Deloitte.

Cloud Computing – What Auditors need to know

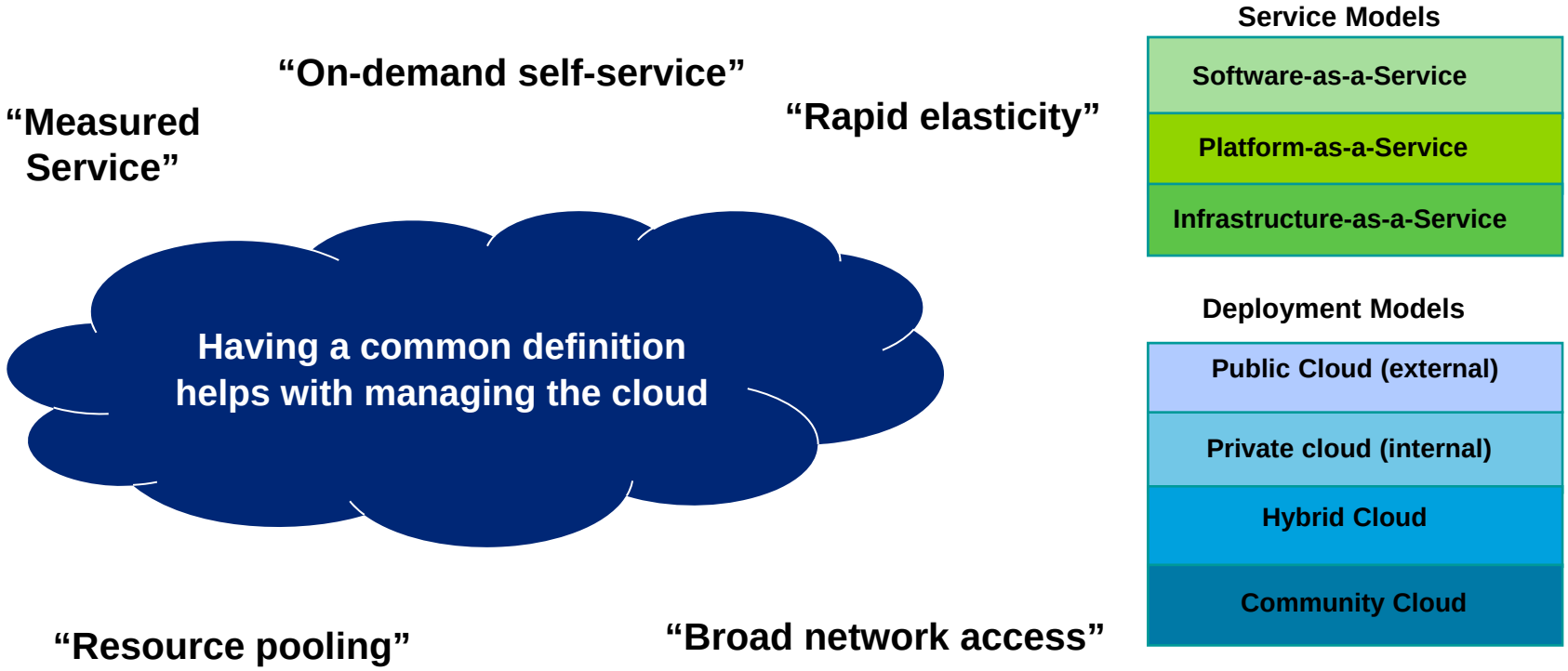
This presentation is provided solely for educational purposes and, in developing and presenting these materials, Deloitte is not providing accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decisions or actions that may affect your business or to provide assurance that any decision or action will be supported by your auditors and regulators. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be liable for any claims, liabilities, or expenses sustained by any person who relies on these courses for such purposes.

Contents

Cloud Overview

Cloud Computing Overview



- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.- ***The NIST 800-145 Definition of Cloud Computing***

Cloud Computing Overview – Deployment Models

Cloud computing technology is deployed in four general types, based on the level of internal or external ownership and technical architectures

Public Cloud	Cloud computing services from vendors that can be accessed across the Internet or a private network, using systems in one or more data centers, shared among multiple customers, with varying degrees of data privacy control.
Private Cloud	Computing architectures modeled after Public 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	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, objectives, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on-premise or off-premise.

Cloud Computing Overview – Service Delivery

Different types of Cloud computing services are grouped into specific categories: Infrastructure, Platform and Software services

Infrastructure as a Service (IaaS)

Definition

- Delivers computer infrastructure, typically a platform virtualization environment as a service. Service is typically billed on a utility computing basis and amount of resources consumed.

Customization

- Customization where technology being deployed requires minimal configuration

Operational notes

- Easier to migrate applications
- User of Cloud maintains a large portion of the technical staff (Developer, System Administrator, and DBA)

Platform as a Service (PaaS)

Definition

- Delivers a computing platform as a service. It facilitates deployment of applications while limiting or reducing the cost and complexity of buying and managing the underlying hardware and software layers

Customization

- Moderate customization — build applications within the constraints of the platform

Operational notes

- Applications may require to be re-written to meet the specifications of the vendor
- User of the Cloud maintains a development staff

Software as a Service (SaaS)

Definition

- Delivers software as a service over the Internet, avoiding the need to install and run the application on the customer's own computers and simplifying maintenance and support.

Customization

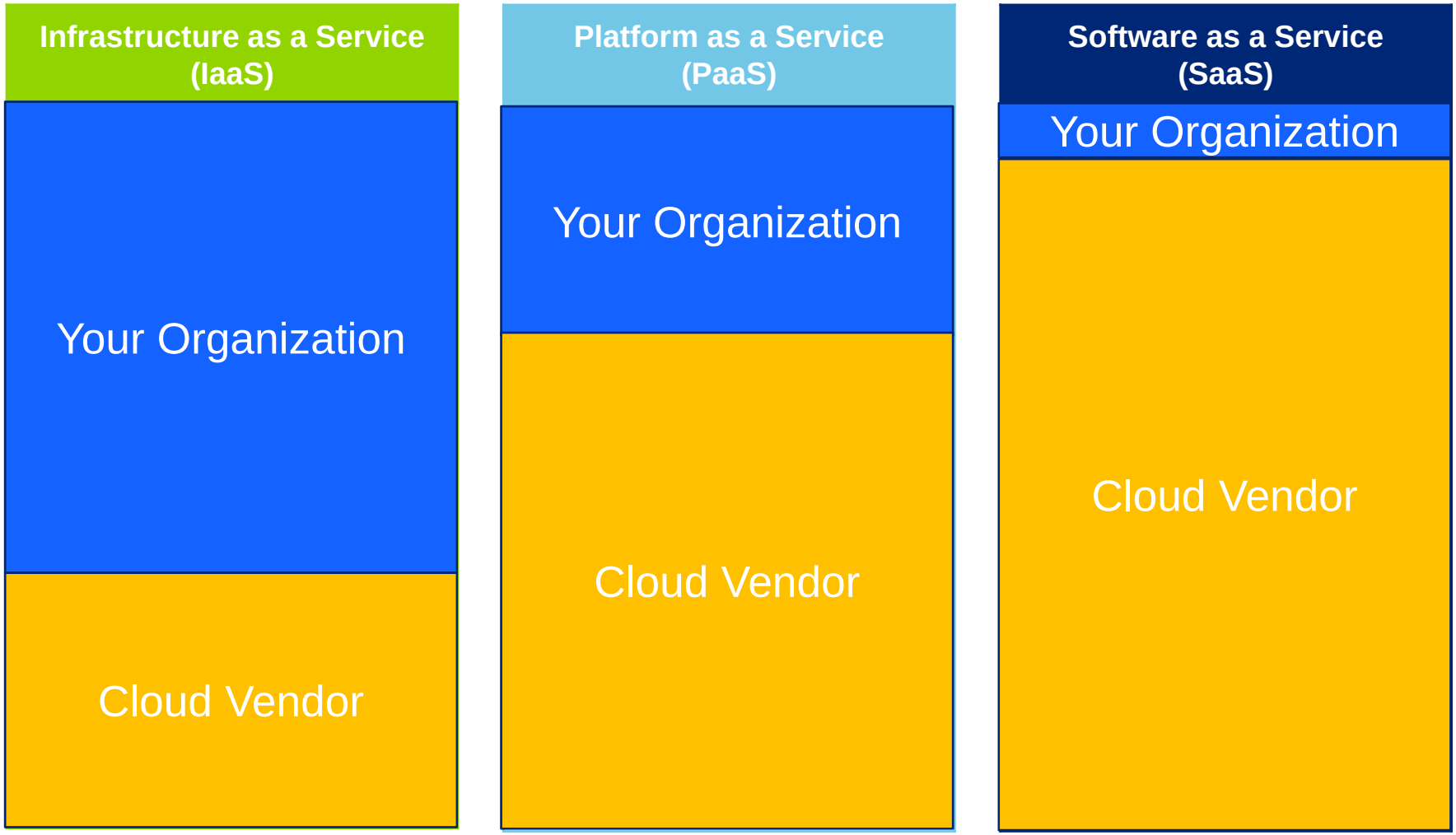
- Limited customization — existing applications likely not be able to migrate

