Adopting Cloud Computing with a RISK Mitigation Strategy

TS Yu, OGCIO

21 March 2013

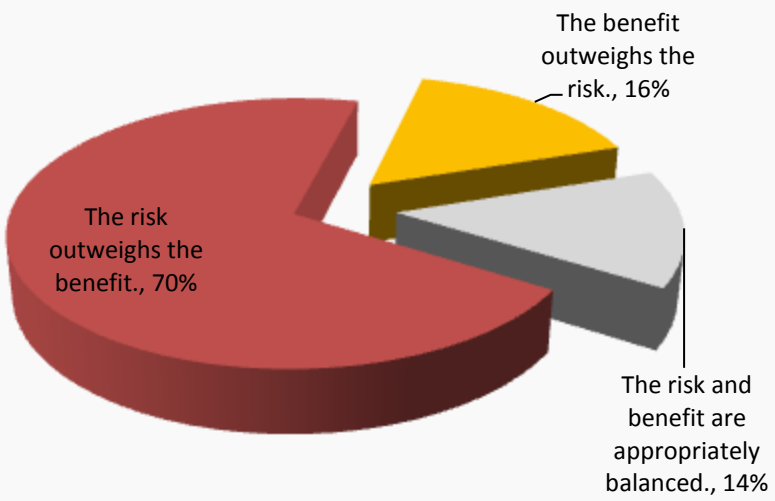
Agenda

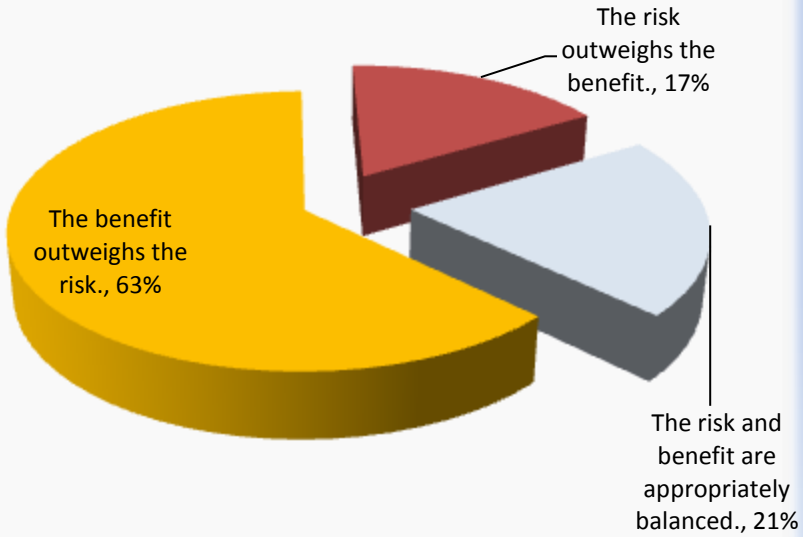
1. Introduction
2. Security Challenges
3. Risk Mitigation Strategy
   - ✓ Before start using
   - ✓ When using
4. Policy & Guidelines
5. Cloud Computing in the Government
6. Conclusion

Introduction

ISACA's 2012 IT Risk/Reward Barometer (HK/China)

- IT professionals remain wary of public clouds.





→ 70% believe that the risk of using **public** clouds outweighs the benefit.

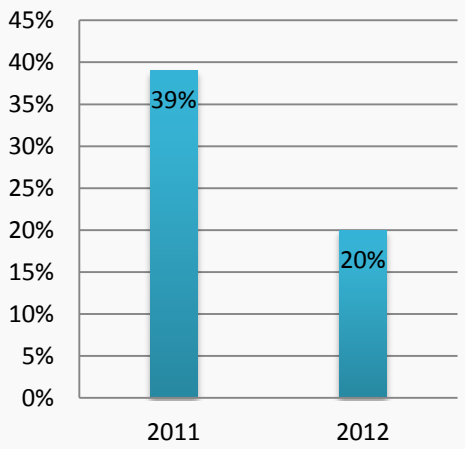
→ 63% believe that the benefit of using **private** clouds outweighs the risk.

