Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Cloud Computing Security

[ISPG-SM04]

Version 2.0

April 2024

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Added a new chapter on information security management, aligned references with other practice guides, added emerging cloud security service and technologies in Section 5, Section 5.7, Section 5.9.2 and Annex B.	Whole document	1.1	July 2018
2	Updates were made on the requirements of CSP to provide proper data protection in Section 5, Section 5.1, Section 5.3, Section 5.4, Section 5.5 and Section 5.7; and de-identification techniques for personal data protection in Section 5.4 and Annex B; and emerging solutions in Annex B.	15-18, 20-22, 26, 42, 44, 49	1.2	June 2021
3	Updated Section 3.1 on the cloud service models. Added a shared responsibility concept in Section 4.1. Updated Section 4.2 on the cloud implementation scenarios. Updated Section 5, Section 5.1, Section 5.2, Section 5.3, Section 5.4, Section 5.5, Section 5.7, Section 5.8, Section 5.9, Section 5.12 and Section 5.14 on the security considerations and controls.	6, 9-15, 16-37, 43, 47, Annex A, Annex B	2.0	April 2024

Table of Contents

1. Introduction

This document is intended to serve a diverse group of audience, such as management staff, IT administrators, system owners and information security stakeholders, who have the responsibility to assess the security impact from embracing various cloud computing models for the storage, processing, or transmission of government information.

As cloud computing is rapidly evolving and advancing, new forms of cloud or various derivative combinations of existing ones may emerge. The materials included in this document can generally be applicable. As each cloud computing deployment may have its own characteristics, implementers should consider and select those practices that are applicable to their own environment.

Note: The author of this document does not endorse the use or imply preference for any vendor commercial products or services mentioned in this document. Also, this document is NOT intended to supersede the security regulations, policies and guidelines in the Government and B/Ds' departmental IT security policies.

1.1 Purpose

In response to the increasing use of cloud computing as a global trend, this document is developed for providing guidance notes to Bureaux and Departments (B/Ds) for the purposes as described below:

- Enhance B/Ds' understanding on the basics of cloud security; and
- Facilitate B/Ds on the secure use of cloud computing when building their own private cloud or acquiring cloud services from external parties.

This document highlights common security considerations and industry security best practices for the adoption of cloud computing.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17] , the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3] , the Government of Hong Kong Special Administrative Region
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology – Security techniques – Governance of information security, ISO/IEC 27014:2013
- Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015
- Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO/IEC 27018:2014
- Information technology – Security techniques – Information security for supplier relationships, ISO/IEC 27036:2014
- Information technology – Security techniques – Storage security, ISO/IEC 27040:2015

1.3 Terms and Convention

For the purposes of this document, the terms and conventions given in S17, G3, and the following apply.

Abbreviation and Terms	
Cloud Service Provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organisations and/or individuals, usually for a fee.

1.4 Contact

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email: it_security@ogcio.gov.hk

Lotus Notes mail: IT Security Team/OGCIO/HKSARG@OGCIO

CMMP mail: IT Security Team/OGCIO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk-based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary, so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems and/or data to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. Security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Introduction to Cloud Computing Security

3.1 Cloud Computing

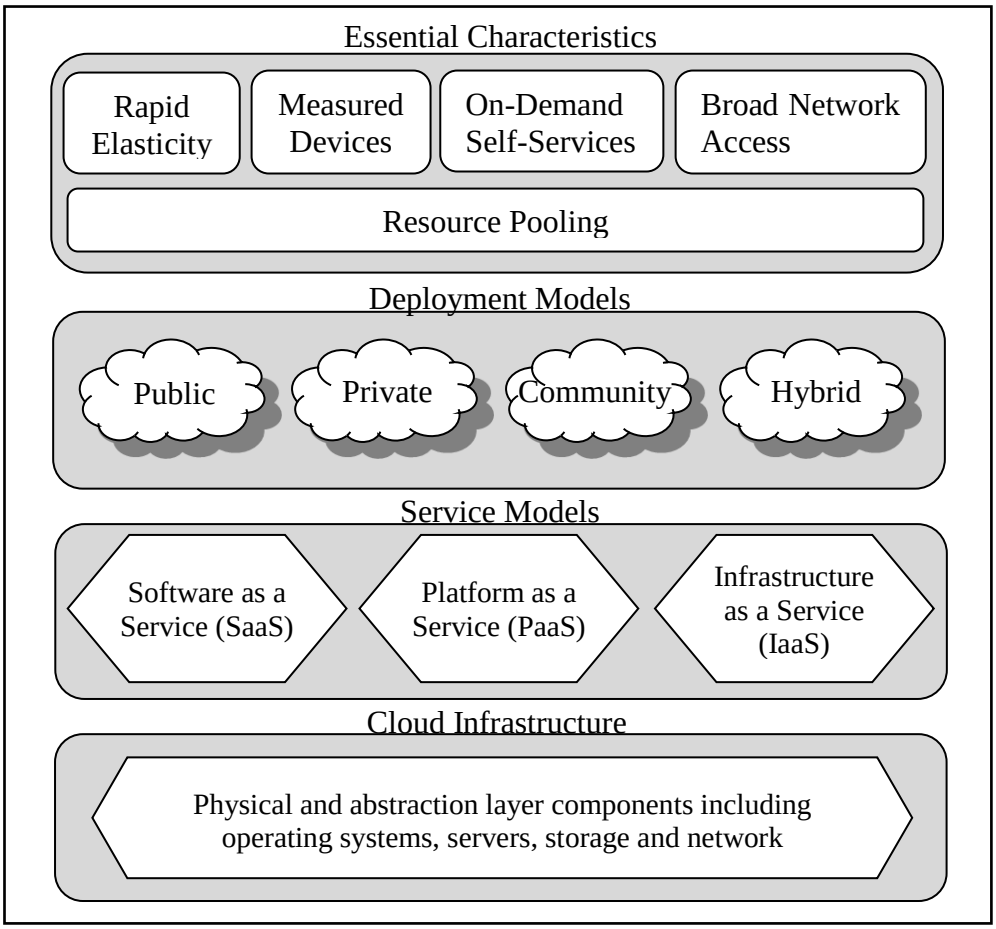

Figure 3.1 Cloud Models

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing under cloud infrastructure can be basically described as three service models and four deployment models[1], which are summarised in the visual model as shown in Figure 3.1 above.

[1] "The NIST Definition of Cloud Computing", SP 800-145, NIST.

3.2 Cloud Infrastructure

A cloud infrastructure is the collection of hardware and software that enables essential characteristics of cloud computing such as resource pooling, rapid elasticity, measured service, on-demand self-service and broadband network access. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually, the abstraction layer sits above the physical layer.

3.3 Cloud Service Models

There are three typical types of cloud service models as follows:

- Infrastructure as a Service (IaaS): Cloud Service Provider (CSP) delivers a service with fundamental computing resources/equipment (storage, hardware, servers and network components) to B/D while the B/D remains in control of the operating system and applications installed;
- Platform as a Service (PaaS): CSP delivers a service with the fundamental computing resources/equipment and the virtualisation environment to B/D, which deploys its own applications on this environment or cloud infrastructure; and
- Software as a Service (SaaS): CSP delivers a service with infrastructure, platform (or virtualisation environment), and software to B/D. Users from B/D connect to this environment and run the IT applications after customisation.

3.4 Cloud Deployment Models

There are four typical types of cloud deployment models as follows:

- Public Cloud: the cloud infrastructure is provisioned for the public. It supports multi-tenancy. It may be owned, managed, and operated, or in any combination of them by a third party; it is hosted on the CSP's premises;
- Private Cloud: the cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple B/Ds. It may be owned, managed, and operated, or in any combination of them, by the organisation (i.e. In-house Private Cloud), a third party (i.e. Outsourced Private Cloud); it is hosted on or off premises;
- Community Cloud: the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have common goals, interests and/or shared concerns. It may be owned, managed, and operated, or in any combination of them, by one or more of the organisation(s) in the community; it is hosted on or off premises; and

- Hybrid Cloud: the cloud infrastructure is composed of two or more distinct cloud infrastructures (private, community, or public) that may be provisioned by different CSPs. This model enables data and application portability.

3.5 Comparison of the Four Deployment Models

A comparison table on the aspects relating to information security for the four deployment models is given below:

Aspects	**Public Cloud**	**Private Cloud**	**Community Cloud**	**Hybrid Cloud**
Service Delivery	Delivered over the Internet	Delivered via a (virtual) private network	Delivered via a (virtual) private network	Combination of Internet and private networks
Service Level Agreement (SLA)	SLA defined by CSP	SLA defined by the organisation	Shared SLA by participating organisations	Mix of different SLAs
Examples of Use	Productivity, business and social media applications and other cloud IT services.	Internal government services hosted in infrastructure provisioned for exclusive use by the Government.	Services for community of the Government and Non-Government Organisations with shared business needs.	A private cloud application connected to a public cloud service for capacity needs that cannot be met by the private cloud.

The move to cloud computing is a business decision, in which the business case should consider relevant factors such as transition cost, life-cycle cost and readiness of the applications besides security. Nevertheless, B/Ds should assess the sensitivity of their data and determine the suitable deployment model for processing and storing their data. B/Ds shall ensure that classified data are protected no matter which cloud service model it adopts and all government security requirements are fulfilled as well as business needs are catered. With an overall security assessment of a potential cloud platform, B/Ds should identify gaps in security protections offered by the CSP and determine effective approaches to mitigate risks to their data.

4. Cloud Security Overview

As with any new computing model or technology, cloud computing may pose new security risks. A risk-based approach should be adopted when considering use of cloud computing. It is important for B/Ds to consider various security areas such as data confidentiality, integrity, redundancy, resilience, jurisdiction, etc. It is also important to understand what data are being considered moving to the cloud, their risk tolerance, and the service and deployment models being chosen. Users or potential users of cloud services must understand the challenges and risks involved so that they can be better prepared to mitigate or control them. Appropriate security measures and controls should be deployed commensurate with the assessed risk level and the value of the data.

4.1 Cloud Service Model and Information Security

As a general principle, a B/D can have greater security control over more resources as one moves from SaaS to PaaS and again from PaaS to IaaS service model. Figure 4.1 shows the scope of control between responsible parties in cloud:

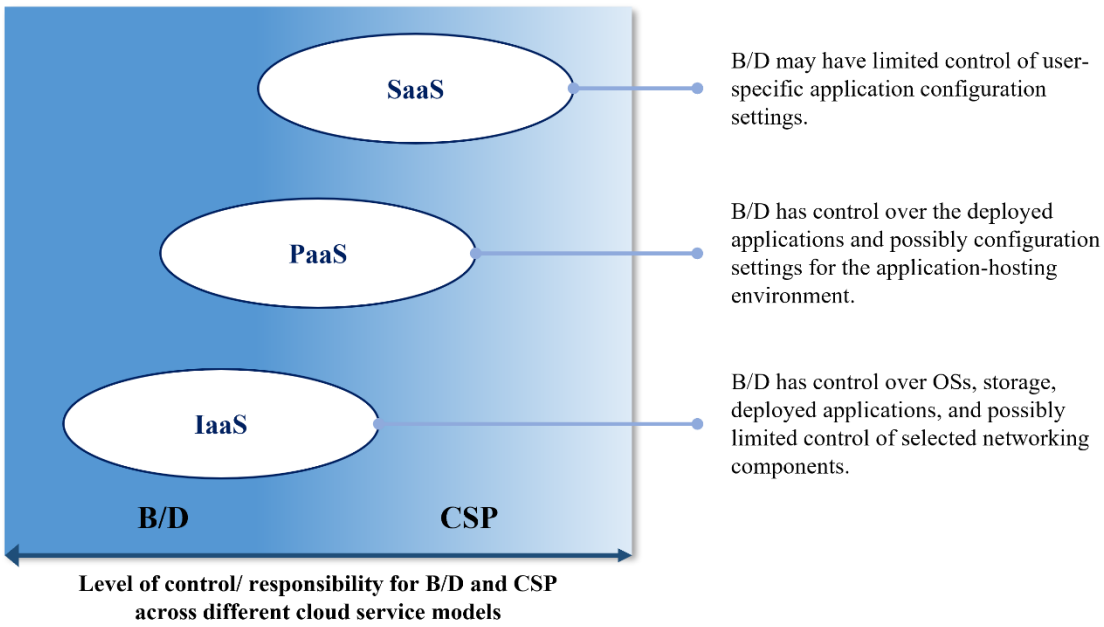

Figure 4.1 Level of control responsibility for B/D and CSP across different cloud service models