Operational notes

- Applications may require to be re-written to meet the specifications of the vendor
- User utilizes the vendors IT staff and has limited to no technical staff

Cloud Computing Overview – Service Delivery

Responsibility chart – Your Organization vs Cloud Vendor

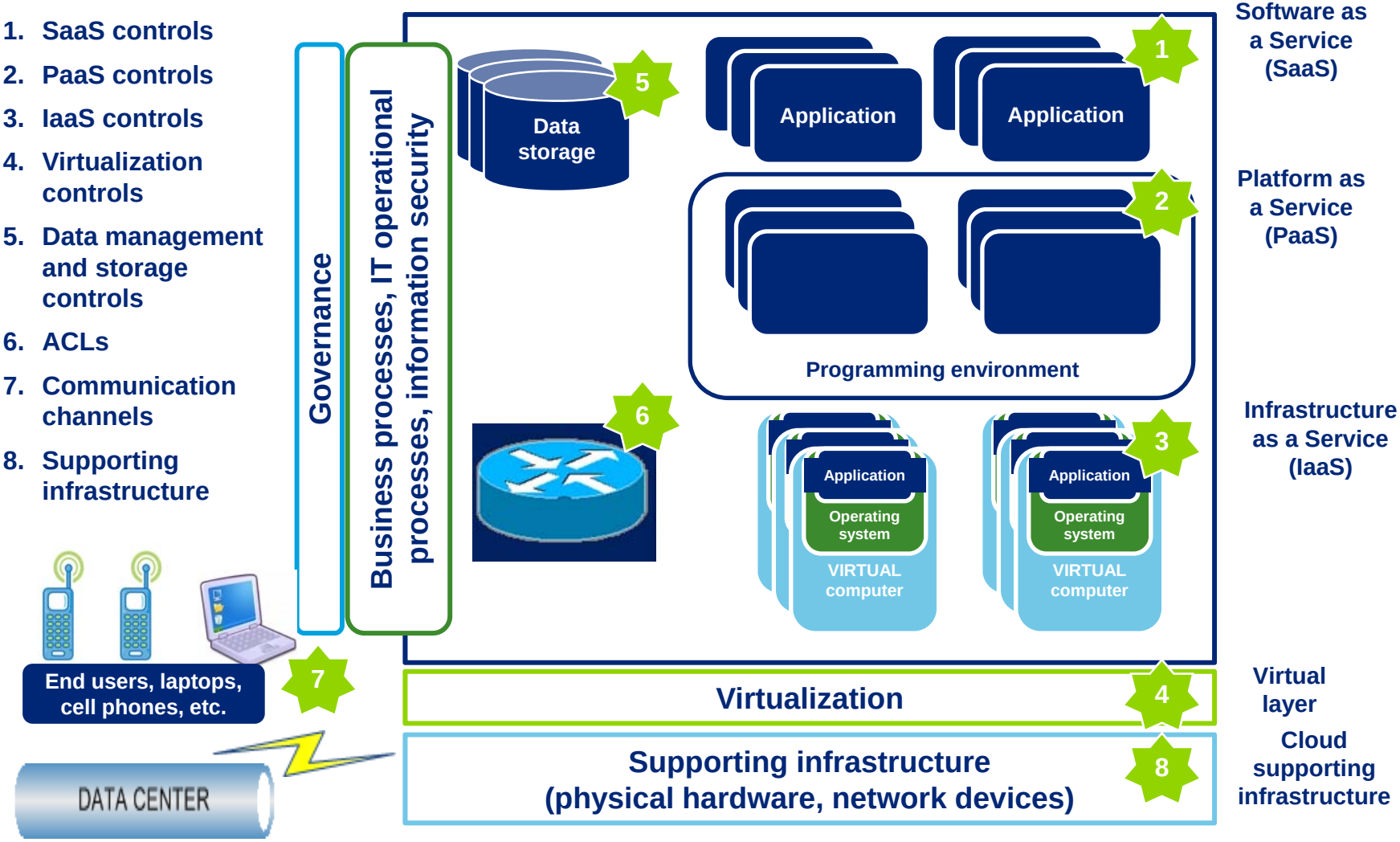


Risk and Controls

Risks (and Controls) are Widespread

We believe that cloud architectures can be a disruptive force enabling new business models and structures to deliver information services

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



Auditing Challenges with Cloud Computing

A disruptive technology, like cloud computing, can impact “how” to audit

- **Understanding the scope of the cloud computing environment**
  - Do you use the same matrix for public clouds as for private clouds? (internal vs external)
  - The concept of a perimeter in a multi-tenant environment doesn’t make sense anymore
  - Where does the cloud start and stop?
- **Can your current risk assessment capture the risks correctly?**
- **Sample selection**
  - What is the universal population from which to pick a sample from?
  - What would your sample selection methodology be in a highly dynamic environment?
  - A snapshot in time may depend if it’s a high or low peak point in time
- **Audit trails**
  - How do you “test” historical data if there was no audit trail?
- **Other**
  - Educating the audit committee
  - Overcoming internal barriers restricting the early involvement of internal audit as a ‘risk advisor’ to the business and IT

Internal Audit’s Role

Internal Audit's Role

What should the role of internal audit be in your organization's move to the Cloud?

