Cloud Computing Master Class
Risk, Control and Audit

Prof. Frank Yam

CISA, CIA, CFSA, CFE, FHKCS, FHKIoD, FFA, FIPA, FHKITJC, CCP, CSP, CDP

Chairman & CEO - Focus Strategic Group Inc

Warning!!!

- All information discussed in this Master Class is the personal opinion of the Master Class Leader and is meant to stimulate new ideas from the participants.
- Under no circumstances should any of the opinion be relied upon for decision making or used for any other purposes.
- The Master Class Leader does not assume any liabilities for the opinion expressed in this seminar.
- Audio, video, or any other form of electronic recording is strictly prohibited.

Agenda

- Understanding Cloud Computing
- Benefits and Opportunities
- Risks and Challenges
- Audit and Control

Understanding Cloud Computing

Understanding Cloud Computing

Even if you may not recognize it, you're probably already using cloud computing and are pretty savvy in using it.

Examples:

- web email such as Gmail, Hotmail and Yahoo email;
- social networking sites like Facebook and Twitter
- video streaming sites like youtube
- productivity software sites like Google Docs and Microsoft's Office 365
- file synchronisation and backup services Apple iCloud, Dropbox and Microsoft SkyDrive.

Who Started All This?

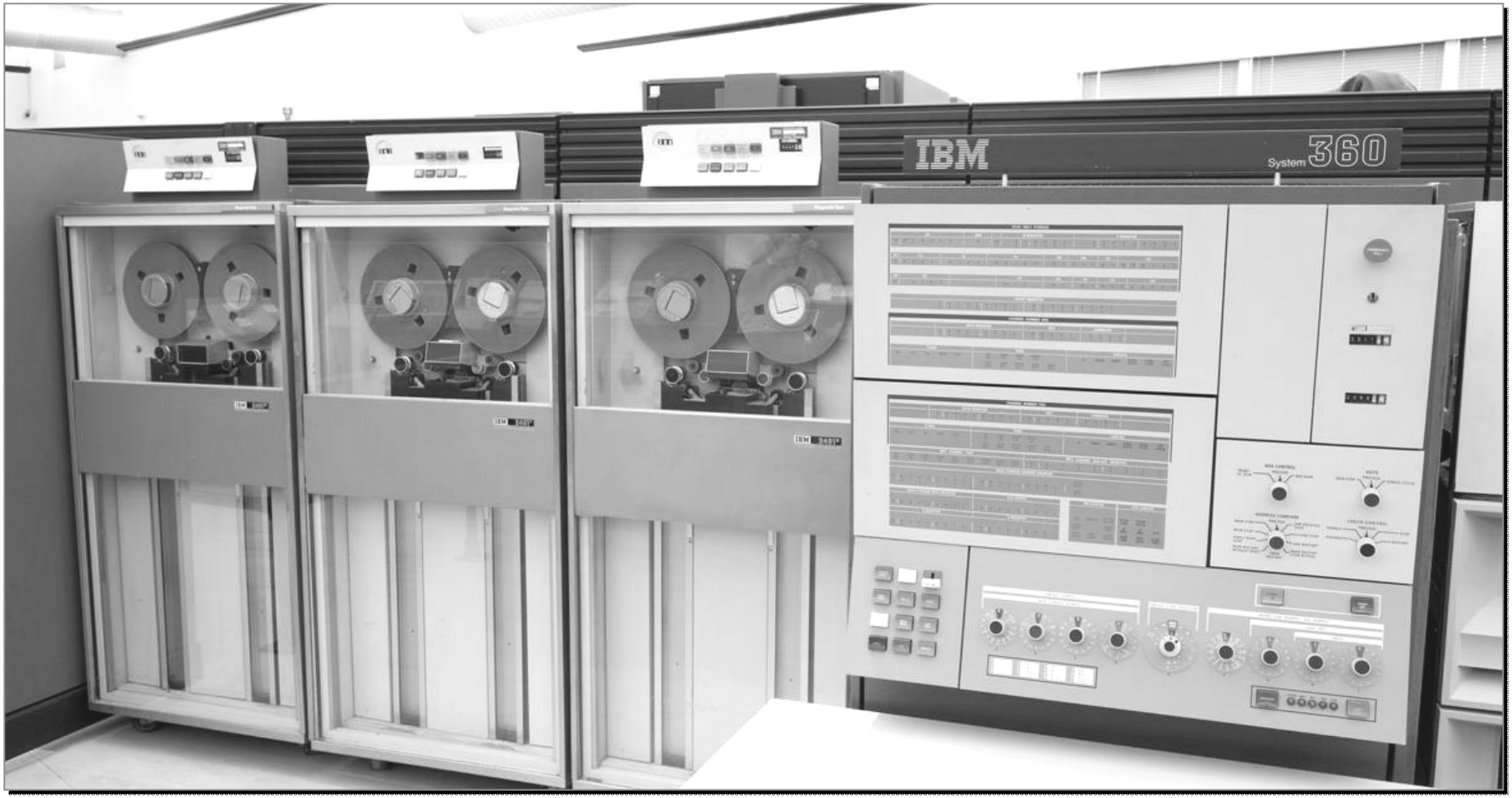
"What's interesting [now] is that there is an emergent new model, and you all are here because you are part of that new model. I don't think people have really understood how big this opportunity really is. It starts with the premise that the data services and architecture should be on servers. We call it **cloud computing – they should be in a "cloud" somewhere**. And that if you have the right kind of browser or the right kind of access, it doesn't matter whether you have a PC or a Mac or a mobile phone or a BlackBerry or what have you – or new devices still to be developed – **you can get access to the cloud**."

Mr. Eric Schmidt, Chairman & CEO Google

Search Engine Strategies Conference, 9th of August 2006

Evolution – “First Computer”

Evolution – Mainframe Computer



Evolution – Mini Computer, PCs and Internet

Evolution - Cloud Computing

Evolution - Cloud Computing

Computing is being **organized as a public utility** just as the telephone system is a public utility. Likewise, factories used to provide their own power using water wheels. With electrification, factories do not need to produce their own power. They just need to plug into the electricity grid.

Organizations are providing their own computing resources. In future, most organizations will **just plug into the cloud for their computing resources**. The computer utility is becoming the basis of a new and important industry.

Understanding Cloud Computing

Defining Cloud Computing:

"*A model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction.*

In layman's language - Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a **utility** (like the electricity grid) **over a network** (typically the Internet).- From Wikipedia

Understanding Cloud Computing

Cloud Computing is composed of:

- five essential characteristics,
- three service models,
- and four deployment models.

