BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Appendix of RMIT:

Cloud Technology Risk Assessment Guideline (CTRAG)

Exposure Draft

Applicable to:

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers, including professional reinsurers
5. Licensed takaful operators, including professional retakaful operators
6. Prescribed development financial institutions
7. Approved issuer of electronic money
8. Operator of a designated payment system

This exposure draft set out the guidelines for the assessment of common key risks and considerations of control measures when financial institutions adopt cloud services. The proposed expectations serve as supplementary guidance to the Risk Management in Technology (RMiT) policy document to strengthen financial institutions' cloud risk management capabilities.

The Bank invites written feedback on the proposals in this exposure draft, including suggestions on areas to be clarified or elaborated further and alternative proposals that the Bank should consider. The written feedback should be supported with clear rationale, accompanying evidence or illustrations as appropriate to facilitate the Bank's assessment.

Responses must be submitted electronically in the prescribed format and addressed to trsu@bnm.gov.my by **15 July 2022.**

Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of providing your feedback, you may direct any queries to the following officers: -

1. Atikah Adnan (atikahadnan@bnm.gov.my)
2. Ahmad Rusdi Ahmad Sabri (rusdi@bnm.gov.my)
3. Nur Aqilah Zulkafali @ Zulkifli (nuraqilah@bnm.gov.my)

Appendix 10: Key Risks and Control Measures for Cloud Services (CTRAG)

This appendix provides additional guidance for the assessment of common key risks and considerations of control measures when financial institutions adopt cloud services. The guidance is broadly applicable across various cloud service models.

The guidance consists of two (2) parts:

- **Part A: Cloud governance** – describes the considerations governing the cloud usage policy, and technology skills capacity to implement cloud services securely and effectively.
- **Part B: Cloud design and control** – describes the considerations related to designing robust cloud infrastructure and in operationalising the cloud environment. This places emphasis on cloud architecture, cloud application delivery model, high velocity software development, cloud backup and recovery, business continuity management, key management, user access management, data protection and cybersecurity management.

Part A: Cloud Governance

A financial institution should ensure robust cloud governance processes are established prior to cloud adoption and are subject to on-going review and continuous improvement. This should cover the following areas:

1. Cloud risk management

(a) A financial institution's board should promote sound governance principles throughout the cloud service lifecycle in line with the financial institution's risk appetite to ensure safety and soundness of the institution.

(b) A financial institution's senior management should develop and implement a cloud risk management framework, for the Board's approval, proportionate to the materiality of cloud adoption in its business strategy, to assist in the identification, monitoring and mitigating of risks arising from cloud adoption.

(c) Common cloud service models[1] are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), wherein each presents a different set of capabilities offered to the financial institution as the cloud consumer, and hence a different set of shared responsibilities. In view of

[1] Cloud service models consist of SaaS, PaaS and IaaS. For SaaS, where financial institutions, as a consumer, uses the cloud service provider's applications running on a cloud infrastructure. PaaS is a service model where financial institutions deploy application onto cloud infrastructure using the platform capabilities e.g., programming languages, libraries services and tools supported by the cloud service provider. IaaS is a service model where cloud service provider offers fundamental computing resources such as compute, network, or storage, where financial institutions can deploy application and operation systems.

this, the cloud risk management framework of the financial institution should be:

i) an integral part of the financial institution's enterprise risk management framework (ERM);
ii) tailored to the cloud service models, both currently in use or being considered for use; and
iii) specify the scope of the financial institution's responsibility under each shared responsibility model, as the associated risks may vary.

(d) Financial institution's responsibilities to protect control over protection of data stored in cloud may vary based on the cloud service models and the cloud service providers. Therefore, the financial institutions should understand the specific details of the cloud arrangement, particularly what is or not contractually agreed.

(e) Regardless of the cloud arrangement with cloud service providers, the financial institutions will continue to be ultimately accountable for protecting customer information and ensuring service reliability.

