CLOUD AUDIT TOOLKIT FOR FINANCIAL REGULATORS

DECEMBER 2021

ASIAN DEVELOPMENT BANK

CLOUD AUDIT TOOLKIT FOR FINANCIAL REGULATORS

DECEMBER 2021

ASIAN DEVELOPMENT BANK

© 2021 Asian Development Bank
6 ADB Avenue, Mandaluyong City, 1550 Metro Manila, Philippines
Tel +63 2 8632 4444; Fax +63 2 8636 2444
www.adb.org

Some rights reserved. Published in 2021.

ISBN 978-92-9269-208-7 (print); 978-92-9269-209-4 (electronic); 978-92-9269-210-0 (ebook)
Publication Stock No. TIM210485-2
DOI: http://dx.doi.org/10.22617/TIM210485-2

The views expressed in this publication are those of the authors and do not necessarily reflect the views and policies of the Asian Development Bank (ADB) or its Board of Governors or the governments they represent.

ADB does not guarantee the accuracy of the data included in this publication and accepts no responsibility for any consequence of their use. The mention of specific companies or products of manufacturers does not imply that they are endorsed or recommended by ADB in preference to others of a similar nature that are not mentioned.

By making any designation of or reference to a particular territory or geographic area, or by using the term "country" in this document, ADB does not intend to make any judgments as to the legal or other status of any territory or area.

Please contact pubsmarketing@adb.org if you have questions or comments with respect to content, or if you wish to obtain copyright permission for your intended use that does not fall within these terms, or for permission to use the ADB logo.

Corrigenda to ADB publications may be found at http://www.adb.org/publications/corrigenda.

Notes:
In this publication, "$" refers to United States dollars.
ADB recognizes "Hong Kong" as Hong Kong, China.

Cover design by Cleone Baradas.

Contents

Table and Figures

Table

Figures

About This Toolkit

Cloud technology continues to transform the way businesses operate in the financial services industry. Its use remains at the center of the discussion when it comes to digital transformation. However the use of new technologies introduces new risks. This toolkit was developed to provide financial regulators in developing member countries of the Asian Development Bank guidance on how to improve their supervisory work processes, taking existing practices from around the globe on supervising and regulating the use of cloud computing technology.

The aim of this toolkit is to assist regulators in effectively and efficiently carrying out their supervisory work, provide them an understanding of the relevant issues associated with cloud computing, appreciate the key risks and challenges in its use within the context of the financial services industry, and assess the adequacy of existing processes for regulatory supervision.

As technology evolves and matures, auditors will need to continuously improve existing processes and procedures ensuring that it is in step with new advancements and developments.

Acknowledgments

This toolkit was prepared as part of the Asian Development Bank's (ADB) support to knowledge work on digital financial services among its developing member countries. We would like to acknowledge Bangko Sentral ng Pilipinas (BSP) for their support and for allowing us to test the Toolkit with them. Special thanks to the team in the Technology Risk and Innovation Supervision Department of the BSP, led by Melchor T. Plabasan, for sharing their insights and expertise garnered from their supervisory work at the BSP.

Lisette Cipriano, senior digital technology specialist (Financial Services), Sustainable Development and Climate Change Department (SDCC) led the effort to coordinate and contributed to the development and production of this toolkit. Expertise and learnings were provided by May Ann Lim, managing director of TRPC Pte Ltd and concurrently the executive director of the Asia Cloud Computing Association (ACCA). Peter Lovelock, director, TRPC Pte Ltd, for providing the strategic support and advise. Junkyu Lee, chief of Finance Sector Group, SDCC provided overall direction and supervised the production of the toolkit.

The peer reviewers of this toolkit were Peter Fizelle, chief information security officer and Yuen Tsung Wong IT specialist (Information Security). We are most grateful for their feedback and advice and acknowledge their contribution.