Understanding Cloud Computing

The five essential characteristics of Cloud Computing:

- On-demand self-service
- Broad network access
- Measured service
- Rapid elasticity
- Resource pooling

Understanding Cloud Computing

Characteristic 1: On-demand self-service

A consumer can provision for addition system resources (processing capability, software, storage) and network resources as needed without any human interaction with the cloud provider.

Understanding Cloud Computing

Characteristic 2: Broad network access

It is network based, and accessible from anywhere, from any standardized platform (i.e. desktop computers, mobile devices, etc.).

Understanding Cloud Computing

Characteristic 3: Measured Service

Usage of the cloud services are controlled and monitored by the cloud service provider. This is crucial for billing, access control, resource optimization, capacity planning and other tasks

Understanding Cloud Computing

Characteristic 4: Rapid Elasticity

Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

Understanding Cloud Computing

Characteristic 5: Resource Pooling (multi-tenancy)

The computing resources in the cloud are shared. This means that numerous clients may be using the same set of resources at the same time. It is essentially an **economy of scale**: you don't want to spend the money to buy your own infrastructure, so someone makes it their job to provide you with access to that infrastructure.

Understanding Cloud Computing

The 3 service models are as follows:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Understanding Cloud Computing

Infrastructure as a Service (IaaS) - customers get on-demand computing and storage to host, scale, and manage applications and services. IaaS delivers computer infrastructure – typically a platform virtualization environment – as a service. Rather than purchasing **servers, software, data-centre space and network equipment**, customers buy those resources as fully outsourced services.

Understanding Cloud Computing

Platform as a Service (PaaS) – provides the **application development sandbox** in the cloud. PaaS provides the capability to deploy customer-created, or acquired, applications that are developed using programming languages and tools that are offered by the provider.

Understanding Cloud Computing

Software as a Service (SaaS) - the service provider hosts the **software** so you don't need to install it, manage it, or buy hardware for it. Just connect and use it.

Understanding Cloud Computing

You will also hear other associated service models in the future, for example:

- Security as a Service (SecaaS)
- Storage as a Service (StaaS)
- Disaster Recovery as a Service (DRaaS)
- Identity as a Service (IDaaS)

Understanding Cloud Computing

The 4 deployment models, which can be either internally or externally implemented, are summarized by NIST as follows:

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

Understanding Cloud Computing

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept‘‘

Understanding Cloud Computing

Community cloud - Shares infrastructure between several organizations from a specific community with common concerns (e.g. education, security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

Understanding Cloud Computing

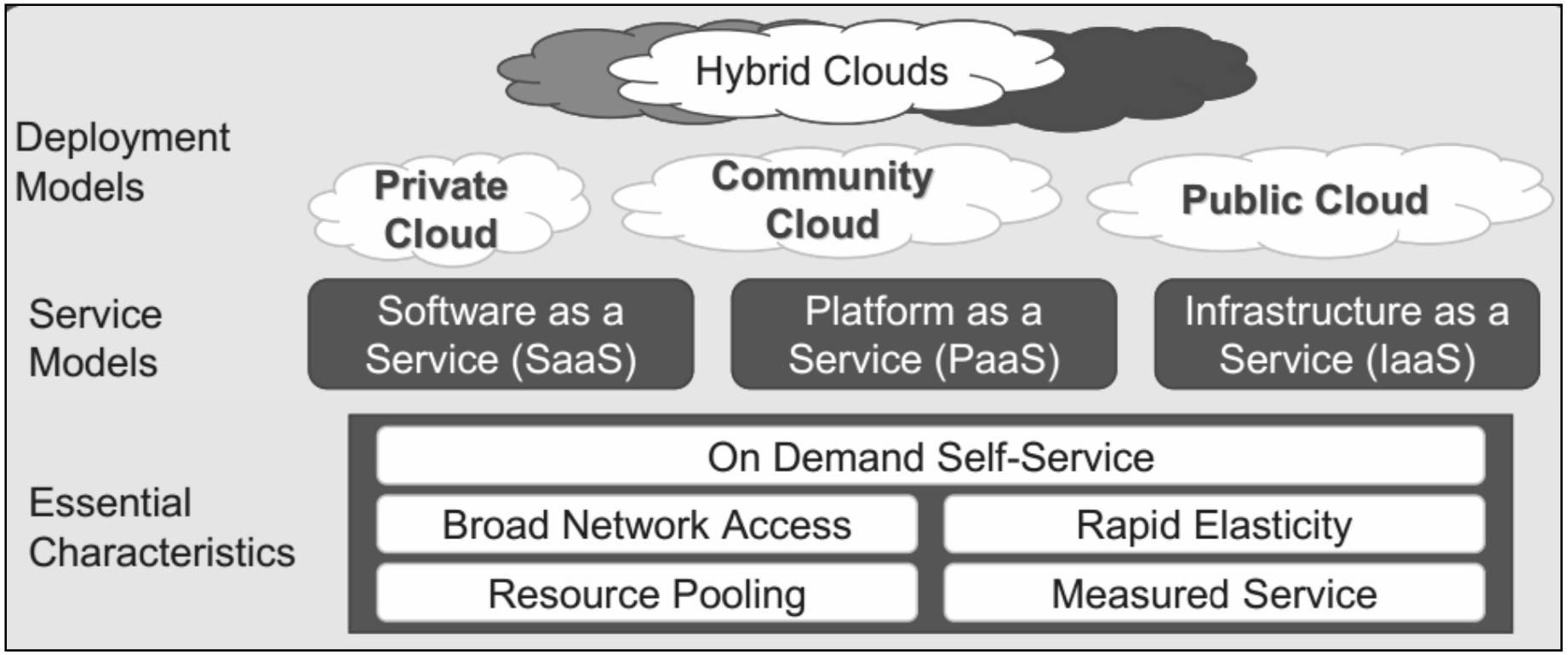
Public cloud - applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model.

Generally, public cloud service providers like Microsoft and Google own and operate the infrastructure and offer access only via Internet**.**

Understanding Cloud Computing

Hybrid cloud - is a combination of two or more previously defined deployment models (private, community or public) within the same organisation**.** A hybrid cloud leverages the advantages of the other cloud models, providing a more optimal user experience.