(f) The use of cloud services may represent a paradigm shift in technology operation management as compared to on-premises IT infrastructure. Business processes may change and internal controls on compliance, business continuity, information and data security may be overlooked due to the ease of subscribing to cloud services. Therefore, the cloud risk management framework should also clearly articulate the accountability of the board and senior management and the process involved in approving and managing cloud service usage, including the responsibility of key functions across the enterprise in business, IT, finance, legal, compliance and audit, over the lifecycle of cloud service adoption.

(g) As the cloud landscape rapidly evolves, a financial institution`s cloud risk management framework should undergo periodic review, at least once every three years to ensure its adequacy and effectiveness to manage new service models over time or upon major cyber security incidents to the cloud services

2. Cloud usage policy

(a) The senior management should develop and implement internal policies and procedures that articulate the criteria for permitting or prohibiting the hosting of information assets on cloud services, commensurate with the level of criticality of the information asset and the capabilities of the financial institution to effectively manage the risks associated with the cloud arrangement.

(b) A financial institution should maintain complete and centralised assets inventory of critical system and information assets hosted on the cloud services, with a clear assignment of ownership, and to be updated upon deployment and changes of IT assets to facilitate timely recalibration of

cybersecurity posture in tandem with an evolving threat landscape. The full visibility and current view of the critical system and information assets should enable effective triaging, escalation and response to information security incidents.

(c) A financial institution should regularly review and update the cloud usage policy at least once every three years. However, where any material changes arise, e.g., adoption of new cloud service deployment model, adoption of cloud service for IT systems with higher degree of criticality, the financial institution should review and update its cloud usage policy immediately.

3. Due diligence

Due diligence on the prospective cloud service providers should be risk-based and conducted to a level of scrutiny that is commensurate with the criticality of the information and technology assets to be hosted on the cloud. It should at minimum:

(a) Include all locations where all financial institutions' data will be processed and stored;

(b) Include an assessment of the potential impact of the cloud outsourcing arrangement on the financial institution's legal, compliance, operational, information security, data privacy and reputational risks;

(c) Address relevant requirements and guidance as stipulated in the Third-Party Service Provider Management section of the RMiT policy document and related sections in Outsourcing policy document (Outsourcing process and management of risks); and

(d) Risk assessment should be promptly reviewed or re-performed upon material changes in cloud risk profile such as jurisdiction risks for data hosted overseas due to evolving foreign legislations and geopolitical development.

4. Access to authoritative third-party certifications

A financial institution should review their cloud service providers' certifications prior to cloud adoption. At a minimum, a financial institution should:

(a) Seek assurance that the cloud service provider continues to be compliant with relevant legal, or regulatory requirements as well as contractual obligations and assess the cloud service provider`s action plans for mitigating any non-compliance; and

(b) Obtain and refer to credible independent external party reports of the cloud platforms when conducting risk assessments. This should address requirements and guidance as stipulated in the Cloud Services section of the RMiT policy document and Outsourcing involving Cloud Services section in Outsourcing policy document.

5. Contract management

(a) A financial institution should set out clearly and where relevant, measurable, contractually agreed terms and parameters on the information security and operational standards expected of the cloud service provider. Such contract terms and parameters should be aligned with the financial institution's business strategy, information security policies and regulatory requirements. The terms of the contract between the financial institution and cloud service provider should address the risks associated with cloud services as stipulated in the Cloud Services section of the RMiT policy document.

(b) The contract terms, obligations, and responsibilities of all contracting parties (this may include sub-contractor(s) if the sub-contractor is material to the provision of critical function(s)) should be explicitly stated in the contract. At a minimum, the contract should address requirements and guidance as stipulated in Third-Party Service Provider Management sections of the RMiT policy document and related sections in the Outsourcing policy document (Outsourcing agreement and Protection of data confidentiality).

