ISACA®
Kolkata Chapter

ANNUAL SEMINAR 2023
Artificial Intelligence and Its Impact on The Security Professionals
Organized by ISACA Kolkata Chapter

The What, Way and How of Performing Practical Cloud Security and Audit

KEYNOTE SPEAKER

CA Abdul Rafeq

FCA, CISA, DISA (ICAI), Fellow Member of ICAI

Topics: The Why and Way of Performing Effective Third Party Risk Management & The What, Why and How of Performing Practical Cloud Security and Audit

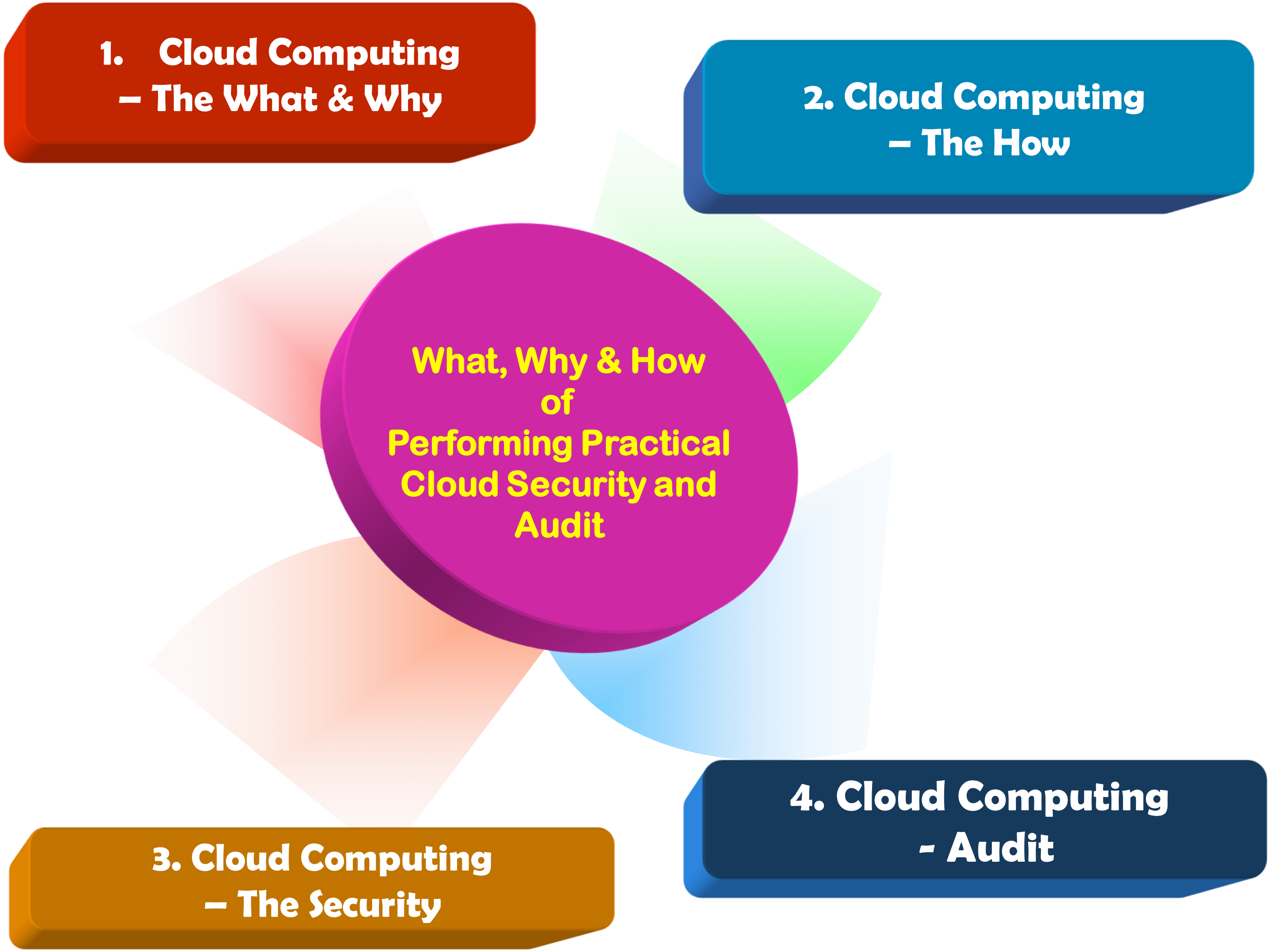
12:00 PM – 01:00 PM & 02:00 PM – 03:00 PM

Managing Director, Wincer Infotech Limited

https://wincaat.com

Saturday, 9th December 2023

Agenda



1. Cloud Computing – The What & Why

2. Cloud Computing – The How

What, Why & How of Performing Practical Cloud Security and Audit

3. Cloud Computing – The Security

4. Cloud Computing - Audit

1. Cloud Computing – The What & Why

Key Definitions

Cloud

- The “**cloud**” in cloud computing is defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service.

Cloud services

- **Cloud services** include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand.

Key Definitions

Access

- **Access** to the cloud is generally provided via multiple technologies (Internet or other) and services can include processing, storage, access to applications and business processes.

Cloud participants

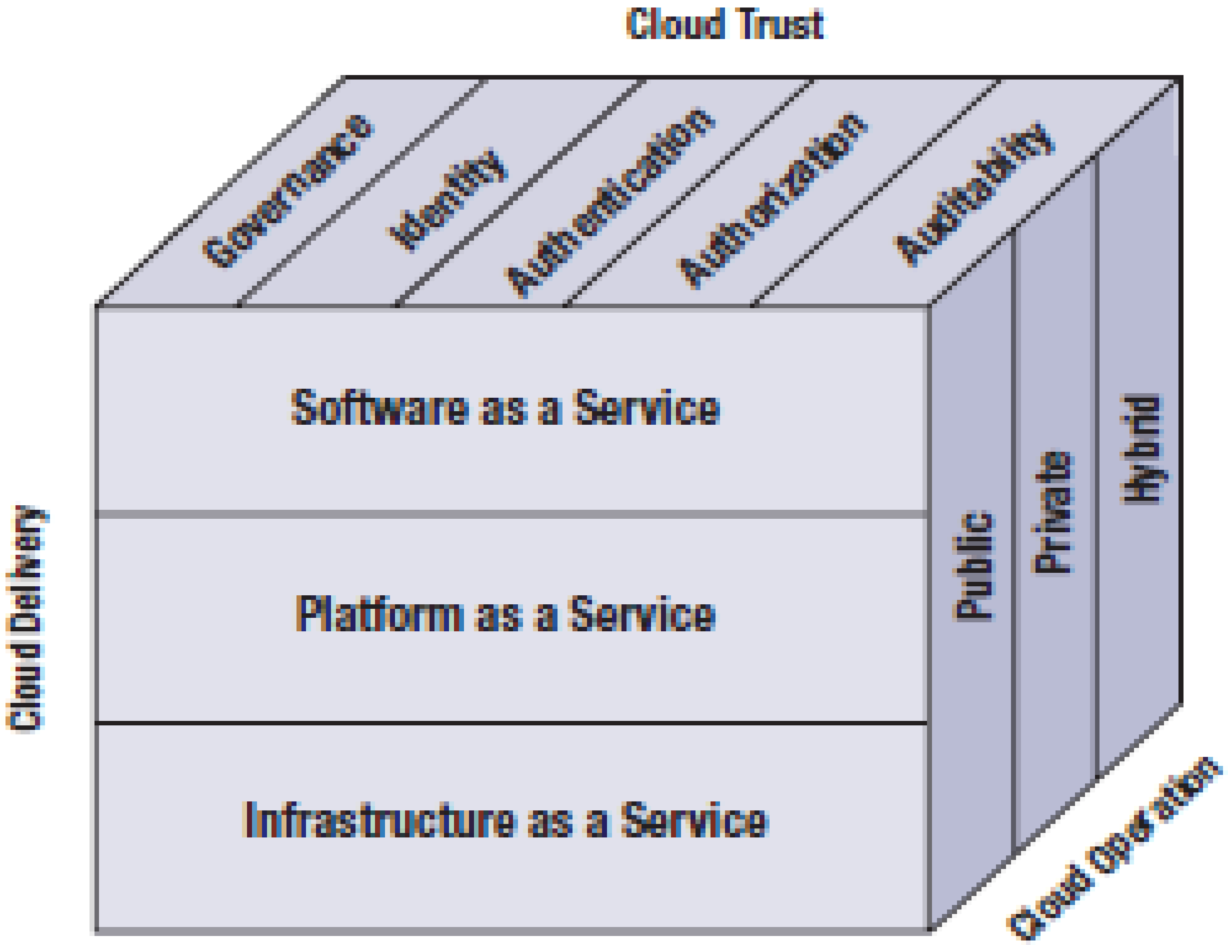
- **The end user** who doesn’t have to know anything about the underlying technology of the cloud.
- **Enterprise management** who are responsible for the management of data or services living in a cloud.
- **The cloud service provider** who is responsible for IT assets and maintenance and for providing the services as per service level agreement.

Cloud Computing Fundamentals

- **On-demand self-service**—Computing capabilities can be provisioned without human interaction from the service provider.
- **Broad network access**—Computing capabilities are available over the network and can be accessed by diverse client platforms.
- **Resource pooling**—Computer resources are pooled to support a multitenant model.
- **Rapid elasticity**—Resources can scale up or down rapidly and, in some cases, automatically, in response to business demands.
- **Measured service**—Resource utilization can be optimized by leveraging charge-per-use capabilities.

Computing Service Delivery and Deployment Model

Figure 1—Cloud Computing Service Delivery and Deployment Model



Source: Trusted Cloud Reference Architecture © Cloud Security Alliance, *cloudsecurityalliance.org*. Used with permission.