The toolkit was financed by ADB's knowledge and support technical assistance 9364: Strengthening Financial Sector Operations in Asia and the Pacific which is financed on a grant basis by ADB's Technical Assistance Special Fund, Financial Sector Development Partnership Special Fund,[1] High-Level Technology Fund,[2] and the Republic of Korea e-Asia and Knowledge Partnership Fund.[3]

The report was produced with the support of a team of ADB consultants comprising Eric Van Zant as editor, Jess Macasaet as proofreader, Edith Creus for typeset and layout, and Cleone Baradas for the graphic design of the cover. Matilde Cauinian, operations assistant, Katherine Mitzi Co, associate operations analyst, and Raquel Borres, senior economics officer, SDCC provided valuable administrative support.

Finally, we would like to appreciate the relentless support that Director General Bruno Carrasco of the Sustainable Development and Climate Change Department has given in the production of innovative financial services projects and initiatives.

[1] Established by ADB. Financing partner: the Government of Luxembourg.
[2] Administered by ADB. Financing partner: the Government of Japan.
[3] Administered by ADB.

Abbreviations

ADB	Asian Development Bank
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BSP	Bangko Sentral ng Pilipinas
CBPR	cross border privacy rules
DMC	developing member countries
EU	European Union
GDPR	General Data Protection Regulation
IaaS	infrastructure as a service
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	information technology
MAS	Monetary Authority of Singapore
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PaaS	platform as a service
PCI DSS	Payment Card Industry Data Security Standard
SaaS	software as a service
SOC	service organization control and/or system organization and control
US	United States

1 Introduction

Financial regulators are increasingly recognizing the power of new technologies such as cloud computing to create new opportunities for improving and accelerating innovation in banking systems.

In the Philippines, for example, Bangko Sentral ng Pilipinas (BSP), the central bank, supported a partnership between the Asian Development Bank (ADB) and Cantilan Bank Inc to pilot a study on cloud-based core banking technology. It placed the project in a "regulatory sandbox" while it processed and updated related regulations. And in January 2019, Cantilan Bank became the first BSP-regulated bank in the Philippines to fully rely on a cloud-based "software as a service" system as their core banking system.

The shift to cloud computing technologies has increased Cantilan Bank's flexibility and given it a more accurate banking system. It has raised operational efficiency and enabled the bank to respond faster than other financial institutions to customer needs, particularly as the coronavirus disease has caused economic lockdowns across the country.

As a result of the pilot, financial institutions' trust in cloud technology has increased and the regulator has strengthened innovation-enabling regulations and adopted an effective supervisory approach that fosters innovations such as cloud computing services for core and non-core banking systems and activities. Indeed, the BSP has since approved over 40 other financial institutions to migrate their core banking to the cloud.

Challenges in Regulating for Cloud Computing

Yet, some regulators may still have questions about how to transition from a pre-cloud to a cloud-first regulatory framework. Questions around data governance frameworks to be put in place, managing security standards, conducting audits and inspections, assessing risk management approaches, business continuity and incident responses, and so on, often arise when regulating financial institutions look to move to the cloud.

This paper addresses the questions regulators may have, particularly common issues surrounding mechanisms for oversight, monitoring, and control of cloud technology in the financial sector.

Introducing the Cloud Audit Toolkit for Financial Regulators

The *Cloud Audit Toolkit for Financial Regulators* is a two-part paper which aims to assist and accelerate opportunities to cloud computing technologies and digital tools to improve the efficiency and efficacy of financial regulators' work processes. It addresses the question: "What do regulators need to know when regulating and/or supervising the adoption of cloud computing services in the financial services sector?"

Using existing practices observed by leading regulators globally, such as the BSP, and the Monetary Authority of Singapore's (MAS) *Guidelines on Technology Risk Practices,*[1] this regulatory toolkit comprises two components:

(i) **Regulatory toolkit paper (this paper)** which develops a framework for financial regulators to oversee technology and outsourcing risks in using and deploying technology tools such as cloud computing.
(ii) **Regulator's checklist** (in Appendix): To assist the regulator in its initial review of current oversight mechanisms.

Cloud Audit Toolkit for Financial Regulators Workshop. Workshop participants from the Bangko Sentral ng Pilipinas Technology Risk and Innovation Supervision Department led by Director Melchor T. Plabasan.

Pilot of the Cloud Audit Toolkit for Financial Regulators Training Program

This toolkit was piloted as a half-day capacity-building training program organized with the BSP on 24 May 2021 for about 50 staff. Due to coronavirus disease travel restrictions, in lieu of an in-person workshop, this was held as a virtual training session.

