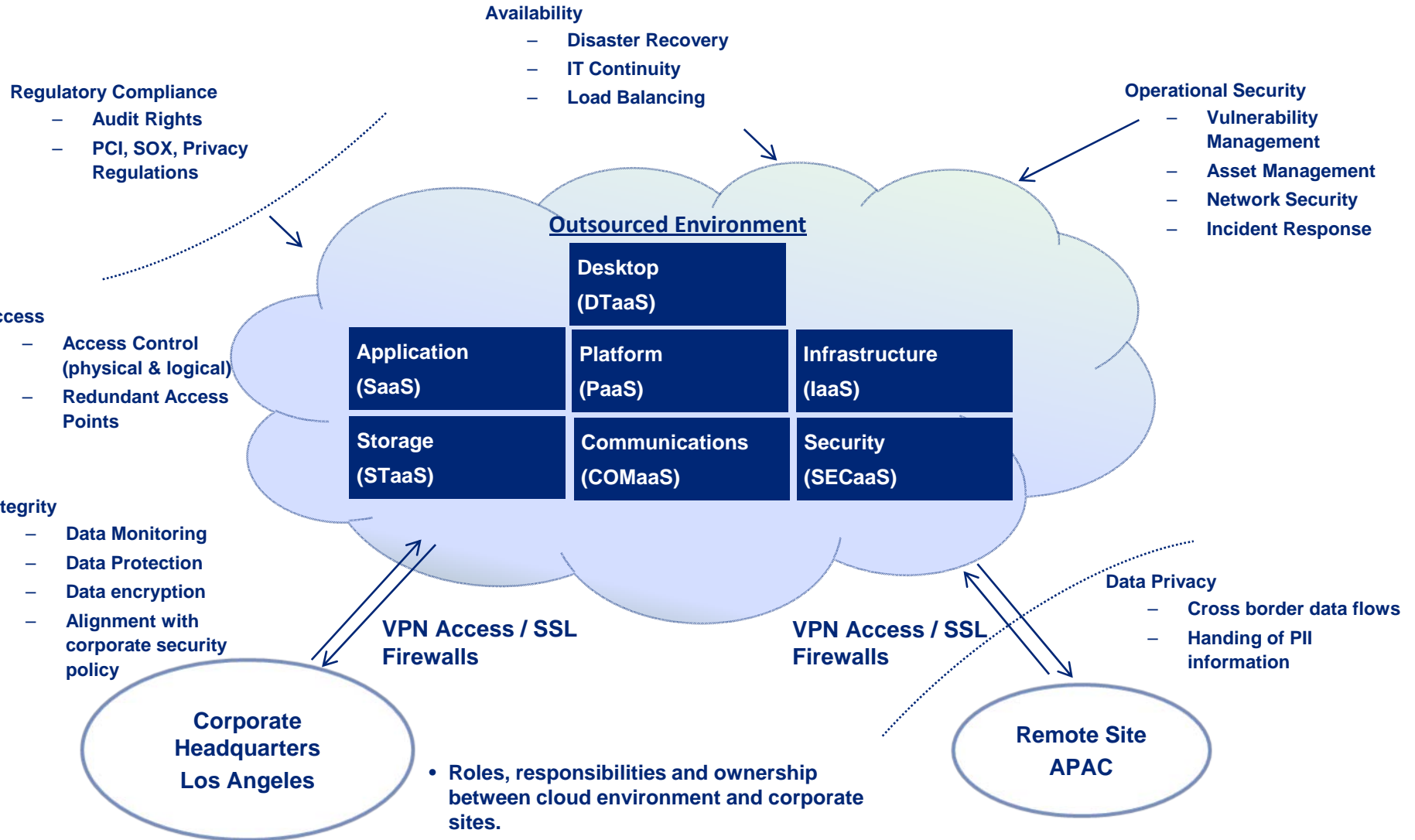
- How do you take a risk-based approach in deciding data elements and communication to be encrypted within the cloud and external to the cloud?
- How do you facilitate consistent data classification and governance?
- How do you facilitate varying privacy policies across SaaS and AaaS consumers?

Cyber security and Cloud

Significant Security and Privacy challenges exist in both the Private and Public cloud environments.