Cloud Deployment Models

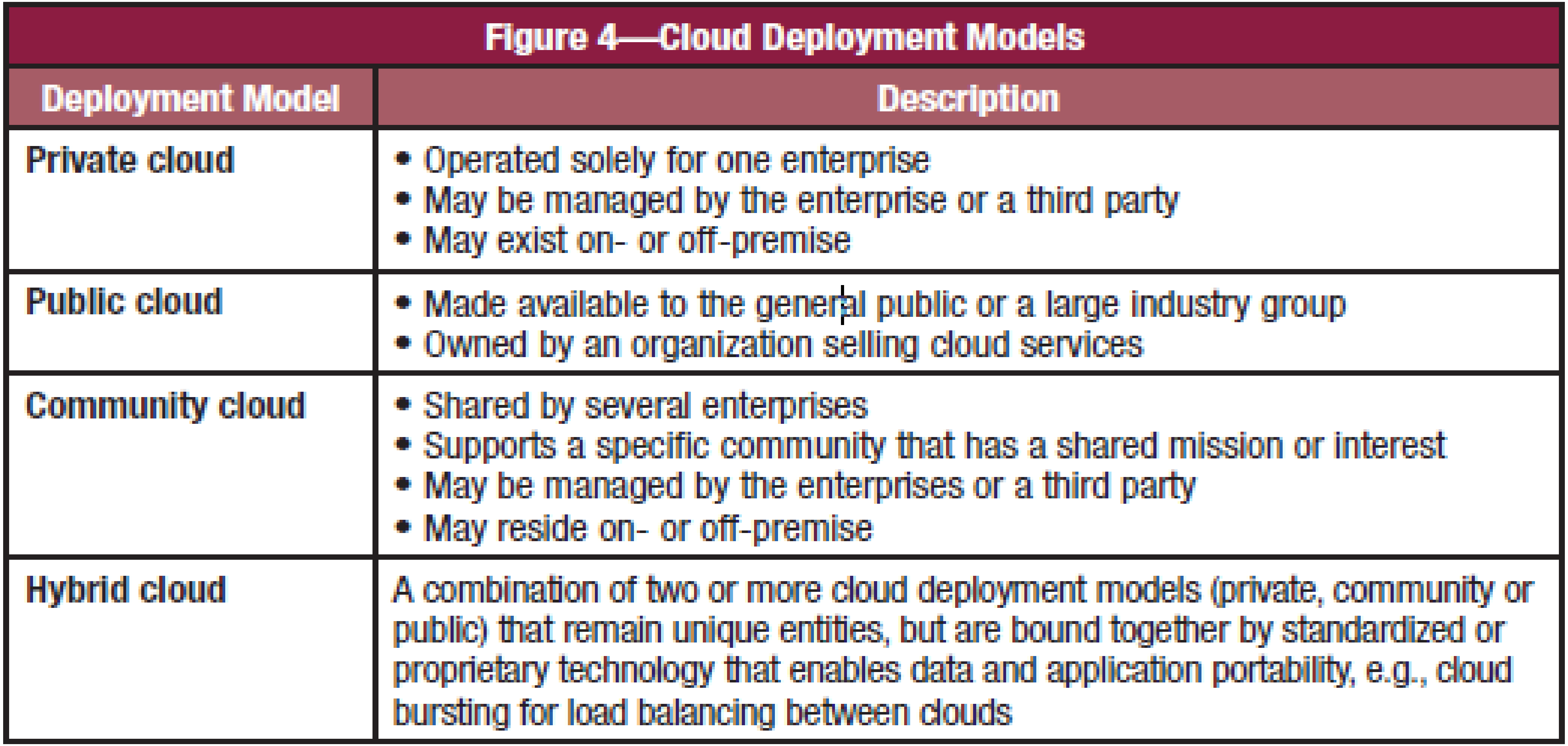
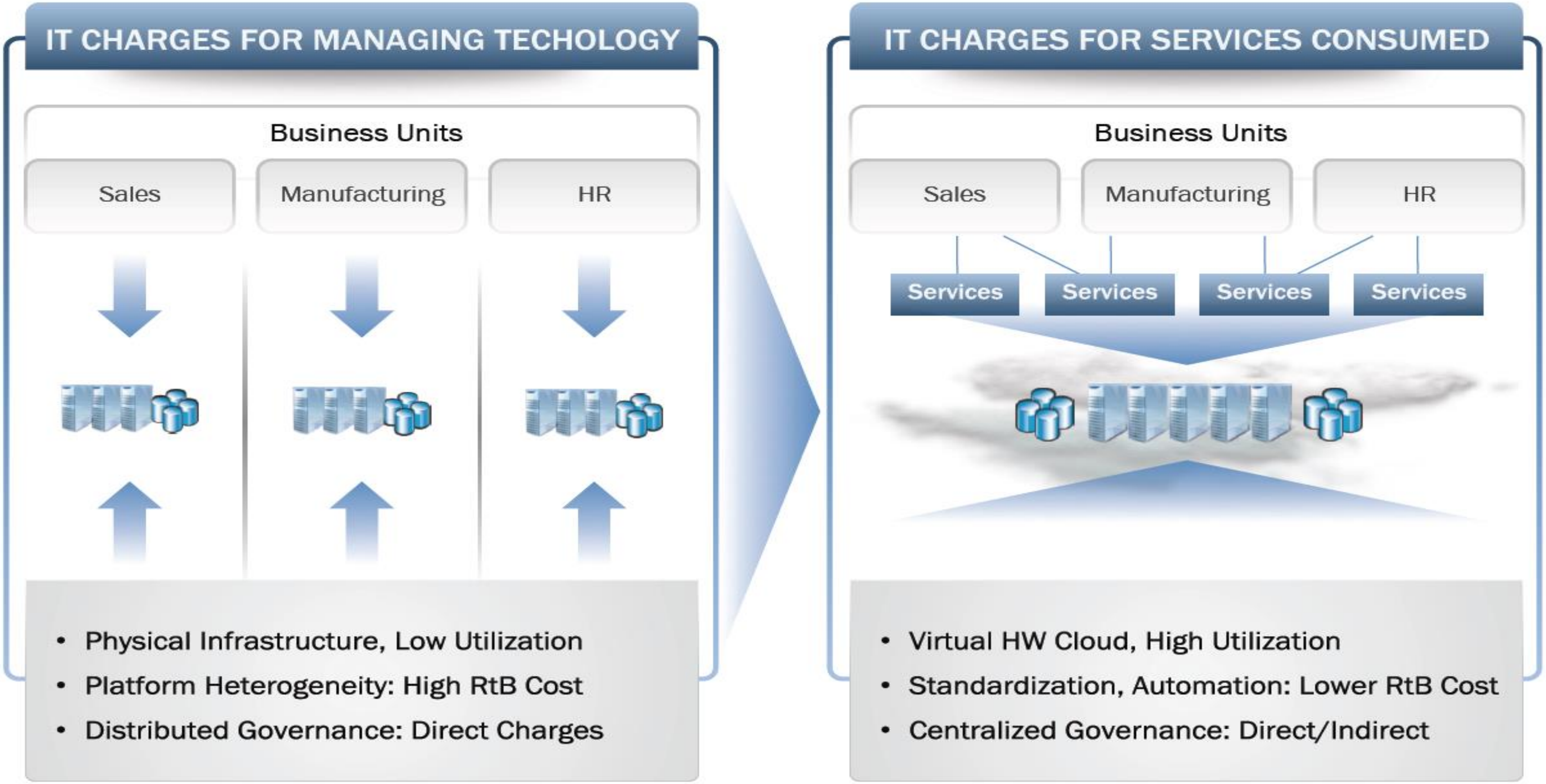


Figure 4—Cloud Deployment Models

Deployment Model	Description
Private cloud	• Operated solely for one enterprise • May be managed by the enterprise or a third party • May exist on- or off-premise
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services
Community cloud	• Shared by several enterprises • Supports a specific community that has a shared mission or interest • May be managed by the enterprises or a third party • May reside on- or off-premise
Hybrid cloud	A combination of two or more cloud deployment models (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability, e.g., cloud bursting for load balancing between clouds

The “Cloud” Story is Straightforward…



IT CHARGES FOR MANAGING TECHOLOGY

Business Units

Sales

Manufacturing

HR

- Physical Infrastructure, Low Utilization
- Platform Heterogeneity: High RtB Cost
- Distributed Governance: Direct Charges

IT CHARGES FOR SERVICES CONSUMED

Business Units

Sales

Manufacturing

HR

Services

Services

Services

Services

- Virtual HW Cloud, High Utilization
- Standardization, Automation: Lower RtB Cost
- Centralized Governance: Direct/Indirect

What can users do with Cloud Computing

With cloud computing, users can remotely store their data into the cloud and use on-demand high-quality applications

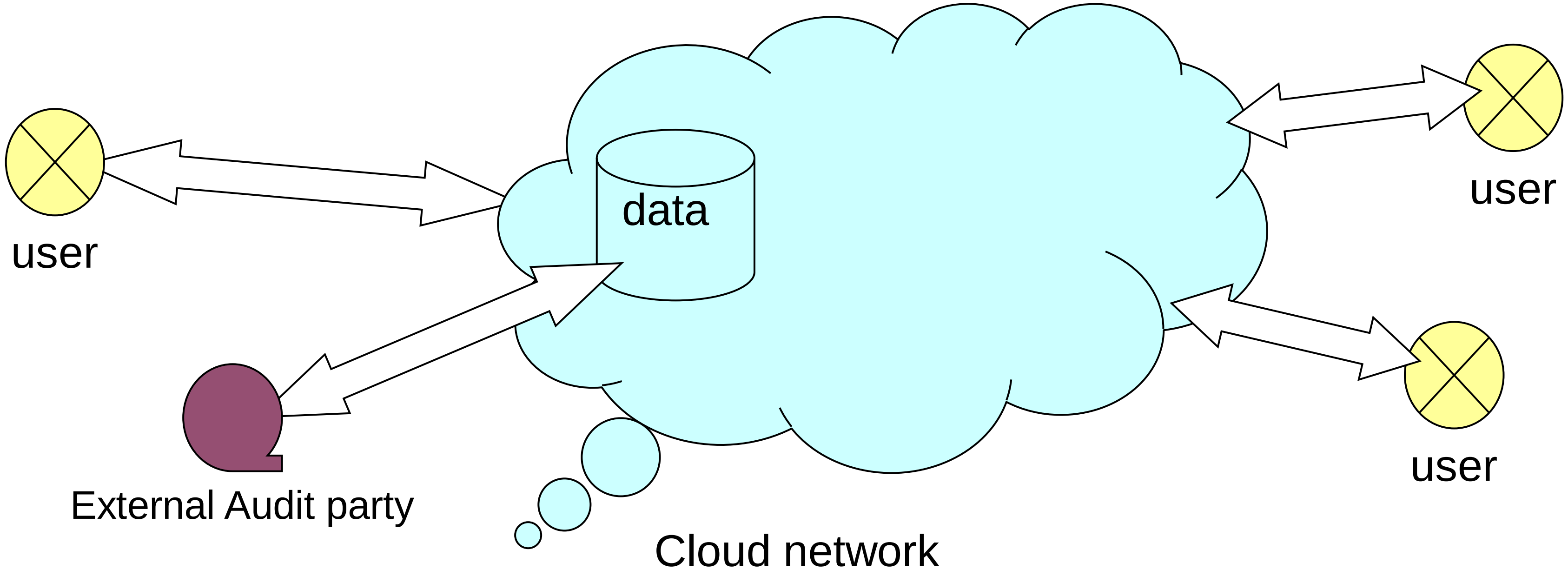
Using a shared pool of configurable computing resources

Data outsourcing: users are relieved from the burden of data storage and maintenance

When users put their data (of large size) on the cloud, the data integrity protection is challenging

Enabling public audit for cloud data storage security is important

Users can ask an external audit party to check the integrity of their outsourced data



6 Core Questions About the "Cloud"…

1. Which **app/service candidates** should be moved to the cloud?

2. What is the **TCO of services** leveraging internal vs. external cloud?

3. How to **price** IT services delivered via a virtual private cloud (VPC)?

4. How do my IT service **costs (& prices) compare** to 3rd parties?

5. How to deliver fair and **accurate showback;** including shadow IT?

6. How to effectively **plan** capacity to meet business demand?

Why Cloud Computing?