There is no cloud service model in which one party takes up all responsibilities. Shared responsibility is an important concept no matter which model is adopted, and the variance of responsibility level depends on the cloud service model. B/Ds shall ensure that the responsibilities of both parties are clearly defined and understood. Figure 4.2 shows the shared responsibilities commonly adopted between responsible parties in the cloud, although there may be variations adopted by specific CSPs due to commercial considerations:

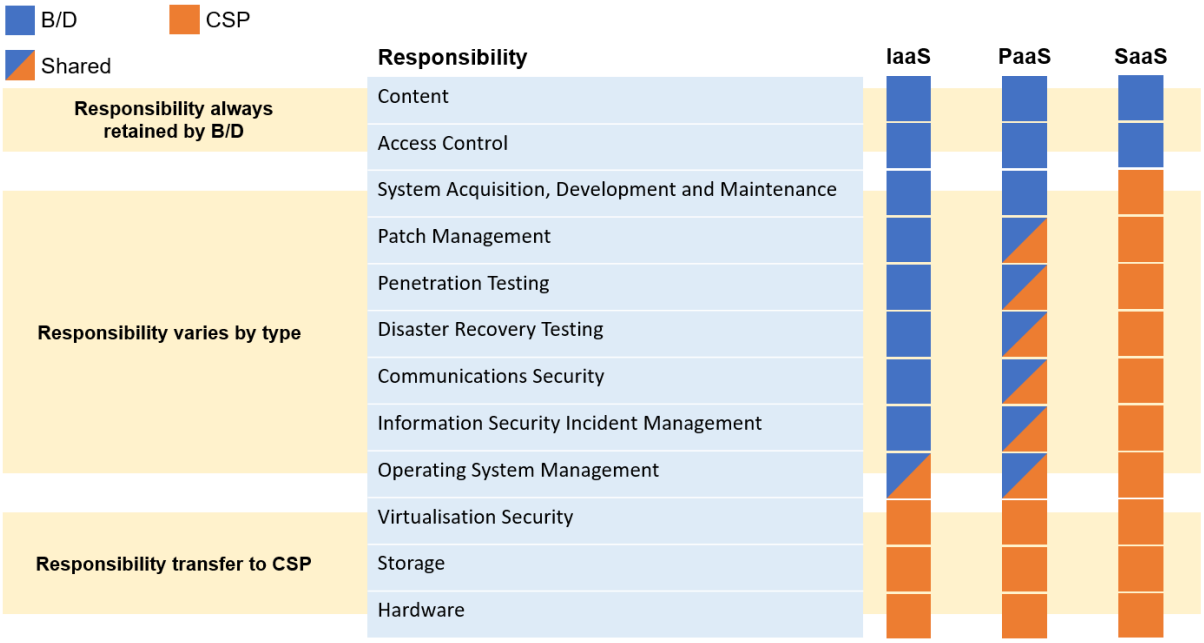

Figure 4.2 Shared responsibilities of B/Ds and CSP across different cloud service models

SaaS services are typically accessed by clients using a web browser over the Internet, and the clients do not manage or control the underlying cloud platform and infrastructure. With SaaS, B/Ds usually have little direct control over the cloud security and service domains. They are only responsible for managing content and access control.

PaaS provides cloud facilities at the middle layer, which tends to be more extensible than SaaS at the expense of customer-ready features. B/Ds have more control over the platform, including content, access control and patch management, while the CSP controls operating system management, virtualisation security, storage and hardware. In this model, B/Ds and CSPs have to discuss, define and agree on managing the remaining security domains.

IaaS requires B/Ds to implement its own applications and set up its platform riding on the infrastructure provided by the IaaS CSP. B/Ds are entitled to have flexibility to manage and control most of the security domains in a cloud environment, including content, access control, system acquisition, development and maintenance, patch management, penetration testing, disaster recovery testing, communications security, and information security incident management, whilst CSP is responsible for managing virtualisation security, storage and hardware. The responsibility for operating system management requires further discussion and agreement between B/Ds and CSP.

CSP is still responsible for controlling and securing the underlying cloud infrastructure components, such as content and access control, no matter which cloud service model. B/Ds are responsible for managing the stored content and

access control. B/Ds and CSPs should understand their responsibilities and closely collaborate and communicate to ensure the cloud environment's security and reliability.

4.2 Cloud Implementation Scenarios and Information Security

The degree of security control under the B/D varies between the public cloud and private cloud models. As public cloud is provisioned for the general public and used by multiple tenants while private cloud is provisioned for exclusive use by a single organisation, private cloud would give the organisation better control over the network infrastructure and security policies with stronger access controls. Hence, the public cloud may face similar security threats if not configured properly. It is important to note that any benefits a private cloud infrastructure offers are limited to its implementation method. Implementation scenarios on whether the cloud services are in-house or outsourced as well as on premises or off premises are also important to the security protection for a cloud environment.

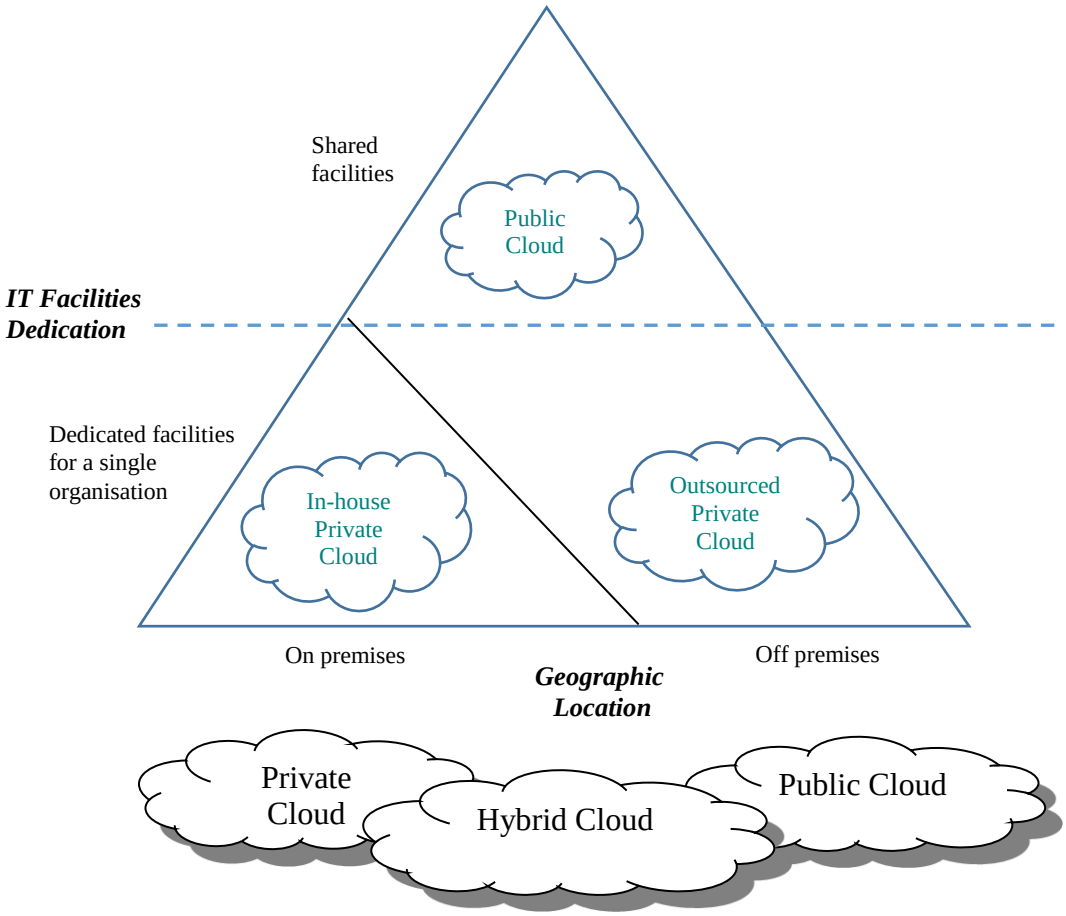

Figure 4.3 Cloud implementation scenarios

For the purpose of further discussion on security considerations and controls for cloud deployment within B/Ds, the four scenarios in Figure 4.2 will be referenced:

- "In-house Private Cloud Scenario" owned and operated by the Government in on premise data centres.
- "Outsourced Private Cloud Scenario" comprising facilities dedicated to the Government in off premise data centres operated by external CSPs, for instance, the Government Cloud Platform (GovCloud).
- "Public Cloud Scenario" provided by external CSPs offering services for use by the public.
- "Hybrid Cloud Scenario" composed of two or more cloud scenarios (private or public)

4.2.1 In-house Private Cloud Scenario

In-house private cloud is located on the premises of an organisation and managed by in-house staff. While non-technical security issues such as outsourcing requirements, data location, and service termination may not be as applicable, it is important to note that organisations may still have a high degree of dependency on commercial vendors to provide software/firmware upgrades, replacement of faulty IT components in servers, IT devices, etc. This dependency on commercial vendors can still pose challenges of security vulnerability from a supply chain perspective. B/Ds should understand their responsibilities in managing supply chain risks, such as vendor management for maintenance and system upgrades, and conduct regular audits and assessments to ensure that commercial vendors follow the organisation's security policies and guidelines.

4.2.2 Outsourced Private Cloud Scenario

An outsourced private cloud is a single-tenant environment fully managed by a third party to achieve higher cost-effectiveness or operational efficiency. Additional benefits of outsourced private cloud computing include that the IT infrastructure for B/Ds could be purchased and maintained by a third-party organisation in its data centre. The third party provides maintenance, upgrades, support, and remote management of the private cloud resources.

B/Ds should leverage the third-party attested reports (e.g., SOC 2 Type 2 Reports) provided by CSPs as a baseline to understand which security domains have been checked by the independent third-party auditor. Since SOC 2 Type 2 reports provide information on CSP's performance across security, privacy, processing integrity, confidentiality and availability domains, B/Ds can have better visibility of CSP performance in terms of operational effectiveness through reviewing such reports. B/Ds should then decide if clarification and further information is needed from CSPs to understand the level of conformance. This aligns with industry best practices adopted by mature CSPs and allows B/Ds to focus on the security of their workloads in the cloud environment instead of cloud infrastructure. As the data centres used by CSPs are not located at B/Ds' premises, B/Ds should require CSPs to adopt robust access logging mechanisms in order to obtain prompt alerts on potential unauthorised data access. The more proactive CSPs are in detecting potential unauthorised data access attempts, the more effective they can become in preventing security incidents from occurring. A common myth is that cloud service buyers often think that CSPs are responsible for all the on-going management responsibilities of the cloud environment in the case of an outsourcing arrangement. However, cloud service buyers still have responsibility for monitoring the performance of CSPs on a regular basis.

4.2.3 Public Cloud Scenario

A public cloud is one in which a third-party CSP manages the underlying computing resources. The CSP is responsible for resource maintenance and guarantees

availability, reliability, and security through service-level agreements. B/Ds do not buy, own or maintain physical data centres and servers. Instead, B/Ds access technology services on an as-needed basis. It is owned by a CSP selling cloud services and, by definition, is external to a B/D. Security of the cloud infrastructure and cloud native services are fully managed by CSPs. Therefore, understanding the public cloud computing environment offered by CSPs and ensuring that a cloud computing solution satisfies organisational security and privacy requirements are essential.

Standard SLA offered for public cloud services by CSPs, documenting a common understanding of services, priorities, responsibilities, guarantees and warranties, often have limited or no room for negotiation. B/Ds should pay attention to the security impacts and the provisioning penalties in case of any breaches of SLA.

4.2.4 Hybrid Cloud Scenario

On top of the above three implementation scenarios, there exists another possible type of implementation scenario – Hybrid Cloud Scenario. As mentioned in Section 3.4, a hybrid cloud infrastructure is typically composed of two or more distinct cloud infrastructures (such as private and public). Hybrid Cloud implementation scenario, consequently, is a composition of the other three implementation scenarios (In-house Private Cloud, Outsourced Private Cloud and Public Cloud scenarios).

Connection of the cloud environment offered by CSPs to the network of B/Ds should not compromise the existing security level. B/Ds should assess the security risks when acquiring cloud service and be based on the principle that stronger security protection is adopted on both sides if the security protection level of the parties is different.