Introduction

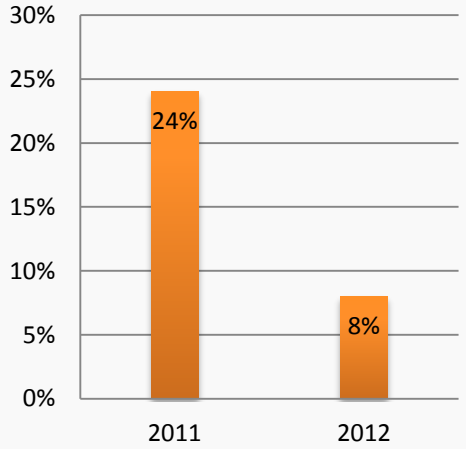
CloudPassage: Security and the Cloud 2012

- People are becoming more confident with some aspects of cloud security

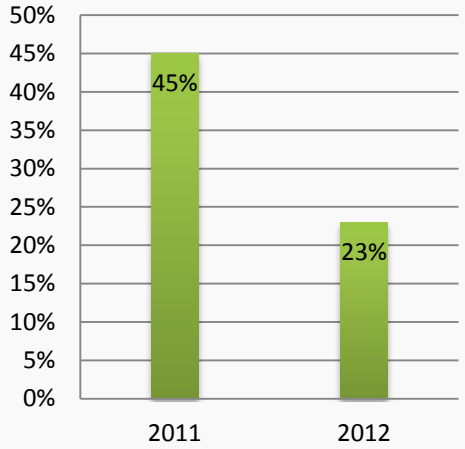
→ Percentage who expressed concern:



Multi-tenancy of Infrastructure of Applications



Providers Having Access to User's Guest Servers



Lack of Perimeter Defences and/or Network Control

Security Challenges – Basic Issues

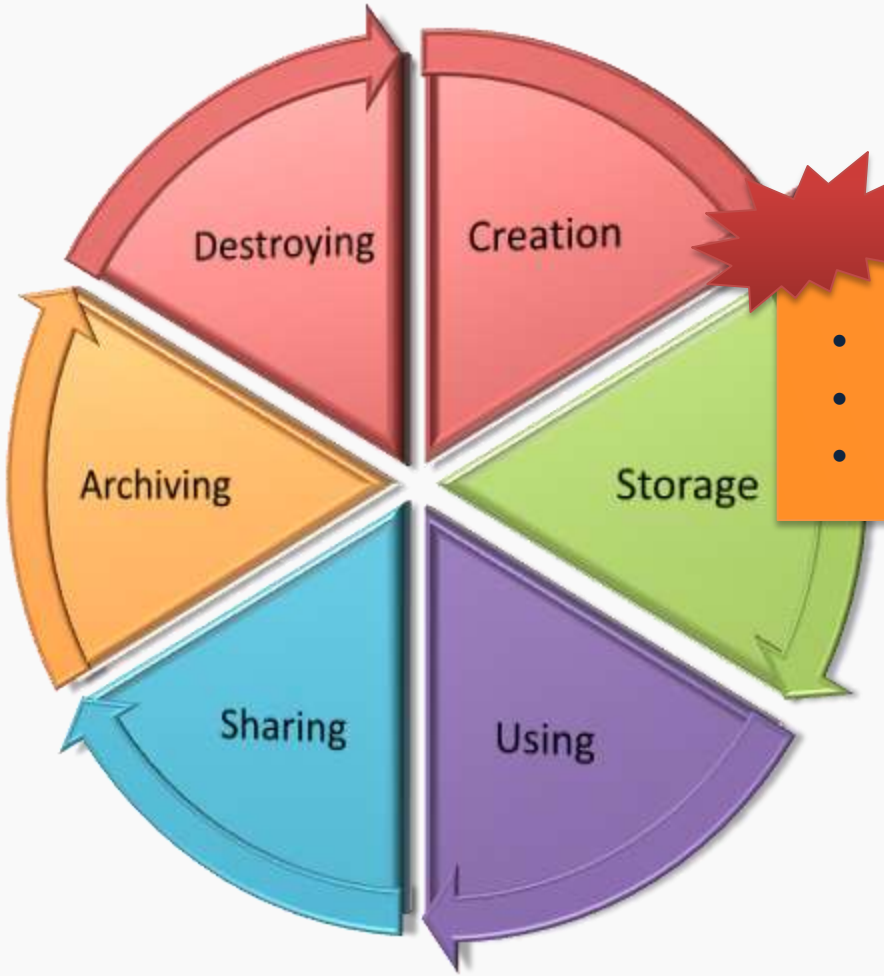
Basically security risks associated with cloud are not really new risks. Cloud computing may change some aspects of those risks, but the risks themselves are not new.