Changes how we invent, develop, deploy, scale, update, maintain, and pay for applications and the infrastructure on which they run.

Cloud Computing Benefits from the provider

Efficiency
Drives cost out of the delivery of services, eliminating capital expense in favor of more easily managed operating expense

Agility
Increases speed and agility in deploying services, adapting to seasonal or cyclical computing needs

Speed
Shortens implementation cycle time

Flexibility
With application deployment decoupled from server deployment, applications can be deployed and scaled rapidly, without having to procure physical servers

Ubiquity
Applications can be made available anywhere, any time

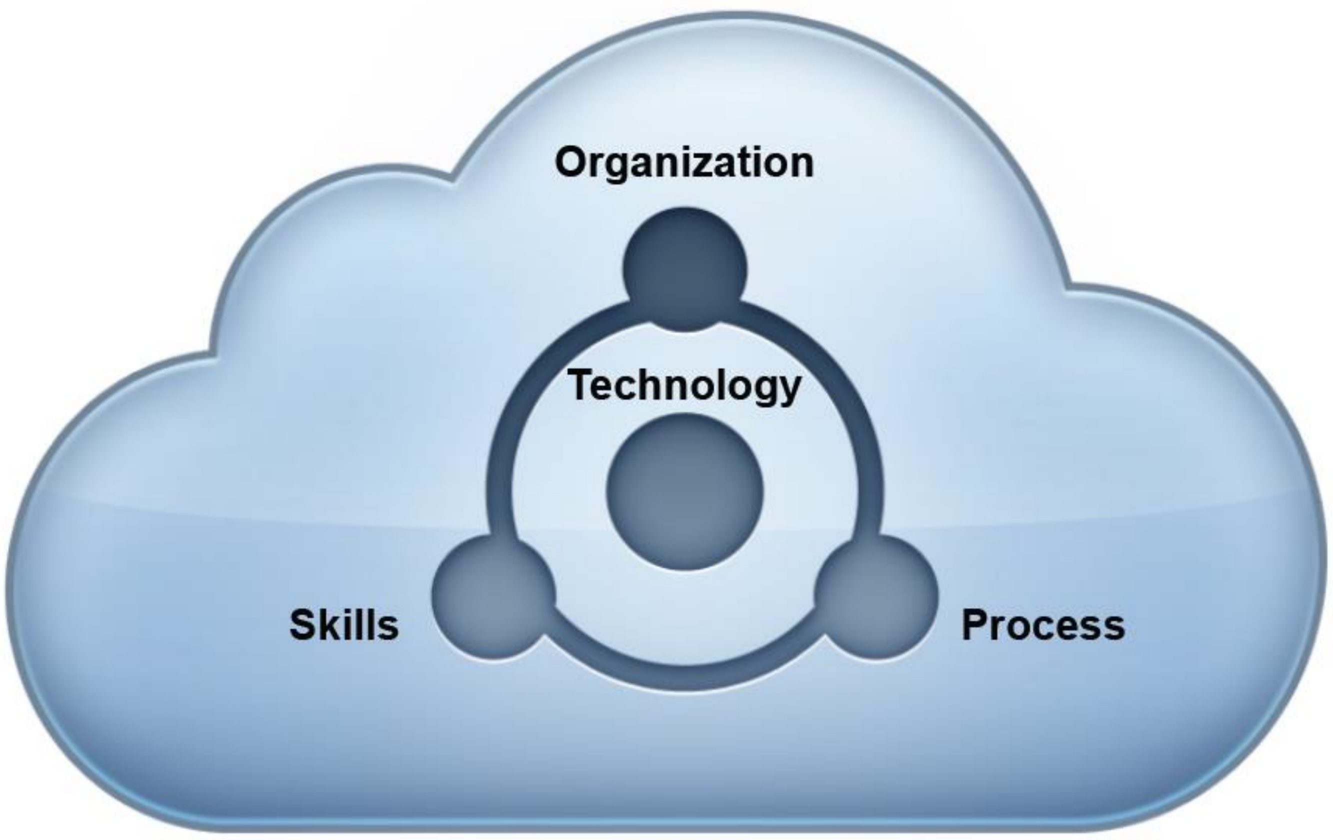
Cost avoidance
Minimizes the risk of deploying physical infrastructure, lowering the cost of entry, thin devices enable Green IT

Accelerated innovation
Reduces run time and response time, increasing the pace of innovation

2. Cloud Computing – The How

Cloud Computing: Key Result Areas

Cloud is an Ecosystem



Cloud Computing: Key Areas

- Business processes
- Different workloads
- Audit requirements
- SLAs
- Compliance
- Latency
- Bandwidth
- Security procedures
- Risk mitigation
- Legal exposure
- Legacy apps
- Staff skills
- Competitive differentiators
- Uptime needs
- Cost focus
- Industry partnerships
- Legal requirements
- Government mandates

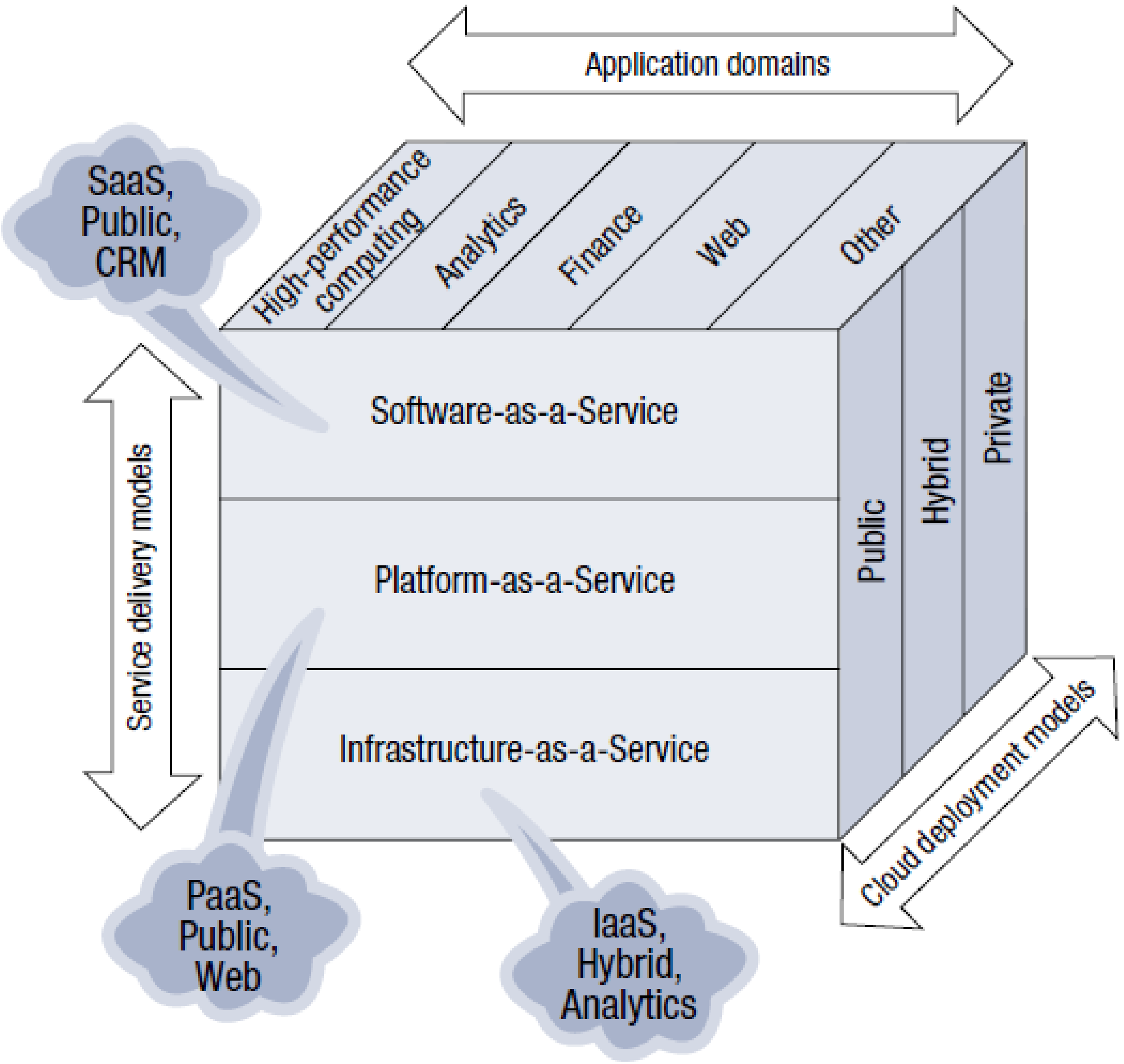
≠

How to Migrate to the Cloud?

- Consider the current IT environment in deciding the right cloud strategy.
- Based on the above, determine the best starting point.
- For example:
  - Implement Infrastructure as a Service so that incremental storage capacity to support a new business initiative.
  - Use Platform as a Service to limit the capital expenses needed to develop a new application.
  - Add Software as a Service such as a Customer Relationship Management (CRM) service to support critical sales efforts without having to expand internal resources.
  - The client may need Business Process as a Service such as a supply chain service on demand to support a pilot test of a new line of business.

3. Cloud Computing – Security

Figure 1.1—Cloud Security Alliance Cloud Computing Service Delivery and Deployment Model



Source: Cloud Computing Service Delivery and Deployment Model, © Cloud Security Alliance, *https://cloudsecurityalliance.org*. Used with permission.