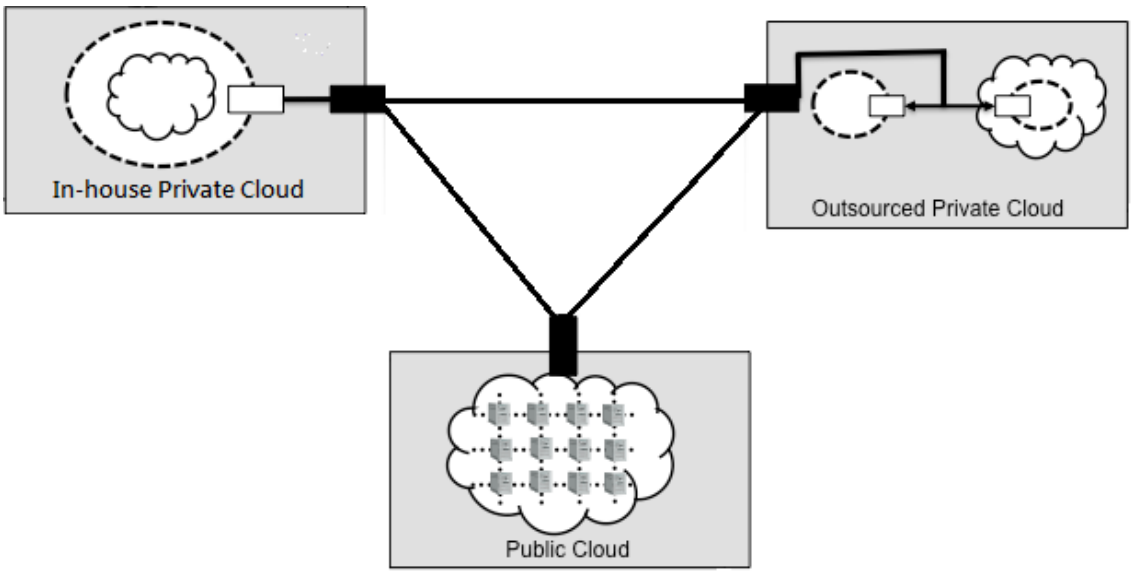

Figure 4.4 Hybrid Cloud Scenario

A common adoption of the Hybrid Cloud scenarios is "cloud bursting", in which an enterprise uses an in-house private cloud for primary operations, but optionally accesses one or more out-sourced private clouds during peak demand periods for the sake of load balancing.

5. Security Consideration and Controls for Cloud Services

After understanding the basic concepts of cloud computing and cloud security, the corresponding security controls are discussed in this chapter. Cloud computing can be viewed as a new way of delivering IT based services to enterprises, rather than a new technology on its own. Specific technologies, of course, have significant importance in a cloud computing environment, such as virtualisation. For the most part, cloud computing uses similar management tools, operating systems, databases, server platforms, network infrastructure, network protocol, storage arrays, and so on. Therefore, security controls in cloud are largely similar to those controls in traditional IT environment. As such, security controls described in government security documents including the Baseline IT Security Policy [S17] and IT Security Guidelines [G3] will still apply. However, due to the characteristics of the cloud service models and deployment models, and the technologies used to enable cloud services, certain risks in a cloud environment may become more or less significant (e.g., automatic security patching with proper configuration) and certain risks that do not exist in a traditional IT environment may exist in a cloud environment. The following sub-sections describe the challenges and cloud-specific security practices for handling such risks. The description will focus on the following security domains.

- Management Responsibilities
- IT Security Policies
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operation Security
- Communications Security
- System Acquisition, Development and Maintenance
- Outsourcing Security
- Security Incident Management
- IT Security Aspects of Business Continuity Contingency Management
- Compliance

For each of the security considerations and controls, tags are included at the end of the control statement indicating which implementation scenarios to which the control should most suitably apply. The security controls of hybrid cloud should be considered with reference to its composition. If the hybrid cloud is comprised of public cloud and in-house private cloud, the security considerations and controls of both cloud implementation scenarios should be observed. The tag only indicates general relevancy. If there is no tag for a certain implementation scenario, it does not mean the control is totally irrelevant.

When adopting cloud services, B/Ds are advised to take a risk-based approach, assess business need and data classification, and ensure that security measures, service levels and management requirements of CSP are commensurate with the data classification and business requirements, and comply with the government security requirements and business needs. As the security level differs for different CSPs, B/Ds should carefully examine and consider the data handling practices adopted by CSPs in all aspects. The following cloud-specific security practices are for general cloud deployment scenarios. Moreover, as cloud technology advances, CSPs may provide new cloud solutions and services to the market. B/Ds are advised to conduct their own research, assess potential risks, adopt best practices, and determine the most suitable deployment model accordingly. Since each installation may have its own specific implementation scenario, implementers should make their own judgement and select the most appropriate security controls. B/Ds should ensure that CSPs provide the necessary controls and services to enable B/Ds to protect government data properly, in particular involving sensitive data, during the design, development, deployment and configuration stages of infrastructure so that proper isolation of sensitive or classified government data from other customer environments can be achieved.

The meaning of the tags is:

"Name of the security considerations and controls" [I] [O] [P]

[I] - "In-house Private Cloud"
[O] - "Outsourced Private Cloud"
[P] - "Public Cloud"

A summary of the security controls for cloud implementation by different domains are provided in **Annex A** for B/D's easy reference.

According to Section 17.3 Public Cloud Services of Baseline IT Security Policy [S17], government data classified as CONFIDENTIAL or above shall not be stored in or processed by public cloud services while government data classified as RESTRICTED shall follow relevant public cloud security framework or guidelines issued by OGCIO for storage and processing by public cloud services.

5.1 Management Responsibilities

Users are ultimately accountable for managing security and control over their organisational data. A risk-based approach should be adopted to incorporate a cloud computing strategy in their information systems strategic plans and/or organisational IT plans. Appropriate security management practices and controls should also be adopted and strictly implemented. Strong management practices are essential for operating and maintaining a secure cloud computing solution. Good practices entail monitoring the organisation's information system assets and implementing policies, guidelines and procedures to establish and preserve the confidentiality, integrity, and availability of information system resources.

In a cloud environment, many CSPs may allow users to decide where their data is stored geographically. Moreover, without consent, data cannot move outside the user's chosen location. Without sufficient user oversight, it is not easy to maintain an auditable record of data location and ascertain whether sufficient safeguards are in place to protect the data under different jurisdictions. Furthermore, CSPs provide their services with the use of emerging technologies, involving advanced hardware infrastructures and complex management tasks. System failure or security incidents could happen if not configured and handled correctly by the CSP. For outsourced private clouds or public clouds, another challenge is cloud lock-in, which refers to a situation in which a B/D is attached to its current CSP due to the complexity of, and hence difficulty in, switching to another CSP. There may be difficulties in having one's business migrated from its current CSP to a new one. Therefore, B/Ds are advised to adopt approaches to address this challenge, including:

- ensuring the implementation of best practices for data backup, data deletion and data portability;
- ensuring the selected CSP provides feasible solutions for B/Ds to migrate out from the selected CSP; and
- working with multiple CSPs to ensure data portability and configurations are optimized for migration from the current CSP to a new one.

- Analyse the impacts to the security procedures in light of different jurisdictions [O] [P]

  B/Ds should ensure that they have visibility into where their data is stored within the CSP's cloud infrastructure. All contracts should clearly describe the governing law and jurisdiction clauses. B/Ds should be aware that data kept in another jurisdiction is subject to the laws of that jurisdiction. Moreover, some CSPs may be subject to the laws of their registered jurisdiction no matter where the data is stored. Even though there are restrictions on data access as stated in the contract or service level agreement, the law of that registered jurisdiction cannot be overridden. Hence, B/Ds should consider that their rights are at risk of being subjected to the CSP registered jurisdiction. Moving data and applications to cloud services will likely have impacts on security procedures in light of the differences in legal and regulatory compliance requirements. B/Ds

shall assess the risk associated with such arrangement in accordance with the nature of data being stored or processed. All these potential impacts should be analysed in detail, and the relevant procedures should be identified. Legal advice should be sought on the contractual arrangements where necessary to ensure sufficient protection of sensitive data from involuntary disclosure. Enhancement to the security measures, such as data encryption and data masking (refer to Section 5.4 Asset Management) should be considered to compensate for any areas outside B/D's direct control. The affected procedures may include incident reporting, activity logging, data retention and application testing.

- Verify the compliance of industry security standards [O] [P]

Security certification is the proof of having attained the required maturity level and ensuring quality assurance of an external CSP. Cloud services should be checked to understand their compliance with globally recognised industry security standards, such as:

- ISO 27001 (Information security management)
- ISO 27017 (Code of practice for information security controls for cloud services)
- ISO 27018 (Code of practice for the protection of personally identifiable information (PII) in public clouds
- SOC 2 Type 2 report (Security, availability, processing integrity, confidentiality, and privacy controls' attestation and assurance)

In addition, CSP should be checked to ensure their adherence to nationally recognised industry security standards such as:

- TRUCS (Trusted Cloud Service, Cloud service assessment framework)
- ITSS (Information Technology Service Standards, Cloud computing service capability assessment)
- DJCP (Multi-Level Protection Scheme in China).

Referencing and benchmarking these standards will ensure compliance with government security requirements and meet operating effectiveness and business needs. The Consensus Assessments Initiative Questionnaire created by the Cloud Security Alliance provides a reference set of questions for assessing a CSP. External CSPs should request Compliance certificates and reports to verify their validity. If confirmed valid, these certifications can be used to assess and validate the security and compliance of CSPs' infrastructure, service, and all security controls in place or being used.

5.2 IT Security Policies

- Review departmental security policy [I] [O] [P]

  Departmental security policy should be reviewed and modified with the necessary adjustments for protecting data to ensure the security controls are effective when deploying business applications in a cloud environment. The adjustments may include new or revised security requirements and controls specific to cloud-related areas such as multi-tenancy, data location, virtualisation and secure use of cloud services. The adjustments should align with industry best practices adopted by CSPs that are published as third-party reports and publicly accessible.

5.3 Human Resource Security

- Define roles and responsibilities on resource control and information security [I] [O] [P]

  Roles and responsibilities of the personnel, including but not limited to the B/D and the CSP, to support the operation and account for information security of the cloud services should be clearly defined and documented such as service level agreement, especially in data centres of an outsourced multi-tenancy cloud environment. B/Ds shall request CSPs to ensure that their employees and contractors who would handle outsourced information systems containing sensitive or classified government data are suitable for the roles. CSPs should be requested to have clear segregation of job duties, for example, a single person should not take up both system administration and security administration activities. Need-to-know principle shall be strictly enforced. Moreover, updated contact information of responsible supervisory authorises should be maintained.

- Request non-disclosure agreement and ensure proper human resource management [O][P]

Where appropriate, staff from the CSP and its subcontractors should agree and sign a non-disclosure agreement. Alternatively, B/Ds should use contractual means such as the cloud contract to ensure that staff from the CSP and its subcontractors undertake the obligation of confidentiality. CSPs shall commit not to transfer or disclose sensitive or classified information to any other third parties unless authorised. In case there are requests from other third party for accessing such information, CSPs shall immediately inform and redirect the requests to B/Ds for handling if such requests cannot be directly rejected unless prohibited by law. The selection of CSP should also consider CSP's background check procedures for staff with high privilege on access authority, as well as clear processes and procedures for employment termination. Background checks may include a review of the person's history on education, employment, and criminal records as appropriate, where permitted by applicable law and to the extent available from applicable government authorities. The employment termination procedure may require the staff to return all assets, particularly classified data, keys and tokens, relating to his/her duties, and all relevant access rights must be removed.

- Issue guidelines or reminders for user awareness [I] [O] [P]

Cloud application specific guidelines or reminders should be issued regularly to ensure that end-users of the cloud services are fully aware of the sensitivity of data and stay vigilant on possible security threats so that necessary actions can be taken during the data lifecycle, such as removing data stored in cloud when the data is no longer used or required to be retained.

- Ensure adequate security training to relevant personnel [I] [O] [P]

Information security awareness training should be provided regularly for internal and external staff, including subcontractors of CSPs in order to ascertain their security awareness and understanding of the security requirements such as prevailing government IT security requirements, beware of information security risks and incident response handling procedures as well as their responsibilities and consequence if they disregard the IT security requirements as laid down by CSPs. It is desirable for personnel who are responsible for security management and operation to have renowned international, national or industry recognised certificates, such as CCSK[2], CCSP[3], CISM[4], CISP[5], CISSP[6], ITIL[7] or equivalent.