(c) Jurisdiction risk may arise because cloud service providers operate regionally or globally in nature and may be subject to the laws and regulatory requirements of its home country, the location of incorporation, and the country where the client receives the service. Therefore, a financial institution should:

i) identify and address potential jurisdiction risks by adopting appropriate mitigating measures, where practically possible, to ensure the use of cloud services does not impair its ability to comply with local law and regulatory requirements;

ii) understand the scope of local customer protection legislation and regulatory requirements as well as to ensure that the financial institution's customers receive adequate protection and recourse in the event of a data breach by the cloud service provider; and

iii) address requirements as stipulated in the Outsourcing policy document for outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia.

(d) Difficulties related to incident response and investigation may arise with cloud services as financial institutions may no longer have full access to the computing components managed by the cloud service providers as compared to an on-premises solution. At a minimum, a financial institution should assess the potential impact and formalise arrangements with cloud service providers to comply with local laws and regulatory requirements for incident investigation and law enforcement purposes. This would include adhering to data retention requirements and data access procedural arrangements to ensure the confidentiality and privacy of the customers are protected.

(e) The provision of cloud services by the primary cloud service provider may interconnect with multiple layers of other fourth-party cloud service providers

(sub-contractors), which could change rapidly. For example, customer data were leaked due to exposure made by fourth party. To mitigate fourth-party risks, financial institutions should:

i) understand the scope of customer information shared across the supply chain and ensure that relevant information security controls can be legally enforced [by the financial institution]; and
ii) ensure Service Level Agreement (SLA) negotiations and contractual terms cover the performance matrix, availability, and reliability of services to ensure all parties agree and are formally aligned on the requirements and standard of services provided.

6. Oversight over cloud service providers

A financial institution should ensure effective oversight over cloud service providers and the cloud service providers' sub-contractor(s). This includes, at a minimum, the following:

(a) Establish and define a continuous monitoring mechanism with alignment to the enterprise vendor management framework (or equivalent) to ensure adherence to the agreed SLA, compliance of the cloud service provider with any applicable legal and regulatory requirements and resilience of outsourced technology services on on-going basis;

(b) Identify, assign and document the key responsibilities within the financial institution for continuous monitoring of cloud service providers to ensure accountabilities are clearly defined; and

(c) Perform periodic assessments of the cloud service provider`s control environment, including business continuity management, to assess the potential impact on the financial institution's business resilience. This should address the requirements and guidance of Outsourcing involving Cloud Services section in Outsourcing policy document.

7. Skilled personnel with knowledge on cloud services

(a) The adoption of cloud services requires commensurate changes to the financial institution's internal resource and process capabilities. In this regard, a financial institution should:

i) equip its board with appropriate knowledge to conduct effective oversight over the cloud adoption; and
ii) ensure its IT operations or relevant personnel are appropriately skilled in the areas of cloud design, migration, security configurations, including administrative, monitoring and incident response.

(b) The effective management of cloud services should not purely be the responsibility of the IT function. Therefore, a financial institution should ensure

relevant internal resources in business operations, finance, procurement, legal, risk and compliance are also adequately skilled and engaged to manage the change in risk profile arising from cloud adoption. This should also enable financial institutions to respond effectively to operational incidents.

(c) A financial institution should equip internal audit and personnel undertaking the risk management and compliance functions with relevant cloud computing skills to be able to verify the effectiveness of the information security controls in alignment with the financial institution's cloud usage policy and information security objectives.

(d) A financial institution should ensure that staff receive adequate training to understand their responsibilities in complying with internal cloud usage policies and are prepared to effectively respond to a range of security incident scenarios developed on a risk-based approach.

(e) A financial institution should establish and implement a formal consequence management process to ensure the cloud usage policy is effectively enforced given that cyber hygiene is critical to ensure the continued security of cloud service usage.

Part B: Cloud Design and Control

A financial institution should design its adoption of cloud services with a degree of portability, scalability and fault tolerance that is proportionate to the materiality of the cloud service to its business operation. It should also ensure robust operational controls are in place to manage its ongoing cloud operations.

1. Cloud architecture

(a) A financial institution should design a robust cloud architecture and ensure such design is in accordance with the relevant international standards for the intended application.