1. Proactive trusted advisor/partner

2. Proactively identify risks to be mitigated in order to optimize the benefits of the outsourcing relationship

3. Internal Audit does not get involved with the move until it is time to audit

4. Advise on the costs savings that would be realized by a reduction of audits

Internal Audit's Role

Internal audit and compliance have a key role to play in helping to manage and assess risk as cloud services evolve, especially for third-party compliance.

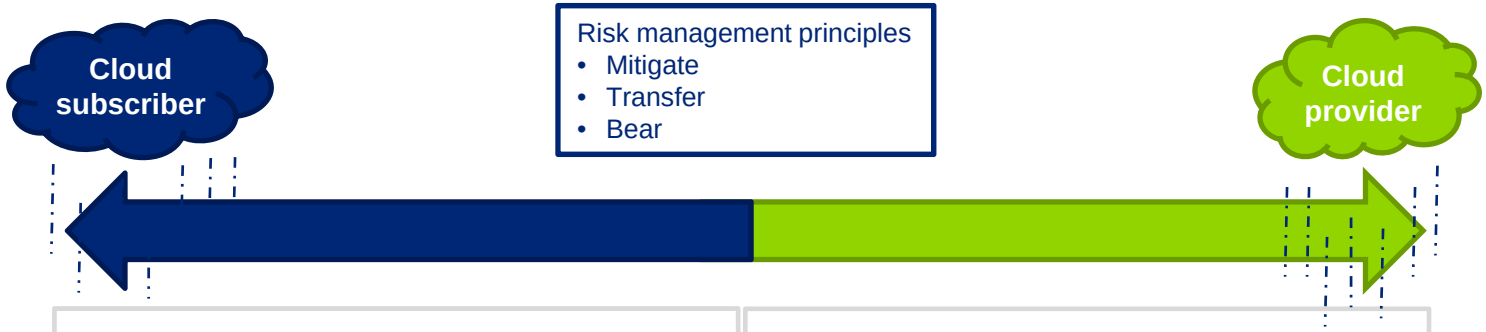
Embrace the "trusted advisor" role as the organization takes on new risks

- Proactively offer a balance of consultative and assurance services
- Educate and engage with the Board/Audit Committee

Recommended approach

- Understand and educate on cloud computing risks
  - Security, privacy, data integrity, contractual clarity and protections, business continuity, process and system reliability, effectiveness/efficiency of new business processes, configuration management, compliance with cross-jurisdictional regulations, etc.
- Help mitigate risks
  - Participate in cross functional discussions to identify risks, vulnerabilities, implications and action plans
  - Participate pre-implementation (such as in product design teams) to help assess risk and design mitigations; considering people, process, policy
  - Assess effectiveness of product/project implementation processes across functions
  - When appropriate, assess adequacy and effectiveness of controls, but recognize the absence of any authoritative control standard/baseline
- Provide objective insights

Managing Cloud Computing Risk



Identity and Access Management (IAM)	•Select an IAM solution based on current and anticipated access control requirements •Secure authorization and mature role-based Access Control life cycles	•Drive access control solutions that align with customer contract requirements and in support of several regulatory requirements for customers •Least privilege access enabled and followed
Regulatory	•Select a Cloud Service Provider (CSP)/vendor that can support your regulatory requirements •Build a vendor oversight program to monitor/measure compliance to contract requirements	•Utilize a rationalized security framework based on multiple regulatory requirements to establish controls and processes
Privacy	•Revise privacy statements and program to adjust for geographic challenges with cloud computing •Define privacy practices and processes	•Develop processes for handling sensitive/privacy-related data with defined acceptable use and data protection processes and standards •Reporting process for unauthorized access
Cyber Threat	•Revise patch and vulnerability assessment policies and standards based on risks •Develop mature security assessments and standards for vendor management	•Establish security monitoring processes in conjunction with vulnerability management program •Establish application-level code reviews, stringent Software Development Life Cycle processes, and provide notification of changes

Managing Cloud Computing Risk

Resiliency and Availability	•Redefine enterprise continuity of operation policies and standards for data replication and backup •Reestablish availability metrics and standards	•Define processes for replication, failover, and reconstitution of services related to disruptions •Reassess availability commitments and confirm testing results for compliance with SLAs
Security Operations	•Create explicit security operations policies and standards for cloud computing •Consider a policy-based approach for consistently consuming cloud services	•Establish a Security Operation Center (SOC) •Define assessment, reporting, and response capabilities •Consider a policy-based approach for consistently managing cloud systems
Application Development	•Use software development lifecycle policies and standards based on common frameworks •Use release and change management policies	•Establish application-level code reviews, stringent SDLC processes, and provide notification of changes and release management •Offer self-service change acceptance processes
Enterprise Resource Planning (ERP)	•Establish security policies and standards for ERP management and acceptable data usage •Define acceptable use of modules and databases	•Establish security zones, data protections, and access-provisioning processes •Offer strong authentication with Single Sign-on capabilities based on customer roles

The Solution

Risk-Based Approach

Risk-Based Approach

Understanding the various cloud models and the related threats and vulnerabilities will help manage risk

Service Delivery Risk

- Evaluate Virtualization risks
- Evaluate SaaS risks
- Evaluate PaaS risks
- Evaluate IaaS risks

Deployment Risk

- Understand public cloud risks
- Understand private cloud risks
- Understand hybrid cloud risks

Business Model Risk

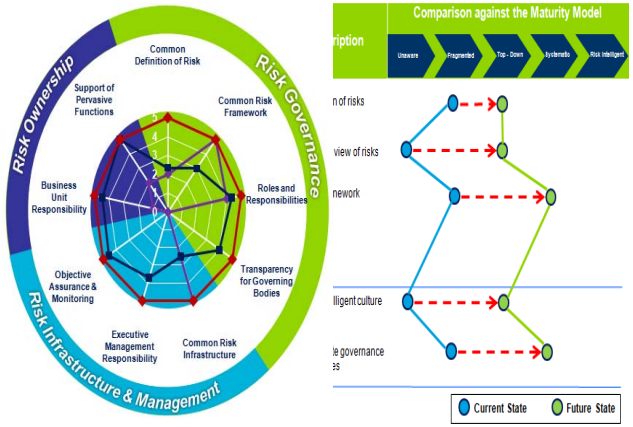
- Evaluate cloud consumer risks
- Evaluate cloud provider risks

