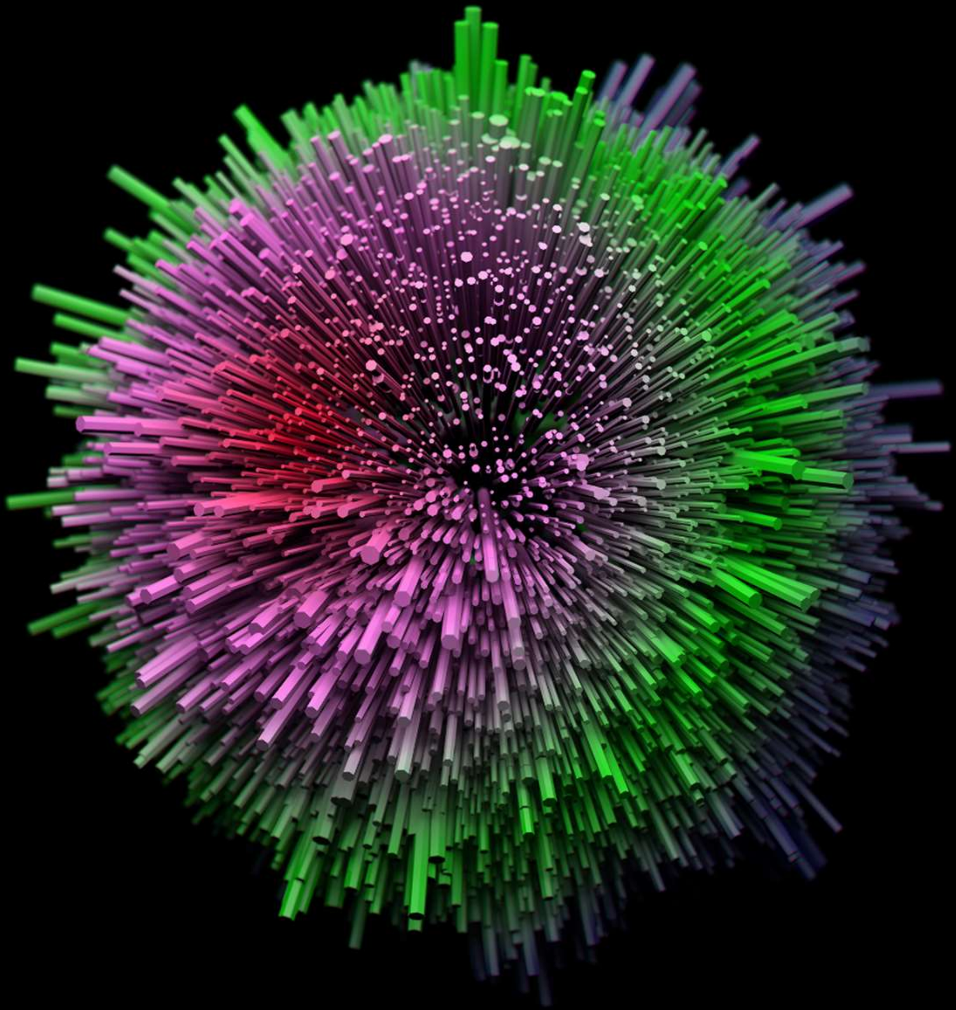