Understanding Cloud Computing
(In Summary)



NIST Visual Definition of Cloud Computing

Key Players

- Microsoft
- HP
- IBM
- Oracle
- Amazon
- Google
- EMC
- Salesforce.com
- Vmware
- OpenStack, Citrix
- Telcos

Current Trends

In many countries, e.g., Australia, government agencies have an **explicit obligation to consider cloud services** when procuring new information and communication technology (ICT) requirements for their test and development needs, and to **migrate public facing web sites to public cloud services**. The agencies **must choose cloud services** when they represent the best value and adequate risk management compared to other available options.

Source: Australian Government Cloud Computing Policy

Current Trends

US Government has released a **Federal Cloud Computing Strategy** in 2011.

Designed to help guide government agencies in moving systems to a cloud computing environment. It includes a **mandatory evaluation of cloud options** before making any investments.

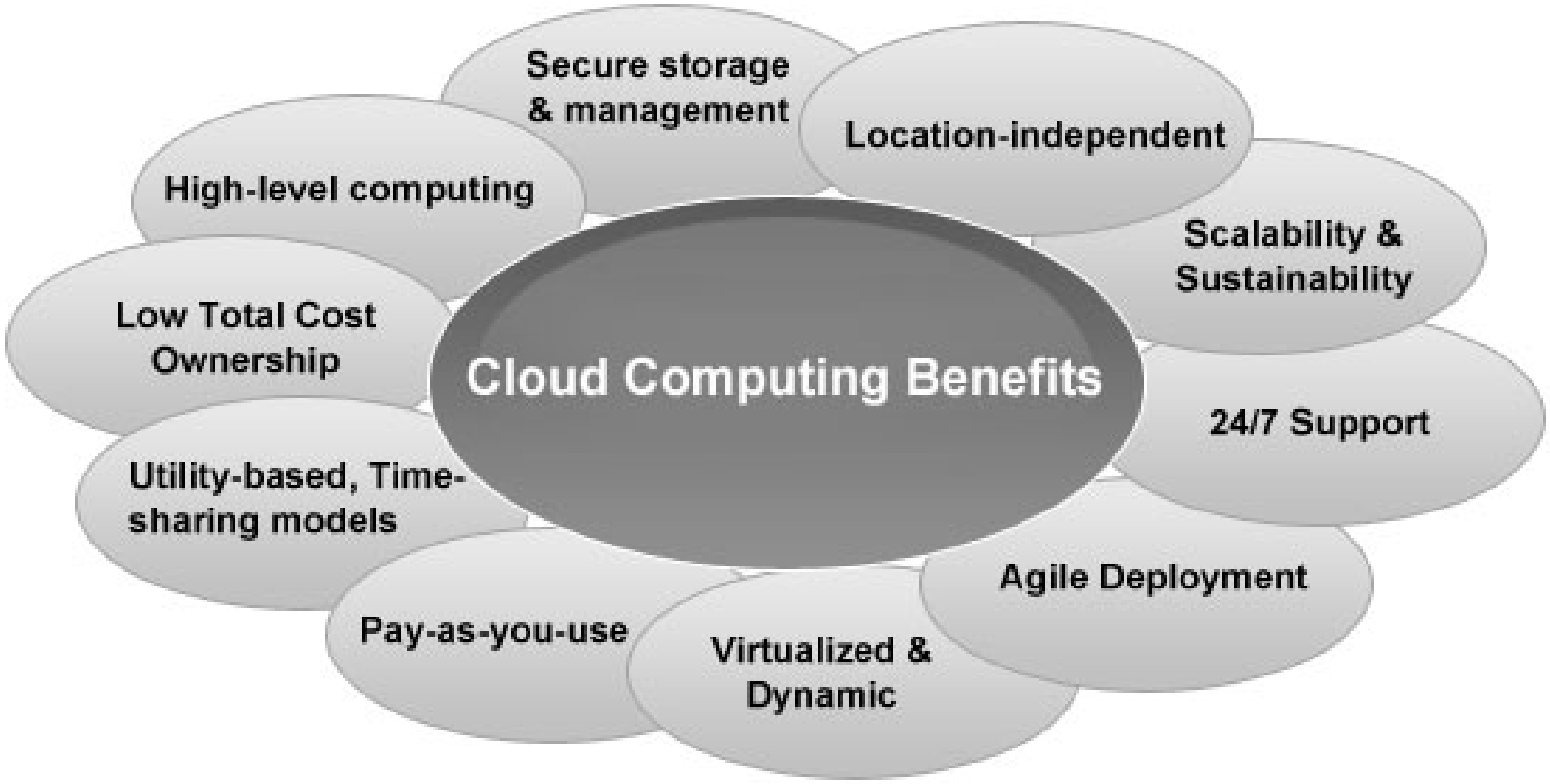
Current Trends

- Big Data
- Stonger emphasis on Security
  - Target, Home Depot, iCloud, Sony, TalkTalk, Vodafone ……
- Movement towards Platform Services (PaaS)
- Difficulty in finding cloud application developers
- Smaller players will be squeezed out
- Disaster recovery
- Hybrid (with private-line access) will be the new normal