Cloud Delivery Models and Risks

Risks of Cloud Computing

Greater dependency on third parties:

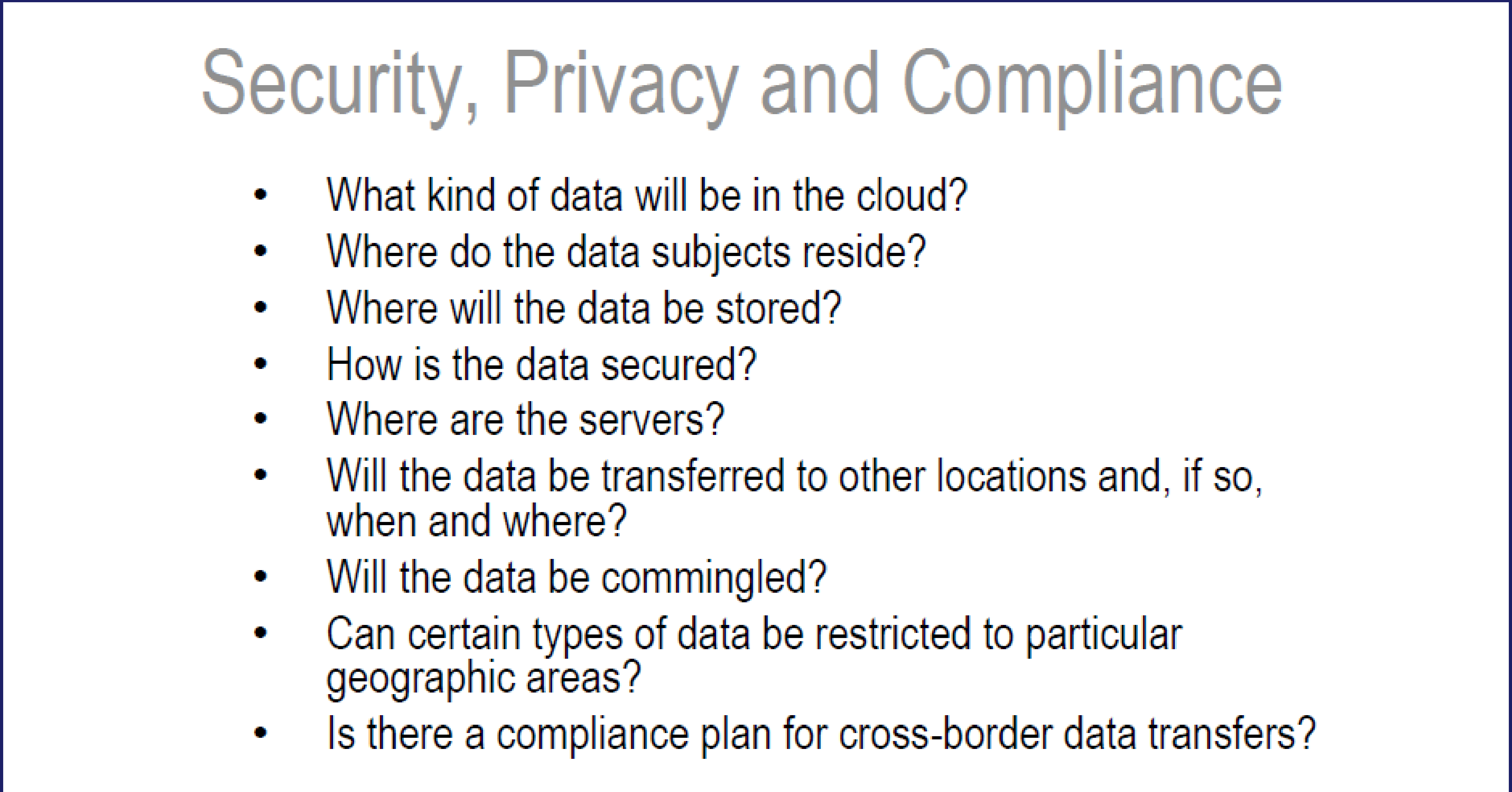
- Increased vulnerabilities in external interfaces
- Increased risks in aggregated data centers
- Immaturity of the service providers with the potential for service provider going concern issues
- Increased reliance on independent assurance processes

Increased complexity of compliance with laws and regulations:

- Greater magnitude of privacy risks
- Transborder flow of personally identifiable information
- Affecting contractual compliance

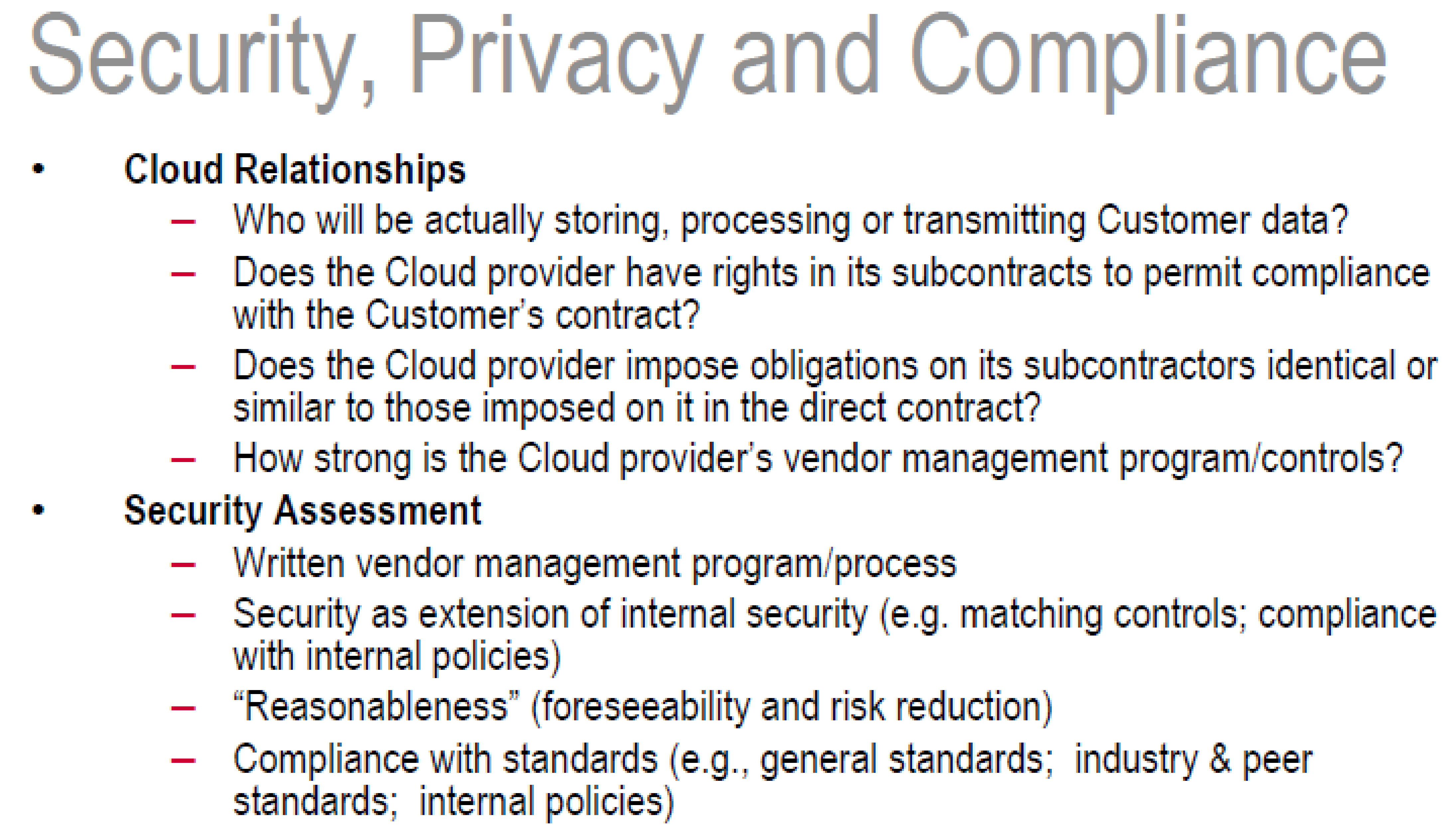
Cloud Computing: Challenges to Consider

- Data location
- Commingled data
- Security policy/procedure transparency
- Cloud data ownership
- Lock-in with Cloud Service Provider Proprietary APIs
- Record protection for Forensic Audits
- Identity and Access management (IAM)
- Screening of other cloud computing clients
- Compliance requirements
- Data disposal
- Portability
- Cloud Service Provider Viability
- Backup and rollout capabilities



Security, Privacy and Compliance

- What kind of data will be in the cloud?
- Where do the data subjects reside?
- Where will the data be stored?
- How is the data secured?
- Where are the servers?
- Will the data be transferred to other locations and, if so, when and where?
- Will the data be commingled?
- Can certain types of data be restricted to particular geographic areas?
- Is there a compliance plan for cross-border data transfers?



Security, Privacy and Compliance

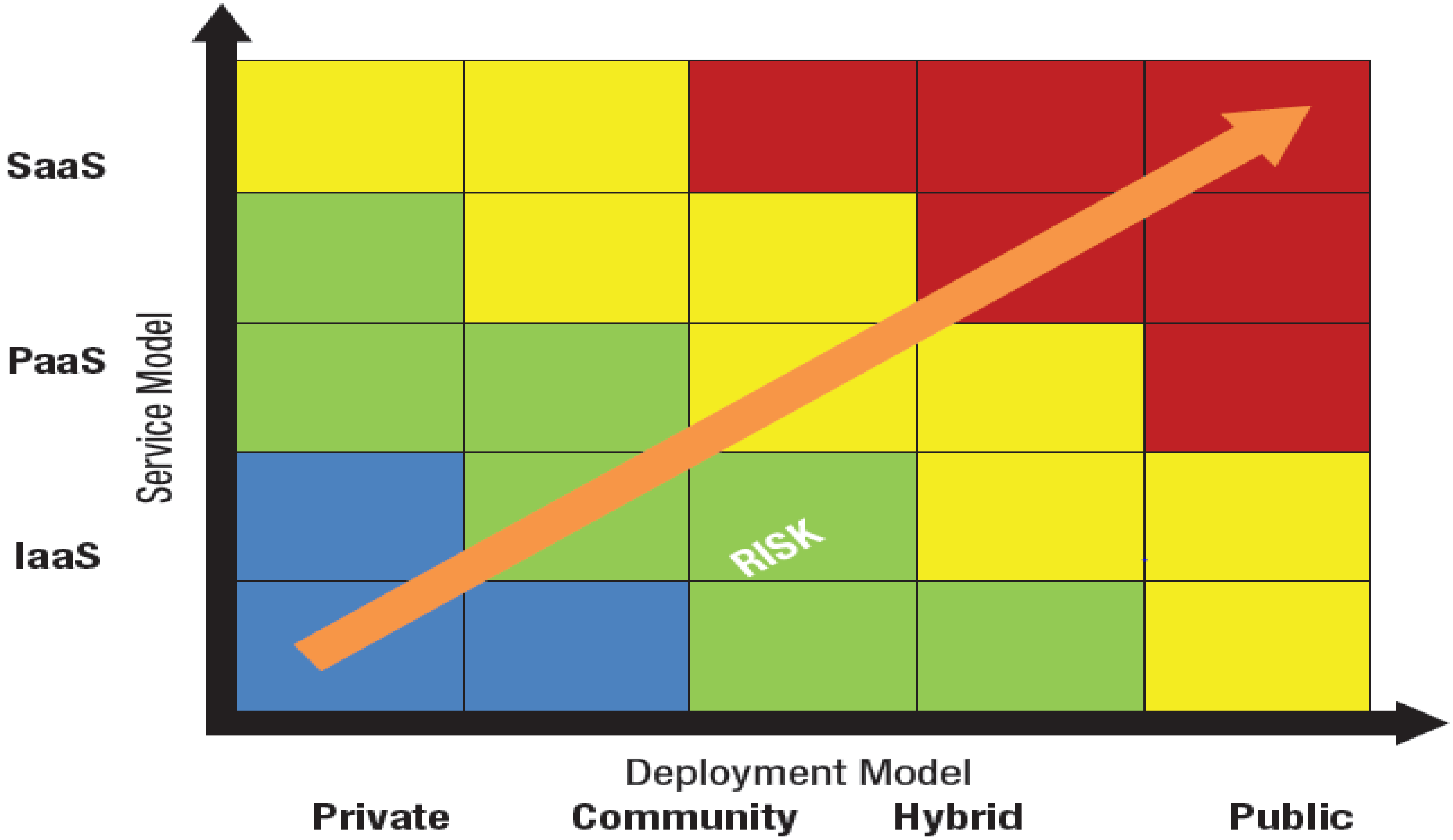
- **Cloud Relationships**
  - Who will be actually storing, processing or transmitting Customer data?
  - Does the Cloud provider have rights in its subcontracts to permit compliance with the Customer's contract?
  - Does the Cloud provider impose obligations on its subcontractors identical or similar to those imposed on it in the direct contract?
  - How strong is the Cloud provider's vendor management program/controls?
- **Security Assessment**
  - Written vendor management program/process
  - Security as extension of internal security (e.g. matching controls; compliance with internal policies)
  - "Reasonableness" (foreseeability and risk reduction)
  - Compliance with standards (e.g., general standards; industry & peer standards; internal policies)

