CMSGu2014-04

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Cloud Security

CERT-MU

National Computer Board
Mauritius

Version 1.0

October 2014

Issue No. 4

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide a practical reference to help IT staffs and business decision makers when they analyse and consider the security implications of cloud computing within their organisations.

1.2 Audience

The target audience for this document includes information technology and security staffs responsible for the implementation of a cloud environment.

1.3 Document Structure

This document is organised into the following sections:

This document is organised into the following sections:

Section 1 outlines the document's content, the targeted audience and the document's structure.

Section 2 provides an overview on cloud computing.

Section 3 highlights the cloud security landscape.

Section 4 gives some security recommendations for implementing a cloud environment.

Section 5 elaborates on the general cloud security principles.

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

2.0 An Overview on Cloud Computing

Cloud Computing is a flexible, cost-effective and proven delivery platform for providing business or consumer information technology (IT) services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned on demand, regardless of the user location or device.

Thus, cloud computing gives organisations the opportunity to increase their service delivery efficiencies, streamline IT management and better align IT services with dynamic business requirements. Cloud computing facilitates traditional computing in many ways, supporting core business functions along with the capacity to develop new services.

Both public and private cloud models are now in use. Public models are available to anyone having access to the Internet. Examples are Software as a Service (SaaS) clouds, such as Salesforce, Platform as a Service (PaaS) clouds, such as Google App Engine, and Infrastructure as a Service (IaaS) clouds, such as Windows Azure. Private clouds are owned and used by a single organisation. They offer many of the same benefits as public clouds, and they give the owner organisation greater flexibility and control. Below is an illustration of the different public cloud models.

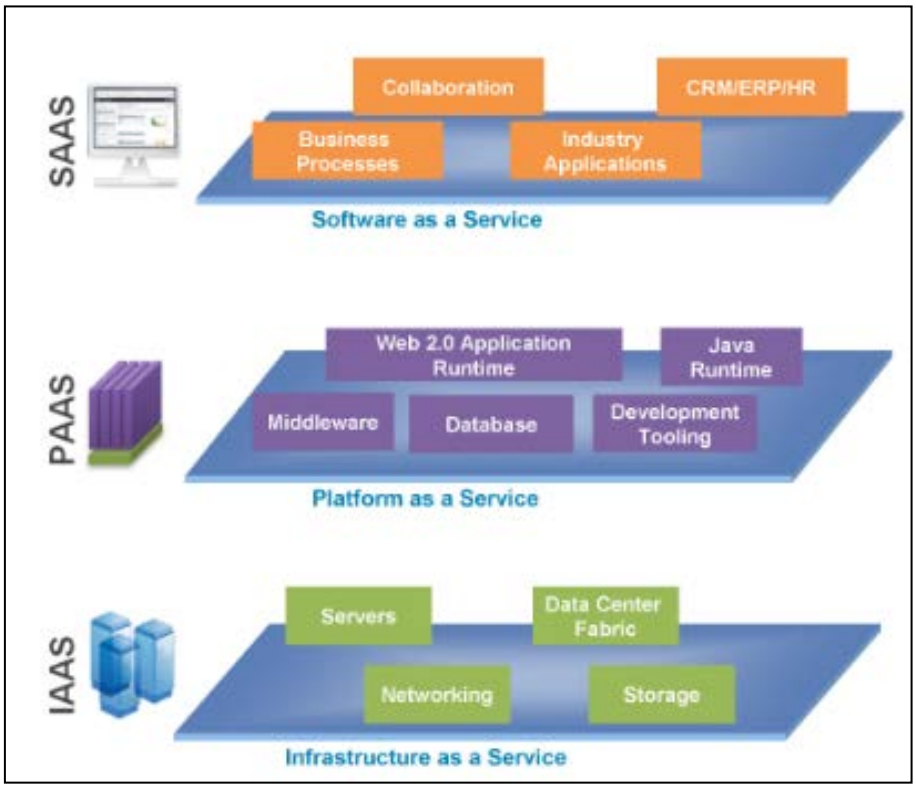

Figure 1 Cloud Computing models

Furthermore, private clouds can provide lower latency than public clouds during peak traffic periods. Many organisations adopt both public and private cloud computing by integrating the two models into hybrid clouds. These hybrids are designed to meet specific business and technology requirements, helping to optimize security and privacy with a minimum investment in fixed IT costs. Even though the benefits of cloud computing are clear, there is still a need to develop proper security for cloud implementations.

3.0 Cloud Security Landscape

In recent years, interest in the cloud computing area has grown rapidly mainly because of the advantages of greater flexibility and availability in obtaining computing resources at lower cost. However, security and privacy are a concern for organisations considering transitioning applications and data to public cloud computing environments.

Migrating to public cloud computing involves a transfer of responsibility and control to the cloud provider over information as well as system components that were previously under the organisation's direct control.