Benefits and Opportunities

Business Benefits

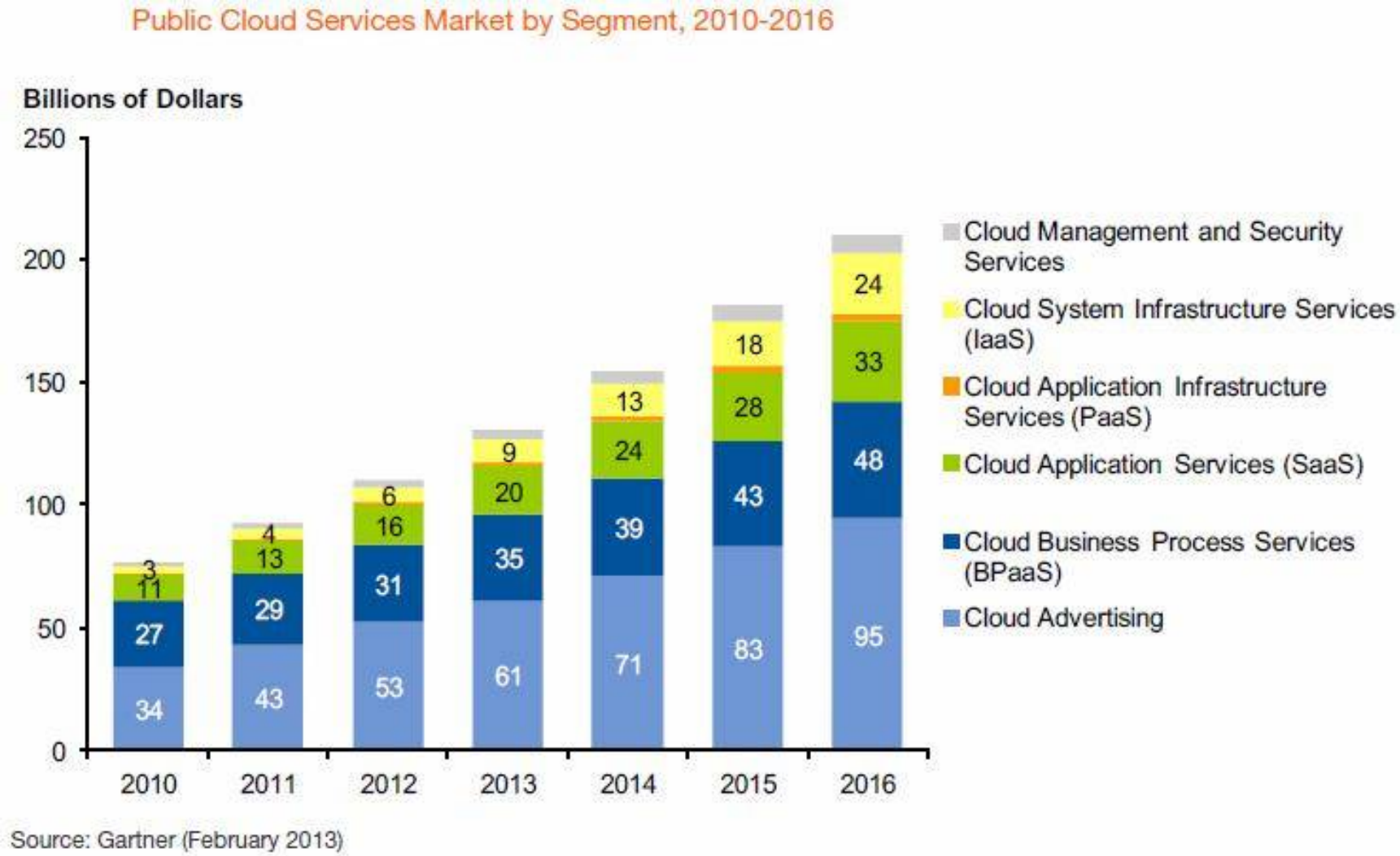
Cloud Computing Benefits



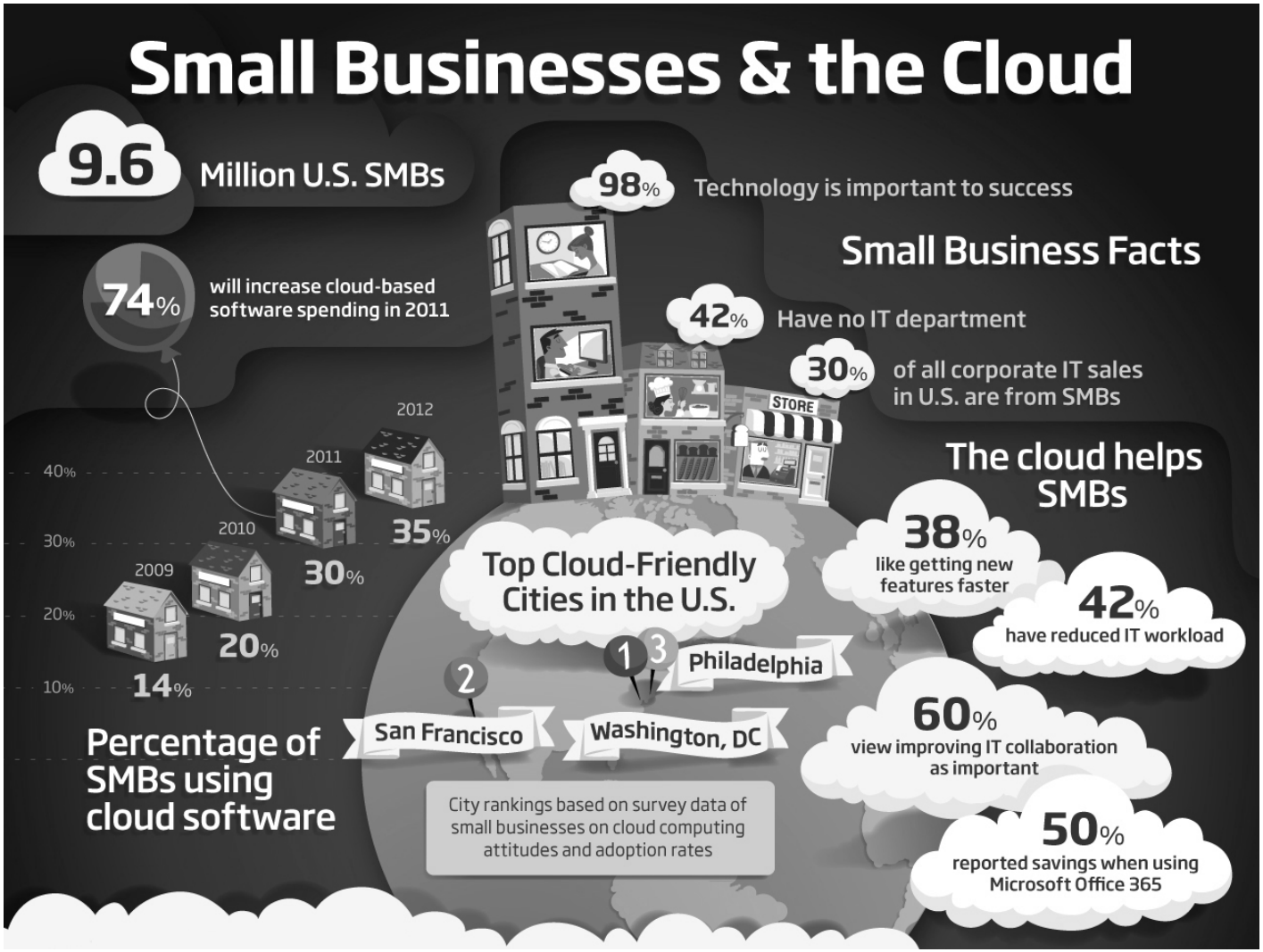
Cloud Computing Benefits

- Cost savings (CAPEX to OPEX)
- Optimized resource utilization
- Lower Power Consumption (“green”)
- Speed to Deployment
- Near instant scalability, provisioning
- ‘Service On demand’ (better responsiveness)
- A ‘Pay as you go’ billing system
- Resilience (reduces risk of downtime)