Key Questions to Consider for Risk Assessment of Cloud

- What is the enterprise's expected availability?
- How are identity and access managed in the cloud environment?
- Where will the enterprise's data be located?
- What are the CSP's disaster recovery capabilities?
- How is the security of the enterprise's data managed?
- How is privileged user access to data managed?
- How is the enterprise's information protected from user abuse?
- What type of isolation can the enterprise expect?
- How is the enterprise's information secured on a virtualized environment?
- How is the entire system protected from Internet threats?
- How are activities monitored and audited?
- How will the enterprise ensure that no one has tampered with its data?
- What type of certification or assurances can the enterprise expect from the provider?

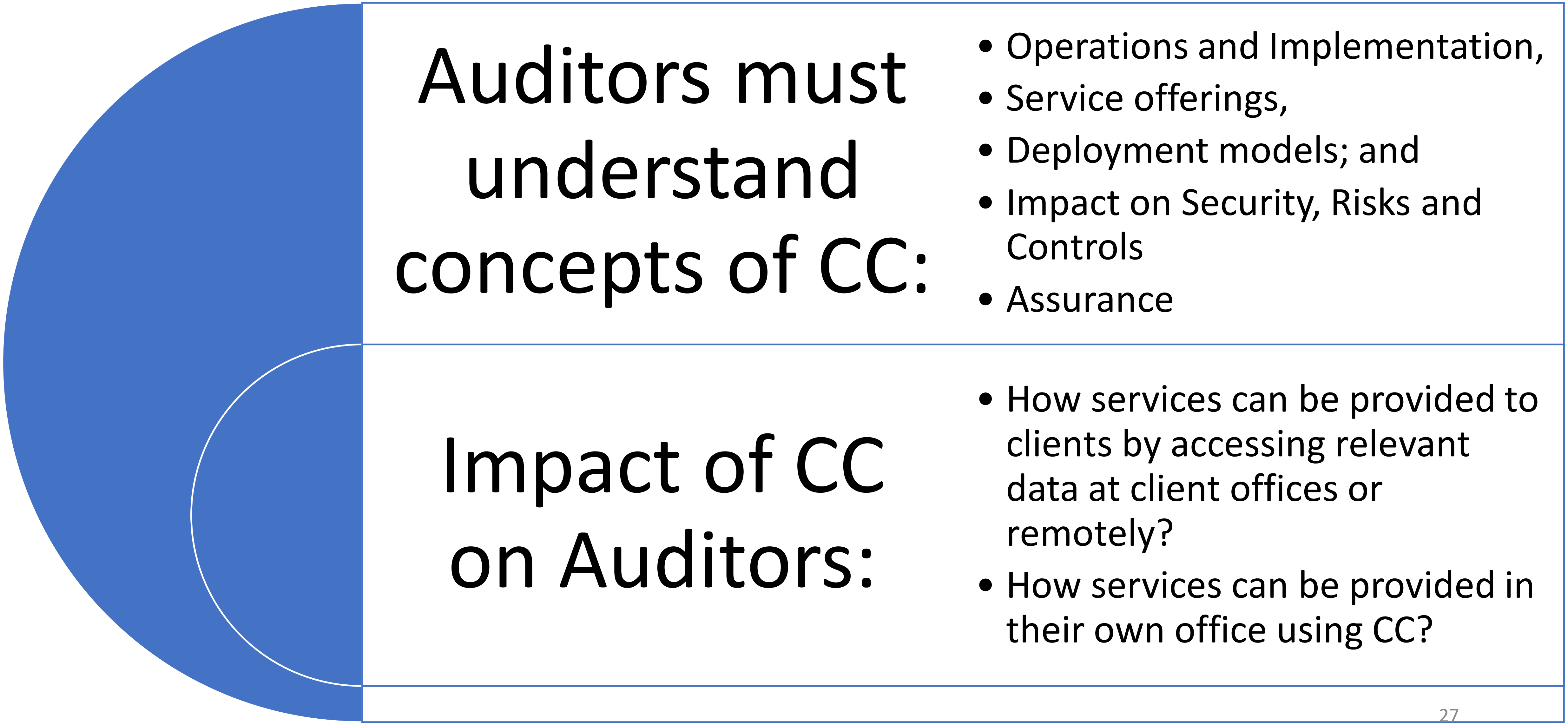
Cloud Computing Risk Map

Figure 3—Cloud Computing Risk Map



4. Cloud Computing – Audit

Cloud Computing and Role of Auditors



Auditors must understand concepts of CC:

- Operations and Implementation,
- Service offerings,
- Deployment models; and
- Impact on Security, Risks and Controls
- Assurance

Impact of CC on Auditors:

- How services can be provided to clients by accessing relevant data at client offices or remotely?
- How services can be provided in their own office using CC?

Cloud Migration Roadmap

1. Vision	• What is the business vision and who will own the initiative?
2. Visibility	• What needs to be done and what are the risks?
3. Accountability	• Who is accountable and to whom?
4. Sustainability	• How will it be monitored and measured?