Security Risk

- Perform an analysis of the security risks

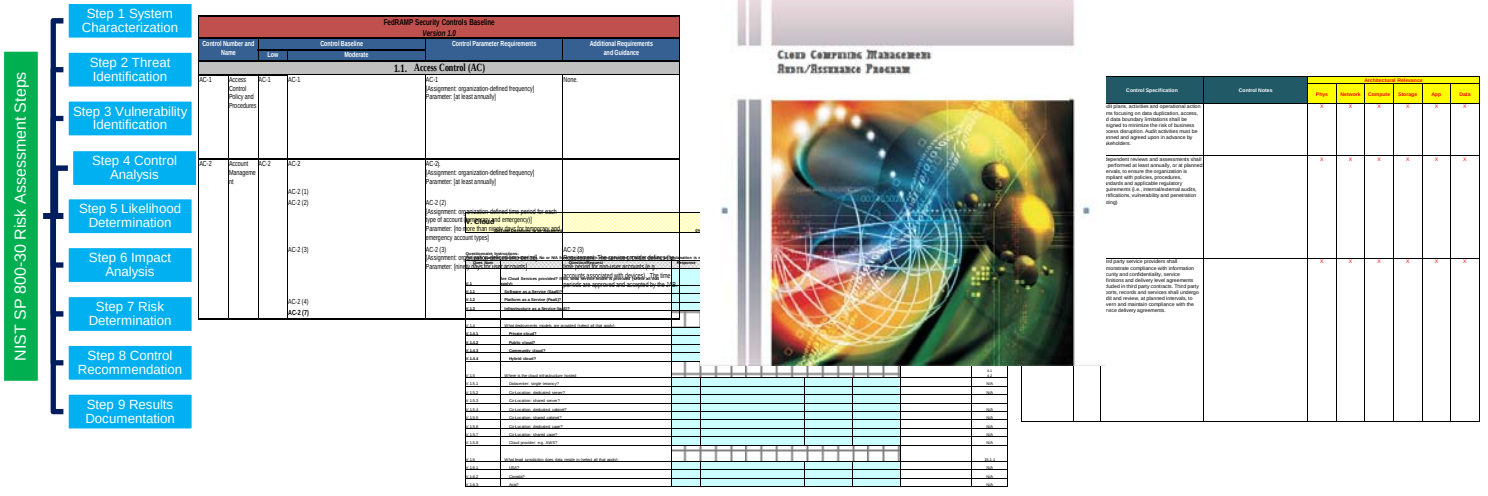
Other Risks

RISK = ASSET × THREAT × VULNERABILITY × LIKELIHOOD × IMPACT (NIST SP 800-30)



Sample of tools and frameworks -

- NIST SP 800-53, NIST SP 800-144, SP 800-30
- Deloitte Cloud Computing Risk Intelligence Map
- Cloud Security Alliance - Cloud Controls Matrix
- ISACA Cloud Computing Audit Program
- Federal Risk and Authorization Management Program - (FedRAMP)
- Shared Assessments - Standard Information Gathering (SIG 7.0)



National Institute of Standards and Technology

Use and Benefits

NIST SP 800-30

As a provider or a subscriber, to evaluate a Company's cloud computing environment, you can use a commonly accepted risk assessment standard.

The National Institute of Standards and Technology (NIST) SP 800-30 "Risk Management Guide for Information Technology Systems defines a set of risk assessment activities in nine (9) steps.

Source: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST SP 800-144

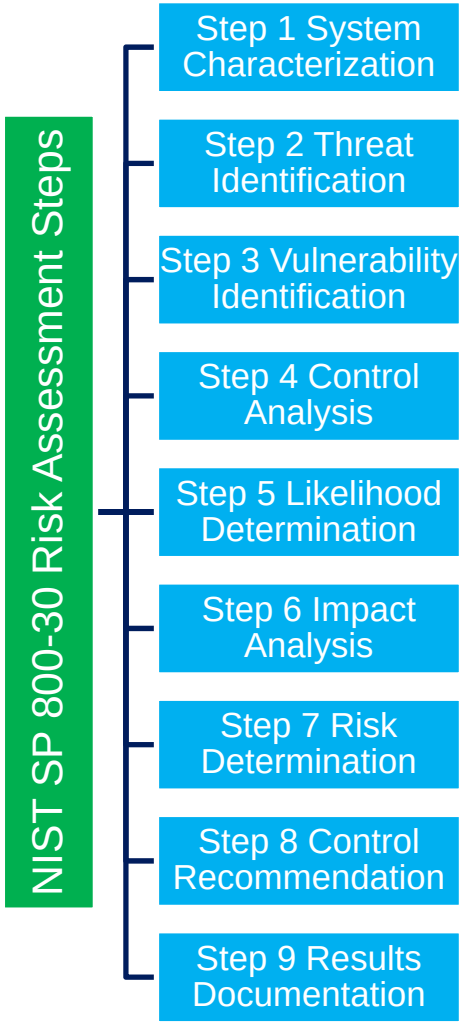
Guidelines on Security and Privacy in Public Clouds

Source: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

NIST SP 800-53

Security and Privacy controls for Federal Information Systems and Organizations

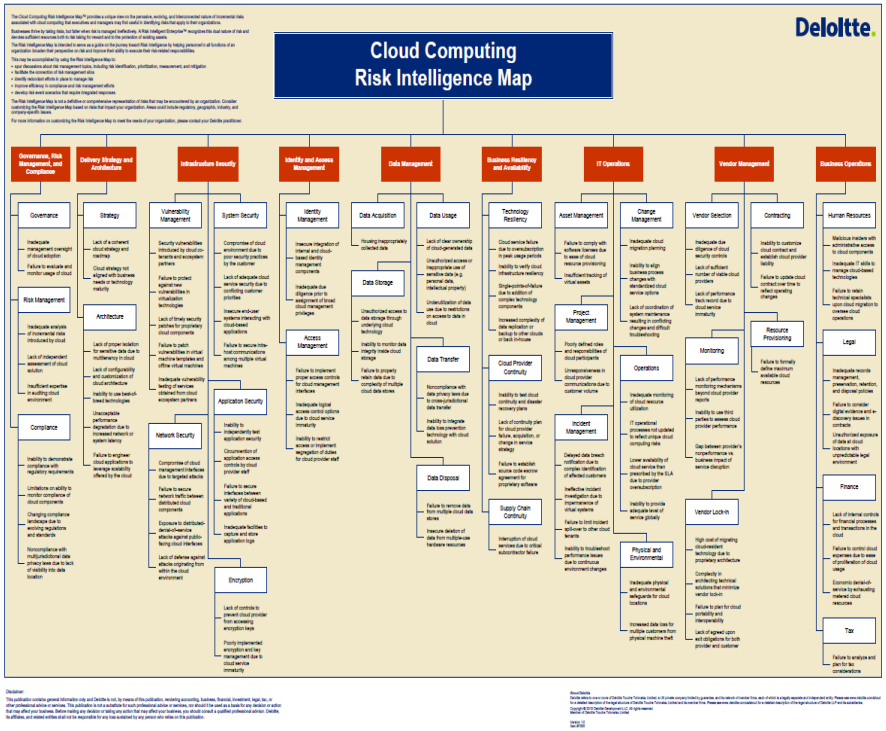
Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf