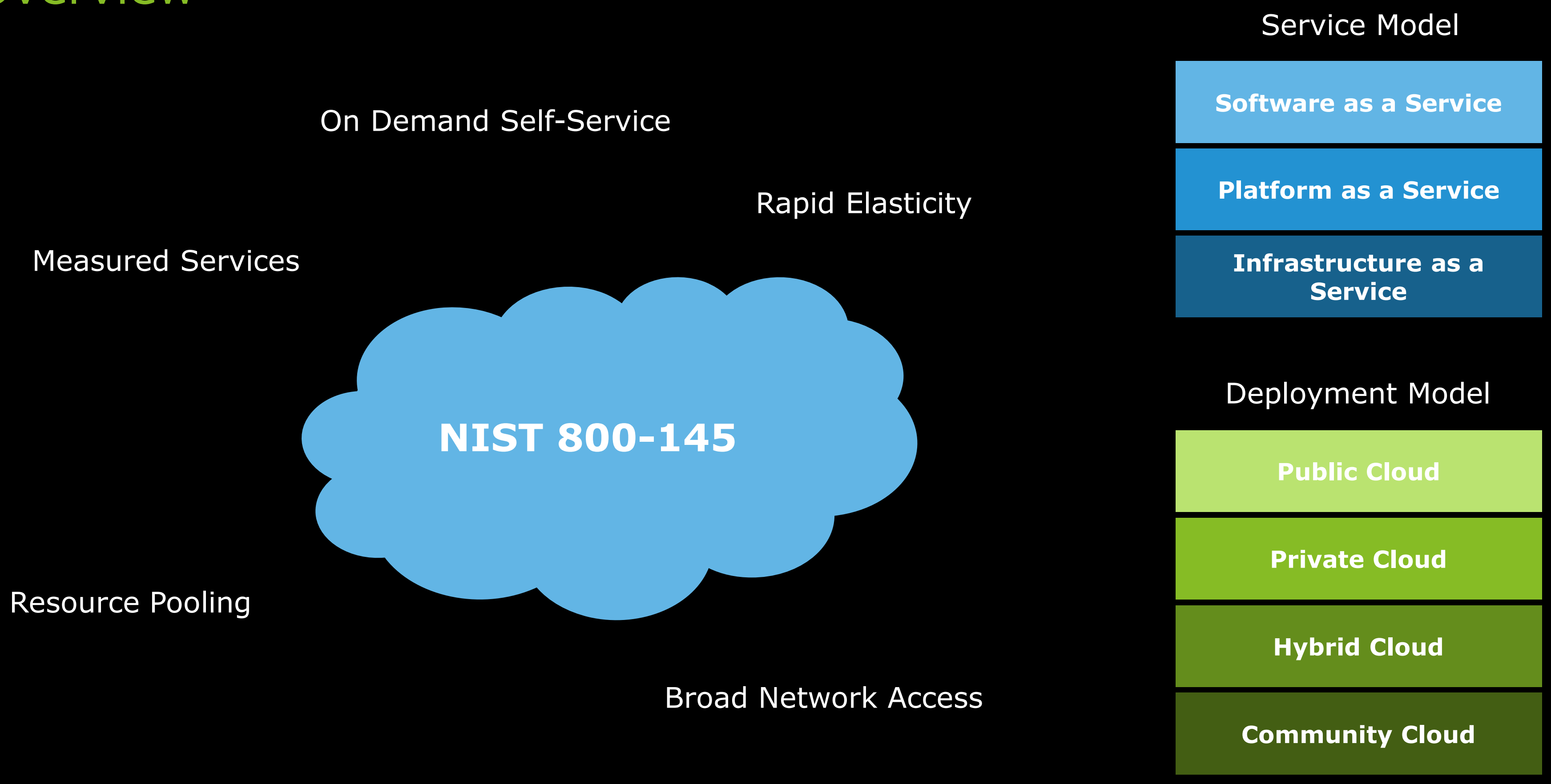