The transition is usually accompanied by loss of direct control over the management of operations and also a loss of influence over decisions made about the computing environment. Despite this intrinsic loss of control, the cloud service consumer still needs to take responsibility for their use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organisation. The consumer achieves this by ensuring that the contract with the provider and its associated service level agreement (SLA) has appropriate provisions for security and privacy. In particular, the SLA must help maintain legal protections for privacy relating to data stored on the provider's systems. The consumer must also ensure appropriate integration of the cloud computing services with their own systems for managing security and privacy. Cloud computing represents a very dynamic area at the present time, with new suppliers and new offerings arriving all the time. There are a number of security risks associated with cloud computing that must be adequately addressed:

- **Loss of governance**

  For public cloud deployments, consumers necessarily give up control to the cloud provider over a number of issues that may affect security. At the same time, cloud service level agreements (SLA) may not offer a commitment to provide such capabilities on the part of the cloud provider, thus leaving gaps in security defenses.

- **Lack of responsibility**

  Given that use of cloud computing services spans across the consumer and the provider organisations, responsibility for aspects of security can be spread across both organisations, with the potential for vital parts of the defenses to be left unguarded if

there is a failure to allocate responsibility clearly. The split of responsibilities between consumer and provider organisations is likely to vary depending on the model being used for cloud computing (for example Iaas versus SaaS).

- **Isolation failure**

  Multi-tenancy and shared resources are major characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between different tenants (for example so-called guest-hopping attacks).

- **Vendor lock-in**

  Dependency on proprietary services of a particular cloud provider could lead to the consumer being tied to that provider. Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.

- **Compliance and legal risks**

  Investment in achieving certification (for example, industry standard or regulatory requirements) may be put at risk by migration to use cloud computing if the cloud provider cannot provide evidence of their own compliance with the relevant requirements or if the cloud provider does not permit audit by the cloud consumer. It is the responsibility of the cloud consumer to check that the cloud provider has appropriate certifications in place, but it is also necessary for the cloud consumer to be clear about the division of security responsibilities between the consumer and the provider and to ensure that the consumer's responsibilities are handled appropriately when using cloud computing services.

- **Handling of security incidents**

  The detection, reporting and subsequent management of security breaches is a concern for consumers, who are relying on providers to handle these matters.

- **Management interface vulnerability**

  Consumer management interfaces of a public cloud provider are usually accessible through the Internet and mediate access to larger sets of resources than traditional

hosting providers and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

- **Data protection**

  Cloud computing poses several data protection risks for cloud consumers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud consumer (in the role of data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is aggravated in cases of multiple transfers of data, for example, between associated cloud services.

- **Malicious behavior of insiders**

  Damage caused by the malicious actions of insiders working within an organisation can be substantial, given the access and authorizations they may have. This is multiplied in the cloud computing environment since such activity might occur within either or both the consumer organisation and the provider organisation.

- **Insecure or incomplete data deletion**

  Requests to delete cloud resources, for example, when a consumer terminates service with a provider, may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a consumer perspective), either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other clients. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the consumer than is the case with dedicated hardware.

- **Business failure of the provider**

  Such failures could render data and applications essential to the consumer's business unavailable.

- **Service unavailability**

  This could be caused by a host of factors, from equipment or software failures in the provider's data center, through failures of the communications between the consumer systems and the provider services.

While the above security risks need to be addressed, use of cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of many organisations. Cloud service providers should be able to offer advanced facilities for supporting security and privacy due to their economies of scale and automation capabilities, potentially a boon to all consumer organisations, especially those who have limited numbers of personnel with advanced security skills.

4.0 Security Recommendations

A number of significant security and privacy issues were covered in the previous section. Table 1 below summarizes those issues and related recommendations for organisations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Areas	Recommendations
Governance	• Extend organisational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organisational practices are followed throughout the system lifecycle.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Set up a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support ongoing risk management decisions.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organisation.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organisation and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and

	electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organisational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organisation. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organisation can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organisational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. • Take into consideration the risk of collating organisational data with that of other organisations whose threat profile s are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organisation.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organisation's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a

	serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organised manner.

Table 1 Security Recommendations for Cloud Implementation

5.0 Cloud Security General Principles

This section highlights the essential security principles to consider when evaluating cloud services, and why these may be important to your organisation. Some cloud services will fulfil all of the security principles, while others will only meet a subset.

- **Consumers** of cloud services should decide which of the principles are important, and how much (if any) assurance they require in the implementation of these principles.
- **Providers** of cloud services should consider these principles when presenting their offerings to public sector consumers. This will allow consumers to make informed choices about which services are appropriate for their needs.

The Cloud Security General Principles are summarised in the table below.

Cloud Security Principle	Description	Why this is important
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage.
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers cannot prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service.
4. Governance	The service provider should have a	If this principle is not implemented,

framework	security governance framework that coordinates and directs their overall approach to the management of the service and information within it.	any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments.
5. Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it.
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased.
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity.
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles.
9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data.
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data or denial of service may occur.

11. External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it.
12. Secure service administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data.
13. Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales.
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers.

Table 2 Cloud Security Principles

6.0 Conclusion

Cloud computing has far-reaching effects on organizations compared to traditional computing. However, security and privacy in the cloud still remains a concern in the area. Hence, organisations must ensure that security and privacy controls are implemented correctly and operate as intended, throughout the implementation of the cloud environment.

7.0 References

- **https://www.gov.uk**
- **http://www.cloudstandardscustomercouncil.org**
- **www.redbooks.ibm.com**
- **https://cloudsecurityalliance.org**
- **http://csrc.nist.gov**