All the potential risks and security challenges may diminish the intention of cloud adoption by potential users.

There are more or less secure cloud environments, just as there are more or less secure local data centers.

Adoption of cloud computing is not risk-free. Organizations need to fully understand the risks associated with cloud computing and adopt a risk-based approach to incorporate a cloud computing strategy in their IT plans.

Security Challenges – Data Lifecycle Perspective

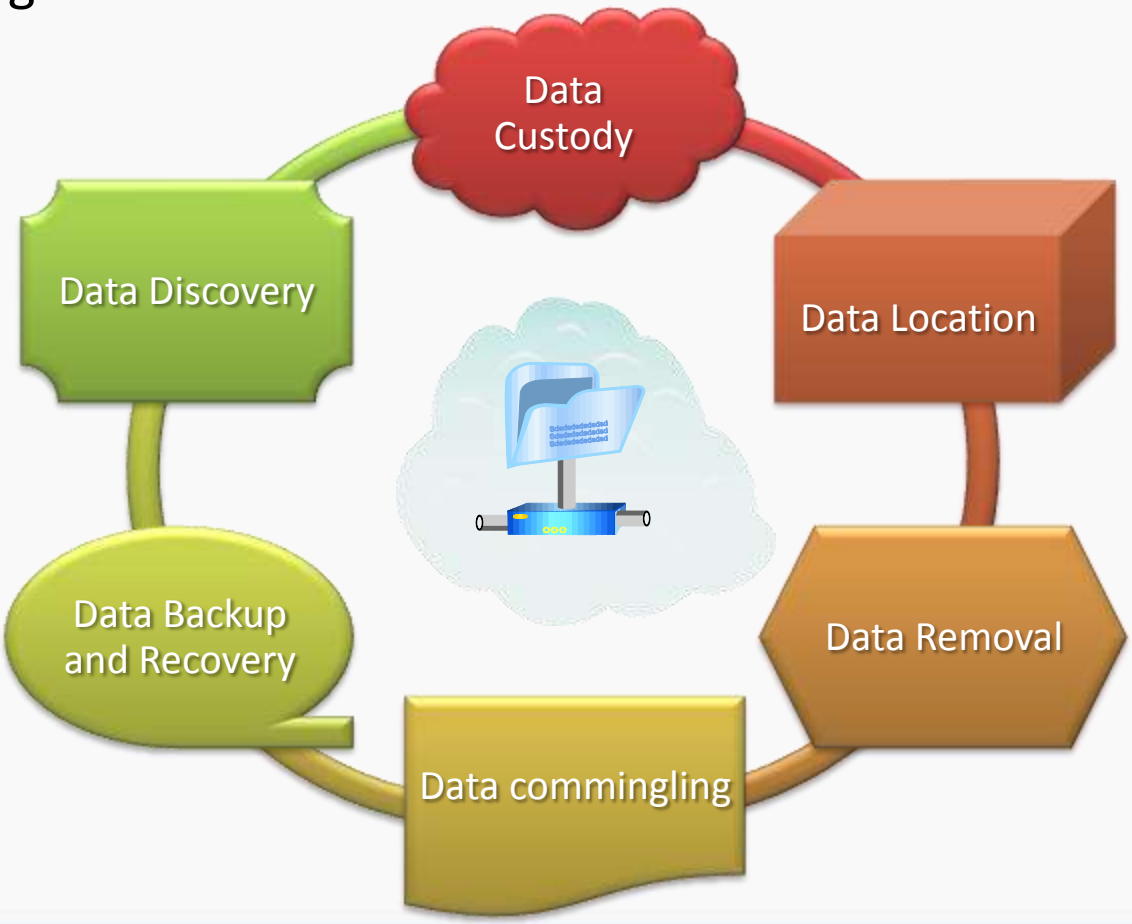


New Challenges!

- Who's responsibility?
- Multi-tenancy
- Virtualized environments

Security Challenges – Data Lifecycle Perspective

Some key challenges regarding data lifecycle security in cloud computing environment include:



Other Security Challenges (1)

- Identity and Access Management
  - Requires secure and timely management of provisioning and de-provisioning of users in the cloud
  - Authorization will continue to be the weakest point for cloud data stores (Georgia Institute of Technology)
- Portability and Interoperability
  - Needs to reduce the risk of vendor lock-in and inadequate data portability
  - Service providers may suddenly go out of business or discontinue one or more of the cloud services

Other Security Challenges (2)

- Service Availability, Business Continuity and Disaster Recovery
  - Occasional outage of cloud services
  - Internet service loss may interrupt cloud services
- Incident Response, Notification and Remediation
  - Complexity of security incidents in a cloud environment
  - Efficiency of notification and remediation

Risk Mitigation Strategy for Adopting Cloud Computing

Planning Strategy

- ***Initial Risk Assessment***
  - Is there a business need?
  - What are the benefits?
  - What part of the business is suitable to be put onto the cloud?
  - Are there any impediments to outsourcing?
  - What types of workloads are being deployed on public and private clouds?
  - What challenges and threats are relevant?
  - What is the impact if data is lost or service is unavailable?
  - Can the benefit outweighs the risk?
- ***Major Affecting Factors***