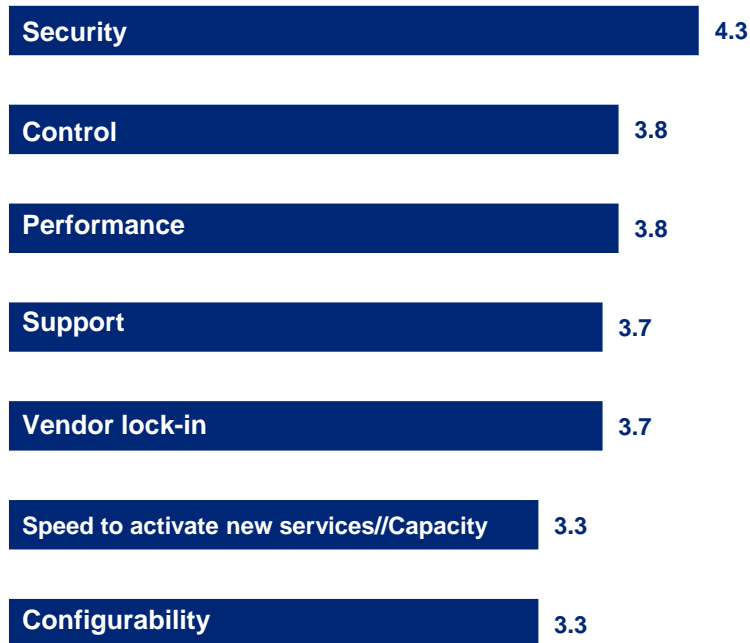
	Potential Benefits of Private versus Public Clouds	Potential Drawbacks of Private versus Public Clouds
Access	Keep credentials in-house. Full control over physical layer. Authenticate to external apps	Cannot offset administrative overhead of access management. Difficult to authenticate back to apps inside Chevron
Multi-Tenancy	Reduced risk of external compromise (from other tenants)	Still need to address multi-tenancy issues due to potential internal threat vectors
Confidentiality & Data Privacy	Consolidated (virtual) view of data internally. Facilitates more centralized approach to data management. Full control of data retained	Own all the overhead associated with data lifecycle management, encryption, capacity planning, DR and BC
Operational Security	Full control of cyber threat intelligence, vulnerability management, patching and Incident response. No 'noise' from other tenants. More granular control, higher flexibility in environment	Potentially high cost to build and manage everything internally. Technology rapidly evolving, not mature. External third-party access to the cloud may be challenging
Data Leakage & IP Protection	Custody and full protection of data/IP. May avoid extra security layers in some instances. Full control over protective measures such as DLP, IDS/IPS	Harder to collaborate externally (if necessary). Higher burden on the WAN links.
Availability	Full control over redundancy SLA, archival and alignment with storage/retention policies.	Need to cover full costs of additional infrastructure capacity
Integrity	Full control of creation, configuration, management, and life cycle of the cloud environment and virtual machines	n/a

Cloud computing environment – security risks



Security continues to be a top risk management concern...