Cloud Enterprise Risk Management (CERM) Governance Checklist

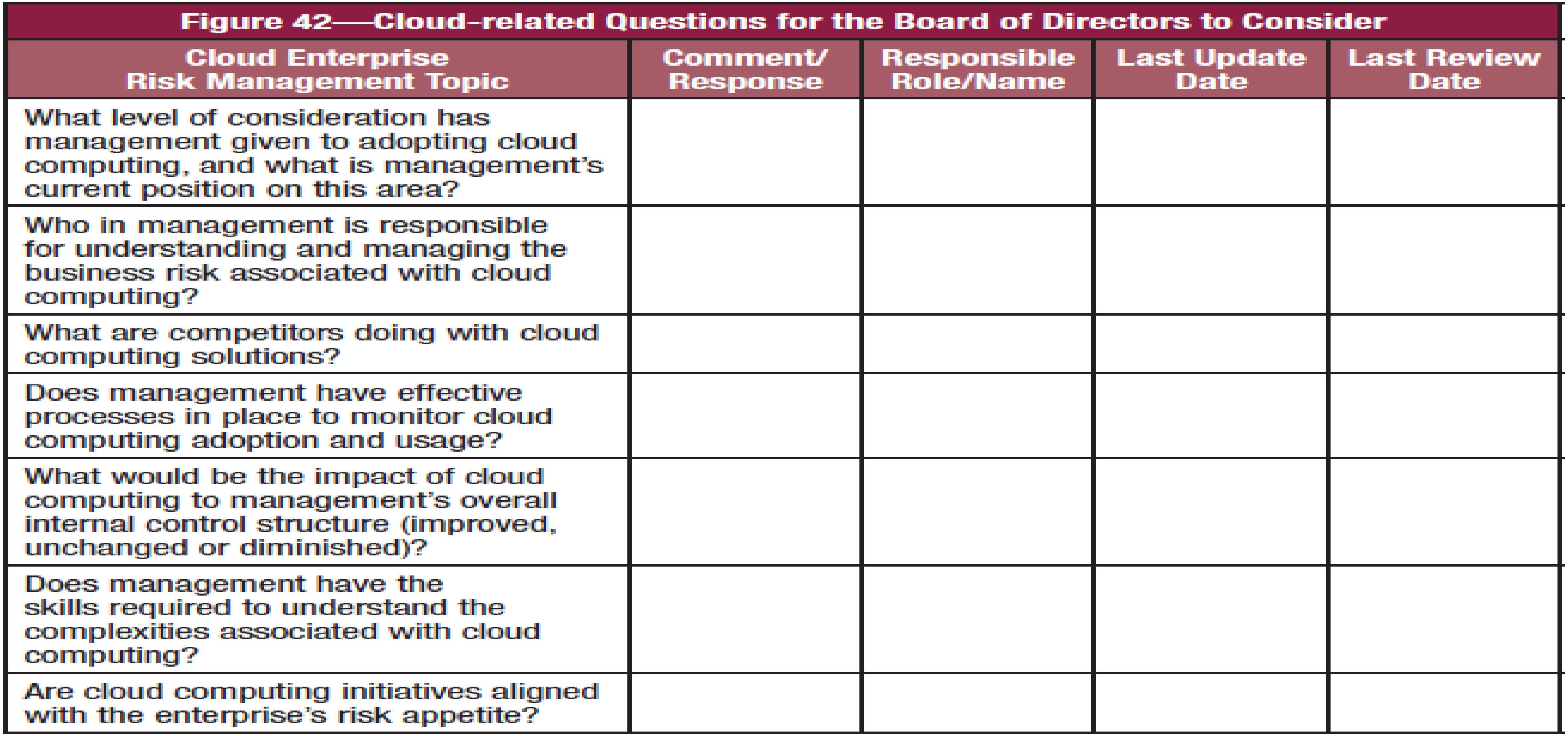


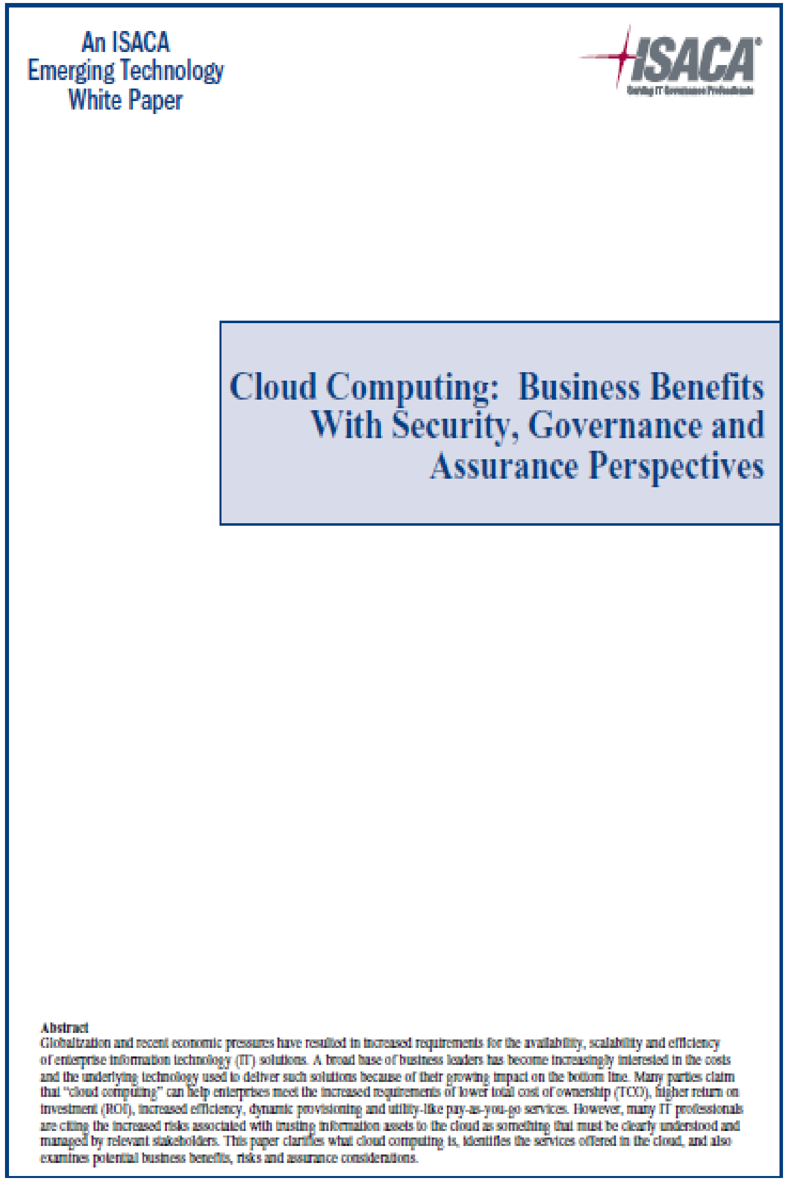
Figure 42—Cloud-related Questions for the Board of Directors to Consider

Cloud Enterprise Risk Management Topic	Comment/ Response	Responsible Role/Name	Last Update Date	Last Review Date
What level of consideration has management given to adopting cloud computing, and what is management's current position on this area?				
Who in management is responsible for understanding and managing the business risk associated with cloud computing?				
What are competitors doing with cloud computing solutions?				
Does management have effective processes in place to monitor cloud computing adoption and usage?				
What would be the impact of cloud computing to management's overall internal control structure (improved, unchanged or diminished)?				
Does management have the skills required to understand the complexities associated with cloud computing?				
Are cloud computing initiatives aligned with the enterprise's risk appetite?				

How to Review the Strategy Used for Implementing Cloud Computing

- Are the technology and application architecture mapped for the cloud?
- Is a list of services which can be provided using cloud computing prepared and analysed?
- What are the services which can be offered using cloud computing?
- What are the risks of cloud deployment and have these been mitigated by implementing right risk mitigation strategy?
- Based on the risk assessment, how to determine and implement the right cloud computing strategy for the enterprise?
- Has the cost benefit analysis of offering the services via the cloud computed?
- What services could be outsourced versus what can be built internally?
- Which Cloud delivery model is appropriate for the enterprise?
- How to ensure the quality, timeliness and availability of the services are managed?
- How to protect IT investments now and in the future?
- How to manage the cloud environment?
- What are the compliances and whether these are adhered to through Service Level Agreement?
- How to ensure privacy, security and availability of the data?

ISACA Publications on Cloud Computing

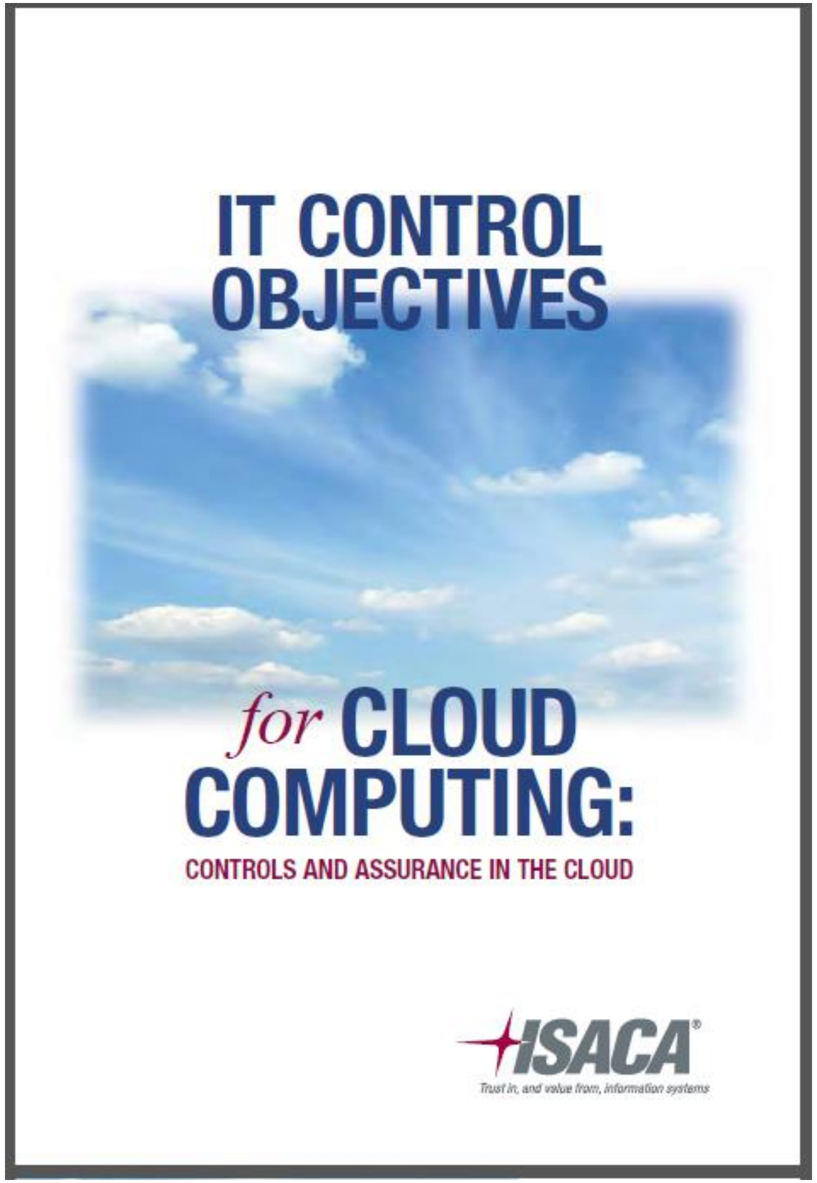


An ISACA
Emerging Technology
White Paper

ISACA
Serving IT Governance Professionals

Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

Abstract
Globalization and recent economic pressures have resulted in increased requirements for the availability, scalability and efficiency of enterprise information technology (IT) solutions. A broad base of business leaders has become increasingly interested in the costs and the underlying technology used to deliver such solutions because of their growing impact on the bottom line. Many parties claim that "cloud computing" can help enterprises meet the increased requirements of lower total cost of ownership (TCO), higher return on investment (ROI), increased efficiency, dynamic provisioning and utility-like pay-as-you-go services. However, many IT professionals are citing the increased risks associated with trusting information assets to the cloud as something that must be clearly understood and managed by relevant stakeholders. This paper clarifies what cloud computing is, identifies the services offered in the cloud, and also examines potential business benefits, risks and assurance considerations.