  - Sensitivity of data to be stored or processed
  - How the chosen service provider has implemented their cloud services and corresponding security measures
- ***When to Conduct Risk Assessment***
  - Before adopting, periodically after using, and after major changes

Risk Mitigation Strategy for Adopting Cloud Computing - before start using

Selection of a Cloud Service Provider

- Terms of Service and Security & Privacy Policy, and Note :
  - how your company can use the cloud service;
  - how your data is stored and protected;
  - whether the service provider has access to your data, and if so, how that access is restricted;
  - how to report an incident;
  - how to terminate the service and if data is retained after service termination;
  - whether the Privacy Policy follows the data protection principles of the Personal Data (Privacy) Ordinance
- Negotiate the Terms of Service with the service provider if not all the terms are found acceptable. If you cannot find a service provider meeting your requirements, you should re-consider the use of cloud services.
- Understand whether there are “secondary uses” of your account information without your knowledge or consent.

Risk Mitigation Strategy for Adopting Cloud Computing - before start using

Selection of a Cloud Service Provider

Reference:

- Cloud Security Alliance (CSA) - Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. https://cloudsecurityalliance.org/star/

Risk Mitigation Strategy for Adopting Cloud Computing - before start using

Data Ownership

- Check whether the service provider reserves rights to use, disclose, or make public your information.
- Check whether the intellectual property rights of data you own remain intact.
- Check whether the service provider retains rights to your information even if you remove your data from the cloud.
- Understand whether you can move or transfer your data and the service to another provider when you want to, and whether export utilities are available and are easy to use.
- Check whether data can be permanently erased from the cloud, including any backup storage, when you delete this data or when you end the service.