Top IT cloud concerns*



Security areas

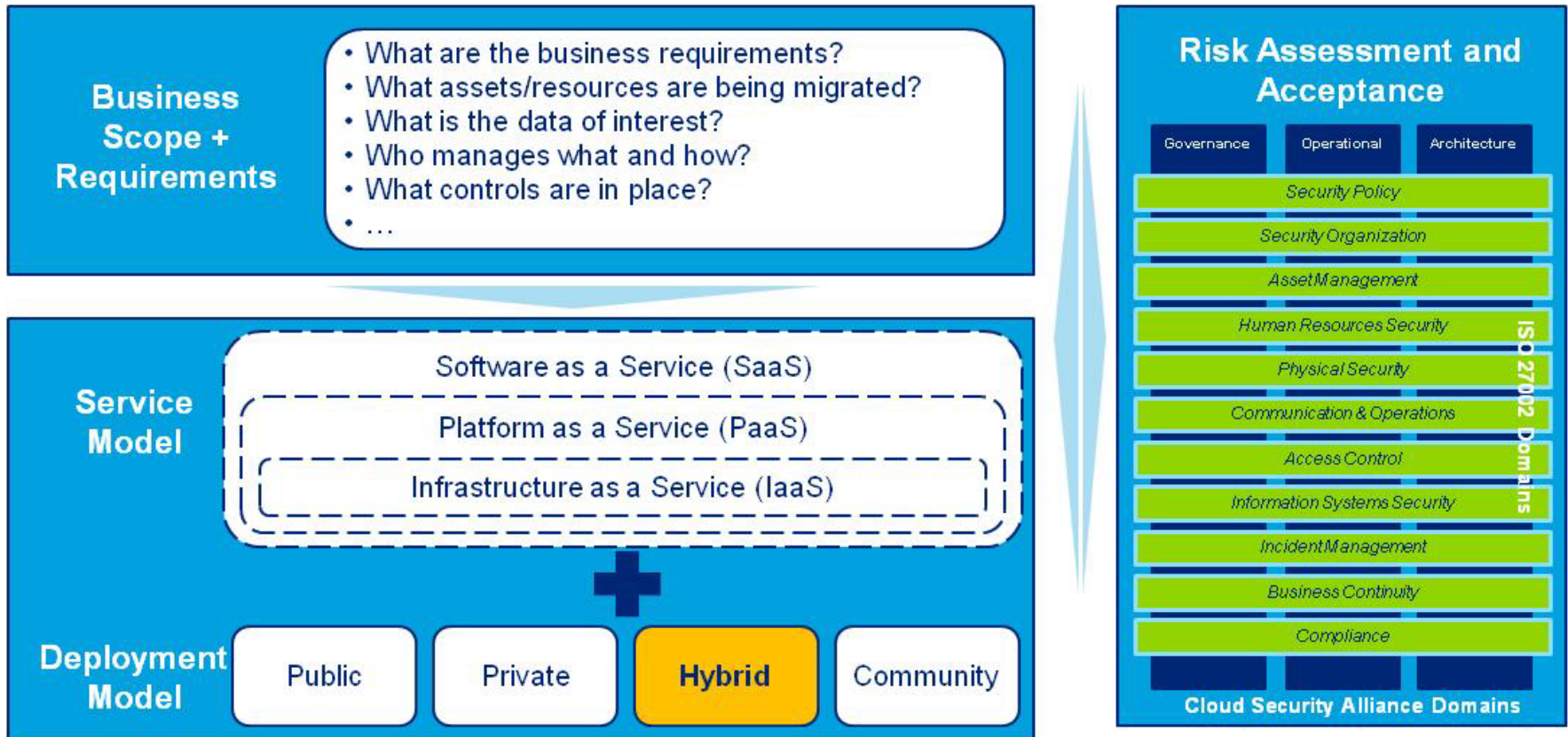


*Data: InformationWeek Analytics Cloud Computing Survey of 453 business technology professionals. A recent survey was conducted of 244 IT executives/CIOs about their companies' use of, and views about, IT Cloud Services.

Asking the right questions is half the battle, good guidance from CSA, Jericho, Burton Group, etc.

It is important to choose the appropriate deployment model that fits the business need, work load characteristic and risk profile

Understanding the cloud computing deployment model is the first step...



Do benefits outweigh the risks?
Only you or rather your business can decide.

Next, form a risk profile using available guidance...

- Gaps against your Corporate IS policy
 - Is policy too restrictive?
 - Are regulations too restrictive?
- Assess Risks across the CSA/ISO domains
 - Evaluate risks and controls
 - Agree on the controls that you “cannot compromise”
 - Redefine “architecture” or “deployment model” if necessary
 - Define options for cost modeling
- Engage both IS and the business in risk acceptance and decisioning
 - Business case — cost vs. risks
 - Decision process
 - Ongoing monitoring and reporting
 - Compliance and certification

Risk Assessments Must Consider “Context”

Data Risk is Contextual in Nature

Risks	New Risk Implications
Geography	Given various countries and various regulatory authorities, controls for supporting appropriate cross border data views and use must be maintained
Definition of Ownership, Custodianship, Processing & Use Rights and Obligations	Clear establishment of rights and obligations associated with data assets must be established. Often rights and obligations are dependent on the physical location of the data owner, custodian and user. Designing and implementing effective controls to support appropriate rights and obligations may be complex.
Multi-Tenancy	In a multi-tenant cloud environment, users may access shared resources, possibly gaining unauthorized access or may attack other tenants. This may have less risk in a private cloud, but more risk in a vendor hosted cloud
Data seizures	In a cloud provider environment, server seizures for one customer may include another customer, simply because they were on the same physical server. Seizing the hardware may lead to data loss or data disclosure of other customers. This may only apply to certain vendor-based models.
Data Loss	On ephemeral or transient systems, a cloud vendor provider instance failure may lead to permanent loss of system information including system configuration and data stored locally
Ephemeral/transient systems	The concept of a “disposable” server challenges the role of change control

Risk associated with any particular data type may vary with association, location, age, etc due the flexible nature of Cloud Computing. Identifying true risk and managing risk becomes difficult.