(b) A financial institution is encouraged to adopt zero-trust principles[2] to provide enhanced access control via micro-segmentation of application and infrastructure with "deny-by-default", "least privilege" access rights or on a 'need-to-have' basis.

(c) A financial institution should continuously leverage enhanced cloud capabilities to improve the security of the cloud services, amongst others, financial institutions are encouraged to:

i) use immutable infrastructure[3] for deployment to reduce the risk of failure when new deployment of applications enter production by creating a new environment with the latest version of the software. The on-going monitoring of the cloud environment should include automating the detection of changes to immutable infrastructure to combat evolving cyber-attacks;

ii) use the latest network architecture approach such as Software-defined wide-area networking (SD-WAN)[4] for managing and monitoring granular network security and centralized network provision in managing complexity of the cloud network environment; and

iii) leverage available tools and services to enforce and monitor access control to cloud services. Examples of common tools and services include

[2] Zero-trust principles is a security paradigm designed to prevent data breaches and limit internal lateral movement of threat actors by requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and validated before being granted the access.

[3] Immutable infrastructure is an infrastructure paradigm where servers are never modified after deployment. The servers are replaced rather than changed.

[4] SD-WAN is a combine software-defined networking (SDN) concepts with traditional WAN technology to improve traffic routing and network operations. While SDN refers to a broad and developing concept that enable the network to be intelligently and centrally controlled using software applications. The objective is to provide control plane to manage the entire network consistently and holistically, regardless of the underlying network technology

the use of Cloud Access Security Brokers (CASBs)[5] or Secure Access Service Edge (SASE)[6].

(d) A financial institution should establish and utilise secure and encrypted communication channels for migrating physical servers, applications, or data to the cloud platforms. This includes the use of a network segregated from production networks for cloud migration and on-going administration of the management plane.

(e) For financial institutions leveraging their financial group's cloud infrastructure, consider an appropriate level of network segregation (e.g., logical tenant isolation in the shared environment of the cloud) to mitigate the risk of cyber-attacks from propagating cross-border or cross-entity and affecting the Malaysian financial institution's operations.

(f) The increasing use of application programming interfaces (API) to interconnect with external application service providers could achieve efficiency in new service delivery. However, this may increase the cyber-attack surface and any mismanagement may amplify the impact of an information security incident. A financial institution should ensure APIs are subject to rigorous management and control mechanism which include the following:

i) APIs should be monitored under the financial institution's patch and end-of-life (EOL) management framework to minimise security vulnerabilities;
ii) APIs should be tracked in the technology asset management and are de-commissioned on a timely basis when no longer in use;
iii) APIs should be configured for secure communication with external application service providers with appropriate access controls;
iv) APIs should be designed for service resilience to avoid the risk of single points of failure and included in the financial institution's business continuity arrangement; and
v) APIs should be monitored against cyber-attacks with adequate incident response measures.

2. Cloud application delivery models

(a) A financial institution should review its risk management policies and practices should be reviewed at least once every three years to ensure effective oversight over the cloud application delivery model.

(b) Cloud application delivery models may evolve to support faster time-to-market in response to consumer demand. Currently, DevOps and Continuous

[5] Cloud Access Security Brokers is a software tools or services that function as an intermediary between cloud users and cloud applications and monitors all activity and enforces security policies.

[6] Secure Access Service Edge are solutions that combine networking and security services, which may include the capabilities of Secure Web Gateway (SWG), Firewall as a Service (FWaaS), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) and Service Delivery WAN (SD WANs) to enforce security and compliance policies for usage of public cloud.

Integration / Continuous Development (CI/CD)[7] are amongst the prevailing practices and processes for cloud application delivery. For instance, the ability to enforce segregation of duties for CI/CD where application developers may require access to the management plane for service configuration. A financial institution should ensure CI/CD pipelines are configured properly to enhance security of automated deployments and immutable infrastructure.