Audit - Cloud

Deloitte Risk Advisory

Cloud Computing

Overview



NIST 800-145

On Demand Self-Service

Rapid Elasticity

Measured Services

Resource Pooling

Broad Network Access

Service Model

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Deployment Model

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud

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

Deployment Models

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
Service Delivery

Software as a Service

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 rewritten to meet the specifications of the vendor.

User utilizes the vendors IT staff and has limited to no technical staff.

Platform as a Service

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 rewritten to meet the specifications of the vendor.

User of the Cloud maintains a development staff.

Infrastructure as a Service

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.

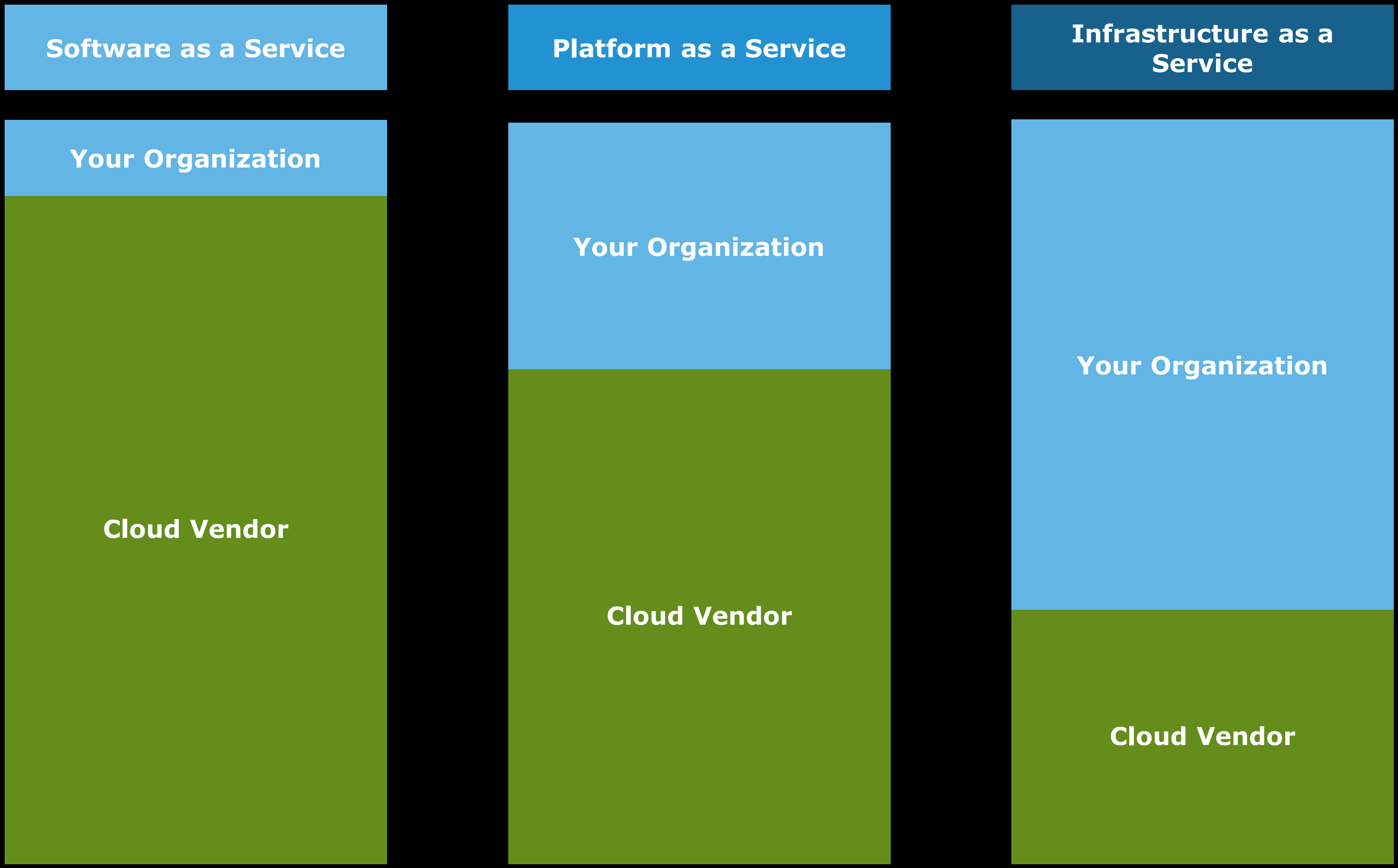
Customization:

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).