Risks considerations / questions

Risks	Operational risk examples
Ownership of data	Who will own the data when one subscribes to cloud computing service? Is the data you create, use, and store within a cloud yours?
Data controls	Could your data be viewed, accessed, or used without your knowledge; sold to third parties, used for unknown purposes, etc.?
Backup, retention, and disposal	Is data retention meeting your policy requirements? Is deleted data “really” gone, or still preserved somewhere within the cloud? How are data backups and restores handled?
Availability and reliability	How is reliability, access, and availability “guaranteed” by cloud services providers, through service-level agreements?
Disaster recovery	Is your data is protected in the event of a disaster? What are the recovery time objectives and service-level agreements?
Legal compliance	Is your cloud provider adhering to laws/regulations for your industry, and in every jurisdiction which applies?
Scalability	Can your service provider support growing demand from all clients, and provide reliable services at high scalability?

Risks considerations / questions (cont.)

Risks	Security risk examples
Availability	Is data replication allowed? Is there an impact to Recoverability Point Objectives (RPO) and Recovery Time Objectives (RTO)?
Access	Is multi-tenancy okay within the organization? How do you control data access in a cloud environment? Can you securely delete data?
Authentication	Would you trust placing all user credential in the cloud? How would you perform external and multi-cloud authentication? Could you use a federated authentication mechanism?
Security forensics	How do you “image” a system that no longer exists for forensics analysis? How effective is log correlation if systems no longer exist?
Integrity	How do you maintain “integrity” in a shared environment? What are the various KPI for data monitoring? Should you rely on encryption?
Privacy	There are legal uncertainties with cloud computing. Is there individual rights or confidentiality for data in the cloud? Does it still match your privacy policy? What about data that replicates across borders?
Operational security	How does this impact your vulnerability management program? How do you track changing systems in your asset management system? How do you harden the Operating System if it’s been abstract?
Key management	Do you have a solid key management system for encryption?

Risks considerations / questions (cont.)

What do you really control, what you can influence, what do you have no control over?

- In some cases, contracts are the only risk mitigation strategy — but are they?
- Who handles what operational processes? What are the hand-off points?

How can you gain assurance?

- Many vendors have SAS 70, but are they really adequate?
- How relevant is penetration testing and how “wide and deep” can it really be?
- What transparency can be gained with respect to — vulnerabilities, results of the secure development lifecycle, security incidents, logging and monitoring, audit reports, etc.?
- What testing can we do and get transparency around privileged user controls, ability for other clients to impact your workload?
- What security and risk metrics (KRI and KPI) will the cloud vendor make available to a customer?
- How does one integrate Security operations?

Risks considerations / questions (cont.)

How does one handle the “grey areas” with respect to legal and regulatory issues?

- Breach at cloud provider impacting customer data?
- Regulatory compliance failures — who is accountable?
- Regulations still require management to be responsible for controls in an outsourced environment — is that really possible in the cloud?

How does establish strong “Governance and Risk Management” over movement to cloud?

- Organization and related processes — Business decision making, IT decision making, Technology and Security Architecture, Legal, Compliance, etc.
- Re-tooling of IT Service Management capabilities
- Ongoing risk assessment, monitoring and reporting — implications on vendor management programs
- Stronger enforcement and management of SLAs

Regulatory and compliance requirements must be integral to a cloud computing solution

Examples

- Financial services
 - GLBA
 - FFIEC
 - SEC 17A-3
 - Information Barriers
 - Supervisory Rules
- Data breach laws
 - 30 States from CA to NY
- Privacy laws
 - US and Global