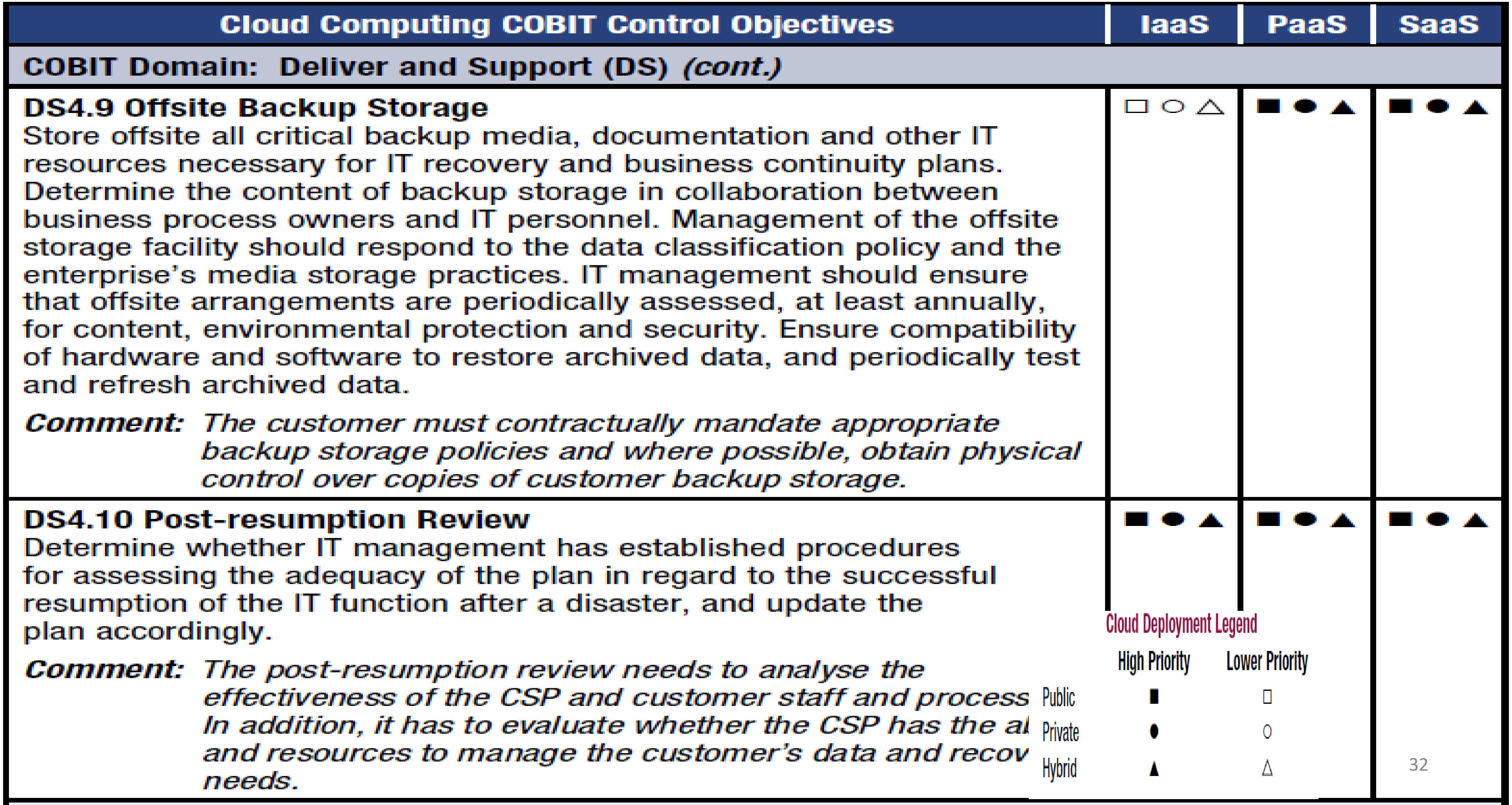


IT CONTROL OBJECTIVES *for* CLOUD COMPUTING:

CONTROLS AND ASSURANCE IN THE CLOUD

ISACA
Trust in, and value from, information systems

Controls and Control Objectives for Cloud Deployment - Examples

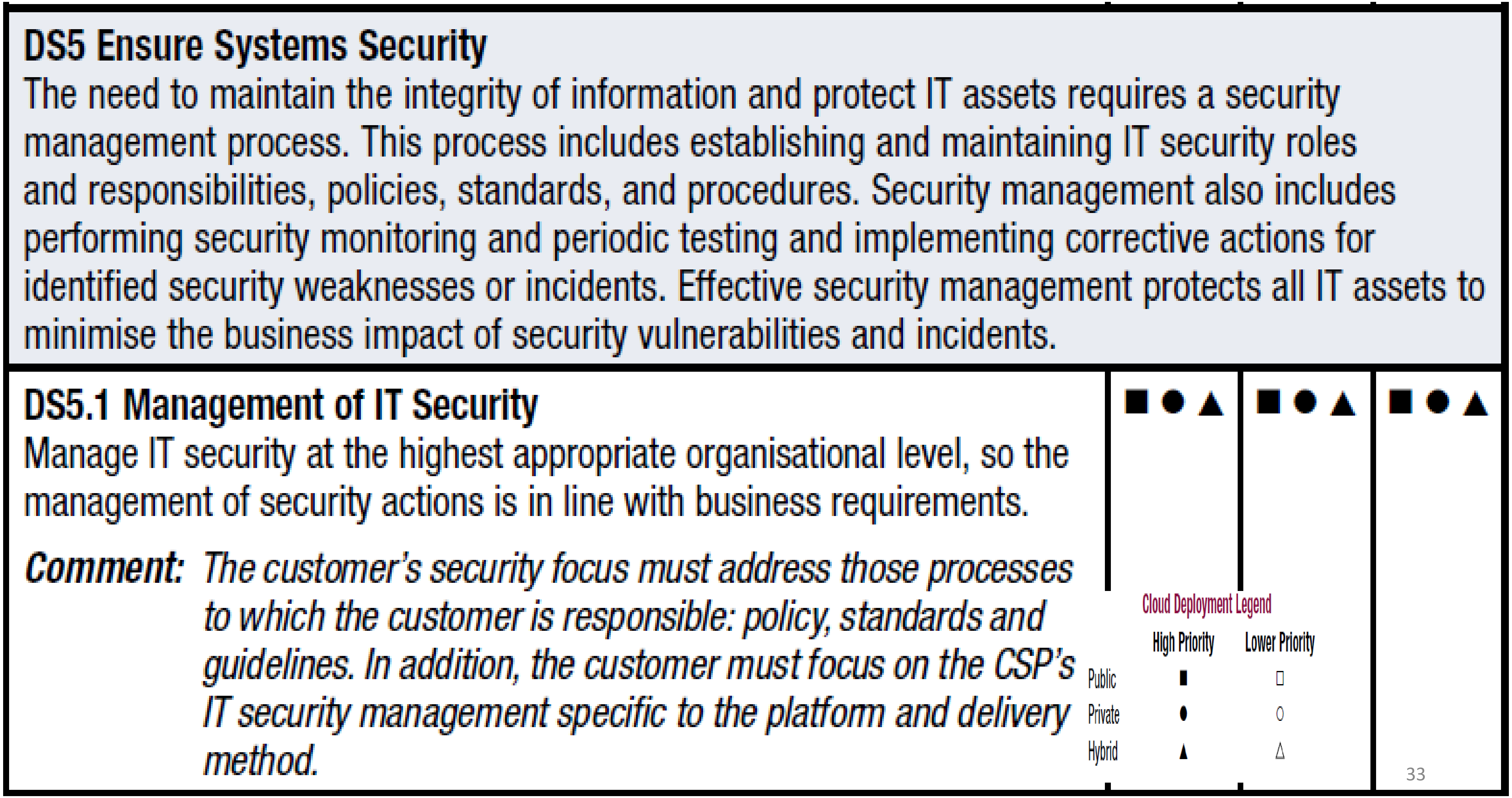


Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Deliver and Support (DS) ***(cont.)***			
DS4.9 Offsite Backup Storage Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data. ***Comment:*** *The customer must contractually mandate appropriate backup storage policies and where possible, obtain physical control over copies of customer backup storage.*	□ ○ △	■ ● ▲	■ ● ▲
DS4.10 Post-resumption Review Determine whether IT management has established procedures for assessing the adequacy of the plan in regard to the successful resumption of the IT function after a disaster, and update the plan accordingly. ***Comment:*** *The post-resumption review needs to analyse the effectiveness of the CSP and customer staff and process In addition, it has to evaluate whether the CSP has the al and resources to manage the customer's data and recov needs.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

Controls and Control Objectives for Cloud Deployment - Examples



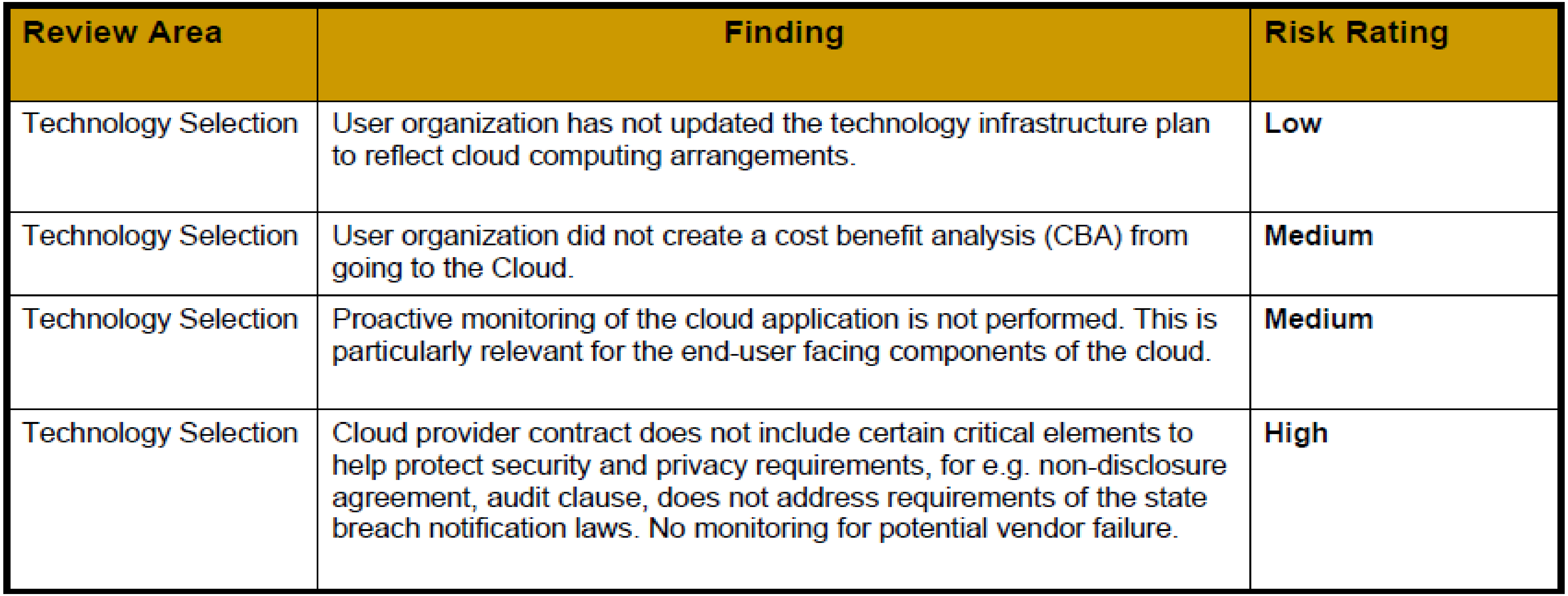
DS5 Ensure Systems Security The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.			
DS5.1 Management of IT Security Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements. **Comment:** *The customer's security focus must address those processes to which the customer is responsible: policy, standards and guidelines. In addition, the customer must focus on the CSP's IT security management specific to the platform and delivery method.*	■ ● ▲	■ ● ▲	■ ● ▲