[2] CCSK - Certificate of Cloud Security Knowledge
[3] CCSP - Certified Cloud Security Professional
[4] CISM – Certified Information Security Manager
[5] CISP – Certified Information Security Professional
[6] CISSP – Certified Information System Security Professional
[7] ITIL – Information Technology Infrastructure Library

5.4 Asset Management

Off premises, outsourced data centre, multi-tenancy, use of the Internet and many other cloud features dovetail security threats of unauthorised access to sensitive data through physical and network access. Data confidentiality may also be affected due to potential risks of misconfiguration by clients and CSP's lack of commitment to protecting client data and exposing the client applications and data to cyber threats. Moreover, it may be difficult or impossible for B/Ds to reclaim data from an external CSP under unexpected service termination situations, such as company merging and amalgamation, CSP bankruptcies, service shutdowns and other unexpected events.

- Protect data by encryption [I] [O] [P] [8]

Data encryption is a way to enhance data confidentiality. B/Ds should confirm that encryption capabilities provided on cloud services are adequate in accordance with the cryptographic policy on the use of cryptographic controls. Classified data shall be protected using strong encryption method both at rest and in transit in accordance with government security requirements and business needs. Open and proven encryption algorithms should be adopted to avoid locking in proprietary algorithms. Encryption keys should be properly protected and managed throughout the key lifecycle (refer to Section 5.6 Cryptography).

- Observe data protection and privacy legislation for outsourced data centres [O] [P]

Data protection and privacy legislation shall be observed. For protection of the privacy of individuals in relation to their personal data in Hong Kong, the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486), particularly the Data Protection Principle 4 (on security of personal data), shall be observed.

With increasing demand on a better cost-effective model, some outsourced data centres are located offshore. Data storing at or moving between the offshore data centres where information crossing borders may be subject to local legislations of the data centres, hence the adoption of offshore outsourcing may be considered for unclassified data hosting, while the sensitive/classified data transactions should only occur within onshore data centres with proper security control.

For local legislation development, Section 33 of the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486), although not yet enacted, should be made reference if applicable. Section 33 restricts the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The Office of the Privacy Commissioner for Personal Data (PCPD) published a document "Guidance on Personal Data Protection in Cross-border Data Transfer" providing relevant information for reference. B/Ds must ensure service providers seek their approval before allowing information to leave outside Hong Kong borders.

[8] While there is no specific regulation on encryption of unclassified information, as a good practice to protect data privacy, B/Ds may adopt encryption to protect unclassified information when using public cloud service.

- De-identification of personal data [I] [O] [P]

Consider adopting an additional layer of data protection by de-identifying information systems' data involving collecting, processing, storing, archiving, and disclosing data subjects' particulars. Data de-identification refers to the algorithm and processes to alternate the original dataset to prevent data subjects' identity from being revealed with the processed result without hampering business purposes.

Apart from the data protection point of view, policy compliance is another driver of its adoption; it has become evident that regulations and privacy frameworks expressed their interest in personal privacy protection and mandated that varying degrees of data de-identification be included[9,10] to better protect personal data.

When it comes to de-identification, there is no one-size-fits-all approach to follow; subject to factors like the quantity of personal data acquired, the sensitivity of the application, and the effect on government reputation in the event of an incident involving personal privacy, the protection measure could begin with "pseudonymisation"[11] and extended to "anonymisation"[12] for full protection. Technical measures such as generalisation[13], randomisation[14], tokenisation,[15] and synthetic data[16] could be considered.

The risk-based approach is useful for determining the level of de-identification required; evaluation tools such as the Privacy Impact Assessment are useful for ensuring compliance and to locate residue risk left unaddressed. The concept of Privacy by Design shall be incorporated as far as possible during system design.

[9] CT.DP-P2, NIST Privacy Framework v1.0 stipulated that "Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization)."

[10] Recital 28, GDPR stipulated that "The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations."

[11] Data pseudonymisation replaces personally identifiable information within a data record with one or more artificial identifiers, called pseudonyms. The pseudonyms make personal data less identifiable from the data record while remaining suitable for data analysis and data processing.

[12] Data anonymisation is the process of turning data into a form such that the identification of individuals is not likely to occur.

[13] Data generalisation reduces the precision in the data while preserves data truthfulness at the record level. It is done by reducing the granularity of information contained in a selected attribute or in a set of related attributes in a dataset.

[14] Data randomisation adds noise to a data filed. It does not preserve data truthfulness at the record level but reduces the risk of singling out identifying attributes. Generally the values are modified so that their new values differ from their true values in a random way.

[15] Data tokenisation is replacing sensitive data elements with substitutes without extrinsic meaning, usually refers to as a token. This token can be mapped back to sensitive data afterward.

[16] Synthetic data generates artificial data that has some of the statistical characteristics as the targeted data. A synthetic dataset does not contain any data collected from or about existing data principals but looks realistic for the intended purposes.

- Keep track of data location [O] [P]

  Data location is one of the reasons most cloud users favour a private cloud solution over a public cloud. B/Ds should be aware of the cloud services that CSPs offer as part of their cloud adoption and ensure they have full visibility of where their content is transacted as part of architecting in their virtual cloud environment. Customer's data location should be made known for data at rest, data in transit, as well as for the backup location. Commitments should be made with CSPs to ensure the data will not move to other regions when sensitive information, particularly personal information, is involved, unless with B/Ds consent.

- Detect and prevent unauthorised data migrations to the cloud [O] [P]

  In addition to traditional data security controls (like access controls or encryption), B/D should prevent government data, particularly classified data, moving to cloud without prior approval by either monitoring large internal data migrations with Database Activity Monitoring (DAM) and File Activity Monitoring (FAM) or monitoring data moving to cloud with URL filtering and Data Loss Prevention (DLP).

- Maintain an up-to-date inventory of assets [I] [O] [P]

  Assets include all elements of software and hardware that are found in the cloud environment, while types of B/D's assets vary depending upon the cloud service model. An up-to-date inventory of B/D's assets in the cloud environment shall be identified and maintained. The assets should include the following:

  (i) Business information.
  (ii) Legal/contractual documents (e.g., public domain names registrations and related IP addresses, physical locations of data storage, etc.)
  (iii) Virtualised equipment.
  (iv) Virtualised storage.
  (v) Software.

- Ensure the controls for disposal of computer equipment that has reached its end of useful life and re-use of equipment are adequate and properly implemented [I] [O] [P]

The completeness and effectiveness of mechanisms for locating and securely deleting data before the disposal or re-use of computer equipment such as hard disks and backup media should be well aware, as some multi-tenant environments such as public cloud service may be difficult to support secure data destruction. The requirements of secure data destruction for disposal at the expiry or termination of service or upon request of the Government, or re-use of computer equipment containing classified information should be included as one of the selection criteria for external CSPs. B/Ds should work with CSPs and take into consideration ensuring sensitive data are properly deleted in accordance with industry best practices such as ISO 27001 Secure disposal or re-use of equipment and YDB144-2014 (Cloud computing services agreement reference framework) 5.2 Data Destruction. CSPs shall put in place the procedures in securely erasing the government data in all their platforms with written confirmation after such data erasure. Relevant security audit reports should be obtained periodically from the CSP for analysis to ensure the required security requirements are met.

5.5 Access Control

B/Ds using any type of cloud model may question the people who access data and system, and those who manage data. Since access control is the first line of defence of system security, inadequate visibility and management of people accessing and managing the system and data will significantly impact system security. Sufficient understanding on security controls for monitoring and protection against unauthorised access, especially to privileged accounts offered by CSPs, should be obtained prior to procurement and deployment of cloud services. Mechanism should be established to resume access to privileged user account in case a privileged user is denied access.

Due to the multi-tenancy environment in a cloud environment, there exist risks of compromise to data via third party access to common information storage through the network in the cloud. If there is a lack of granular access control to the information, the associated risks of sensitive data disclosure to unauthorised persons would become higher.

B/Ds should be aware of the risks posed in the multi-tenanted cloud environment and work with CSPs to understand the logical separation controls implemented to mitigate the risk of unauthorised data access. Moreover, if the cloud applications hold different sets of user identities, the update between the corporate user directory and its cloud applications will introduce a lag time in the revocation of user access rights, causing possible access to the sensitive data by unauthorised staff before changes effected.

B/Ds should implement procedures for key management so that the keys would not be shared with the CSPs when sensitive or classified information is involved. In other words, B/Ds should employ their own key management or a separate and distinct key management service for data storage encryption in a public cloud environment containing sensitive or classified data. B/Ds may also leverage on the cloud native Hardware Security Module (HSM) service that CSPs offer to implement a tightly knitted secure cloud environment without creating additional security dependency with other third-party vendors. The cloud native HSM service provided by CSPs should be checked with compliance standards that have been tested and certified by the State Cryptography Administration (SCA) and satisfy the requirements stated in:

- (GM/T 0030 Cryptographic server technical specification);
- (GM/T 0045 Specification of financial cryptographic server) ;
- (GM/T 0029Sign and verify server technical specification).

Regardless of which type of cloud model, B/Ds should implement the aforementioned data security controls as additional security layers to mitigate the risks of unauthorised data access.

- Define logical access control clearly [I] [O] [P]

Operating a cloud environment may involve many parties including operator team, application support team, infrastructure support team and data centre maintenance team. The authorised persons may be in-house or employed by the CSP or its subcontractors. Allowing more people to handle information assets would increase the risks on unauthorised access to the data. Thus, authentication and authorisation on logical access control should be clearly defined, such as who should be granted with the rights to access the data, what their access rights are, and under what conditions these access rights are provided. A "Default Deny All" policy should be maintained and least privilege principle shall be followed for staff accessing the cloud data.

- Establish Identity and Access Management (IAM) architecture [I] [O] [P]

Identity and Access Management (IAM) architecture should be considered. It allows broadening of the IAM practice using open standards, such as OpenID, to manage user account provisioning, authentication, and authorisation in the cloud. Mature and industry-proven authentication and authorisation standards, such as Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), could further improve the security status. Security features specified by these standards, such as XML Signature and XML Encryption for message-level security in SAML, should be used as appropriate. Adoption of identity federation in IAM architecture can facilitate the interconnection of disparate identity repositories, allowing users make use of single sign-on when accessing different applications.

- Adopt access control standards [I] [O] [P]

Once adopting a cloud service, users' identities may be extended into the cloud by connecting the identity repository or directory service to the CSP. When selecting cloud services, it is desirable that they should leverage industry standards (e.g., SAML) for implementing secure single sign-on solutions for passing identity and attributes, as well as enforcing authorisation policies.

- Ask for strong authentication options [I] [O] [P]

Since the cloud services could be accessed through various devices and different channels, authenticating with a simple user ID and password may not be strong enough to protect accounts from being compromised. When selecting cloud services, those cloud services with two-factor authentication (2FA) should be considered and 2FA should be enabled for as many accounts, especially privileged user accounts, as possible. Some common 2FA authentication options are One-Time Passwords, biometrics and digital certificates.

For further protection, user access, especially privileged user account, should be limited to dedicated workstation, network or location. The e-Authentication Framework[17] published by the OGCIO provides a basis to evaluate the risks, determine the security requirements and implement the appropriate authentication methods. The Framework should be followed in determining and implementing the electronic authentication requirements of electronic transactions for cloud services.

- Restrict and control the use of privileged utility programs [I] [O] [P]

Unauthorised use of privileged utility programs running in the cloud environment might be capable of overriding system and application controls. B/Ds should request the CSP for the functional specifications of the privileged utility programs to ensure the security controls on the use of the programs accessing cloud service are in place.

[17] https://www.infosec.gov.hk/en/best-practices/person/securing-access-using-e-authentication

5.6 Cryptography

- Manage and protect cryptographic keys [I] [O] [P] [18]

Cryptographic keys should be managed and protected properly in accordance with security regulations and policies. Key management on storage should be enforced and keys should be managed in the custody of the B/Ds. Processes for a key management lifecycle should be defined: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Cryptographic operations and key management may be bound to the identity and access management systems for strengthening the security protection. B/Ds should not re-use a key across different cloud platforms to avoid the risk of compromising all cloud platforms especially under hybrid cloud scenario.