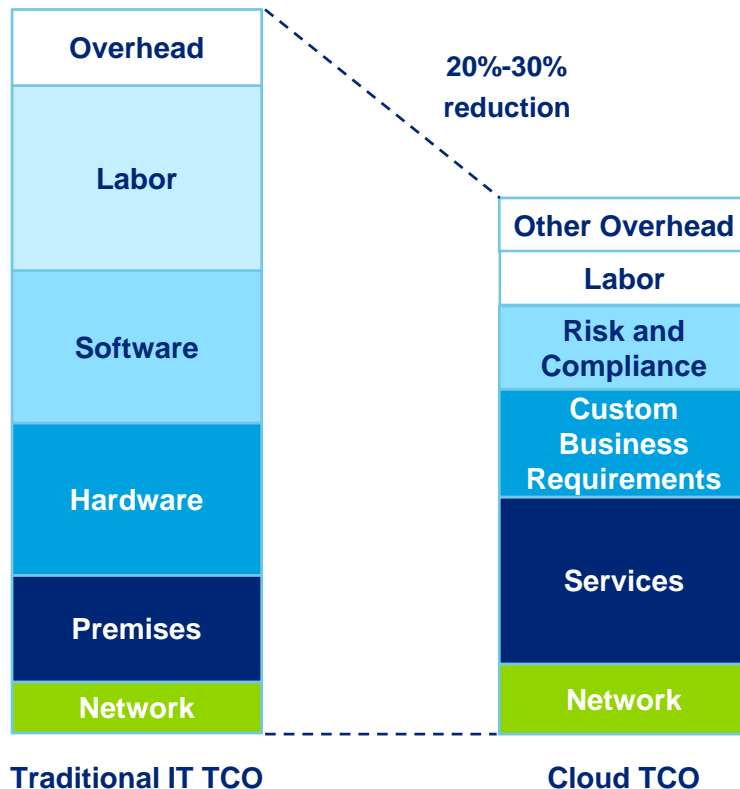
Polling questions

- How does one obtain assurance from a provider in order to do the “regulatory certification”?
- Do costs add up such that internal cloud is a better option than hybrid or public?
- Have you evaluated your cloud provider and found that regulatory implications will prevent migration to cloud?
- Can we really avoid regulatory situations and still get benefits from cloud deployment?

Option analysis and total cost of ownership

Total cost of ownership

Dynamics



- Clients are demanding a minimum 20%-30% reduction in TCO
- Vendors are offering utility like pricing to large customers
- Option analysis required — to decide Private vs. Hybrid deployments — since risk requirements and appetites are different, with different cost benefit
- Base services cost often do not fully account for all “risk and control requirements”
- Factor in transition and re-architecture costs into an overall ROI view
- Early adopters have reported efficiency gains through use of cloud services — but acknowledge the rethinking of “risk acceptance” practices

Does utility pricing mean an optimal TCO — not always?

Security in the Cloud- Summary

- Take a Risk Based approach
 - Risk Assessments
 - Risk Profile
- Address key security areas such as:
 - Identity and Access Management
 - Vulnerability Management
 - Privacy and Data Protection
 - Audit and Compliance
 - Data Governance

Cloud Computing Audit Considerations



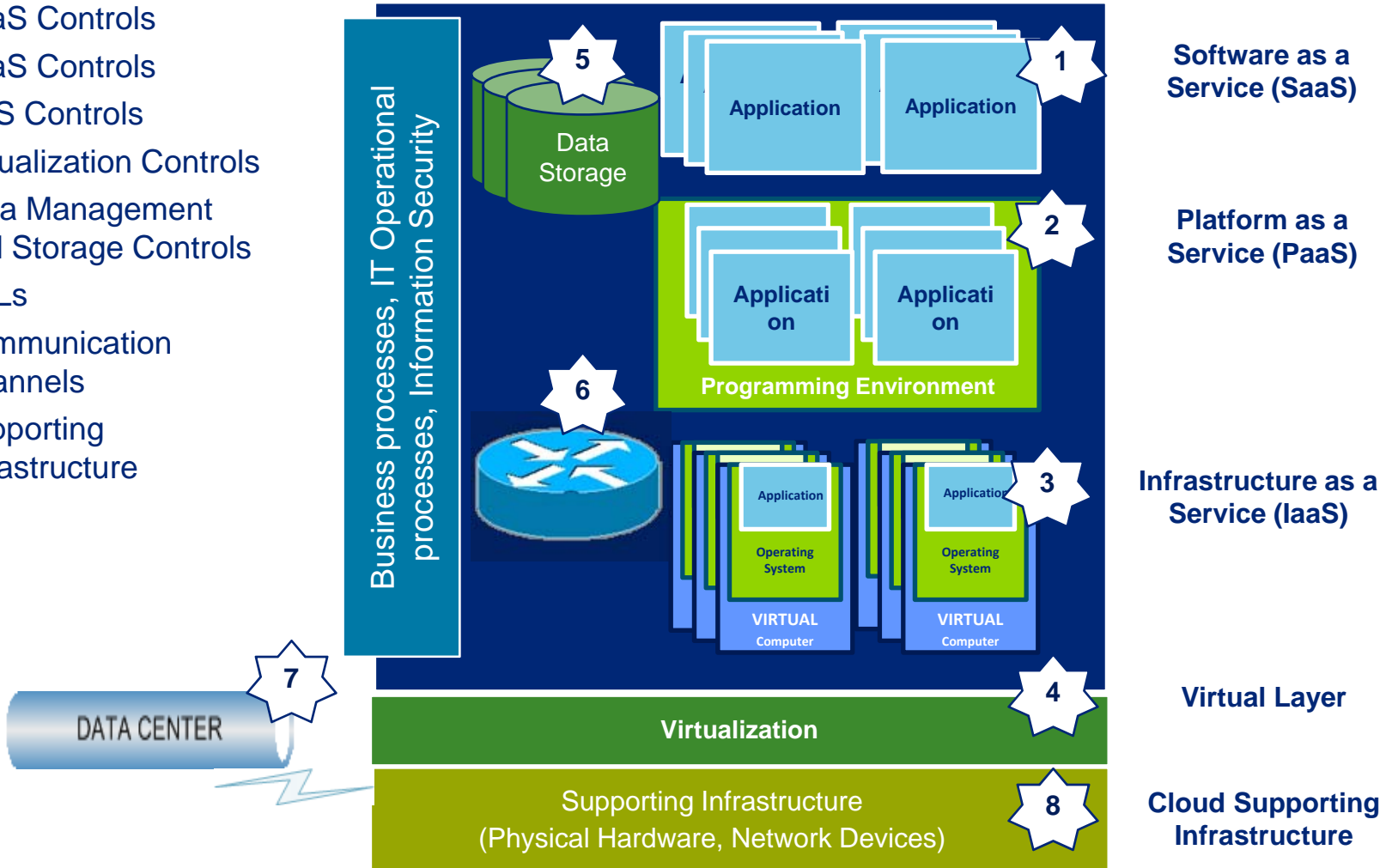
Business challenges with auditing/assessing a cloud computing environment