Cloud Deployment Legend

	High Priority	Lower Priority
Public	■	□
Private	●	○
Hybrid	▲	△

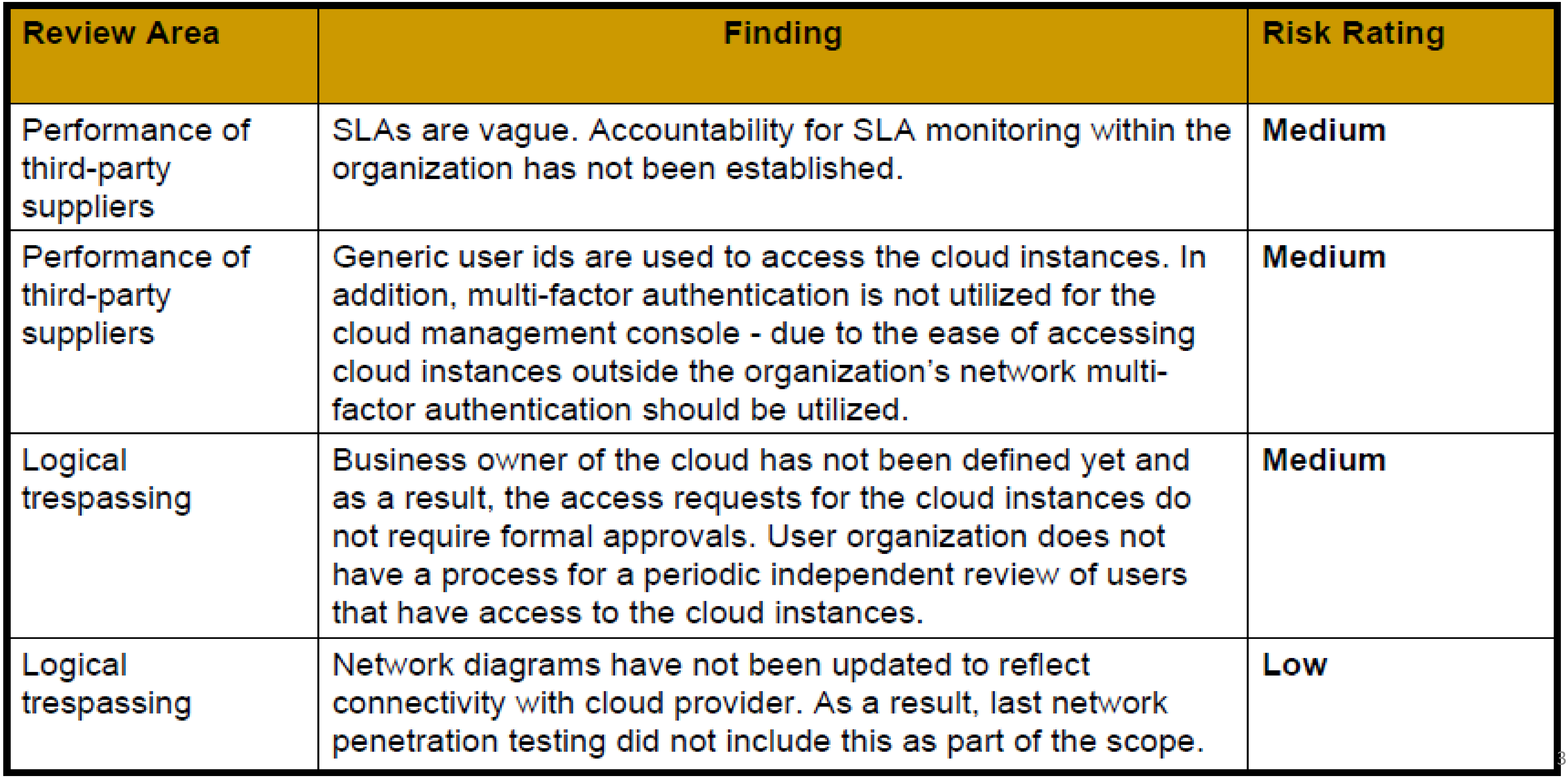
Sample Audit Report

- The following table summarizes the Review Area, the relevant Finding, and the corresponding Risk Rating. The detailed description of the issue is presented in the next section of the report. It includes detailed information describing the issue, the risks associated with the issue, and suggested strategy to mitigate the risk.



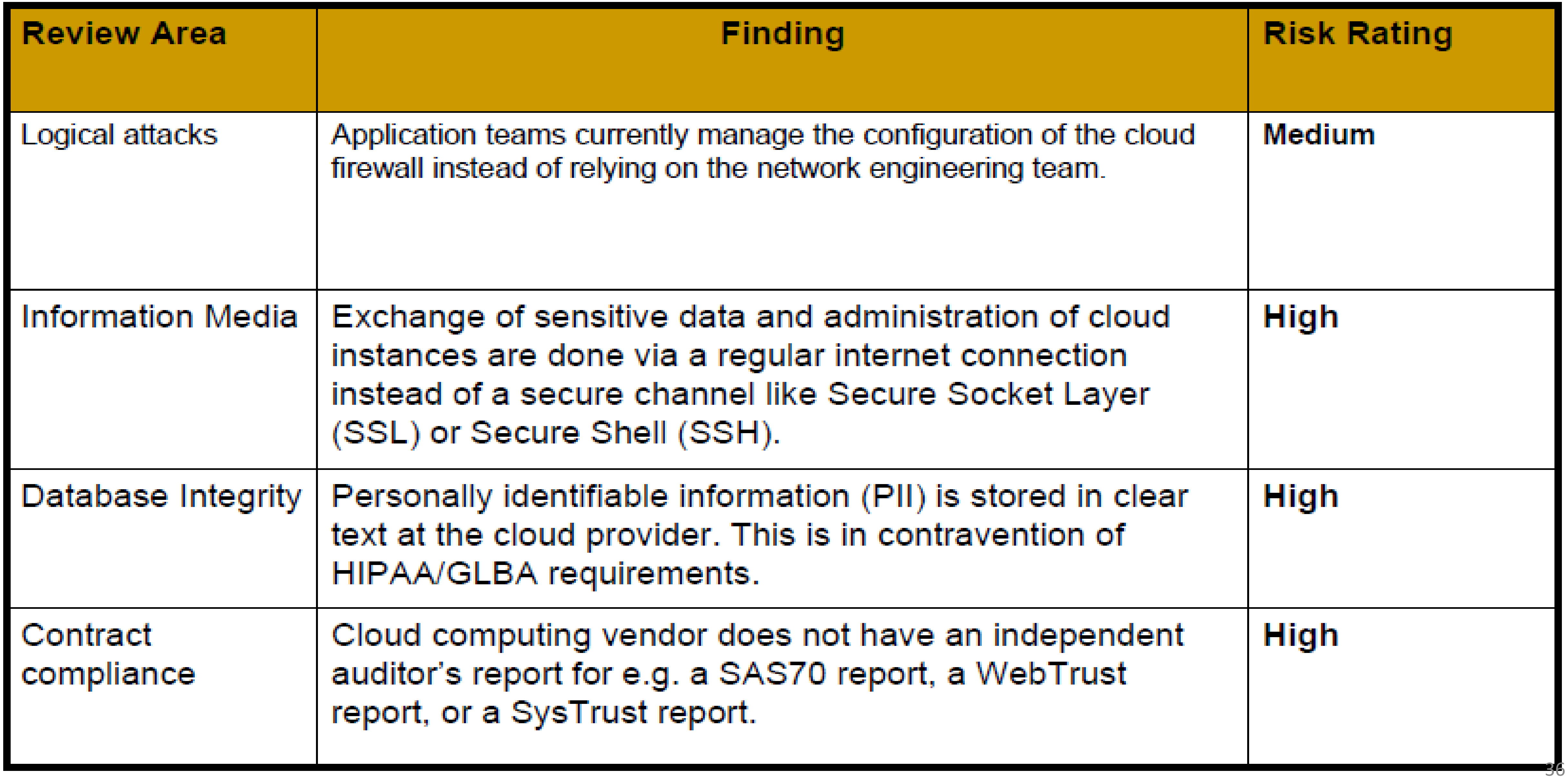
Review Area	Finding	Risk Rating
Technology Selection	User organization has not updated the technology infrastructure plan to reflect cloud computing arrangements.	**Low**
Technology Selection	User organization did not create a cost benefit analysis (CBA) from going to the Cloud.	**Medium**
Technology Selection	Proactive monitoring of the cloud application is not performed. This is particularly relevant for the end-user facing components of the cloud.	**Medium**
Technology Selection	Cloud provider contract does not include certain critical elements to help protect security and privacy requirements, for e.g. non-disclosure agreement, audit clause, does not address requirements of the state breach notification laws. No monitoring for potential vendor failure.	**High**

Sample Audit Report



Review Area	Finding	Risk Rating
Performance of third-party suppliers	SLAs are vague. Accountability for SLA monitoring within the organization has not been established.	**Medium**
Performance of third-party suppliers	Generic user ids are used to access the cloud instances. In addition, multi-factor authentication is not utilized for the cloud management console - due to the ease of accessing cloud instances outside the organization's network multi-factor authentication should be utilized.	**Medium**
Logical trespassing	Business owner of the cloud has not been defined yet and as a result, the access requests for the cloud instances do not require formal approvals. User organization does not have a process for a periodic independent review of users that have access to the cloud instances.	**Medium**
Logical trespassing	Network diagrams have not been updated to reflect connectivity with cloud provider. As a result, last network penetration testing did not include this as part of the scope.	**Low**

Sample Audit Report



Review Area	Finding	Risk Rating
Logical attacks	Application teams currently manage the configuration of the cloud firewall instead of relying on the network engineering team.	**Medium**
Information Media	Exchange of sensitive data and administration of cloud instances are done via a regular internet connection instead of a secure channel like Secure Socket Layer (SSL) or Secure Shell (SSH).	**High**
Database Integrity	Personally identifiable information (PII) is stored in clear text at the cloud provider. This is in contravention of HIPAA/GLBA requirements.	**High**
Contract compliance	Cloud computing vendor does not have an independent auditor's report for e.g. a SAS70 report, a WebTrust report, or a SysTrust report.	**High**

IS AUDIT/ASSURANCE PROGRAM

Cloud Computing

With Ready to Use Checklist in Excel

Key Concepts to Take Away

- Successful cloud implementation requires that enterprises work with legal, security and audit professionals to ensure that the appropriate levels of security and privacy are achieved.
- In migrating to cloud, consider not only the cost savings but also assess the potential risks and ensure that these risks are mitigated.
- Based on the potential cost savings and risk mitigation strategy, enterprises can make better decision on what cloud platform to choose and how these services will be offered.
- Auditors should conduct BIA and risk assessments to inform business leaders of potential risks to their enterprise.
- Auditors can provide independent assurance by evaluating whether the required controls have been implemented.
- The challenge for auditors is to understand how cloud computing works, related risks, security and controls.
- Use Global best practices like COBIT 2019 to provide Assurance and Consulting services.

The Seven+ Seven Ps for being Successful as a Professional and in Life

1. Passionate Action
2. Pro active Approach
3. Possibility Thinker
4. Principle Oriented
5. Potential Explorer
6. Problem Solver
7. Peaceful Mindset

1. Purpose Oriented
2. Patient Perseverance
3. Planning in advance
4. Pleasant Demeanor
5. Pragmatic Thinking
6. Positive Thinker
7. Pleasing Personality

Thank You

Questions?

rafeq@wincaat.com