5.7 Physical and Environmental Security

In public clouds, like outsourced private clouds, data centres are located off premises and a cloud may span across multiple data centres in different geographic locations. When the data move to the cloud data centre which is not managed by the B/D, physical controls on data are handed over to the CSP. Due to multi-tenancy nature of public clouds, the risks of unauthorised physical access by unknown co-tenants or third parties become one of the key security concerns.

Adequate physical security measures in a cloud data centre could protect against trespassing activities to the computing resources at the physical layer. For some CSPs, only computer racks without key lock are provided. It is obviously not enough for multi-tenancy environment. Anyone who has the right to access the data centre will have the opportunity to access the computer devices holding data of its tenants. The environment security and equipment security as well as physical access control in an off premises cloud data centre are the primary concerns in physical security domain.

Usually, services offered by public cloud services CSPs are not targeted for single tenant environment. From time to time, these CSPs may offer new solutions and services to cater for market needs, such as single tenant solution for cloud users. B/Ds are advised to study and validate the entire cloud solution package, including infrastructure and operating effectiveness of the security controls of the CSP through examining the valid compliance certifications carefully when choosing the appropriate deployment model. For example, if B/Ds are considering a private cloud to meet business needs and security requirements, then single tenant solution is just one of the considerations. B/Ds should also evaluate whether the cloud infrastructure should be dedicated so as to match the requirements as private cloud solution. In short, B/Ds

[18] While there is no specific regulation on encryption of unclassified information, as a good practice to protect data privacy, B/Ds may adopt encryption to protect unclassified information when using public cloud service with cryptographic keys management and protection.

should assess what security control on overall infrastructure should be implemented based on their business needs and government security requirements.

- Analyse risks for selection of site location and its facilities [O] [P]

  In practice, an off-premise data centre may not be designed or managed with security as the first priority, instead most of the CSPs focus on cost-effectiveness. Therefore, operating control effectiveness of related facilities such as uninterruptible power supply (UPS), air conditioning and ventilation, fire suppression system as well as water damage and flood control system should be validated by the appropriate globally recognised industry security standards (i.e. ISO27001, ISO 27019, GB/T 22239, DJCP, etc.). The site location of data centres, disaster recovery (DR) centres and their operation functions should be assessed in consideration of natural hazards, locality (e.g., local jurisdictions), network dependency (e.g., Internet network hubs), etc. If on-site inspection is not feasible, B/Ds should review the third party reports indicating annual audits by independent third party auditors on CSPs to ensure that these physical security controls meet the certification audit requirements (i.e. ISO 27001, SOC 2 Type 2, etc.).

- Adopt adequate physical protection for all IT equipment and data storage media for outsourced data centres [O] [P]

  In an outsourced cloud data centre, there may be potential unauthorised access due to the multi-tenant nature. Security requirements of proper physical protection for all IT equipment and data storage media within the shared data centre, and also for all off-site backup media should be defined. Implementation of security measures by the CSP should meet the security requirements.

- Adopt an isolated area for dedicated use as necessary [I] [O]

  If there is special requirement of not sharing equipment or equipment racks with application systems of other tenants due to the sensitivity of data or other security requirements, an isolated area could be considered to segregate the application owner's data and resources from that of other tenants. The segregated components usually include servers, network equipment, storage, power supply and signal cabling. The area under the perimeter of the application owners in a data centre should be clearly identified. Access to the area should be restricted to authorised persons only. In addition, entries into the data centre should not be open and easily accessed by the general public. It is desirable that the isolated area should not be at or near the common area, such as corridors and the main exit, in order to limit unauthorised or unavoidable access. All physical access to the data centre should be approved by the data centre manager with records.

- Restrict access to the isolated area [I] [O]

  Access to the isolated area should be under strict control by means of electronically controlled access system or other equivalent access control measures. The isolated area should always be locked even when attended. Dual control should be enforced in the authorisation and approval for access to, including authorisation and approval for adding in and removal from standing access lists, the isolated area. The standing access list should be authorised by the application owner or other authorised person. All physical access to the isolated area and equipment racks on a need basis should obtain the authorised approval with proper records. Periodic reviews of the area access logs, for example on a quarterly basis, should be performed to ensure completeness and accuracy. Also, the standing access list should be reviewed regularly.

- Consider defining different security levels of controlled area [I] [O]

  For outsourced information systems containing sensitive or classified information, B/Ds shall ensure the service providers have implemented proper controls to manage access to physical areas holding the information systems and restrict unauthorised access from other clients or outsiders and only personnel or visitors approved by the Government are allowed to enter.

  To achieve a higher level of security, implementation of areas with different levels of controls in a data centre is worth considering. Generally, the levels of physical access controls may be determined based on the importance of the application service and the sensitivity of information hosted in the area. The physical and management controls for the controlled areas should be clearly documented and labelled.

- Ensure adequate access controls for multiple application systems sharing the same equipment rack [I] [O]

  If sharing of equipment rack among application systems is adopted, it is important to note that the approval for physical access should be defined at the equipment level rather than the equipment rack level. In addition, other access controls, such as individual key locks, account lockout policy and regular system log review, should be implemented to mitigate the risks of sharing of equipment racks.

5.8 Operations Security

5.8.1 Information Backup

- Backup data regularly [I] [O] [P]

  The data of a customer stored on backup media held by the CSP might be commingled with other cloud tenants' data. CSPs may not provide separate or dedicated backup media to individual cloud tenants. For systems considered as important to the business, B/Ds should ensure that at least one offline regular backup copy of operational data be obtained that can be used to recover to the most up-to-date state. Under such a scenario, recovery tests shall be conducted regularly to assure that recovery procedures are up-to-date and effective. Backups and other copies of logs, access records, and any other pertinent information which may be required for legal and compliance reasons should be securely stored and accessible by authorised persons only.

5.8.2 Logging

- Keep and protect logs for auditing, analysis, and investigation [I] [O] [P]

  Regardless of public or private cloud, it is critical to obtain the key log data that provide a clear view into the operational and security events. Certain types of log data can be used to mitigate operation and security risks. B/Ds should define the log types and details, such as audit logs on network, system, application, administration and change management activities. Log information should be complete and able to reflect cloud's dynamic nature, such as the details about adding or removing VM instances. Log retention period should be well defined and the logs should be tampering resistant. For public cloud services, B/Ds should understand whether the CSP would offer users with options to change the log settings and supply the required log data. B/Ds should have log review procedures commensurate with the system criticality. Event correlation tools could be used to augment the log analysis function.

5.8.3 Configuration Management & Control

- Ensure security processes and procedures are properly put in place [I] [O] [P]

  Processes and procedures should be developed to collect and store audit logs, activity reports, copies of system configurations, change management reports and other test procedure outputs. Depending on the cloud service model, this information should be supplied by the CSP as and when needed.

5.8.4 Patch Management

- Ensure sufficient control over patch management processes [I] [O] [P]

  Patches enable additional functionality, and address bugs or security vulnerabilities within a program. However, patches are additional/modified pieces of code which may impose substantial risk of unexpected adverse side effect to the program that could significantly impact data confidentiality, integrity, and availability. In this connection, B/Ds should understand how CSP acts to mitigate vulnerabilities, including the ways in which CSP prioritises what to patch, and the timescales in which the patches are applied. Besides, the patch management processes should be agreed between the B/D and CSP.

5.9 Communications Security

In a cloud data centre, physical servers and network components are virtualised and probably shared by multiple tenants. Security measures applied to traditional network systems may not effectively protect against network attacks between virtual machines (VM) on the same server in the cloud environment. As some security threats are unique to a virtualisation infrastructure including communication blind spots, inter-VM attacks, and mixed trust level VMs, the dynamic and fluid nature of VM will make it difficult to maintain the security standards and ensure that records can be audited. The ease of cloning and distribution between physical servers could result in the propagation of configuration errors and other vulnerabilities. These security threats and issues arising from virtualisation are required to deal with when adopting and implementing cloud infrastructure. B/Ds are advised to validate the operating effectiveness of security controls through examining the valid compliance certifications attained by CSPs.

Furthermore, for cloud services, data may be transported across untrusted network (e.g., Internet, public network) and/or government network as data are shared in distributed cloud deployments. Data in transit should be well secured. The security practices on network and communication are crucial to a cloud service.

5.9.1 General Network Protection

- Protect data during transmission [I] [O] [P]

  In a multi-tenant or outsourced data centre environment, B/Ds should strengthen the protective level of the network security for classified data transmitted between the server machines and network components. Communication security encryption protocol, e.g., Transport Layer Security (TLS), should be implemented in data transmission over the communication network within the data centre to prevent eavesdropping. For adoption of security measures for protection of data confidentiality and integrity during

transmission over public network (e.g., Internet) or government network, secure protocols (e.g., Virtual Private Network (VPN), TLS) are recommended when connecting to cloud services. If applicable, data level encryption can also be considered so that data can be encrypted before transmission.

- Protect computing resources on network [I] [O] [P]

  Many devices such as server, desktop, notebook, smartphones and tablets have the ability to connect through the Internet to the cloud servers. External intruders may take advantages of system vulnerabilities to launch attacks to the network components and servers of a cloud environment. Besides, the possibility of internal intrusion through the inter-cloud traffic in a multi-tenancy environment should not be neglected. Proper network security components for protecting computing resources within the sphere of influence such as network firewalls, application firewalls, IDS/IPS and log monitoring should be implemented. It should be noted that a successful defence against attacks requires securing both the client and server sides of cloud computing.

5.9.2 Virtualisation Security

Virtualisation is an essential mechanism for a cloud to achieve system elasticity and on-demand services for a multi-tenant or multi-application environment. While it enables CSPs to get more computing resources from the spare capacity of physical servers, virtualisation will also bring about security risks. The nature of cloud computing makes it more difficult to determine what to do in case of a security incident, data breach or other security issues that require investigation.

As mentioned in Section 5.7, the offer provided by CSPs of public cloud services are usually not targeted for single tenant environment or single application environment. Along with the technology and market development, CSPs may provide new solutions and services to the industry. Some CSPs of public cloud services has expanded their solutions to allow tenant to have more control in cloud resources like single tenant or single application environment. Thus, some of the security considerations for virtualisation which are previously available in private cloud are also applicable to public cloud service.

Similarly, B/Ds are advised to study and validate carefully its entire cloud infrastructure and operating effectiveness of the security controls of the CSP through examining the valid compliance certifications when choosing the appropriate deployment model. For example, if B/D is considering a private cloud to meet business needs, then a single tenant environment with or without virtualisation is just one of the considerations when evaluating whether it is a dedicated cloud infrastructure or not. Because of this, B/Ds should make assessment on what security control on overall infrastructure should be implemented based on their business need and government security requirements. In respect of the security practices on virtualisation, please make reference to the following:

- Keep the host OS thin and hardened [I] [O] [P]

  To reduce the risks for being attacked and the frequency for patching, host OS with minimum required functions should be configured. The installed host OS should be hardened, like disabling unnecessary services and ports, and should also be as thin as possible so as to lower the ability to load arbitrary components, libraries or software.

- Deploy High Availability (HA) technologies [I] [O] [P]

  Resilience capabilities such as VM clustering on host machines should be considered to compensate for single point of failure. For example, losing power on a host machine may cause impact to several VMs. In the event of hardware failure, affected VMs could be automatically restarted on cluster nodes with spare capacity. The service impact could be minimised.

- Determine the security requirements for each individual component in virtualisation and harden them accordingly [I] [O] [P]

  Security of a full virtualisation solution is heavily dependent on the individual security of each of its components, from the hypervisor and host OS to guest OSs, applications and storage. All these components should be hardened in accordance with relevant security policies and standards. The host OS and guest OSs should be regularly scanned with vulnerability scanning tools which cover the virtualisation technologies used. Configuration management procedures should be developed and implemented to cover all the security settings of physical and virtual machines in the virtualised environment.

- Enable VM-specific network security features [I] [O] [P]

  VMs can communicate over a hardware backplane, rather than a cabled network. This backplane traffic cannot be monitored or in-line blocked by traditional network protection tools when suspected traffic is passing through. VM-specific security mechanisms, such as host firewall on VMs, virtual network and virtual firewall in hypervisor layer, should be adopted to provide granular monitoring for in and out traffic crossing VM backplanes. Remote access to the management console of VMs should be restricted to authorised personnel only.