A disruptive technology, like cloud computing, can impact several areas



- Requests for numerous audits and assessments targeting vendors and cloud providers
 - Reliance on agreed upon procedures from SAS70s and Systrusts
 - But do these audits provide enough coverage?
- Lack of a specific cloud computing standard
 - May not meet existing standards or regulatory requirements (i.e. PCI Level 1)
 - SAS70s (type I and II) focus on financial statement assertions
 - Systrust focuses on 4 areas (availability, security, integrity, maintainability)
 - ISO 27000 series can be used to covers additional areas not met by a SAS70 or Systrust
 - ISAE3402 (Assurance Reports on Controls at a Third Party Service Organization)

What do you audit/assess?


1. SaaS Controls
2. PaaS Controls
3. IaaS Controls
4. Virtualization Controls
5. Data Management and Storage Controls
6. ACLs
7. Communication Channels
8. Supporting Infrastructure





Cloud computing controls

Area	Examples of control objectives areas
 <p>Software as a service (SaaS)</p>	<p>Licensing</p> <ul style="list-style-type: none"> Examine tools used for usage tracking and licensing Examine accuracy of reporting <hr/> <p>Environment separation</p> <ul style="list-style-type: none"> Separation from other applications <hr/> <p>Software development life cycle (SDLC)</p> <ul style="list-style-type: none"> New risks may exist as Cloud Computing can expand and shorten the SDLC cycle <hr/> <p>Management of software dependencies</p> <ul style="list-style-type: none"> Due to technical architecture complexity and potentially restrictions by the cloud provider, replicating data back to the enterprise or to another provider may be difficult
 <p>Platform as a service (PaaS)</p>	<p>Application development</p> <ul style="list-style-type: none"> Specific requirements and controls are in place to filter or detect unwanted code/malicious code <hr/> <p>Environment separation</p> <ul style="list-style-type: none"> Separation from other applications <hr/> <p>Software development life cycle (SDLC)</p> <ul style="list-style-type: none"> New risks may exist as cloud computing can expand and shorten the SDLC cycle



Cloud computing controls (cont.)