Risk Mitigation Strategy for Adopting Cloud Computing - before start using

Additional Selection Considerations

- Select a service provider that can explain clearly what security features are available, preferably supported by an independent information security management certification (e.g. ISO/IEC 27001).
- Select a service provider with no major security incident reported, or one that can provide transparency to previous security incidents with cause and remediation explained.
- Select a service provider that ensures data confidentiality by using encryption to transmit data and to protect stored static data. (If not, you have to use your own encryption before storing data in the cloud. In that case remember to keep your encryption key safe.)

Risk Mitigation Strategy for Adopting Cloud Computing - before start using

Key Management in the Cloud

- Encryption key at service provider's side
  1. a single master key for all users managed by the cloud provider
  2. per-user key managed by the cloud provider
  3. per-user key managed by the user

- Encryption key at user's side
  1. key stored on individual user’s device
  2. installing a key management server in user’s datacenter

- Encryption key at third party
  1. encryption-as-a-service – use another SaaS solution to manage your keys away from your cloud provider of choice

Risk Mitigation Strategy for Adopting Cloud Computing - when using

Identification and Authentication

- Use a strong authentication method, such as two-factor authentication, if available from the cloud service.
- Use strong passwords for each account.
- Use different passwords for different accounts.
- Use different accounts for different staff.
- Change passwords periodically.
- Delete access accounts or change passwords immediately when there are staff changes.

Risk Mitigation Strategy for Adopting Cloud Computing - when using

Data Protection

- Understand and keep a record of what type of data is stored in the cloud.
- Avoid sharing out data to unintended parties by -
  - ensuring only the intended recipients have the access permissions if you share sensitive data with others through the cloud;
  - defining proper default permissions of files or folders;
  - understand the location (and thus the jurisdiction) of your data including resilient copies

Risk Mitigation Strategy for Adopting Cloud Computing - when using

Cloud Administration

- Establish a simple access account policy for using the cloud service.
- Establish simple usage policies for your staff.
- Appoint suitable staff (who has a basic understanding of the characteristics of cloud services) as the cloud service administrator.
- Conduct regular reviews of access rights on staff having access to cloud data.
- Provide basic security awareness training for staff using the cloud service.

Risk Mitigation Strategy for Adopting Cloud Computing - when using

Service Continuity

- Obtain service support contact information from the service provider; especially keep a list of telephone numbers for reporting computer security incidents.
- Evaluate the potential damage to the company when the service is unavailable, data is lost or when data is accessed in an unauthorized manner.
- Develop a business continuity plan and work out alternatives when the cloud service or data is not available.
- Prepare an exit strategy and ensure termination procedures permit the transfer of data back to the company.
- Maintain a local backup copy of your important data so that this data can still be available when the service provider is out of service temporarily (e.g. network outage) or permanently.

Policy & Guidelines for Cloud Computing

- Security Policy - written in broad and generic terms and provides high level description on security requirements.
- Security Guidelines - operational guides that details how security controls should be implemented and managed.
- Creating a new security policy for cloud may not be necessary, but instead extend existing security policies to accommodate this additional platform.
- ISO 27017 (being drafted) - expected to be a guideline or code of practice recommending relevant information security controls for cloud computing. ISO 27017 will recommend, in addition to the information security controls recommended in ISO 27002, cloud-specific security controls.

Policy & Guidelines for Cloud Computing

Security Policy

Outsourcing Security

Enhance outsourcing security requirements in the areas of (a) manage and review the confidentiality and non-disclosure agreements and (b) assess risks of external services (c) reserve audit and compliance monitoring rights