- Enforce the least privilege and segregation of duties [I] [O] [P]

  In a distributed and virtualised environment, it is challenging to define granular roles and responsibilities of computer users, including different system administrators. Administrators of cloud, hypervisor, storage, network and system should perform their own duties without being able to gain access to the sensitive data residing on the systems they manage. Segregation of duties

should be regularly reviewed and strictly enforced by B/Ds to protect against different attacks, including external attacks (e.g., Advanced Persistent Threat (APT) attack) and insider abuse. In addition, accounts, roles and personnel for security administration should be separated from other administrative activities, so that computer resources and audit trails can be further protected from unauthorised modification.

- Establish security zones for isolating VMs of different trust levels [I] [O] [P]

  Efficacy and feasibility of segregating VMs should be explored in the early stage for development of VM environment. Creating security zones based on development phase (e.g., design, testing and production), classification of data (classified data and unclassified data), architecture layer (e.g., network, application, database and file) or system criticality level (mission-critical system and non-critical system) on separate physical servers is advised. If sharing of different nature of data/system on the same physical server cannot be avoided, isolation of VMs by combining virtual local area network, firewalls, and IDS/IPS could be treated as a countermeasure. Connection of the virtualised environment to the internal network should not compromise the existing security level.

- Consider bare-metal (type 1) hypervisor for more critical systems [I] [O]

  In general, there are two types of hypervisor, namely bare-metal (type 1) and hosted (type 2). Bare-metal hypervisor runs on hardware product while hosted hypervisor is installed on top of a host OS (e.g., Linux). Hosted hypervisor would probably inherit the vulnerabilities from the host OS and be exposed to more security threats under a relatively complex environment. In contrast, bare-metal hypervisor often provides a more compact and secure hardware OS. Furthermore, this type of hypervisor communicates directly to the hardware with less security concerns. In general, compared to private cloud, B/Ds using public cloud may need to consider other considerations when the cloud infrastructure is shared with other users. So, even bare-metal hypervisor is offered by public cloud service provider, it may not be suitable for critical systems especially when classified information is involved. Hence, this security consideration and control does not apply to public cloud scenario.

- Analyse related security risks [I] [O] [P]

  Before implementing virtualisation, security risks should be analysed by comparing with options without virtualisation. It should be treated as part of the risk management process before CSPs or products are selected.

- Review the resources requirement of VMs and applications [I] [O] [P]

To avoid resource contention, the use of resources such as CPU, memory, I/O throughput, disk space and network capacity on VMs and applications should be well-planned and reviewed.

- Protect against unauthorised access between two VMs [I] [O] [P]

  Principle of least privilege for communication between VMs should be enforced. For example, VMs should be properly configured to prevent unauthorised access by applying tightened host firewall rules and disabling unnecessary network protocols.

- Maintain inventory records [I] [O] [P]

  Documentation is required to record the virtualised environment deployed. As some network components (e.g., virtual switches/firewalls) under a virtualised environment may not be easily identified through on-line tools, an auditable comprehensive list of virtual machines and infrastructure components should be depicted with details and should be maintained up-to-date.

- Ensure the validity and sufficiency of software licences [I] [O] [P]

  Virtualisation is changing the way software is licensed. Licensing model of different software vendors may be varied, for instance, instance-based (physical or virtual), hardware-based (physical or virtual), usage-based or client-based (e.g., seats or concurrent connections). In many cases, B/D has to evaluate, negotiate, and refine a custom licensing agreement with major vendors in virtualised environments.

- Apply the latest security patches and virus signatures for offline VMs [I] [O] [P]

  Dormant VMs can be easily overlooked and inadvertently left out of security and monitoring practices resulting in the VM being exposed to known vulnerabilities. In this regard, the update of security patches and virus signatures of dormant VMs should be enforced by B/D. Some advanced security tools that address the patching needs for dormant VMs could be considered where applicable.

- Verify security status after VMs are restored from snapshots [I] [O] [P]

  Most VMs allow creating "snapshot" to save their setting and configuration state at different points of time for backup and maintenance activities. If it is necessary to restore a VM from a past snapshot which was taken for some time ago, verification on the patch level as well as security settings and

configurations is particularly important. Audit trail for tracing the activities, including patching exercises, on the VMs should be enabled.

- Protect the virtualisation images and configuration files [I] [O] [P]

  Since VM can be copied from one host machine to another along with the data and applications they held, intruder may bring up the copied VM on an unsecured hypervisor and gain access to the data and configuration files on the compromised VM. B/D should protect resource pool such as CPU, memory, and storage I/O from unauthorised access and modification by tightening logical and physical access controls with full auditing features.

- Disable unnecessary communication ports, services and virtual hardware [I] [O] [P]

  All unnecessary communication ports, services and virtual hardware such as USB port, clipboard capabilities between VMs, virtual network adapters, etc. should be disabled on VMs so that they are logically isolated with each other. It can be protected from revealing any data to other VMs in case one of the local VMs is compromised.

- Implement hypervisor-based, network-based and host-based protection solutions for each VM or a cluster of related VMs as appropriate [I] [O] [P]

  Network-based firewalls (or IDSs) work effectively for multi-tenant environment. Host-based firewall offers higher granularity of network control. It works for virtual environment but may suffer from workload and management issue for large-scale cloud environment. Hypervisor-based firewall provides security automation for dynamic cloud environment. Malicious traffic amongst VMs could be monitored and blocked. These firewalls should be carefully chosen to fit business needs and properly configured with stringent firewall rules and should be portable when the VM is relocated.

- Log activities for privilege accounts of hypervisor and VM [I] [O] [P]

  Logging all activities of privilege accounts in a VM is essential to trace the sources and events of a security incident. Similarly, since hypervisor has the capabilities to manage and configure the VMs under its purview, logging for the privilege accounts of a hypervisor is also necessary. Security logs should include the events such as access to VM images and snapshots, changes to user access rights, modifications of file permission. Tamper-proof logging and integrity monitoring tools should be considered to ensure the integrity of the log files. The security logs should be monitored and reviewed on a regular basis.

- Manage VM images and snapshots with care [I] [O] [P]

  VM images and snapshots may contain capture of classified data present on the system at the time the image/snapshot was taken. Snapshots can be riskier than images because snapshots contain the contents of active memory at the time the snapshot was taken. If images/snapshots are not secured and protected from modification, intruder may gain access and insert vulnerabilities or malware into it and then re-deploy it throughout the virtual environment. Nevertheless, all VM image copies and snapshots should be wiped when they are no longer needed. The security measures equivalent to the classification of data being processed by the VMs should be in place for the protection of the corresponding VM images and snapshots.

- Clear VM data securely [I] [O] [P]

  When VM is deleted from physical server or moved to another physical server, B/D should ensure that no data are left behind on the disk that makes data recovery possible. VMs should be cleared using secure deletion solutions.

- Protect administrative interfaces [I] [O] [P]

  Security controls should be in place external to the VM's to protect administrative interfaces, e.g., web-based management interface and application programming interfaces (APIs), from being exposed to unauthorised access. All management sessions should be controlled and monitored with audit trail enabled such that unauthorised or suspicious sessions can be detected and then blocked as early as possible.

5.10 System Acquisition, Development and Maintenance

With the rise of cloud computing, security architecture becomes highly dynamic. Cloud characteristics, such as sharing of computing resources by multi-tenancy within a data centre, make configuration management and on-going provisioning far more complex than that in a traditional IT environment. Cloud computing affects all aspects of Software Development Life Cycle (SDLC), and introduces a number of new challenges around the tools and services required to build and maintain running applications.

For some SaaS applications, CSP stores multiple tenant data into an application database by introducing an extra attribute such as "tenant_id" in every table of the database for tenant identification. Through software vulnerabilities, such as scripting bugs or specially-crafted SQL queries, a malicious tenant is possible to compromise the application and access the data of others. Moreover, security weaknesses such as outdated web browsers and unprotected web sessions may lead to compromise of application integrity and data confidentiality. All of the security issues related to application security still apply when applications move to a cloud platform.

- Apply secure software development lifecycle to cloud applications [I] [O] [P]

  Secure software development lifecycle processes (or other development methodology as appropriate), e.g., security design review and software testing, should be applied to applications built on the cloud platform to make application less vulnerable to potential threats after release. The lifecycle addresses security threats throughout the development process by proactive checks during development, including:

  (i) Threat modelling during the design process to identify and mitigate potential security issues early;

  (ii) Following development best practices and secure coding standards (e.g., security code review, de-identification of personal data, data input validation and output encoding requirements) for preventing web application vulnerabilities; and

  (iii) Requiring various tools (e.g., code scanning and analysis tools, testing tools and code obfuscation tools) for testing, verification and code protection before deployment.

- Manage and protect credentials [I] [O] [P]

  Cloud technology enables easy deployment of applications and the deployment tasks are always dedicated to the development staff in the cloud. Managing and protecting credentials for entering to the production environment become critical. Credentials should be kept securely to help prevent unauthorised access to as well as illicit tampering of application programs and control files. Comprehensive policies and procedures should be defined and strictly adhered for maintaining the integrity of the application environment.

5.11 Outsourcing Security

The cloud services of public clouds and outsourced private clouds are not managed or operated by in-house staff. In respect of the relevant security practices for cloud services managed by external CSPs, the following aspects need to be considered:

- Analyse security risks before making decision to commence using outsourced cloud services at outsourced data centres [O] [P]

  All security risks should be analysed with IT security requirements. Results of the analysis will provide a basis for management to make appropriate decisions on commencing outsourced cloud services.

- Define clearly the security requirements of the areas to be outsourced when preparing the outsourcing tender [O] [P]

  Relevant requirements in business and security domains such as physical security, management responsibilities, security incident management and security risk assessment and audit (SRAA) should be defined clearly with measurable performance indicators when preparing the outsourcing tender and the requirements should also be included in a tailored SLA. As in any outsourcing arrangements, data ownership should also be clearly defined and agreed with the CSP.

- Tailor SLA and check on changes [O] [P]

  The consequences of terms in a SLA such as data location, roles and responsibilities of different parties, compliance as well as data backup and recovery should be well aware. Modifications on the SLA are required, as appropriate, to address any potential security issues that may probably lead to security incident. B/Ds should evaluate and ensure the terms in the SLA to fulfil their business and security requirements. For public cloud services, CSP website should be checked periodically for any notices of changes in the common statements of SLA, as CSPs may reserve right to update some terms in the SLA at any time with limited advance notice.

- Ensure the external CSP provides security controls that meet government security requirements [O] [P]

  Control mechanisms should be implemented so as to meet government security requirements commensurate with the involved data classification and sensitivity. B/Ds should apply due diligence and oversight, wherever applicable, for external CSPs satisfying the business, security and privacy needs. B/Ds should develop additional controls to mitigate a given risk that is not fully covered by CSP.

- Ensure external threats are properly addressed [O] [P]

  The outsourced CSP should secure hosts and applications provided by them using best practices against external threats and unauthorised access. Such practices would include, but not limited to, hardening of the OS, keeping it up-to-date with the latest patches, and installing of hypervisor-based, network-based or host-based anti-malware software, Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS), and firewalls as appropriate. Security risk assessments should be regularly conducted by the CSP to ensure the system attains the required security level, and B/Ds should review the SRAA report provided by the CSP regularly.

- Formulate exit strategy [O] [P]

  The existence of exit strategy or exit plan should be ready and should be established at an early stage when adopting cloud services. An exit plan may be provided by the CSP or B/D. The exit plan should include how to retrieve data and the virtual environments out of the CSP, and how to clean up data and the virtual environments. Through the development of this plan, the risk of 'Lock-in' to one CSP is also addressed. Further negotiation on the exit term could also reduce the risk.

5.12 Information Security Incident Management

Despite all necessary security measures adopted in an information system, security incidents do occasionally occur. Security incident handling is a set of continuous processes governing the activities before, during and after a security incident occurs. The nature of cloud computing makes it more difficult for B/Ds to determine what to do in case of a security incident, data breach or other security issues that require investigation. For example, B/Ds may consider classifying a security incident as critical, but the CSP may not agree with the classification and exert limited effort for investigation and following up the case.

The adoption of cloud computing alters the fabric of incident response. Especially, in public clouds, B/Ds do not have direct access to network logs because they do not own the network. Some CSPs, as declared in their standard SLAs, do not have any obligations to investigate any security violations and misuse of services which may lead to security incidents. B/Ds are advised to take note of the security practices on incident monitoring and response as described below.