[1] Monetary Authority of Singapore. 2021. *Guidelines on Risk Management Practices–Technology Risk*. 18 January. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines.

2 Service Provider Oversight

Use of cloud computing in financial services has been growing and financial regulators have been regularly updating regulations and guidelines to allow better oversight and risk management of the technologies their regulated entities are using.

Cloud Computing Regulated as Risk-Based, Outsourcing Arrangement

Regulation of cloud computing has evolved differently in each financial market, but financial regulators have generally considered cloud computing a risk-based outsourcing arrangement, ensuring that regulated entities are identifying the relevant risks and managing them effectively. This technology-neutral approach is preferred over making new regulations specific to cloud computing technologies, which may become outdated as technology and its applications develop. Examples of this arrangement include the following:

- Australian Prudential Regulation Authority regulates the cloud under the *Prudential Standard CPS 231 Outsourcing (Jul 2017)*[2] and the *Prudential Practice Guide PPG 231 Outsourcing (Oct 2006)*.[3]
- MAS addresses cloud computing within its updated *2018 Guidelines on Outsourcing,*[4] supported by additional *Technology Risk Management Guidelines*.[5]
- The Hong Kong Monetary Authority regulates cloud computing technology under *SA-2 Outsourcing (Dec 2001)*[6] —major supervisory concerns, and *IC-1 Risk Management Framework (Oct 2017)*.[7]
- BSP regulates cloud computing technology guided by *BSP Circular No. 808 on Information Technology Risk Management,*[8] and *BSP Circular No. 899 on Outsourcing*.[9]

This regulatory toolkit therefore recommends checklist items under cloud computing regulated as risk-based, outsourcing arrangement in the Appendix (1.1.1 to 1.1.3).

[2] Australian Prudential Regulation Authority. 2017. *Prudential Standard CPS 231 on Outsourcing*. July. https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.

[3] Australian Prudential Regulation Authority. 2006. *Prudential Practice Guide PPG 231 on Outsourcing*. October. https://www.apra.gov.au/sites/default/files/PPG-231-Outsourcing-Oct-06.pdf.

[4] Monetary Authority of Singapore. 2018. Guidelines on Outsourcing. 5 October. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

[5] Monetary Authority of Singapore. 2021. MAS Enhances Guidelines to Combat Heightened Cyber Risks. 18 January. https://www.mas.gov.sg/news/media-releases/2021/mas-enhances-guidelines-to-combat-heightened-cyber-risks.

[6] Hong Kong Monetary Authority. 2017. *Supervisory Policy Manual SA-2*. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.

[7] Hong Kong Monetary Authority. 2017. *Supervisory Policy Manual IC-1 Risk Management Framework*. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/IC-1.pdf.

[8] Bangko Sentral ng Pilipinas. 2013. *Circular No. 808 Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions*. 22 August. https://www.bsp.gov.ph/Regulations/Issuances/2013/c808.pdf.

[9] Bangko Sentral ng Pilipinas. 2016. Circular No. 899 Amendments to the Guidelines on Outsourcing. 18 January.

Technology Oversight, Monitoring, and Control

The management and control of outsourcing arrangements of a financial institution or regulated entity are based on the nature and extent of risks in the outsourcing arrangements. The regulated entity itself is best placed to determine the specific monitoring and control measures to be instituted for oversight of outsourcing agreements. Financial regulators should allow regulated entities the flexibility to customize their outsourcing arrangement through a risk-based approach, possibly augmented with suggestions for baseline standards or guidelines which advise how regulated entities can exercise their oversight responsibilities.

How is Oversight Different in the Cloud?

Though the basic rationale behind oversight in the cloud is the same as in other forms of outsourcing, the cloud presents unique challenges and advantages. Importantly, regulators should bear in mind that some cases may need regulated entities to maintain more mechanisms for oversight, monitoring, and control when using the cloud. The increasing sophistication of cloud technology has revealed that traditional oversight mechanisms which do not incorporate information technology (IT) expertise may insufficiently address these risks.[10] It has also demanded that regulated entities and the financial regulator have strong technical knowledge to understand and address the risks arising from technology usage.