(c) A financial institution is encouraged to adopt industry best practices such as Infrastructure as Code (IaC)[8] to automate the provisioning of IT infrastructure in a consistent, scalable and secure manner.

(d) Where relevant, a financial institution should implement appropriate controls on the IaC process to minimise the risk of misconfiguration and reduce the cyber-attack surface. This includes the following measures that should be taken by the financial institution:

  i) conduct vulnerabilities scanning on IaC, and ensure issues are remediated prior to the provisioning of IT infrastructure;
  ii) enable audit logs for real-time monitoring and identification of cyber threats. The logs should be retained for investigations and forensics purposes for at least three years;
  iii) ensure virtual machine images (VMI) or container images of IaC templates are trusted and digitally signed; and
  iv) implement appropriate access control to prevent unauthorized changes to IAC templates.

3. Virtualization and containerization management

The guidance provided in this paragraph is relevant for PaaS and IaaS cloud service models.

(a) A financial institution should ensure virtualization services are configured in line with the prevailing guidance from the cloud service provider and industry best practices, commensurate with the evolution of cloud computing technologies.

(b) A financial institution should ensure virtual machine and container images are configured, hardened, and monitored appropriately. This includes the following:

  i) use latest images and keep images up to date;
  ii) store and use images from trusted repositories or registries;
  iii) scan images for vulnerabilities, remediate any vulnerabilities prior running in production;
  iv) enforce “least privilege” access;
  v) harden images based on industry best practices; and

[7] CI/CD is a set of methods that enables developers to deliver code changes more frequently using automation.

[8] The process of managing and provisioning an organization’s IT infrastructure using machine-readable configuration files, rather than employing physical hardware configuration or interactive configuration tools.
- NIST Special Publication 800-172, U.S. Department of Commerce, February 2020

vi) stored images are subjected to security monitoring from unauthorised access and changes.

4. Change management

(a) A financial institution should ensure its existing change management process is extended to cover cloud services to promote effective and secure system development.

(b) A financial institution should define and establish appropriate escalation levels including approval authority matrix with clear accountability from cloud service provider and financial institution ("Authority Matrix"). The Authority Matrix should address the appropriate responsibility based on selected deployment model. The following control measures should be applied for change management:

i) ensure change requests are approved by the relevant approving authority and implemented by authorised personnel based on the change Authority Matrix; and

ii) establish emergency change escalation protocols and approval requirements in the Authority Matrix to ensure critical changes can be implemented and additional risks are mitigated promptly.

(c) A financial institution should establish a process to systematically manage releases by cloud service providers in relation to existing infrastructure, network, upstream and downstream systems to minimize the impact of any service disruption.

(d) All critical changes deployed to the production environment should also be timely applied to the disaster recovery environment where appropriate.

5. Cloud backup and recovery

(a) As part of an effective recovery capability, financial institutions should ensure existing backup and recovery procedures are extended to cover cloud services, which includes the following:

i) define and formalise backup and recovery strategy at the planning stage of cloud adoption;

ii) conduct periodic reviews of the cloud service providers' restoration and recovery capabilities;

iii) for critical system hosted on cloud, conduct testing of recovery strategy prior deployment of the system.

(b) A financial institution should ensure backup and restoration procedures are periodically tested to validate recovery capabilities. Remedial actions should be taken promptly for unsuccessful backups.

(c) A financial institution should ensure sufficient backup and recovery of virtual machine and container including backup configuration settings (for IaaS and PaaS, where relevant), which includes the following:
   i) ensure the capability to restore a virtual machine and container at point-in-time[9] as per the business recovery objectives;
   ii) make virtual machine and container images available in a way that would allow the financial Institutions to replicate those images at alternate and recovery site[10] ; and
   iii) allow virtual machine and container images to be downloaded and ported to new cloud service providers.