5.12.1 Security Incident Monitoring

- Define incident monitoring and reporting responsibility [O] [P]

  External CSP's support to the B/D in incident monitoring should be defined clearly in the SLA. Information security incidents originated from the CSP's infrastructure might have an impact on the B/D's resources, which should be reported to the B/D with sufficient details. B/D should establish communication plan with CSP for reporting and escalation in the event of an incident. The SLA should document a well-defined incident classification scheme and reporting obligations as well as service levels to be achieved by the CSP.

- Make information available for incident analysis [O] [P]

  The B/D should be allowed to access the data sources and information that are relevant for incident detection and the CSP should provide appropriate facilitations for incident analysis. Backups and other copies of logs, access records, and any other pertinent information should be able to be migrated from the cloud environment. For public cloud services, availability of log details may depend on the option selected by users. Audit trail and logging features should be enabled and properly configured according to business needs and data classification.

5.12.2 Security Incident Response

- Ensure that the incident response requirements are met [I] [O] [P]

  B/D should be well aware of the overall incident handling philosophy of the CSP and ensure that the steps to be taken by the CSP and the timing of response in a security incident satisfy their requirements. The role of CSP in the incident response should be clearly defined. The B/D should agree with the CSP on how to collect, store, and share supporting evidence for incident investigation (e.g., security log records).

- Review the history of the CSP [O] [P]

  A CSP's track record and experience for incident response management, if available, should be obtained and reviewed. Recommendations from existing subscribers about its incident response plan will be useful as reference.

- Develop incident response management and procedures for off-premises cloud services [I] [O] [P]

  B/Ds should work closely with their CSP on incident response measures. They should have incident handling management and procedures for cloud services put in place and properly documented. Similar to regular systems, the incident handling procedures should include reporting to GIRO and subsequent actions specified in the Practice Guide for Information Security Incident Handling. An effective mechanism should be defined and established to report, notify, investigate and handle information security incidents or security breaches. The CSP should report to a nominated contact from the B/D on an agreed timing and report all security related issues. An internal escalation procedure should also be available for incident handling, aiming to have fast response and derive appropriate resolutions in order to minimise the impacts to the operation of the B/D. Performance metrics elaborated from these arrangements may be set as SLA when necessary.

- Conduct rehearsals for an incident response plan with the CSP [I] [O] [P]

  B/Ds shall conduct rehearsals for the incident response plan, in collaboration with the CSP if feasible. Possible ways to rehearse the plan include: paper-based exercises, telephone cascading and a full rehearsal. Areas of improvement should be properly documented into the newer version of the incident response plan.

5.13 IT Security Aspects of Business Continuity Management

- Ensure effective data backup and Disaster Recovery (DR) arrangements [I] [O] [P]

  No matter the DR arrangements are managed by B/D or CSP, B/D should ensure the effectiveness of these arrangements and align with B/D's requirements. Recovery Point Objective (RPO) and Recovery Time Objective (RTO), location of the DR centre, roles and responsibilities of the recovery teams, lines of communication for the event of DR, and the restoration priorities should be defined and be correlated with SLA.

- Develop Business Continuity Plan (BCP) [I] [O] [P]

  Business Continuity Plan (BCP) of B/Ds should include scenarios for loss of the CSP's services and third party-dependent capabilities. Testing of this part of the plan should be coordinated with the CSP. If possible, CSP's BCPs should also be inspected. It would be good to ask for evidence of active management support and periodic review of the CSP's BCPs.

5.14 Compliance

In consideration of economy of scale, CSPs implement multi-tenancy environment and commingle resources pool. Particularly for public clouds, the data centres, computing devices, data storage and human resources are shared by users. Due to privacy issues, conducting in-depth assessment and audit exercises by specific B/Ds is normally not permitted. In most public clouds, the CSP may not be able to agree to custom audit obligations for a specific B/D. If a CSP does not allow clients to directly conduct SRAA on it, it should be requested to provide third party audit reports which meet industry standards and satisfy B/D's requirement.

It is important to note that cloud computing can refer to several different service models, including SaaS, PaaS and IaaS. The risks and security controls associated with each model as well as the key considerations in outsourcing for the model of service will differ. As a result, the process for conducting the SRAA may also be different.

5.14.1 Security Risk Assessment

- Assess security risks for cloud systems or applications [I] [O] [P]

  As with traditional applications, a security risk assessment should be performed before production, and prior to major enhancements and changes associated with the cloud systems or applications. The security risks in the cloud should be evaluated and appropriate security controls should be implemented to mitigate the risks. The effectiveness of the controls should be periodically reviewed and enhanced as necessary because new technologies would emerge which may provide better protection to cloud services (**Annex B** provides some more emerging technologies related to cloud security). If the required security control should exist in the CSP's side, knowledge of the CSP's security implementation should be obtained.

- Conduct security risk assessment regularly [I] [O] [P]

  Security risk assessment is an on-going activity. For private cloud, the frequency of the security risk assessment should be defined according to the IT security policies. For public cloud services, B/Ds should ensure security risk assessment would be conducted regularly by the CSP's 3rd party auditor with the frequency aligned with B/D's security policy or at a mutually agreed frequency, for example, re-evaluating security risks and controls annually or bi-annually depending on the system criticality.

5.14.2 Auditing

- Reach agreement for auditing [O] [P]

  B/Ds may seek the right to audit where feasible. The B/D and CSP need to agree in advance to what extent the B/D has access to the CSP to audit and verify the existence and effectiveness of security controls specified in the SLA. The pre-engagement security controls audit then becomes the benchmark for on-going audits once the cloud contract is in place. Both sides should agree on how to collect, store, and share compliance evidence (e.g., audit logs, activity reports, system configurations).

  B/Ds should also engage independent auditors to perform audits regularly, including penetration testing and vulnerability assessments, and provide relevant rationale and evidence to substantiate judgement regarding the compliance of security requirements. If conducting security audit on the CSP is not feasible, the CSP should be requested to provide third party audit reports.

- Align breadth and depth of security audit [O] [P]

  Third-party auditor should be mutually disclosed or selected in advance, jointly by the B/D and CSP if possible. The breadth and depth of security audit should be aligned between the B/D and CSP. The audit reports should be obtained periodically from the CSP for analysis to ensure the required security requirements are met.

- Ensure security compliance in cloud [I] [O] [P]

  Compliance with government security regulations and policies should be checked and clearly included in the specifications of the service contract and in SLA before the cloud service is adopted. The deliverables to be provided from the CSPs for compliance check may include information security policy, contingency plan and test reports, incident response procedures, security audit reports, authorisation review documents, segregation of duties matrix, information security awareness and training records, system baseline configuration standard documents, configuration management plan, as well as results of periodic reviews.

- Onsite security check [I] [O] [P]

  CSP should assist B/D to perform onsite security audit and gain understanding of the current security measures adopted in data centres. The audit team should involve the parties from various areas including IT, Information Security, Business Continuity and Physical Security. B/Ds should request the CSP for business continuity plan, disaster recovery plan, relevant certifications (e.g., ISO[19], ITIL standards), audit reports and test plans prior to visit for checking.

*** ENDS ***

[19] ISO - International Organisation for Standardisation

Annex A: Summary of Security Controls by Cloud Implementation Scenarios

Security Controls	[I]	[O]	[P]
4.1 Cloud Service Model and Information Security			
• Define and understand shared responsibility of all parties	√	√	√
5.1 Management Responsibilities			
• Analyse the impacts to the security procedures in light of different jurisdictions		√	√
• Verify the compliance of industry security standards		√	√
5.2 IT Security Policies			
• Review departmental security policy	√	√	√
5.3 Human Resource Security			
• Define roles and responsibilities on resource control and information security	√	√	√
• Request non-disclosure agreement and ensure proper human resource management		√	√
• Issue guidelines or reminders for user awareness	√	√	√
• Ensure adequate security training to relevant personnel	√	√	√
5.4 Asset Management			
• Protect data by encryption	√	√	√
• Observe data protection and privacy legislation for outsourced data centres		√	√
• De-identification of personal data	√	√	√
• Keep track of data location		√	√
• Detect and prevent unauthorised data migrations to the cloud		√	√
• Maintain an up-to-date inventory of assets	√	√	√
• Ensure the controls for disposal of computer equipment that has reached its end of useful life and re-use of equipment are adequate and properly implemented	√	√	√
5.5 Access Control			
• Define logical access control clearly	√	√	√
• Establish Identity and Access Management (IAM) architecture	√	√	√
• Adopt access control standards	√	√	√
• Ask for strong authentication options	√	√	√
• Restrict and control the use of utility programs	√	√	√
5.6 Cryptography			
• Manage and protect cryptographic keys	√	√	√
5.7 Physical And Environmental Security			
• Analyse risks for selection of site location and its facilities		√	√
• Adopt adequate physical protection for all IT equipment and data storage media for outsourced data centres		√	√
• Adopt an isolated area for dedicated use as necessary	√	√	
• Restrict access to the isolated area	√	√	
• Consider defining different security levels of controlled area	√	√	

Security Controls	[I]	[O]	[P]
• Ensure adequate access controls for multiple application systems sharing the same equipment rack	√	√	
5.8 Operations Security			
5.8.1 Information Backup			
• Backup data regularly	√	√	√
5.8.2 Logging			
• Keep and protect logs for auditing, analysis, and investigation	√	√	√
5.8.3 Configuration Management & Control			
• Ensure security processes and procedures are properly put in place	√	√	√
5.8.4 Patch Management			
• Ensure sufficient control over patch management processes	√	√	√
5.9 Communications Security			
5.9.1 General Network Protection			
• Protect data during transmission	√	√	√
• Protect computing resources on network	√	√	√
5.9.2 Virtualisation Security			
• Keep the host OS thin and hardened	√	√	√
• Deploy High Availability (HA) technologies	√	√	√
• Determine the security requirements for each individual component in virtualisation and harden them accordingly	√	√	√
• Enable VM-specific network security features	√	√	√
• Enforce the least privilege and segregation of duties	√	√	√
• Establish security zones for isolating VMs of different trust levels	√	√	√
• Consider bare-metal (type 1) hypervisor for more critical systems	√	√	
• Analyse related security risks	√	√	√
• Review the resources requirement of VMs and applications	√	√	√
• Protect against unauthorised access between two VMs	√	√	√
• Maintain inventory records	√	√	√
• Ensure the validity and sufficiency of software licences	√	√	√
• Apply the latest security patches and virus signatures for offline VMs	√	√	√
• Verify security status after VMs are restored from snapshots	√	√	√
• Protect the virtualisation images and configuration files	√	√	√
• Disable unnecessary communication ports, services and virtual hardware	√	√	√
• Implement hypervisor-based, network-based and host-based protection solutions for each VM or a cluster of related VMs as appropriate	√	√	√
• Log activities for privilege accounts of hypervisor and VM	√	√	√
• Manage VM images and snapshots with care	√	√	√
• Clear VM data securely	√	√	√
• Protect administrative interfaces	√	√	√
5.10 System Acquisition, Development And Maintenance			
• Apply secure software development lifecycle to cloud applications	√	√	√
• Manage and protect credentials	√	√	√

Security Controls	[I]	[O]	[P]
5.11 Outsourcing Security			
• Analyse security risks before making decision to commence using outsourced cloud services at outsourced data centres		√	√
• Define clearly the security requirements of the areas to be outsourced when preparing the outsourcing tender		√	√
• Tailor SLA and check on changes		√	√
• Ensure the external CSP to provide security controls that meet government security requirements		√	√
• Ensure external threats are properly addressed		√	√
• Formulate exit strategy		√	√
5.12 Security Incident Management			
5.12.1 Security Incident Monitoring			
• Define incident monitoring and reporting responsibility		√	√
• Make information available for incident analysis		√	√
5.12.2 Security Incident Response			
• Ensure that the incident response requirements are met	√	√	√
• Review the history of the CSP		√	√
• Develop incident response management and procedures for off-premises cloud services	√	√	√
• Conduct rehearsals for an incident response plan with the CSP	√	√	√
5.13 IT Security Aspects Of Business Continuity Management			
• Ensure effective data backup and Disaster Recovery (DR) arrangements	√	√	√
• Develop Business Continuity Plan (BCP)	√	√	√
5.14 Compliance			
5.14.1 Security Risk Assessment			
• Assess security risks for cloud systems or applications	√	√	√
• Conduct security risk assessment regularly	√	√	√
5.14.2 Auditing			
• Reach agreement for auditing		√	√
• Align breadth and depth of security audit		√	√
• Ensure security compliance in cloud	√	√	√
• Onsite security check	√	√	√

Annex B: Emerging Technologies of Cloud Security

With wide adoption of cloud computing, traditional security controls may not be sufficient to protect information assets of an organisation in cloud environment. Because of this, security vendors introduce some new measures for cloud computing security in order to address the related security concerns. Below highlights some examples of emerging technologies in related to cloud security.