One benefit of cloud technology is that the standards for oversight are well-established and being kept up–to–date, and moving financial services into the cloud can in fact facilitate and improve oversight functions. For example, major cloud providers are certified in international standards such as the ISO/IEC 27000 series and conduct regular third-party audits, which automatically raises a regulated entity's oversight and standard of outsourcing arrangements.

Regtech and Suptech

Among the new technologies and cloud computing useful in financial services are data analytics and artificial intelligence to assist regulators with supervisory and regulatory monitoring mechanisms, i.e., "regtech" and "suptech." Efforts could range from ensuring the entire process of regulatory review and supervision is available in digital formats (moving from analog reporting to digital), to developing sophisticated methods for real-time monitoring of regulated entities. For example:

- Alessa is a Canadian regtech solution which offers real-time due diligence, transaction monitoring, sanctions screening, and other regulatory reporting capabilities to comply with anti-money laundering and counter terrorist funding regulations.[11]
- 360factors is a United States (US) regtech solution which designs bespoke cloud-based regulatory and risk reporting mechanisms for the financial sector.[12]
- 6Clicks is a British regtech solution which offers their clients a dashboard-style automated assessment and compliance management platform.[13]
- 8of9 is a US regtech solution which captures financial regulations and legislation in real-time and provides timely alerts to clients.[14]

[10] A Levite and G. Kalwani. 2020. Cloud Governance Challenge: A Survey of Issues. *Carnegie Endowment for International Peace.* 9 November. https://carnegieendowment.org/2020/11/09/cloud-governance-challenges-survey-of-policy-and-regulatory-issues-pub-83124.

[11] Alessa by Tier1 Financial Solutions. https://tier1fin.com/alessa/.

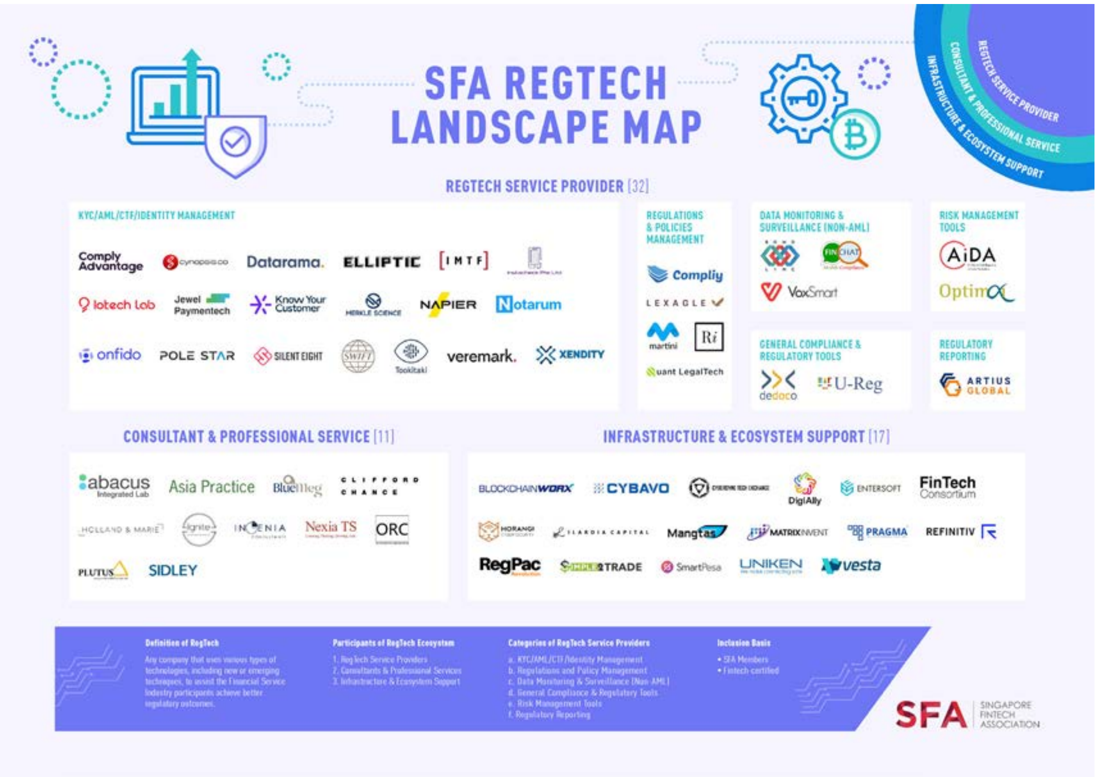
[12] 360 Factors. https://www.360factors.com/.