Area	Examples of control objectives areas
<div data-bbox="164 364 285 478" style="text-align: center;">  <p>3</p> </div> <div data-bbox="112 506 351 606"> <p>Infrastructure as a service (IaaS)</p> </div>	<div data-bbox="396 364 695 396"> <p>Virtual server images</p> </div> <div data-bbox="396 406 1400 485"> <ul style="list-style-type: none"> • Are there controls for how a virtual server images are created/destroyed? • Are there controls for maintaining the integrity of server images? </div> <hr/> <div data-bbox="396 506 724 539"> <p>Virtual server inventory</p> </div> <div data-bbox="396 549 1487 582"> <ul style="list-style-type: none"> • IaaS servers should have an audit record for when they were started and ended </div> <hr/> <div data-bbox="396 604 714 636"> <p>Suspension of servers</p> </div> <div data-bbox="396 646 1729 756"> <ul style="list-style-type: none"> • Some technologies allow for the suspension of virtual systems, which can become out of date with respect to patches, software updates, configuration settings and tools • Affects availability metrics, depending on how it is included </div> <hr/> <div data-bbox="396 778 608 811"> <p>Security policy</p> </div> <div data-bbox="396 821 1796 928"> <ul style="list-style-type: none"> • To manage large scale systems that are constantly in flux, a security policy should be used to configure the security of each system, or the use of consistent automated tools • Who will manage the kernels? </div>
<div data-bbox="164 963 285 1078" style="text-align: center;">  <p>4</p> </div> <div data-bbox="135 1092 328 1125"> <p>Virtualization</p> </div>	<div data-bbox="396 949 782 982"> <p>Virtualization configuration</p> </div> <div data-bbox="396 992 1091 1153"> <ul style="list-style-type: none"> • Is there a protected environment? • How are host systems secured? • Are resources utilized and released as expected? • How are virtual resource interconnected? </div> <hr/> <div data-bbox="396 1175 917 1208"> <p>Virtualization maintenance & support</p> </div> <div data-bbox="396 1218 1023 1250"> <ul style="list-style-type: none"> • Is there automation and management tools? </div> <hr/> <div data-bbox="396 1272 792 1305"> <p>Key performance indicators</p> </div> <div data-bbox="396 1315 1023 1348"> <ul style="list-style-type: none"> • What is being monitored at the virtual layer? </div>

Cloud computing controls (cont.)

Area	Examples of control objectives areas
 <p data-bbox="123 496 343 654">Data management and data storage</p>	<p data-bbox="397 368 736 404">Data storage design</p> <ul data-bbox="397 418 1779 544" style="list-style-type: none"><li data-bbox="397 418 1779 496">• Cloud provider may not be able to match in-house IT service availability, recovery time objectives (RTO), and recovery point objectives (RPO)<li data-bbox="397 504 1779 544">• Cloud providers may drastically change business model or discontinue cloud services <hr/> <p data-bbox="397 568 645 604">Access to data</p> <ul data-bbox="397 618 1779 696" style="list-style-type: none"><li data-bbox="397 618 1779 696">• Complexity introduced by cloud computing environment results in more pieces that can go wrong, and more complex recovery procedures <hr/> <p data-bbox="397 721 803 756">Sensitive data treatment</p> <ul data-bbox="397 771 1464 806" style="list-style-type: none"><li data-bbox="397 771 1464 806">• Cleansing data may not be successful if it exists in multiple places <hr/> <p data-bbox="397 831 942 866">Administration and maintenance</p> <ul data-bbox="397 881 1779 959" style="list-style-type: none"><li data-bbox="397 881 1779 959">• Due to technical architecture complexity and potential restrictions by the cloud provider, replicating data back to the enterprise or to another provider may be difficult
 <p data-bbox="108 1106 359 1178">Access control lists</p>	<p data-bbox="397 982 639 1018">Network ACLs</p> <ul data-bbox="397 1032 1508 1118" style="list-style-type: none"><li data-bbox="397 1032 1170 1068">• Is there appropriate ingress or egress filtering?<li data-bbox="397 1075 1508 1118">• Are there ACLs that segment the environment from other resources?

Cloud computing controls (cont.)

Area	Examples of control objectives areas
 <p data-bbox="112 492 351 568">Communication channels</p>	<p data-bbox="397 368 562 401">Protocols</p> <ul data-bbox="397 419 1734 554" style="list-style-type: none"><li data-bbox="397 419 1707 458">• What communication protocols are used to communicate with other data centers?<li data-bbox="397 468 1290 506">• Are there any clear text administration protocols used?<li data-bbox="397 516 1734 554">• Can you monitor communication in and out of the cloud as well as within the cloud?
 <p data-bbox="117 758 345 872">Cloud supporting infrastructure</p>	<p data-bbox="397 634 886 666">Underlying host environment</p> <ul data-bbox="397 685 1742 906" style="list-style-type: none"><li data-bbox="397 685 1742 761">• What assurance can be obtained about underlying cloud management software and supporting infrastructure?<li data-bbox="397 775 1311 813">• How will privileged access be monitored and controlled?<li data-bbox="397 823 1124 862">• What are failover and recovery procedures?<li data-bbox="397 872 1342 906">• What are scenario plans to handle catastrophic disasters?