(d) A financial institution should assess the resilience requirements of the cloud services and identify appropriate measures that commensurate with the criticality of the system, to ensure service availability in the extreme adverse scenarios. To ensure service availability, financial institution should consider a risk-based approach and progressively adopt one or more of the redundancy approaches, including diversifying away from a single CSP. Amongst the viable options are:
   i) leverage cloud services' high availability and redundancy features to ensure production data centres have redundant capacity in different availability zones;
   ii) achieve geographical redundancy by having data centres in different geographical regions;
   iii) adopt hybrid cloud (combination of on-premises and public cloud setup);
   iv) establish back-up cloud service providers and identify appropriate arrangement for porting of data and application to ensure timely service resumption; and
   v) adopt multi-cloud strategy, with the use of services from different cloud service providers to mitigate concentration risks and geopolitical risks.

6. Interoperability & Portability

Interoperability standards for cloud services continue to evolve such that porting data, related configuration and security logging across different cloud service providers may be challenging. To facilitate the smooth process of interoperability and portability between on-premise IT systems and alternate cloud service providers, financial institutions are encouraged to:

(a) ensure technical requirements for interoperability and portability are included in the contractual agreement with the cloud service provider to avoid vendor lock-in;

---

[9] Point-in-time is the concept that a particular set of data can be restored to an exact state of time rather than just to the time of the last backup file.

[10] The alternate and recovery sites could either be in-house arrangements, or available through agreement with third-party recovery facility provider, or a combination of both options.

(b) maintain a list of cloud service providers and tools that are needed to facilitate a smooth transition;

(c) ensure usage of standardized network and communication protocols for ease of interoperability and portability with on- premise IT systems or alternate cloud platforms;

(d) ensure the use of common electronic data formats, where applicable, to ease the movement of data between cloud service providers or to on-premises IT system; and

(e) extend patch and EOL management to ensure technology solutions employed remain effective and protected against system vulnerabilities.

7. Exit strategy

(a) A financial institution should establish a robust cloud exit strategy as part of its cloud risk management framework to prepare for extreme adverse events such as the unplanned failure or termination of cloud service providers. The exit strategy should:

i) be developed during the cloud deployment planning phase rather than on an ex-post basis;

ii) identify alternative cloud service providers (multi-cloud approach) or third-party solutions to ensure no business recovery objectives disruption or vendor lock-in;

iii) be properly documented including details on the various exit trigger scenarios, roles, responsibilities and sufficient resources to manage exit plans and the transition activities; and

iv) be updated in a timely manner to reflect any material developments.

(b) A financial institution's exit strategy should be supported by an exit plan that establishes the operational arrangements to facilitate an orderly exit from a cloud service provider, which include the following:

i) conduct impact assessment to determine potential costs, resources and timing implications of transferring cloud services to an alternative cloud services provider or back to in-house arrangement at the financial institution;

ii) identify appropriate methods to port data and applications to an alternative arrangement;

iii) obtain written confirmation from the cloud service provider or via an independent external service provider's attestation that all sensitive data has been completely removed and destroyed from the cloud service provider's facilities upon completion of the exit process; and

iv) conduct testing to validate the effectiveness of the exit plan, to obtain a reasonable degree of assurance of its effectiveness.

8. Cryptographic key management

(a) A financial institution should implement appropriate and relevant encryption techniques to protect the confidentiality and integrity of sensitive data stored on the cloud.

(b) A financial institution should ensure its policies and procedures on cryptography are extended to cover cloud services where relevant, to promote the adoption of strong cryptographic controls.

(c) For critical systems hosted on the cloud, financial institutions should retain ownership and control of the encryption key (themselves or with an independent key custodian), independent from the cloud service provider, to minimize the risk of unauthorised access to the data hosted on the cloud. As example, this could be achieved by deploying the hardware security module (HSM) on-premises or by utilising HSM-as-a-service from a different cloud service provider.

(d) Multiple encryption key management systems may add complexity and introduce new challenges of comprehensively maintaining and managing all the cryptographic keys as the usage would increase as cloud adoption increases. A financial institution should consider implementing a centralised key management system to unify key management and encryption policies for efficient scale operation.