[13] 6 Clicks. https://www.6clicks.io/.

[14] 8of9. https://www.8of9.nyc/.

The Singapore Fintech Association has published a list of the various types of regtech which have been developed, and the companies which have solutions (Figure 1.)

Figure 1: Regtech Landscape


SFA REGTECH LANDSCAPE MAP
REGTECH SERVICE PROVIDER
CONSULTANT & PROFESSIONAL SERVICE
INFRASTRUCTURE & ECOSYSTEM SUPPORT
REGTECH SERVICE PROVIDER [32]
KYC/AML/CTF/IDENTITY MANAGEMENT
ComplyAdvantage
cynopsis.co
Datarama.
ELLIPTIC
[IMTF]
Iotech Lab
Jewel Paymentech
Know Your Customer
MERKLE SCIENCE
NAPIER
Notarum
onfido
POLE STAR
SILENT EIGHT
SWIFT
Tookitaki
veremark.
XENDITY
REGULATIONS & POLICIES MANAGEMENT
Compliy
LEXAGLE
martini
Ri
Quant LegalTech
DATA MONITORING & SURVEILLANCE (NON-AML)
FINCHAT
VoxSmart
RISK MANAGEMENT TOOLS
AiDA
Optimai
GENERAL COMPLIANCE & REGULATORY TOOLS
dedoco
U-Reg
REGULATORY REPORTING
ARTIUS GLOBAL
CONSULTANT & PROFESSIONAL SERVICE [11]
abacus Integrated Lab
Asia Practice
BlueMeg
CLIFFORD CHANCE
HOLLAND & MARIE
Ignite
INCENIA
Nexia TS
ORC
PLUTUS
SIDLEY
INFRASTRUCTURE & ECOSYSTEM SUPPORT [17]
BLOCKCHAINWORX
CYBAVO
DigiAlly
ENTERSOFT
FinTech Consortium
HORANGI
ILARDIA CAPITAL
Mangtas
MATRIXINVENT
PRAGMA
REFINITIV
RegPac
SIMPLE2TRADE
SmartPesa
UNIKEN
vesta
Definition of RegTech
Any company that uses various types of technologies, including new or emerging techniques, to assist the Financial Service Industry participants achieve better regulatory outcomes.
Participants of RegTech Ecosystem
1. RegTech Service Providers
2. Consultants & Professional Services
3. Infrastructure & Ecosystem Support
Categories of RegTech Service Providers
a. KYC/AML/CTF/Identity Management
b. Regulations and Policy Management
c. Data Monitoring & Surveillance (Non-AML)
d. General Compliance & Regulatory Tools
e. Risk Management Tools
f. Regulatory Reporting
Inclusion Basis
• SFA Members
• Fintech certified
SFA SINGAPORE FINTECH ASSOCIATION

Source: Singapore Fintech Association. Regtech Sub-Committee. https://singaporefintech.org/regtech-subcommittee/.

A final note on regtech and suptech—in some instances, it has been useful for the public sector to work with the private sector to develop these solutions together, to ensure that regulatory reporting is fully compliant and interoperable with a country's financial regulatory submissions. Austrian Reporting Services, for example, Europe's largest regulatory reporting utility and reporting hub,[15] was established through partnership between the Austrian National Bank (the central bank) and the country's banks. The regtech speeds up regulatory reporting, including standard template reporting, and *ad hoc* requests from regulators.