Cloud Computing Market



Cloud Computing Opportunities



Cloud Computing Opportunities

Creation of new businesses

- Faster time-to-market, and cost-effective innovation processes
- Dynamic (trans-)formation of open service and business networks
- Leveraging the participation Web and mass programming

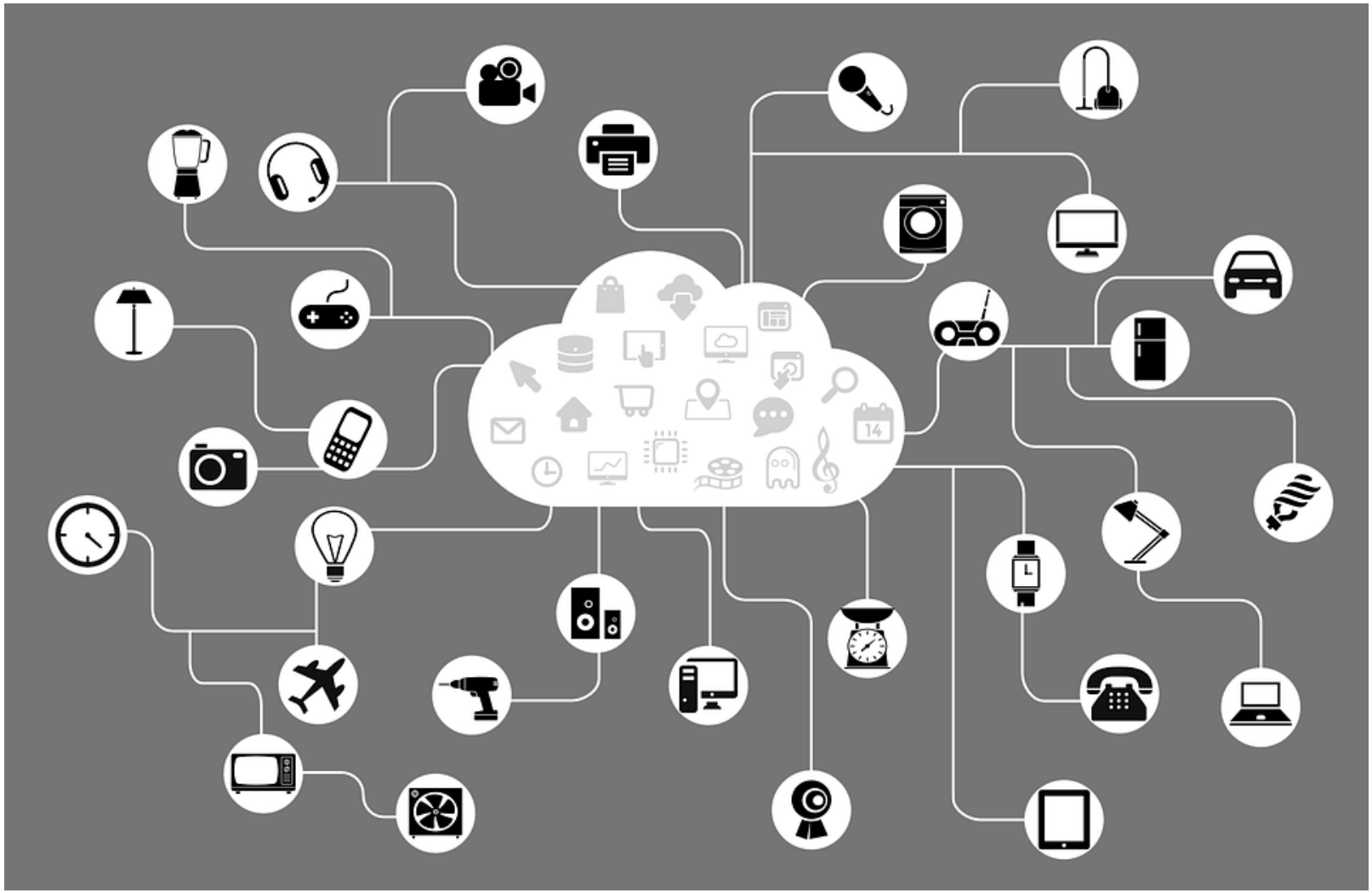
Internet-scale service computing

- Provide and consume sophisticated infrastructure, platforms and business applications as modular (Web) services
- Disrupt traditional industries and offer rich, highly dynamic experiences

Classical enterprise-grade systems management

- Under-utilized server resources waste computing power and energy
- Over-utilized servers cause interruption or degradation of service levels