Deloitte's Cloud Computing Risk Intelligence Map

Use and Benefits

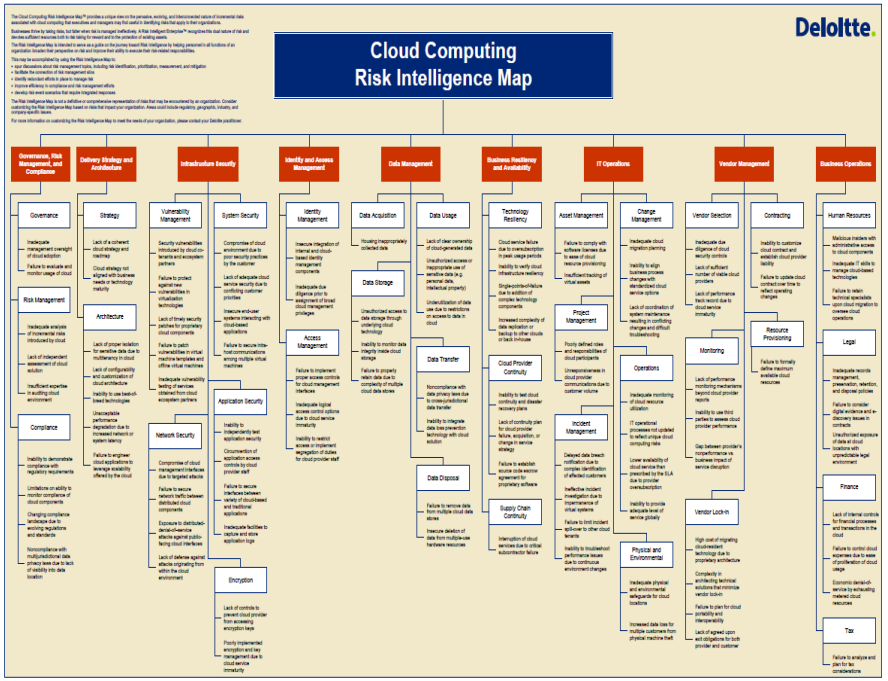
- Identifies significant risks that may be introduced by cloud computing
- Expands the risk discussion to the broad range of risks that need to be considered across the enterprise
- Identifies significant risks that may be introduced by cloud computing
- Expands the risk discussion to the broad range of risks that need to be considered across the enterprise



Deloitte’s Cloud Computing Risk Intelligence Map

The Cloud Computing Risk Intelligence Map Broad Risk Categories

- Governance, Risk management and compliance
- Delivery Strategy and Architecture
- Infrastructure Security
- Identity and Access Management
- Data Management
- Business Resiliency and Availability
- IT Operations
- Vendor Management
- Business Operations (HR, Legal, Finance, Tax)



Cloud Security Alliance - Cloud Controls Matrix

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

- It provides a controls framework is aligned to the Cloud Security Alliance guidance in 16 domains.
- The foundations rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP
- It will augment or provide internal control direction for SOC attestations provided by cloud providers.

Control Area	Control ID	Control Specification	Control Notes	Architectural Relevance					
				Phys	Network	Compute	Storage	App	Data
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.		X	X	X	X	X	X
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)		X	X	X	X	X	X
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.		X	X	X	X	X	X

Cloud Security Alliance - Cloud Controls Matrix

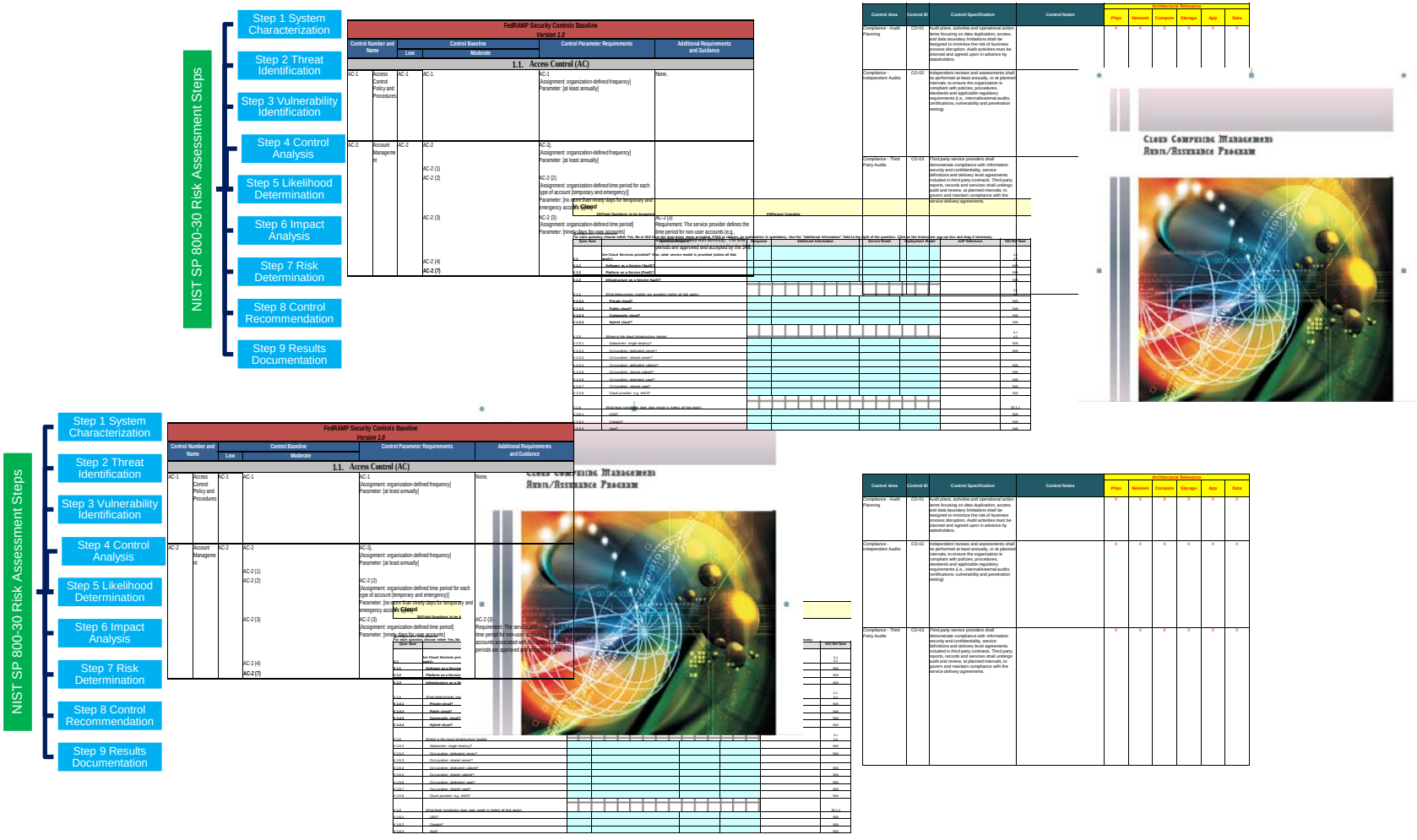
The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) domains.

- Application & Interface Security
- Audit Assurance & Compliance
- Business Continuity Management & Operational Resilience
- Change Control & Configuration Management
- Data Security & Information Lifecycle Management
- Datacenter Security
- Encryption & Key Management
- Governance and Risk Management
- Human Resources
- Identity & Access Management
- Infrastructure & Virtualization Security
- Interoperability & Portability
- Mobile Security
- Security Incident Management, E-Discovery & Cloud Forensics
- Supply Chain Management, Transparency and Accountability
- Threat and Vulnerability Management

Control Area	Control ID	Control Specification	Control Notes	Architectural Relevance					
				Phys	Network	Compute	Storage	App	Data
Compliance - Audit Planning	CO-01	Audit plans, activities and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.		X	X	X	X	X	X
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)		X	X	X	X	X	X
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.		X	X	X	X	X	X