Cloud Computing
Service Delivery – Responsibility Chart



Software as a Service

Your Organization

Cloud Vendor

Platform as a Service

Your Organization

Cloud Vendor

Infrastructure as a Service

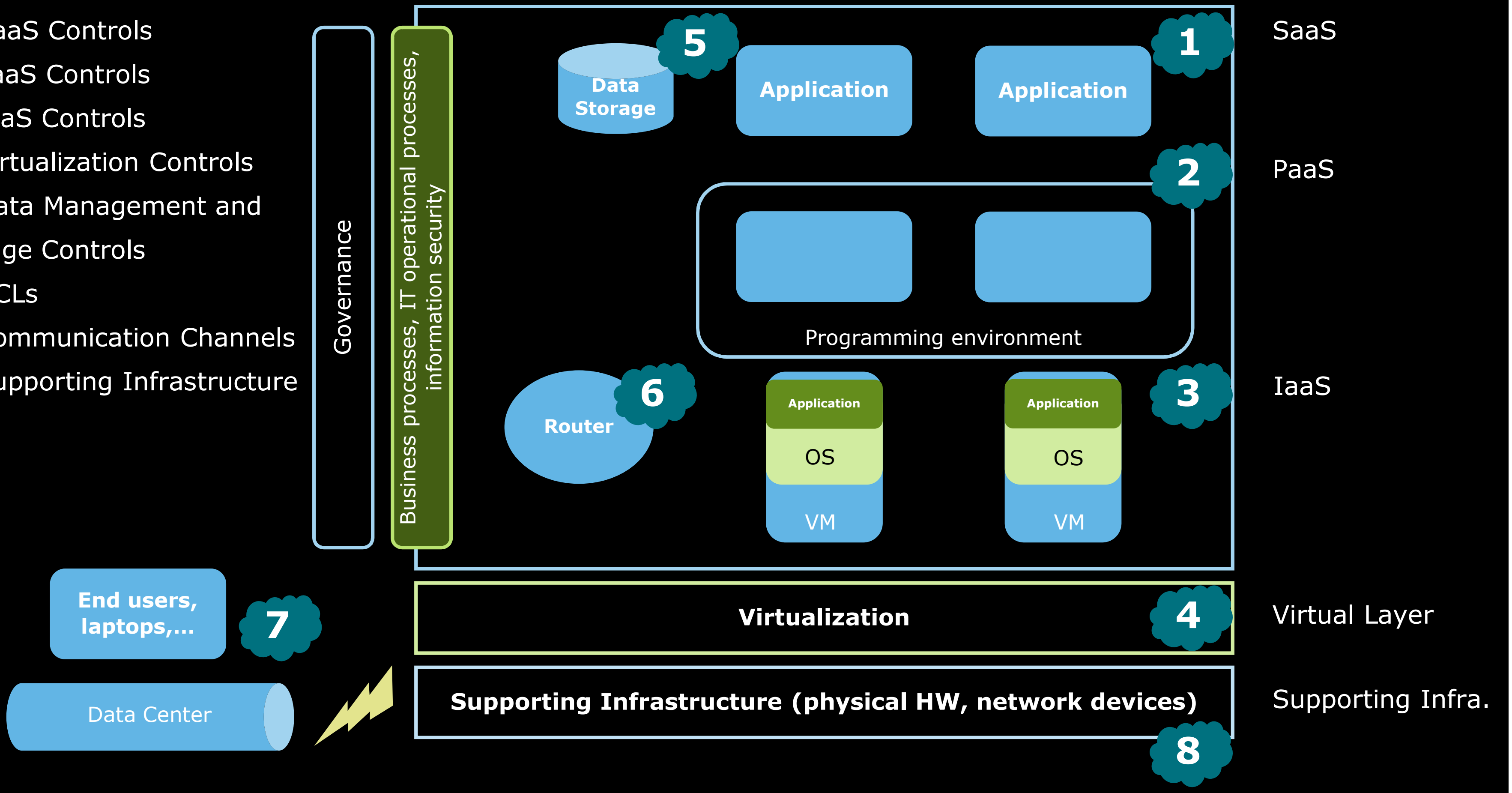
Your Organization

Cloud Vendor

Risk and Controls

…are widespread.

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



Audit Cloud

Challenges with Cloud Computing

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

Audit Cloud

Internal Audit’s Role

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.

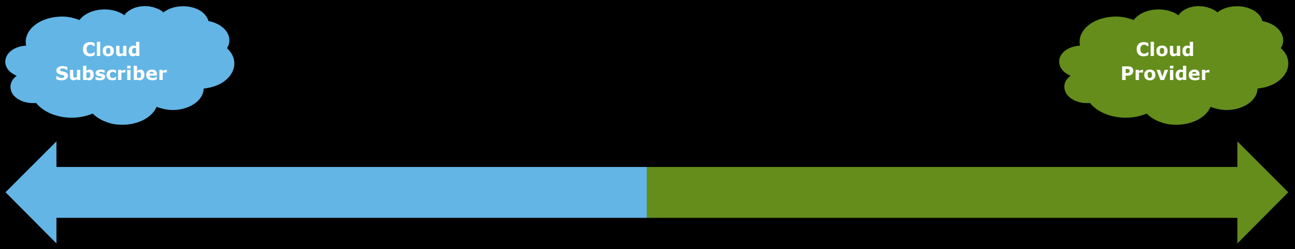
Help mitigate risks

- 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

Audit Cloud

Managing Cloud Computing Risk – part I



	Cloud Subscriber	Cloud Provider
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