Recordkeeping

As a starting point for ensuring effective oversight and monitoring, financial institutions should keep adequate records on outsourcing arrangements, particularly those critical or material. Definitions of what constitutes material or critical may differ slightly from regulator to regulator, but the concept generally encompasses agreements that if not performed or that otherwise suffer a service failure or data breach, would have a material

[15] RegTech. Addressing the complexities of the regulatory environment. https://www.reg.tech/en/knowledge-hub/case-studies/aurep-ukrep-addressing-complexities-regulatory-environment/.

or severe impact on the regulated entity's core operations (see page 29 Setting business continuity and disaster recovery requirements: criticality and materiality.) Materiality can also refer to agreements dealing with customer information, where service failure or breach could result in material impact to the customer.[16]

Recordkeeping may include a register of outsourcing arrangements maintained by the institution for internal review by senior management, as needed, or to be submitted to the regulator on a regular basis, e.g., annually.

It is recommended to refer to checklist items in Appendix under recordkeeping (1.3.1 to 1.3.6).

Qualified Oversight Groups

To facilitate active oversight and monitoring of outsourcing agreements, regulated entities should have processes in place to conduct regular reviews of agreements and assess how the agreements perform against their expectations on risk management and other criteria. One way such oversight is institutionalized is through creation of oversight groups.

Factors to consider in such groups include who is in the group and what the group's responsibilities are. The group's composition should be multidisciplinary so as to leverage the expertise of individuals from across different internal groups and which have familiarity with technical issues in specific outsourcing arrangements and with more general aspects of internal audit, legal, finance, etc.

Please refer to checklist statement in Appendix under qualified oversight groups (1.4.1).

Recently, regulators have begun to take note of the need for specialized personnel to deal with technology risk management. For example, for regulated entities, the MAS *Technology Risk Management Guidelines 2021*[17] now require that regulated entities have a chief or head of information security officer, head of IT, chief technology officer, or a chief information officer. In addition, the board of directors must have a technology risk management function. Similarly, regulators have recognized that they too require personnel with these capabilities to effectively write and implement policies for cloud usage in the financial sector.

Please refer to checklist statement in Appendix under qualified oversight groups (1.4.2).

Responsibilities of the Oversight Group

Among its responsibilities, the oversight group can be tasked with ongoing monitoring of outsourcing arrangements through regular monitoring and control reports and reviews. These reports and reviews are typically intended to be reviewed by senior management and/or the board to ensure awareness of the status of outsourcing agreements and whether they meet the institution's standards from a broader strategic viewpoint.

As such, the content of the reports and reviews should consider the existing risk management plan and other relevant plans and/or strategies formulated, as well as the adequacy of the internal risk management and management information systems. Similar to security and data protection risk management strategies, regulators

[16] Monetary Authority of Singapore. 2016. Guidelines on Outsourcing. 27 July. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf.

[17] Monetary Authority of Singapore. 2021. *Technology Risk Management Guidelines*. 18 January. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

should recognize that the oversight group can be assisted in its monitoring and control functions through third-party audits for international certifications, though these should be taken holistically within the context of the regulated entity's strategies, plans, and systems.

Please refer to checklist statement in Appendix under responsibilities of the oversight group (1.5.1 to 1.5.4).

In addition to ongoing monitoring, the oversight group should be informed and involved in significant events and changes, such as when new outsourcing agreements are entered into, or when amendments are made to existing agreements. In these cases, the oversight group should be responsible for conducting pre- and post-implementation reviews.

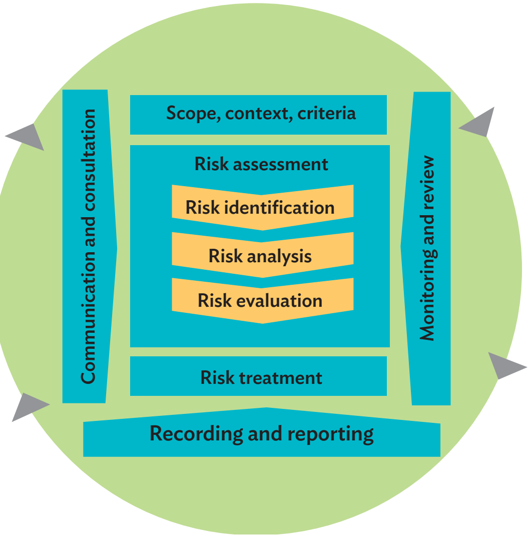
Please refer to checklist statement in Appendix under responsibilities of the oversight group (1.5.5 to 1.5.6).