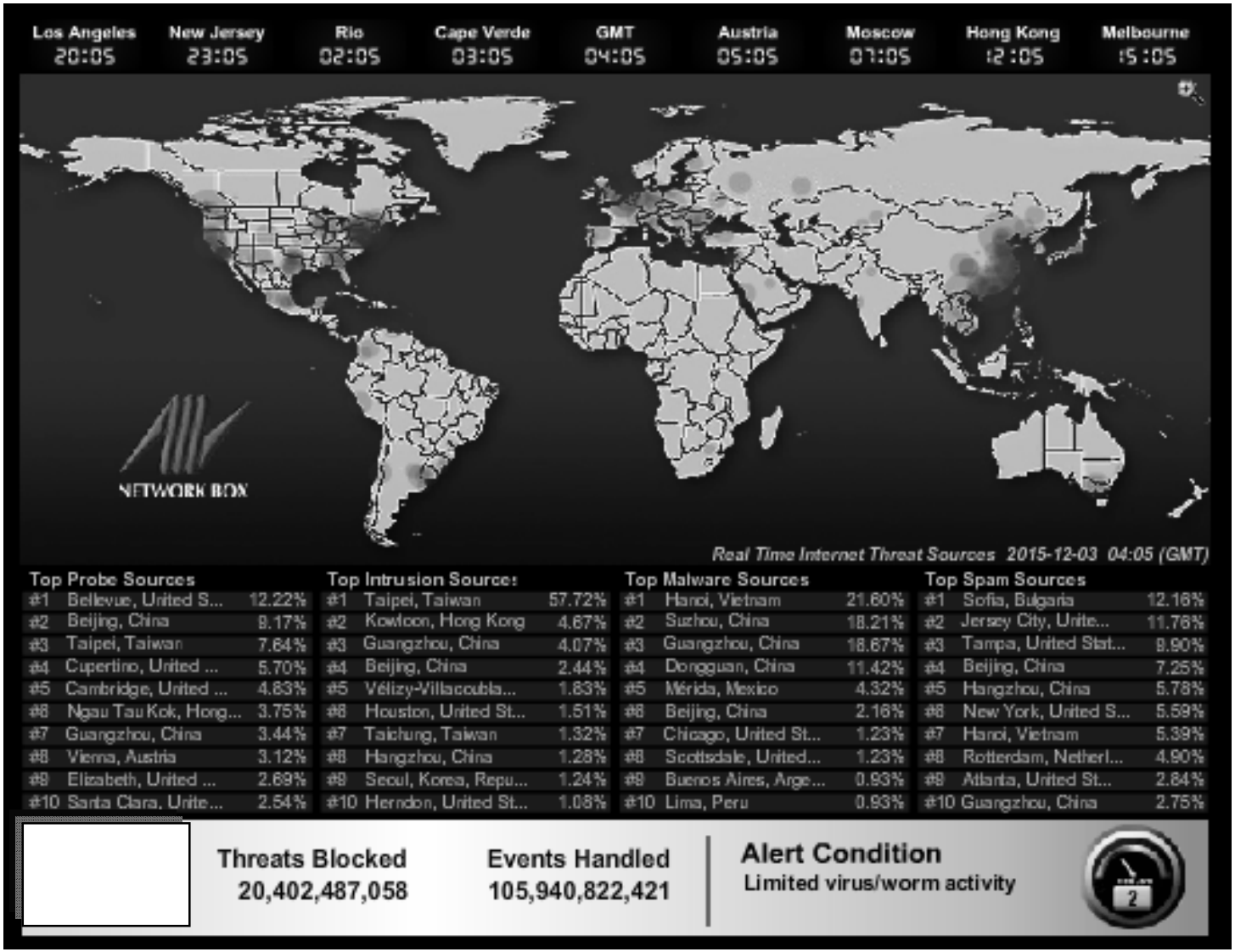
Internet of Things (IoT)



Risks and Challenges

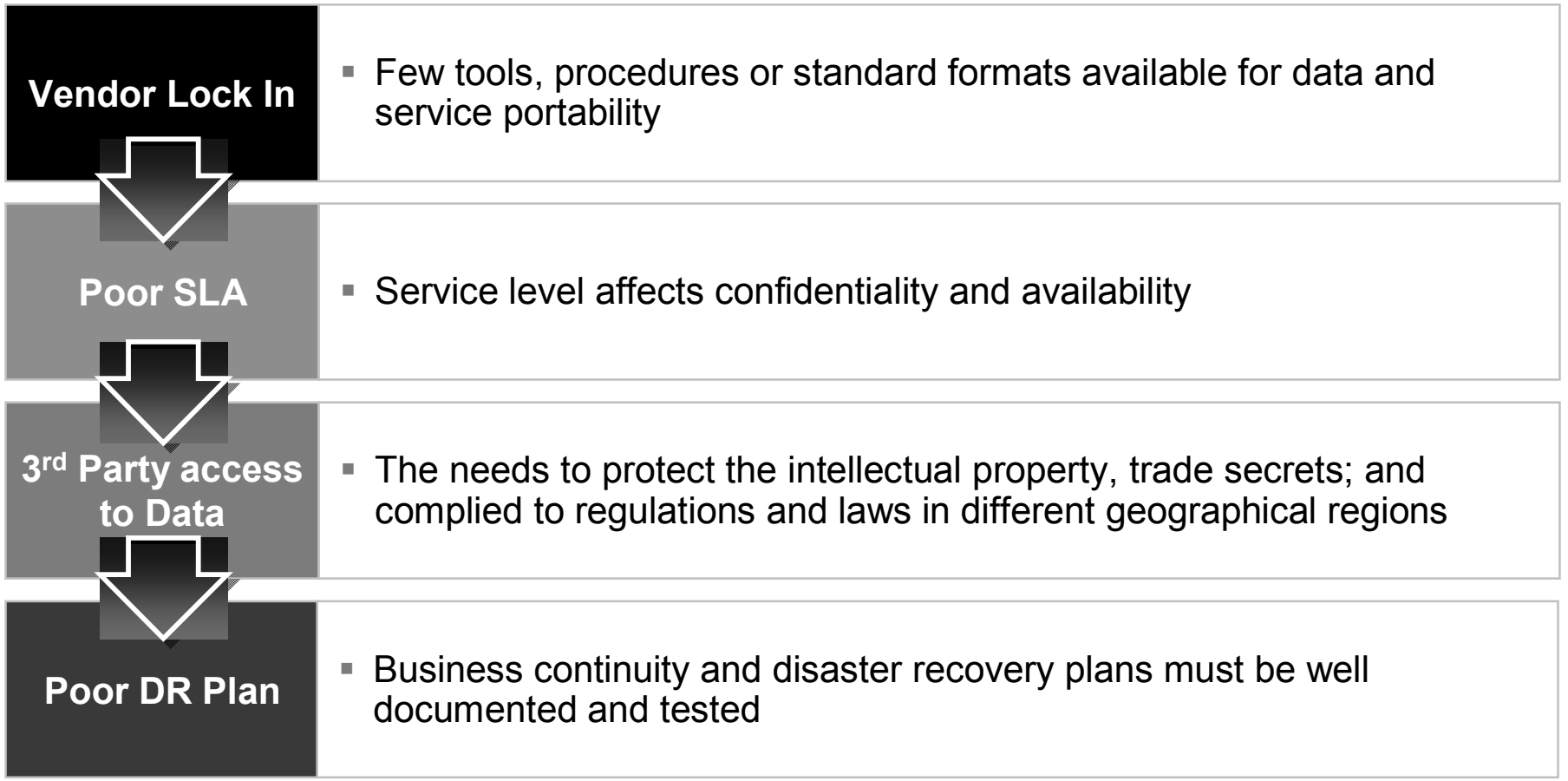
Cloud Computing

Real Time Cyber Threats



Risks and Security Concerns

Service and contractual risks



Risks and Security Concerns

Technology risks

Integration / Bandwidth	▪ How to integrate the in-house systems to the Cloud ? ▪ High speed bandwidth ready ?
Encryption and Key Mgnt	▪ Speedy encryption / decryption; ▪ Key management
Testing and Monitoring	▪ Provider may not allow you to do thorough PEN test, audit; ▪ Are there good monitoring tools available ?
Resource Allocation	▪ Overbooking, underbooking; ▪ Handling of DOS attack; Payment cap

Applicability for Cloud Computing

Source: Federal Reserve System, USA

System Type	Scalability	Availability	Security	
Information site	**Medium**	**Medium**	**Low**	**Public /Hybrid**
External Collaboration	**Medium**	**Medium**	**Medium**	**Public /Hybrid**
Public research / survey	**Low**	**Medium**	**Medium**	**Public /Hybrid**
Internal R&D	**Low**	**Low**	**Medium**	**Public /Hybrid**
Disaster Recovery	**Medium**	**Medium**	**Medium**	**Public /Hybrid**
Application Test and QA	**Low**	**Medium**	**Medium**	**Private**
Application Development	**Low**	**Medium**	**Medium**	**Private**
Production Applications	**High**	**High**	**Medium**	**No**
Mission Critical Applications	**High**	**High**	**High**	**No**

Audit and Control

Can we trust our system and data?