Audit Cloud

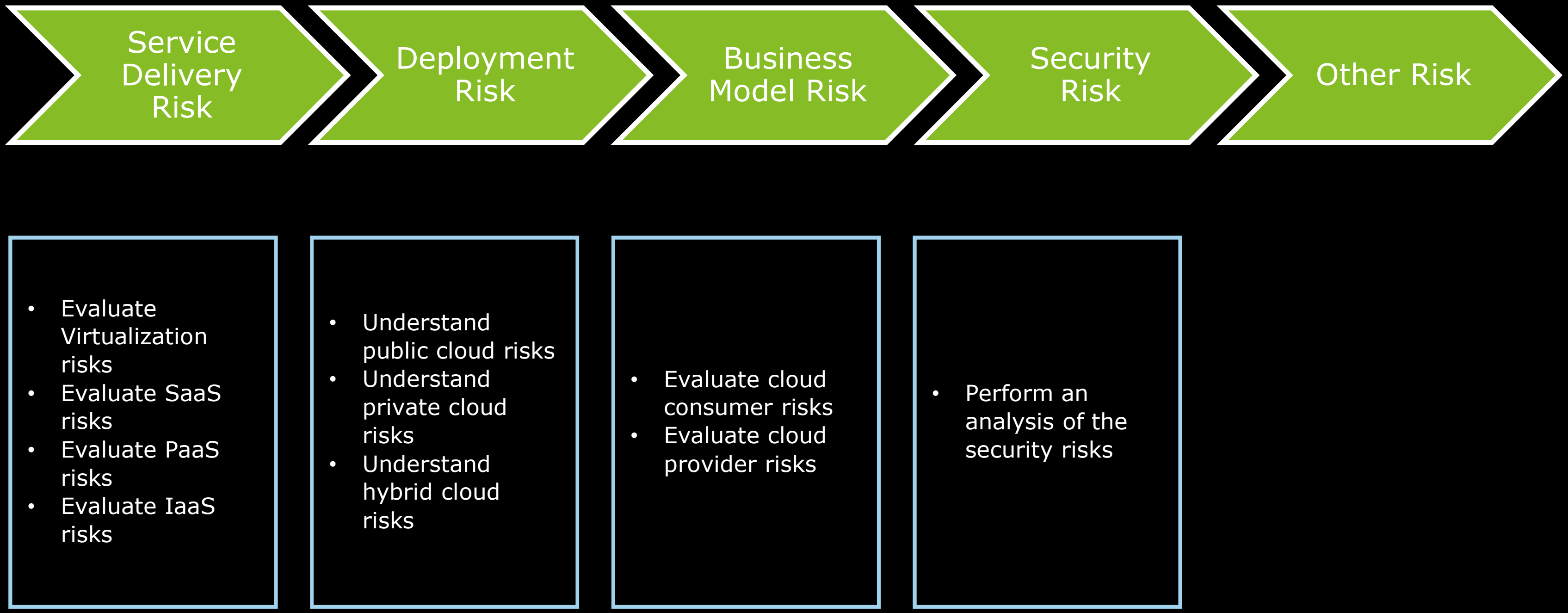
Managing Cloud Computing Risk – part II

	Cloud Subscriber	Cloud Provider
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	• 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

Audit Cloud

Solution – 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 Risk

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

Audit Cloud
Contact

Nik Černomorský

Risk Advisory Lead

Phone:+420 734 755 521

Email: ncernomorsky@deloittece.com

Jan Seidl

Senior Manager | Cyber Risk

Phone:+420 739 647 334

Email: jaseidl@deloittece.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/cz/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, legal, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, the member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Services are provided by the subsidiaries and affiliates of Deloitte Central Europe Holdings Limited, which are separate and independent legal entities. The subsidiaries and affiliates of Deloitte Central Europe Holdings Limited are among the region’s leading professional services firms, providing services through more than 6,000 people in 44 offices in 18 countries.