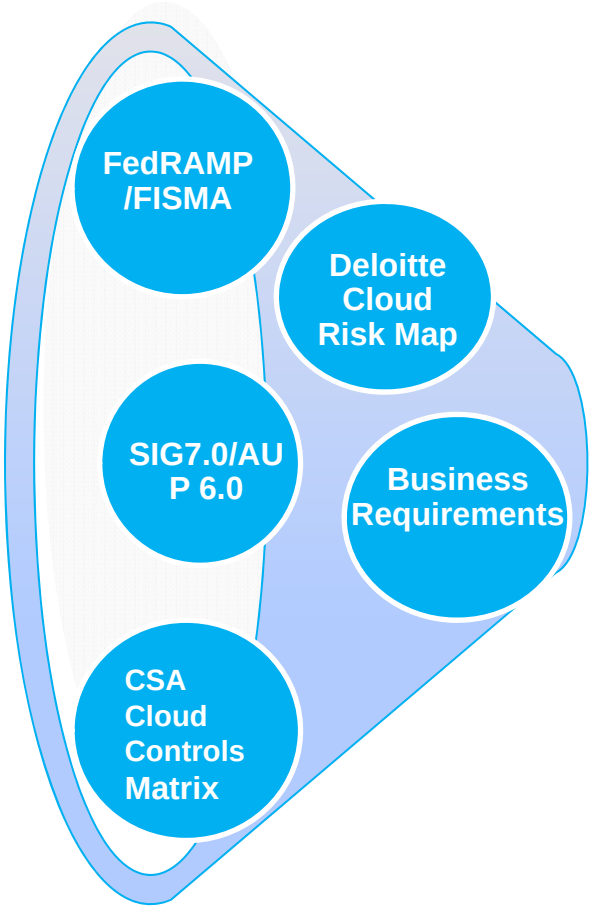
That is a lot of tools..

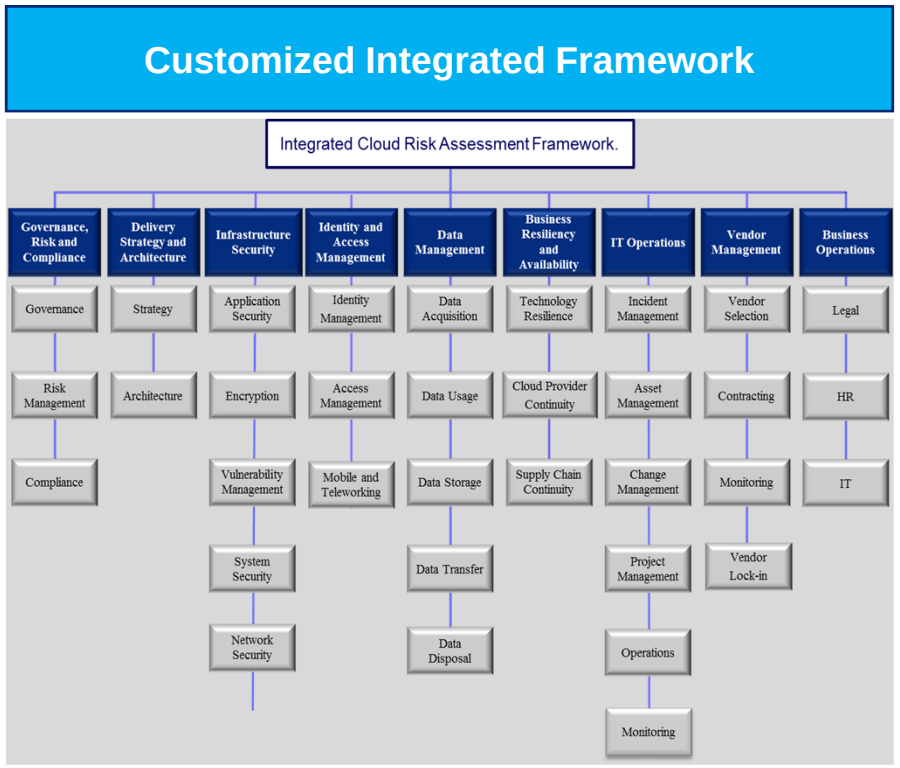
What now?



Customized Integrated risk and control framework

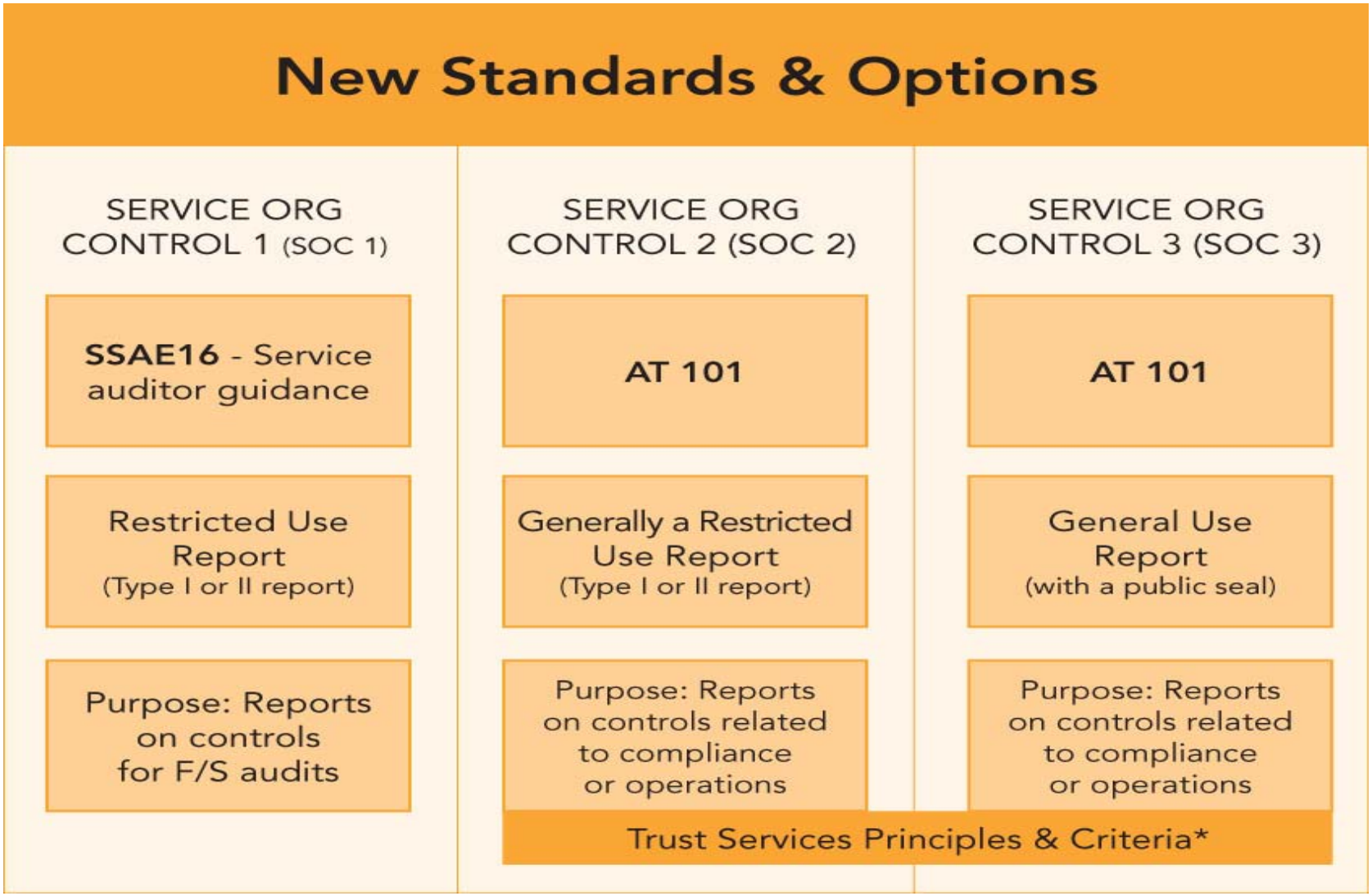
Develop a customized integrated framework to incorporate leading industry standards, your business requirements to provide appropriate coverage of controls to assess the cloud environment