Human Resource Security

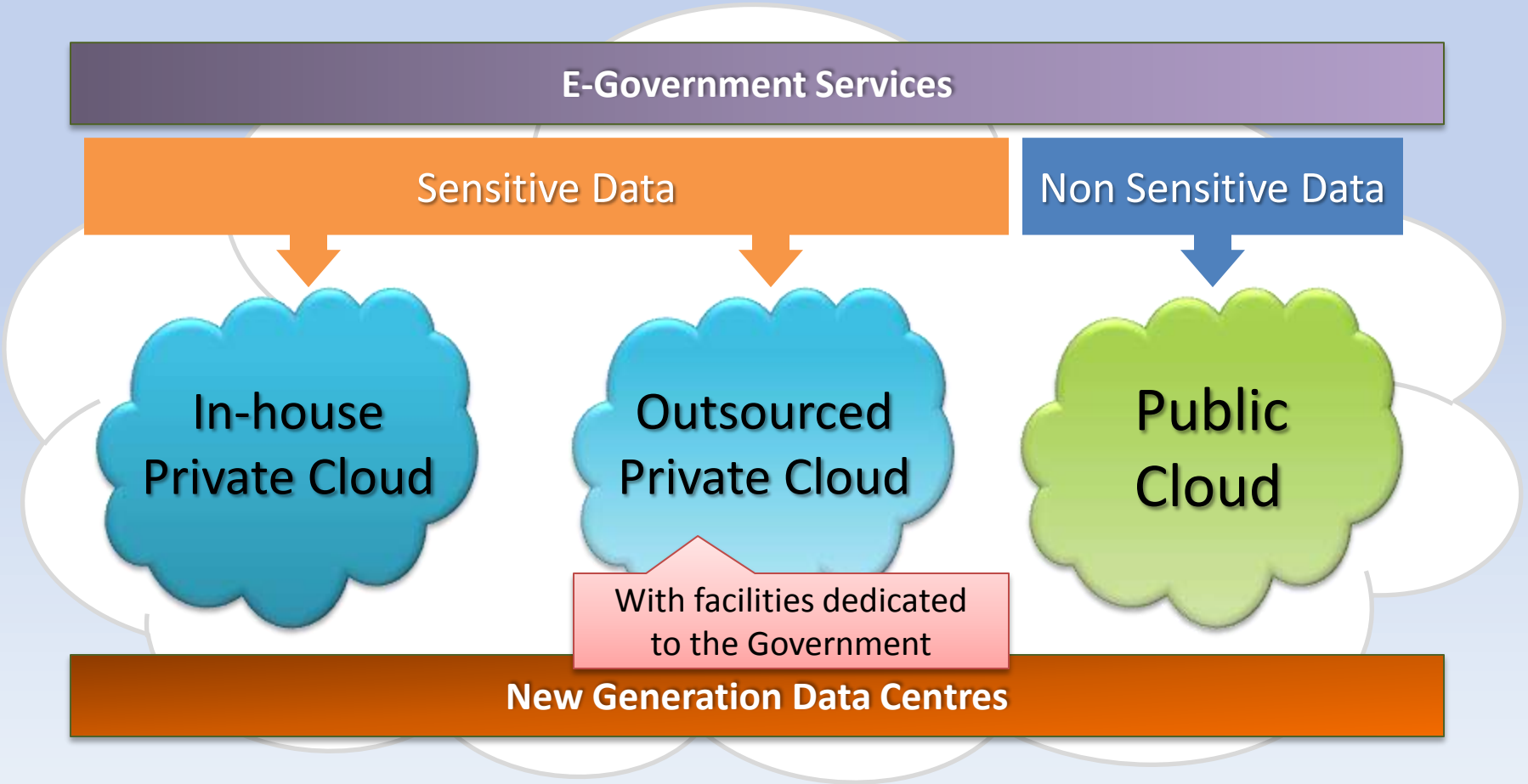
Ensure all staff, including external parties, receive appropriate awareness training

Others – Data access control, User privilege management, mobile computing and remote access