B.1 Identity Management as a Service (IDaaS)

When more and more cloud services are deployed, it is a challenge to manage various user access and their access logs across different cloud applications. Identity Management as a Service ("IDaaS") is a cloud-based service that provides a set of identity and access management functions to manage cloud applications as well as legacy applications in user premises. IDaaS provides the following functionalities:

- Identity governance and administration (IGA) — this includes the ability to conduct identity management such as self-service user provisioning, password synchronisation.
- Identity access — this includes user authentication, single sign-on (SSO), policy enforcement
- Identity analytics — this includes event logging, access reporting

As identity is critical to a platform or system, IDaaS poses the following deployment considerations to cloud users:

- Reliability and integrity of IDaaS service providers
- Availability of IDaaS service on cloud platform and network access
- Resilience and protection of identity data
- Operational and access controls to user identities
- Credential management

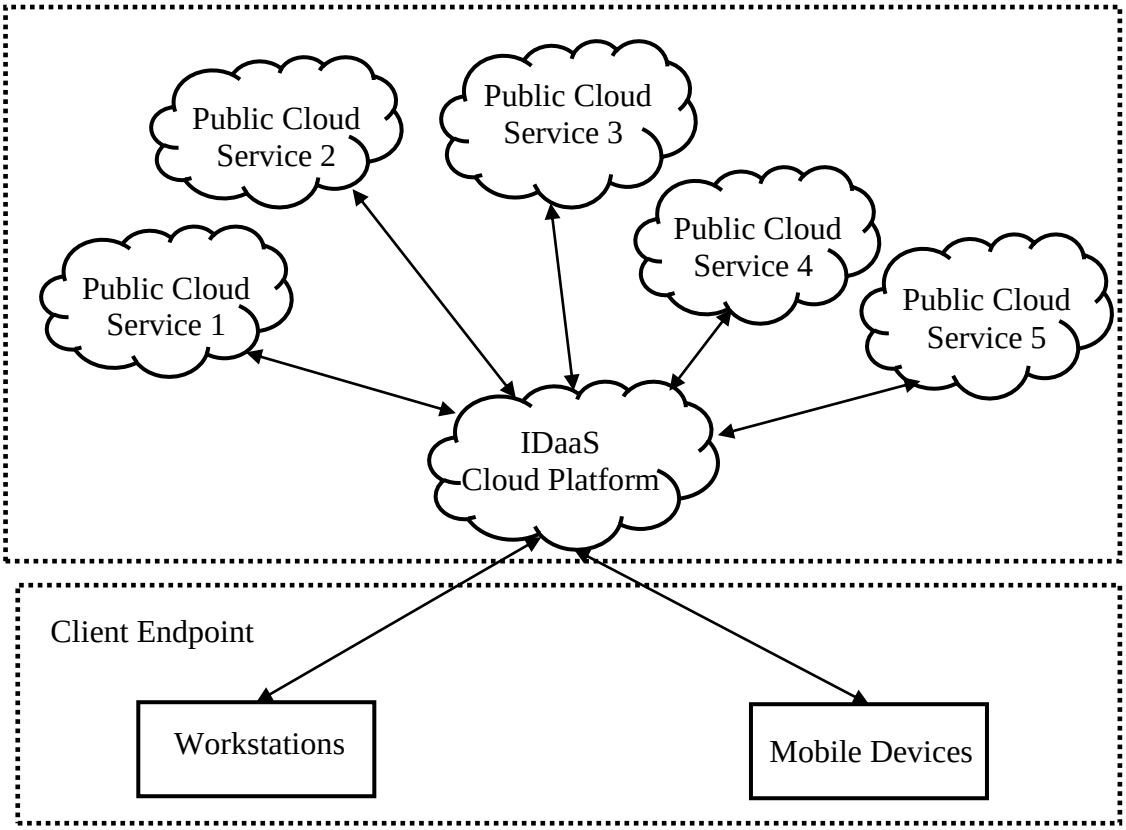

Figure B.1 IDaaS Usage Scenario

A critical risk analysis and detailed compliance review should be conducted before using such cloud services. B/Ds should ensure compliance to government security requirements when handling classified information in cloud platforms, especially when IDaaS service is considered. To reduce the risk of compromising across cloud platforms, re-using the identities across different cloud platforms should be avoided. The best practices described in Section 5 – Security Consideration and Controls for Cloud Services are also applied to the IDaaS as it is also a kind of cloud services.

B.2 Cloud Access Security Broker (CASB)

Cloud Access Security Broker (CASB) is a software that acts as a control point to enforce security policies, compliance and governance across multiple cloud applications. CASB has the following functionalities:

- Cloud access monitoring by providing consolidated view of an organisation's cloud service usage and user access including device used and user location
- Security policy enforcement by restricting access based on data classification, and user activity monitoring on sensitive data access or privilege escalation
- Data protection by providing data encryption at field or file level in cloud services
- Threat protection by preventing those devices, users and application versions that are not yet approved for access

CASB would be useful in monitoring cloud usage when installing at network perimeter and could be considered as an additional security control (Refer to Figure B.2). This software can be on-premises, cloud based or hybrid. The service access can be implemented in different ways, such as reverse proxy, forward proxy, API mode or hybrid / multimode. CASB can be included in the Secure Access Service Edge (SASE) framework, which is designed to strengthen network security by enabling secure access in the cloud-based network based on the identity of the entity thus allowing scaling up security infrastructure. As CASB is relatively new and still evolving, B/Ds should conduct proper market research and product evaluation based on various criteria such as business needs, features, support, pricing, integration with operations and infrastructure, etc. before choosing the suitable solution for deployment.

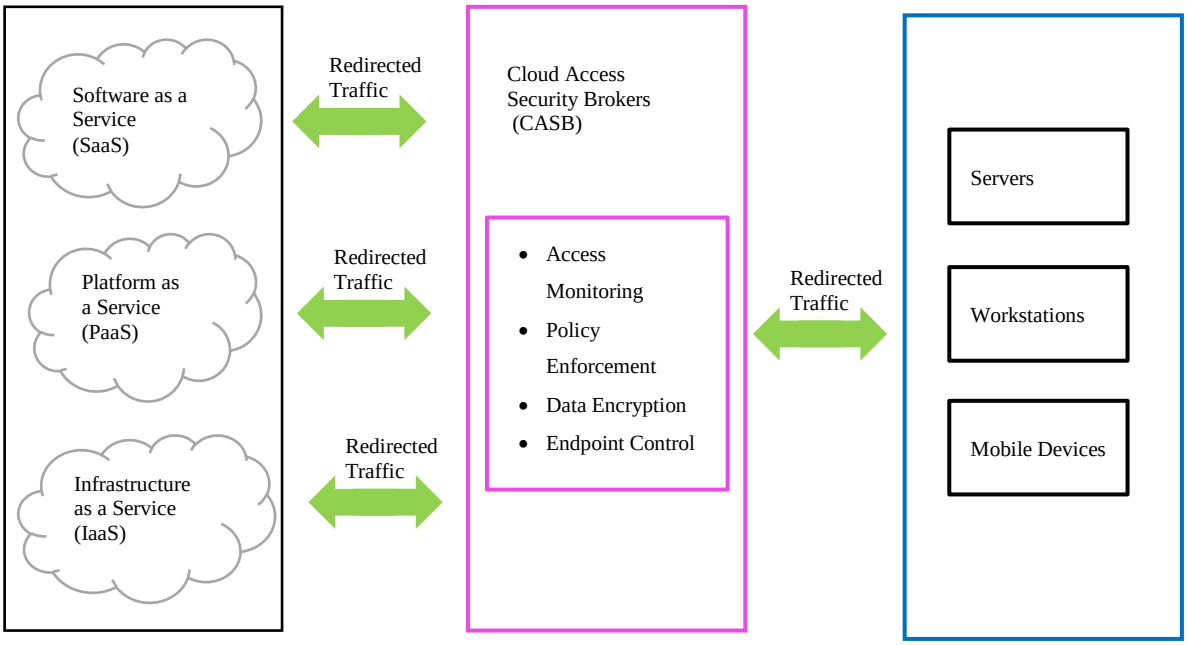

Figure B.2 Access Cloud Services through CASB

B.3 Cloud Workload Protection Platforms (CWPP)

Workload is a generic term used to describe the process performed in physical server, virtual machine or container[20]. Various workloads are created with the increasing adoption of cloud services from different computing platforms. As a result, this would increase the effort and difficulty for administrators to maintain consistent security level of workload across different cloud platforms, especially when involving public cloud service.

[20] The VM has a full image of the underline OS while the cloud container only consists of applications, settings and storage that are needed for that application to run.

In public cloud deployment, the cloud user may not have security control enforced as readily on-premises and also may lack of monitoring to the security control of the cloud service. To cater for this, CWPP is a suite of software to ease the administrative effort in deploying workload protection across various cloud platforms including on-premises, private cloud, and public cloud. CWPP can monitor security policies across hybrid cloud infrastructure through central management so as to enforce consistent security policies (Figure B.3).

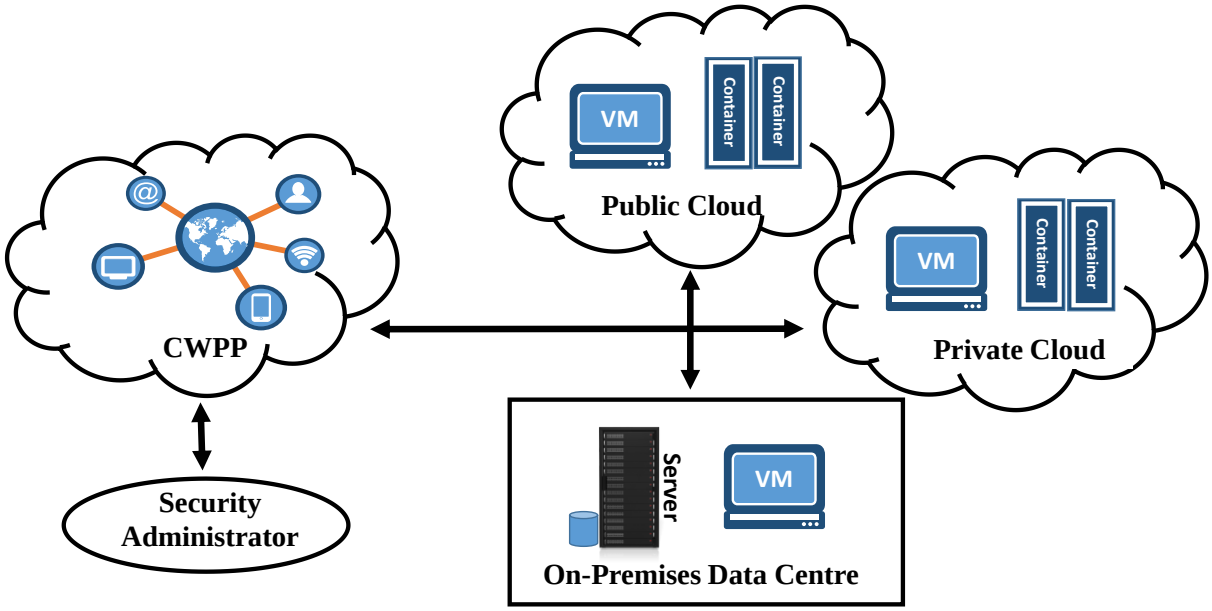

Figure B.3 Cloud Workload Protection Platform

CWPP offers the following management features on workload in hybrid cloud environment:

- System monitoring and management
- Network firewall and segmentation
- Application control
- Configuration and vulnerability management
- Memory Protection

Some CWPP vendors would provide additional protection capabilities such as:

- Data Encryption
- Host Intrusion Prevention System (HIPS)
- Endpoint protection, e.g., Anti-malware etc.

Similar to CASB, CWPP is relatively new and still evolving, B/Ds should conduct proper market research and product evaluation before deployment. In particular, the compatibility of the solutions across heterogeneous environment (such as support to server OS, virtualisation, container, API, etc.) and risks of using centralise software to manage various cloud services should be considered.