Service Organization Controls Reports

Service Organization Controls



Service Organization Controls - SOC 2/3

Security			
▪ IT security policy ▪ Security awareness and communication ▪ Risk assessment ▪ Logical access	▪ Physical access ▪ Environmental controls ▪ Security monitoring (breaches) ▪ User authentication	▪ Incident management ▪ Asset classification and management ▪ Systems development and maintenance	▪ Configuration management
Availability	**Confidentiality**	**Processing Integrity**	**Privacy**
▪ Availability policy ▪ Backup and restoration ▪ Disaster recovery	▪ Confidentiality policy ▪ Confidentiality of inputs ▪ Confidentiality of data processing ▪ Confidentiality of outputs ▪ Information disclosures (including third parties) ▪ Confidentiality of Information in systems development	▪ System processing integrity policies ▪ Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs ▪ Information tracing from source to disposition	▪ Notice ▪ Choice ▪ On-ward Transfer ▪ Access ▪ Security ▪ Data Integrity ▪ Training and Awareness ▪ Enforcement and Compliance

Contact Information

Renetta Haas
Deloitte & Touche LLP
Principal
rhaas@deloitte.com
Tel (310) 251-0517

Carlos Amaya
Deloitte & Touche LLP
Senior Manager
carlamaya@deloitte.com
Tel (714) 791-8278

Charlie Willis
Deloitte & Touche LLP
Specialist Leader
ChWillis@Deloitte.com
Tel (215) 299-4534

Appendix I

Risk Focus Areas for Cloud Computing

Risk Focus Areas for Cloud Computing

Area	Examples
1 **Software as a Service (SaaS)**	**Licensing** • Examine tools used for usage tracking and licensing • Examine accuracy of reporting
	Environment Separation • Separation from other applications
	Software Development Life Cycle (SDLC) • New risks may exist as Cloud Computing can expand and shorten the SDLC cycle
	Management of Software Dependencies • 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
2 **Platform as a Service (PaaS)**	**Application Development** • Specific requirements and controls are in place to filter or detect unwanted code/malicious code
	Environment Separation • Separation from other applications
	SDLC • New risks may exist as cloud computing can expand and shorten the SDLC cycle

Risk Focus Areas for Cloud Computing (Continued)

Area	Examples
3 **Infrastructure as a Service (IaaS)**	**Virtual Server Images** • Are there controls for how a virtual server images are created/destroyed? • Are there controls for maintaining the integrity of server images?
	Virtual Server Inventory • IaaS servers should have an audit record for when they were started and ended
	Suspension of Servers • 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
	Security Policy • 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?
4 **Virtualization**	**Virtualization Configuration** • Is there a protected environment? • How are host systems secured? • Are resources utilized and released as expected? • How are virtual resource interconnected?
	Virtualization Maintenance & Support • Is there automation and management tools?
	Key Performance Indicators • What is being monitored at the virtual layer?

Risk Focus Areas for Cloud Computing (Continued)

Area	Examples
5 **Data Management and Data Storage**	**Data Storage Design** • Cloud provider may not be able to match in-house IT service availability, recovery time objectives (RTO), and recovery point objectives (RPO) • Cloud providers may drastically change business model or discontinue cloud services
	Access to Data • Complexity introduced by cloud computing environment results in more pieces that can go wrong, and more complex recovery procedures
	Sensitive Data Treatment • Cleansing data may not be successful if it exists in multiple places
	Administration and Maintenance • 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
6 **Access Control Lists**	**Network ACLs** • Is there appropriate ingress or egress filtering? • Are there ACLs that segment the environment from other resources?

Risk Focus Areas for Cloud Computing (Continued)

Area	Examples
7 **Communication Channels**	**Protocols** • What communication protocols are used to communicate with other data centers? • Are there any clear text administration protocols used? • Can you monitor communication in and out of the cloud as well as within the cloud? • Are there any end user devices that can download data from the cloud?
8 **Cloud Supporting Infrastructure**	**Underlying Host Environment** • Utilize SSAE16 / ISAE 3402 for financial systems focused controls • Utilize ISO2700 and SOC2 / SOC3 (Assurance Reports on Controls at a Third Party Service Organization) • Trust Principles – Security, Availability, Processing Integrity, Confidentiality, Privacy • Will administrators have “access” to the virtual data?

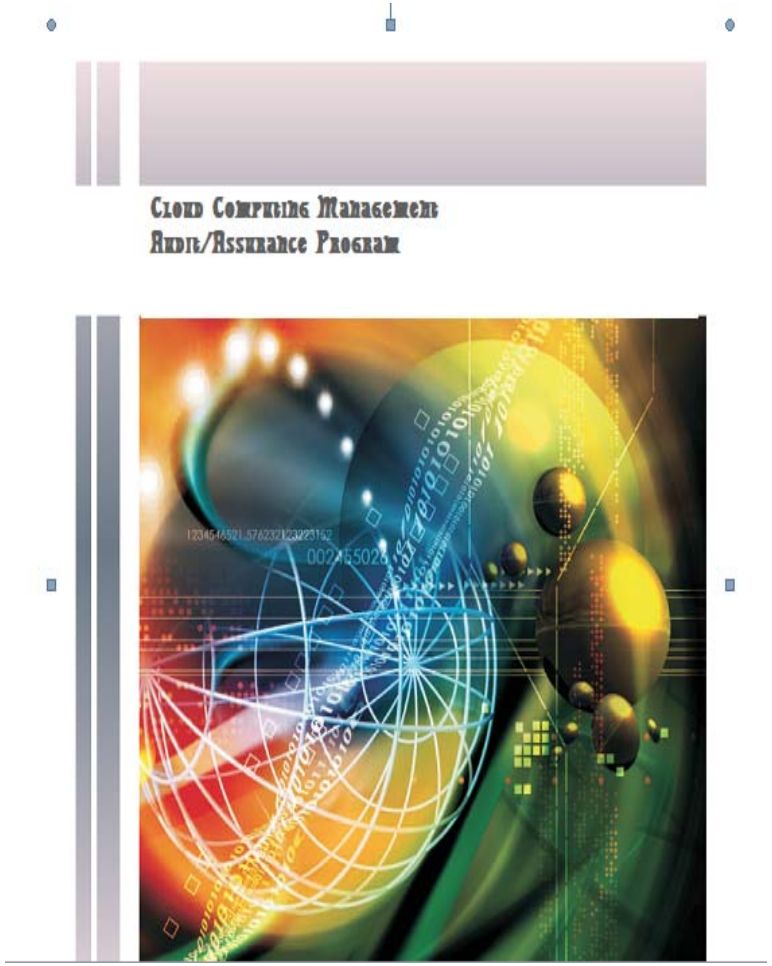
Appendix II

Risk Based Approach Supplement

ISACA Cloud Computing Audit Program

Use and Benefits

- Tool and template to be used as a road map for Cloud audits
- Provide stakeholders with an assessment of the effectiveness of the cloud computing service provider's internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provide audit stakeholders with an assessment of the quality of and their ability to rely upon the service provider's attestations regarding internal controls.
- The review focuses on:
  - The governance affecting cloud computing
  - The contractual compliance between the service provider and customer
  - Control issues specific to cloud computing