Security Guidelines

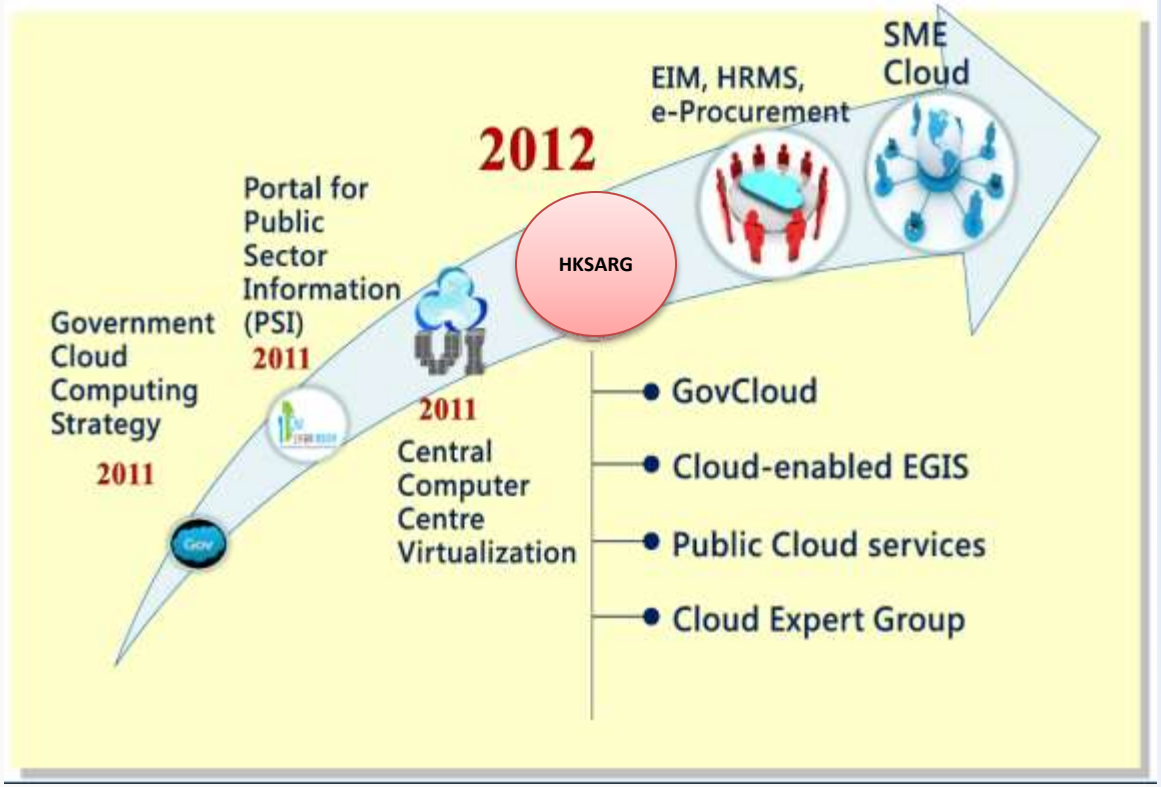
Add guidelines on security considerations when using cloud computing from management, technical and end-user perspectives

Government Cloud Computing Strategy



Government Cloud Computing Strategy

- A step by step approach in order to take full advantage of this new IT model while at the same time minimise the associated risks.



Promotion of Adopting Cloud Computing

Expert Group on Cloud Computing Services and Standards

- To collaborate with the academia, industry and professional bodies
- To promote, develop and adopt best practices and common services for the SMEs

Three working groups were established under the Expert Group including :
- Working Group on Cloud Computing Interoperability Standards (WGCCIS),
- Working Group on Cloud Security and Privacy (WGCSP); and
- Working Group on Provision and Use of Cloud Services (WGPUCS).

Promotion of Adopting Cloud Computing

InfoCloud Portal (www.infocloud.gov.hk)

- To share information, best practices and resources on cloud computing technologies.

References

InfoSec : www.infosec.gov.hk

e-Authentication :
www.e-authentication.gov.hk

電子認證動畫
e-Authentication Animations

Conclusion

- Users or potential users of cloud services must understand the benefits and risks involved so that they can be better prepared to mitigate or control them.
- Potential cloud computing users should take into considerations the security challenges so that potential risks are accounted for before adopting the technology.
- Appropriate measures and controls should be deployed commensurable with the assessed risk level and data sensitivity.
- Organizations need to know what needs to be considered when selecting a cloud service provider, as well as what needs to be considered when using cloud services.


Thank You!