9. Access Controls

(a) The management plane is a key security difference between traditional infrastructure and cloud computing where remote access is supported by default. This access layer could be prone to cyber-attacks thereby compromising the integrity of the entire cloud deployment. In view of this, financial Institutions should ensure the use of strong controls for accessing the management plane which include the following:

i) review the financial institution's patch and EOL management framework to effectively secure the management plan;

ii) allocate dedicated and effectively hardened endpoints and up to date patching of software to access the management console;

iii) implement "least privilege" and strong multi-factor authentication (MFA) e.g., strong password, soft token, privileged access management tool and maker-checker functions;

iv) employ granular entitlement allocation for privileged users;

v) conduct continuous monitoring of the activities performed by privileged users;

vi) adopt robust prevention mechanism against phishing and password guessing attacks, credential stuffing and brute-force attacks. e.g., web application firewall (WAF), anti-phishing tools; and

vii) ensure secure communication protocols are in place for accessing the management plane. e.g., secure end-to-end communication channels, whitelisting of IP addresses and etc.

(b) A financial institution should extend its user access matrix to cover user access rights for both the financial institution and its cloud service providers where relevant for the ongoing access of cloud-related services.

(c) A financial institution should ensure access controls to all hypervisor management functions or administrative consoles for systems hosting virtualized systems are effectively implemented as per the requirements and guidance under the Access Control section of RMiT policy document. These controls should mitigate the risk of any unauthorised access to the hypervisor management functions and virtual machine.

(d) Point-to-point connections with cloud services may proliferate with the ease of cloud adoption, resulting in fragmentation of identity and access management and the risk of unsanctioned data being migrated to the cloud. In view of this, rigorous planning is recommended for the design of identity and access management as it is inherently complex. Financial institutions are encouraged to:

i) implement a federated[11] approach for identity and access management to mitigate risks of identities in cloud services being disjointed from the internal identities, unauthorised access and to ease user access management; and

ii) consider additional attributes in context-aware decisions for identity and access management such as geographical location of access to further mitigate the risks associated with remote access.

10. Cybersecurity Operations

(a) A financial institution should ensure the governance and management of cybersecurity operations is extended to cover cloud services, with appropriate control measures to prevent, detect and respond to cyber incidents in the cloud environment to maintain the overall security posture of the institution.

(b) The interconnected cloud service supply chain could become a source of cyber risk. A financial institution should ensure integrated monitoring and full visibility of cloud services are established. This should include the following:

i) continuous monitoring of system communications between the cloud service provider, on-premise IT systems and other third-party service providers to ensure the security perimeter is not breached; and

ii) ensuring that third-party service providers, including those providing ancillary functions, have adequate capabilities to monitor, detect and

[11] Federated approach for identity and access management is a process / arrangement between multiple systems or enterprises that enables users to use the same identification data to access all related networks.

respond to anomalous activities, with timely communication to the financial institution of relevant cyber incidents.

(c) A financial institution should understand the segregation of responsibility in security management, which varies across the cloud service models. A financial institution should manage the sources of vulnerabilities appropriately including:

i) managing vulnerability assessment and penetration testing (VAPT) for cloud services;
ii) proactively seek assurance of their cloud service providers to conduct periodic VAPT on the cloud infrastructure to ensure tenant isolation and overall security posture remains healthy;
iii) understand the cloud service provider's VAPT policy on cloud infrastructure given the varying degree of financial institution's access to the cloud environment, and establish VAPT arrangement upfront;
iv) tailor the financial institution`s standard operating procedures for VAPT to the scope of cloud configuration under the financial institution's responsibility. This includes conducting VAPT prior to deployment of cloud services;
v) establish appropriate tools to conduct VAPT on cloud services under the financial institution's responsibility, commensurate with the complexity of the cloud environment;
vi) the scope of penetration testing should place emphasis on the API calls to the management plane and credentials of privileged users (e.g., cloud administrators), which form the key elements of cyber-attack surface; and
vii) the financial institution which adopts high velocity methods e.g., Continuous Integration/Continuous Development (CI/CD), should integrate code review, security testing and vulnerability assessment into the system development life cycle (SDLC) process to minimise application vulnerabilities.