ISACA Cloud Computing Audit Program – Areas

1 Planning and Scoping the Audit

- 1.1 Define the audit/assurance objectives
- 1.2 Define the boundaries of review
- 1.3 Identify and document risks
- 1.4 Define the change process
- 1.5 Define assignment success
- 1.6 Define the audit/assurance resources required
- 1.7 Define deliverables
- 1.8 Communications

2. Governing the Cloud

- 2.1 Governance and Enterprise Risk Management (ERM)
- 2.2 Legal and Electronic Discovery
- 2.3 Compliance and Audit
- 2.4 Portability and Interoperability

3. Operating in the Cloud

- 3.1 Incident Response, Notification and Remediation
- 3.2 Application Security
- 3.3 Data Security and Integrity
- 3.4 Identity and Access Management
- 3.5 Virtualization

Shared Assessments - SIG7.0/AUP6.0

Use and Benefits

Version 7.0 of the Standard Information Gathering (“SIG”) questionnaire introduces an entirely new section for assessing Cloud Computing risk. The Agreed Upon Procedures (“AUP”) v 6.0 include the SIG’s new Cloud section .

- It is the first vendor risk assessment tool to provide a comprehensive assessment of all current IT service provider risks.
- It is cross referenced to the Shared Assessment Cloud Computing White paper which provides an expansive review of Cloud risks and controls.

V. Cloud

324 Total Questions to be Answered — 0% Percent Complete

Questionnaire Instructions:
For each question choose either Yes, No or N/A from the drop-down menu provided. If N/A is chosen, an explanation is mandatory. Use the "Additional Information" field to the right of the question. Click on the instruction pop-up box and drag if necessary.

Ques Num	Question/Request	Response	Additional Information	Service Model	Deployment Model	AUP Reference	ISO Ref Num
V.1	Are Cloud Services provided? If so, what service model is provided (select all that apply):						4.1 4.2
V.1.1	Software as a Service (SaaS)?						N/A
V.1.2	Platform as a Service (PaaS)?						N/A
V.1.3	Infrastructure as a Service (IaaS)?						N/A
V.1.4	What deployments models are provided (select all that apply):						4.1 4.2
V.1.4.1	Private cloud?						N/A
V.1.4.2	Public cloud?						N/A
V.1.4.3	Community cloud?						N/A
V.1.4.4	Hybrid cloud?						N/A
V.1.5	Where is the cloud infrastructure hosted:						4.1 4.2
V.1.5.1	Datacenter: single tenancy?						N/A
V.1.5.2	Co-Location: dedicated server?						N/A
V.1.5.3	Co-Location: shared server?						
V.1.5.4	Co-Location: dedicated cabinet?						N/A
V.1.5.5	Co-Location: shared cabinet?						N/A
V.1.5.6	Co-Location: dedicated cage?						N/A
V.1.5.7	Co-Location: shared cage?						N/A
V.1.5.8	Cloud provider: e.g. AWS?						N/A
V.1.6	What legal jurisdiction does data reside in (select all that apply):						15.1.1
V.1.6.1	USA?						N/A
V.1.6.2	Canada?						N/A
V.1.6.3	Asia?						N/A

Shared Assessments - SIG7.0/AUP6.0

The Standard Information Gathering (“SIG”) Questionnaire contains a set of questions to gather and assess information technology, operating and security risks (and their corresponding controls) in an information technology environment. The SIG questions are based on referenced industry standards (including, but not limited to, FFIEC, ISO, COBIT and PCI), and in addition to assessing a third-party’s environment, can be used by a company to self-assess its own control environment. The SIG is in an Excel format which should be familiar to most users.

In addition to questions which gather more general information about the vendor, the SIG consists of fifteen (15) detailed sections which gather detailed information as appropriate to the nature of the services being provided. These sections include:

- **Risk Management**
- **Security Policy**
- **Organizational Security**
- **Asset Management**
- **HR Security**
- **Physical and Environmental Security**
- **Communications and Operations Management**
- **Access Control**
- **Incident Event and Communications Management**
- **Business Continuity and Disaster Recovery**
- **Compliance**
- **Privacy**
- **Cloud Computing**
- **Documentation**
- **Additional Questions**

Federal Risk and Authorization Management Program

Use and Benefits

The Federal Risk and Authorization Management Program (FedRAMP) is a government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

- FedRAMP represents a minimal set of required security controls, a limited subset of the controls most systems would be required to have in place and operating effectively under normal Federal Information Security Management Act (FISMA) authorization processes

FedRAMP Security Controls Baseline
Version 1.0

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
1.1. Access Control (AC)					
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AC-2	Account Management	AC-2	AC-2 AC-2 (1) AC-2 (2) AC-2 (3) AC-2 (4) **AC-2 (7)**	AC-2j. [Assignment: organization-defined frequency] Parameter: [at least annually] AC-2 (2) [Assignment: organization-defined time period for each type of account (temporary and emergency)] Parameter: [no more than ninety days for temporary and emergency account types] AC-2 (3) [Assignment: organization-defined time period] Parameter: [ninety days for user accounts]	AC-2 (3) Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB.

Appendix III

Service Organization Controls (SOC) – AICPA References

Service Organization Controls - SOC 2/3

AICPA guidance — **Trust Services Principles (TSP)** section 100 provides criteria for evaluating and reporting on controls related to security, availability, processing integrity, confidentiality, and privacy.

In TSP section 100, these five attributes of a system are known as principles, and they are defined in paragraph .10 of TSP section 100 as follows;

- **Security** — The system is protected against unauthorized access (both physical and logical).
- **Availability** — The system is available for operation and use as committed or agreed.
- **Processing integrity** — System processing is complete, accurate, timely, and authorized.
- **Confidentiality** — Information designated as confidential is protected as committed or agreed.
- **Privacy** — Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in **Generally Accepted Privacy Principles (GAPP)**

Service Organization Controls - SOC 2/3

AICPA guidance — Footnote 1 of TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids), contains the following definition of a system:

- A **system consists of five key components** organized to achieve a specified objective. The five components are categorized as follows:
  - **Infrastructure** — The physical and hardware components of a system (facilities, equipment, and networks)
  - **Software** — The programs and operating software of a system (systems, applications, and utilities)
  - **People** — The personnel involved in the operation and use of a system (developers, operators, users, and managers)
  - **Procedures** — The automated and manual procedures involved in the operation of a system
  - **Data** — The information used and supported by a system (transaction streams, files, databases, and tables)

Service Organization Controls

AICPA products related to service organization controls

- The AICPA recently developed resources for CPAs, service organizations and user entities who need to build trust and confidence in outsourced services. The sources include:
  - Online source center: www.aicpa.org/SOC
    www.aicpa.org/infotech
  - Online brochure to provide an introduction to the concept of Service Organization Control (SOC) reports.
  - SSAE 16 Publication: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/SSAEs/PRDOVR~PC-023035/PC-023035.jsp
  - SOC 2 Publication: http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/SOC/PRDOVR~PC-0128210/PC-0128210.jsp