Example cloud computing common controls areas

Operational control areas (examples)	Control objectives	Control activities
<p>Change control</p> <ul style="list-style-type: none"> Do you require change control for every server that goes live in the cloud? 	<ul style="list-style-type: none"> Hosted images and applications that can be enabled in production have been controlled through change control to maintain integrity 	<ul style="list-style-type: none"> Images and applications have been managed by change control Separation of production and development images (if possible) All images and applications use change control in the cloud
<p>Measuring utility use</p> <ul style="list-style-type: none"> What resources are being measured and how? 	<ul style="list-style-type: none"> Appropriate metrics to measure cloud computing health have been established 	<ul style="list-style-type: none"> Management tools are configured to provide reports on each metric
<p>Capacity</p> <ul style="list-style-type: none"> How is capacity measured and monitored? 	<ul style="list-style-type: none"> Appropriate metrics to measure cloud computing health have been established 	<ul style="list-style-type: none"> Management tools are configured to provide reports on each metric
<p>Backup</p> <ul style="list-style-type: none"> Cloud computing environments replicate data, would this satisfy as a backup or disaster recovery solution? 	<ul style="list-style-type: none"> Data has been backed up to support disaster recovery requirements 	<ul style="list-style-type: none"> Data repositories are replicated Supporting Metrics and reporting Failover testing

Example cloud computing common controls areas (cont.)

Security control areas (examples)	Control objectives	Control activities
<p>User & administrative access</p> <ul style="list-style-type: none"> How do you manage user access 	<ul style="list-style-type: none"> Virtual layer restricts access to guest systems and applications 	<ul style="list-style-type: none"> Virtual layer has been configured to separate the host/supporting infrastructure and guest systems and applications
<p>Administration</p> <ul style="list-style-type: none"> How is administration performed? 	<ul style="list-style-type: none"> Supporting infrastructure uses a different administrative source than guest systems and applications (separation of infrastructure and virtualized systems) 	<ul style="list-style-type: none"> Administrative access to host/infrastructure uses a different authentication system than administrative access on the guest OS or hosted applications (different directory services)
<p>Vulnerability management</p> <ul style="list-style-type: none"> How are systems in the cloud patched, tested, and monitored for security issues? 	<ul style="list-style-type: none"> Vulnerability management program includes the identification of virtualization related security issues and attacks 	<ul style="list-style-type: none"> Vulnerability assessments include the review of the virtual layers (configuration review, tool assisted assessments) Security patches have been applied to the virtualization application

Example cloud computing common controls areas (cont.)

Security control areas (examples)	Control objectives	Control activities
<p>Data protection</p> <ul style="list-style-type: none"> Sensitive data should use the appropriate data protection treatment based on their data classification 	<ul style="list-style-type: none"> Access to the data repository restrict to a limited set of applications (similar to limiting administrative access to a few sources) 	<ul style="list-style-type: none"> There are access controls that specify specific applications Changes to the access of application Logging of success and failed access to data has been defined (detective control)
<p>Encryption</p> <ul style="list-style-type: none"> How is encryption managed for data in transit and data in storage? 	<ul style="list-style-type: none"> Sensitive information is protected by encryption 	<ul style="list-style-type: none"> Encryption is used for transmitting data classified as confidential
<p>Logging and monitoring</p> <ul style="list-style-type: none"> Since systems are in flux, are they all configured to log appropriately? 	<ul style="list-style-type: none"> Any system or application that going into production has been configured to log access as per policy 	<ul style="list-style-type: none"> Any system or application that is established in production is managed by a policy that contains the correct logging configuration
<p>Patching</p>	<ul style="list-style-type: none"> Any system or application that goes into production has been configured with the latest approved patches 	<ul style="list-style-type: none"> Any system or application that is established in production is managed by a policy that automatically forces the latest approved patches

Key takeaways

- Cloud computing adoption is growing with mainstream organizations piloting targeted deployments
- Leverage guidance — NIST, Cloud Security Alliance, Jericho Forum, ENISA, Burton Group, etc.
- Defining a Cloud Security and Risk Management Strategy — partner with the business and Information Security organizations in conducting formal risk assessments and creation of cloud risk profiles to aid decisioning
- Build skills and capabilities to facilitate adoption of cloud solutions in order to minimize risk — audit organizations are building or renting capabilities around cloud
- While many traditional security risk assessment and acceptance processes apply, many don't — the right people have to be involved in understanding and accepting the business risks

Food For Thought...

- You trusted your banks with your money
- And then the mortgage crisis happened
- But the Feds and FDIC bailed out the banks and you !!!

- You trusted your cloud provider with your critical applications and data
- And then Darth Vader attacked your cloud provider
- So, who will bail you out?



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.