(d) A financial institution should review loss provision to ensure its adequacy to cover cyber incidents based on its scenario analysis of extreme adverse events. Where cyber insurance is adopted to mitigate impact of cyber incidents, the financial institution should:

i) understand the cyber insurance policy scope to ensure it adequately covers the information security events and liability types identified;
ii) understand the insurance policy terms and conditions such as the accuracy of financial institution's attestation on its cyber risk management capability and its on-going responsibility in information security management to ensure any changes to the IT services and associated control measures do not result in unintended exclusions from the insurance policy; and

iii) continue to strengthen cloud risk management to mitigate likelihood of cyber incidents from materialising.

11. Distributed Denial of Service (DDoS)

(a) A financial institution should ensure the subscription of DDoS mitigation service is commensurate with the size and complexity of the cloud adoption.

(b) The risk of a single point of failure (SPOF) may surface when a financial institution leverages solely on a cloud-based solution to mitigate DDoS attacks. As such, a financial institution is encouraged to engage alternative DDOS mitigation providers or establishing circuit breakers to avoid service disruption when the main DDOS mitigation provider is disrupted.

12. Data Loss Prevention (DLP)

(a) A financial institution should ensure the DLP strategy and processes are extended to protect data hosted in cloud services, including the following:

i) tailor control procedures and appropriate technologies to enforce DLP policies over the entire data lifecycle; and

ii) manage the expansion of the endpoint footprint if the financial institution allow staff to use their own devices to connect to cloud services.

(b) As it becomes increasingly easy to distribute digital content to customers via cloud services, a financial institution should adopt the appropriate digital rights management solution to preserve the confidentiality of its proprietary and customer information.

13. Security Operations Centre (SOC)

(a) A financial institution should understand the scope of cloud service providers' responsibility for cybersecurity monitoring and adapt its SOC strategy and processes to ensure proactive and holistic monitoring of its cybersecurity posture. This includes the ability of financial institution to scale up the cybersecurity telemetry and analysis to effectively identify and respond to cyber threats.

(b) The responsibilities of cloud service providers with respect to SOC operations should be formalised in the contractual agreement between the financial institution and the cloud service provider, including retention period required for relevant logs needed for forensic purposes and the right of the financial institution to access the logs, to meet the RMiT requirements on access control and security of digital services.

14. Cyber response and recovery

(a) A financial institution should enhance existing cyber crisis management policies and procedures to remain in a state of readiness to respond to cyber threats in a cloud environment.

(b) A financial institution should extend its Cyber Incident Response Plan (CIRP) to include adverse scenarios that may affect cloud services and establish clear roles and responsibilities between the financial institution and cloud service providers for incident response and remediation. The incident escalation process and turnaround time should be established with cloud service providers and periodically reviewed, to the extent possible, to achieve an effective incident response.

(c) A financial institution should consider the following additional measures in the development of its CIRP:

  i) enhance its ability to detect security breach incidents to achieve effective incident management, including the ability to detect data leakage on the dark web;

  ii) provide adequate assistance to customers in the event of a security breach in view that the complexity of cloud arrangements and sophistication of cyber-attacks often exceed the response range reasonably expected of customers; and

  iii) ensure CIRP is ready to manage cross-border incidents where the cloud service resides in a foreign jurisdiction.

(d) A financial institution should ensure that relevant Cyber Emergency Response Team (CERT) members are conversant with the CIRP covering cloud services to effectively activate the CIRP when incidents occur.

(e) A financial institution should extend the existing incident reporting requirements to include cloud services.

(f) For critical systems hosted on the cloud, a financial institution should establish arrangements with their cloud service providers to conduct annual cyber drills to test the effectiveness of the financial institution's CIRP.

Question

Please identify challenges for your institution to comply with CTRAG, including potential implication to your current cloud design?