We no longer speak using terms like bytes or kilobytes (KB) or gigabytes (GB)

How many bytes in a Terabyte (TB)?

- **10^{12} (or 2^{40})**
- **Equivalent to roughly 1,610 CDs worth of data**

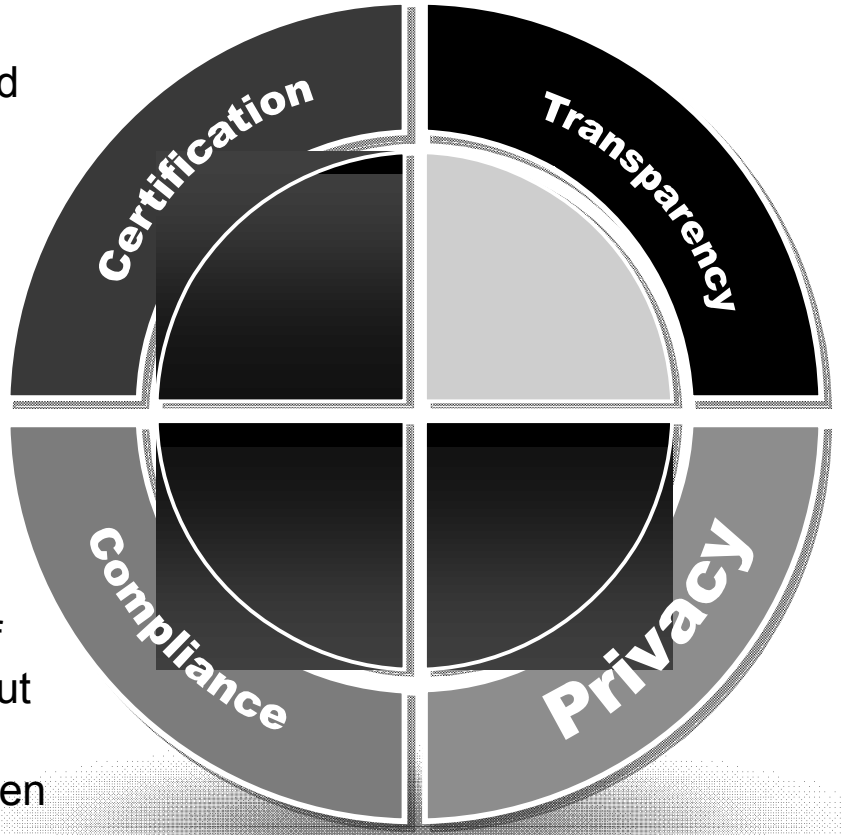
Anyone heard of a Petabyte ? Or an Exabyte?

1 **Petabyte** (PB) is 1,024TB
1 **Exabyte** (EB) is 1,024PB
1 **Zettabyte** (ZB) is 1,024EB
1 **Yottabyte** (YB) is 1,024ZB

Assurance Considerations

Independent assurance from third-party audits and service auditor reports

ISACA
Trust in, and value from, information systems



Must demonstrate existence of effective and robust security controls

Ensure the compliance of various countries' laws, but at the same time able to access your own data when needed

Must prove that privacy controls are in place and able to prevent, detect and react to breaches

AICPA SERVICE ORGANIZATION CONTROLS (SOC) REPORTS ARE EVIDENCE-BASED AUDIT REPORTS

	What it reports on	Who uses it
SOC 1	Internal controls over financial reporting	User auditors & users' controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Management, regulators & others. Shared under NDA
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

Trust Defined

***Definition 1*:** Trust is the ability to predict what a system will do in various situations.

***Definition 2*:** Trust is using an information system without having full knowledge about it.

***Definition 3*:** Trust is giving something now (credit card) with an expectation of some future return or benefit (on line purchase).

***Definition 4*:** Trust is being vulnerable (entering private and sensitive information) while expecting that the vulnerabilities will not be exploited (identity theft).

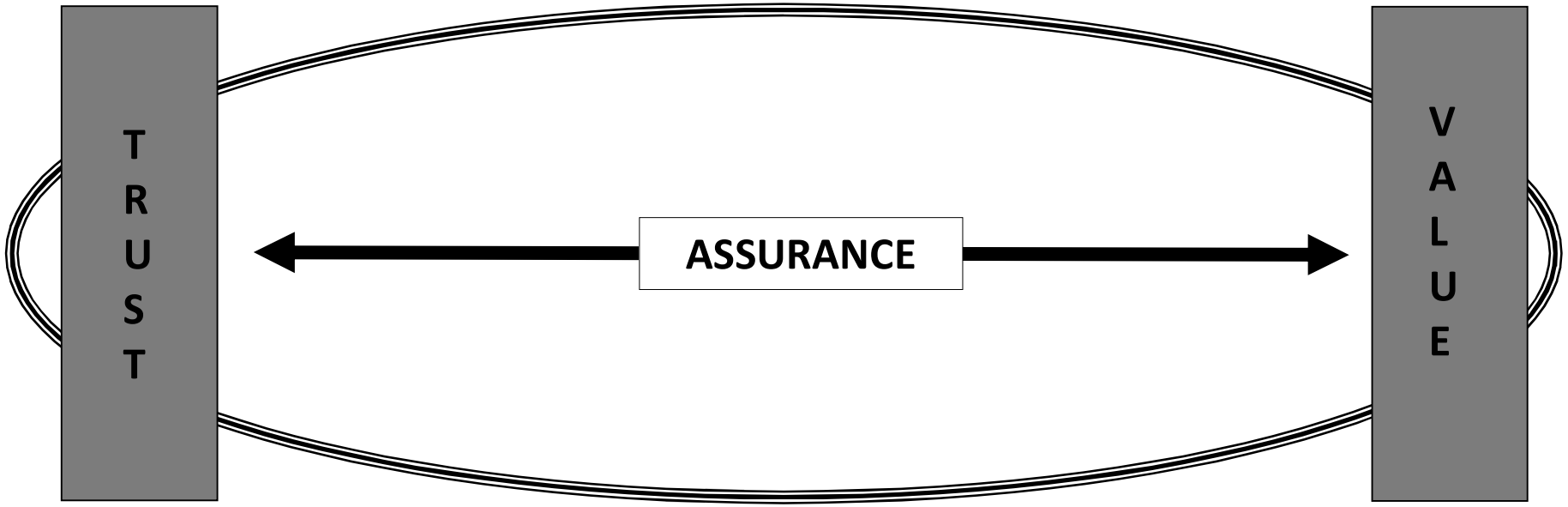
Trust that:

*Private and sensitive information will remain **confidential***

*Process **integrity** is maintained*

*Essential business processes are **available** or recoverable*

Trust and Value Relationship



Trust creates the opportunity for **Value**
Value is based on an expectation of **Trust**
Assurance binds **Trust** and **Value** together

ISACA's Six Guiding Principles for Adopting and Using the Cloud

- Enablement
- Cost benefit
- Enterprise risk
- Capability
- Accountability
- Trust

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Enablement

- Plan for cloud computing as a strategic enabler rather than as an outsourcing arrangement or a technical platform.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Enablement

To plan strategically for cloud adoption and use, enterprises need to:

- Treat cloud computing adoption and use as a strategic business decision.
- Make informed decisions, considering both business and operational needs and the benefits that can be provided by cloud computing.
- Communicate cloud computing arrangements and agreements to internal parties to ensure proper alignment and consistent oversight.
- Periodically review organizational strategies and the contribution of IT to ensure that cloud initiatives maximize value delivery, risk management and resource utilization.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Cost benefit

- Evaluate the benefits of cloud acquisition based on a full understanding of the cost of cloud compared with other technology platform business solutions.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Cost benefit

To properly evaluate the costs and benefits of cloud computing, enterprises need to:

- Clearly document expected benefits in terms of rapid resource provisioning, scalability, capacity, continuity and the cost reductions that the cloud services offer.
- Define the true life-cycle cost of IT services provided internally or through a provider to have a basis for comparing expected and received value.
- Balance cost with functionality, resilience, resource utilization and business value.
- Look beyond cost savings by considering the full benefits of what cloud services and support can provide.
- Periodically evaluate performance against expectations.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Enterprise risk

- Take an enterprise risk management perspective to manage the adoption and use of cloud.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Enterprise risk

To understand the risk implications of cloud computing, enterprises need to:

- Consider the privacy implications of comingling data within the virtualized computing environment.
- Evaluate privacy requirements and legal restrictions, considering client needs as well as provider restrictions and capabilities.
- Determine the accountability addressed in SLAs, the ability to monitor performance and available remedies.
- Understand current risk identification and management practices and how they need to be adapted to address risk management for cloud computing.
- Integrate scenario analysis into business risk management decision making.
- Consider exit strategy and the implications of not being able to render data as enterprise applications are sunset or unavailable.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Capability

- Integrate the full extent of capabilities that cloud providers offer with internal resources to provide a comprehensive technical support and delivery solution.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Capability

To leverage both internal and cloud provider resources effectively, enterprises need to (1 of 2):

- Understand the human and technical resource capabilities that exist in the current infrastructure and how a cloud strategy will impact the need for these or other resources.
- Define the capabilities and constraints that a cloud provider will make available on these resources, including periods of unavailability or priority of use.
- Consider emergency situations and resource requirements necessary to determine causes, stabilize the environment, protect sensitive and private information, and restore service levels.
- Determine how policies, practices and processes currently support the use of technology; how transitioning to a cloud solution will require changes; and the impact these changes will have on capabilities.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Capability

To leverage both internal and cloud provider resources effectively, enterprises need to (2 of 2):

- Ensure that service providers can demonstrate that personnel understand information security requirements and are capable of discharging their protection responsibilities.
- Ensure that internal staff have the skill and expertise to coordinate activities with cloud providers and that they are engaged in cloud service acquisition and ongoing management.
- Ensure that effective channels of communication are provided with provider management and key specialists, particularly for problem identification and resolution.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Accountability

- Manage accountabilities by clearly defining internal and provider responsibilities.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Accountability

To ensure that responsibilities are clearly understood and individuals and groups can be held accountable, enterprises need to:

- Understand how traditional responsibilities are assigned and implemented within the existing organizational structure and as a part of policies and practices to determine how these are addressed within cloud solutions.
- Determine how responsibilities between tenant and provider organizations for cloud solutions are assigned and how communications between accountable individuals and groups will be facilitated.
- Ensure that processes and procedures provide a mechanism to ensure that responsibilities are accepted and accountabilities are clearly assigned.
- Maintain within the governance structure a means of reviewing performance and enforcing accountabilities.
- Consider the risk to the enterprise as part of the enterprise risk management program, the impact of potential lapses in assigned responsibilities, or the impact of not being able to assign accountabilities.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Trust

- Make trust an essential element of cloud solutions, building trust into all business processes that depend on cloud computing.

ISACA's Six Guiding Principles for Adopting and Using the Cloud

Trust

To ensure that business processes that depend on cloud computing can be trusted, enterprises need to:

- Clearly define CIA requirements for information and business processes.
- Understand how reliance on cloud computing solutions may impact trust requirements.
- Structure the efforts of security, risk management and assurance professionals within both tenant and provider organizations to ensure that trust requirements are known and satisfied.
- Monitor changes in business use of cloud computing, vulnerabilities associated with cloud solutions, and implementations across tenant and supplier environments to ensure that threats to trust can be identified and resolved.
- Ensure that cloud infrastructure, platform and software service providers understand the importance of trust and create solutions that can be trusted.
- Provide ongoing assurance that information and info. systems can be trusted.

Seminar Summary

Key Points

- Organisations (and individuals) will rely more and more on Cloud Computing
- We should anticipate more Cloud-related risks (and frauds)
- Internal Auditors will be expected to understand Cloud-related risks and to recommend appropriate controls

Final Thoughts

The ultimate challenge for a professional is to add value .....

At the end, it is attitude, not knowledge, that differentiates one from the other.

Let's get on this journey together,

with the right attitude and enthusiasm.

We appreciate your contributions to IIA!

THANK YOU!