Technology Risk Identification Mechanisms and Due Diligence

After establishing the oversight groups and recordkeeping for outsourcing arrangements, regulators should ensure that regulated entities have a risk-based assessment and management mechanism. The above list of country financial regulators who have addressed cloud computing under outsourcing regulations demonstrates that it may be useful for the regulator to also guide the adoption of cloud computing with specific non-mandatory guidelines which support the adoption of cloud computing. The risk assessment and control checks are commensurate with the criticality of the function being outsourced.

Under a risk management approach and framework, regulators may then ensure that regulated entities have established mechanisms to assess and address the risks, for example, following ISO 31000's standard for risk management. This would include establishing policies, procedures, and practices to work with internal

Figure 2: ISO 31000 Risk Management Process



Source: International Organization for Standardization. ISO 31000:2018(en) Risk Management - Guidelines. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

stakeholders to identify the risks, and develop methods by which the regulated entity can assess, treat, monitor, review, and report the risk. Figure 2 shows these various processes.

This toolkit therefore recommends the technology risk identification mechanisms and due diligence checklist (1.6.1 to 1.6.7) found in Appendix.

Due Diligence

A core component of the outsourcing process is to ensure due consideration for all eligible vendors, and that vendors are reliable and trustworthy. This is to avoid procurement issues such as vendor lock-in, concentration risk, and resiliency risk if the vendor exits the market suddenly.

In this respect, the regulator should ensure due diligence checks which a regulated entity has performed to ensure minimum quality of service standards expected of the cloud vendor. For example, a due diligence check would involve collecting information on the vendor to be selected, and could include evaluation of the following information during the due diligence check, such as the service provider's (footnote 16).

(i) experience and capability to implement and support the outsourcing arrangement over the contracted period;
(ii) financial strength and resources (the due diligence should be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitment of major equity sponsors, and ability to service commitments even under adverse conditions);
(iii) corporate governance, business reputation and culture, compliance, and pending or potential litigation;
(iv) security and internal controls, audit coverage, reporting and monitoring environment;
(v) risk management framework and capabilities, including technology risk management and business continuity management in respect of the outsourcing arrangement;
(vi) disaster recovery arrangements and disaster recovery track record;
(vii) reliance on and success in dealing with subcontractors;
(viii) insurance coverage;
(ix) external environment (such as the political, economic, social, and legal environment of the jurisdiction in which the service provider operates); and ability to comply with applicable laws and regulations and track record in its compliance with applicable laws and regulations.

It could also involve the vendor's employees, such as (i) whether they have been the subject of any disciplinary or criminal procedures; (ii) whether they have been convicted of any offence (particularly involving fraud, misrepresentation, or dishonesty); (iii) whether they have accepted civil liability for fraud or misrepresentation; and (iv) whether they are financially sound.

This due diligence should be documented and performed regularly, with frequency depending on the nature of the outsourcing service.

Please refer to checklist statement in Appendix under due diligence (1.7.1 to 1.7.2).

Procurement and Use of International Standards for Prequalification or Baseline Certifications

One key characteristic of cloud computing is that it is a measured service, and therefore regulated entities have the ability to purchase it as a utility instead of as single expense. In addition, there are differences between cloud services, as some companies may choose to procure a mixture of infrastructure as a service, platform as a service, software as a service, or other types of cloud services (Figure 3).[18]

The result of this is that there is no one-size-fits-all approach toward procurement of cloud services, and this has required a shift in how regulators oversee the management and controls of a cloud-based financial ecosystem. One approach is to ensure that vendors considered by regulated entities meet some form of internationally recognized baseline standard. Some governments that have established government cloud projects have taken this approach. For example:

- The Philippines government's *Cloud First Policy* has instituted a security framework which sets up baseline certification standard requirements for cloud vendors if they are to be considered eligible to host classified government data.[19] This includes
  - ISO/IEC 27001 Information Security Management,[20]
  - Payment Card Industry Data Security Standard,[21]
  - Service Organization Control (SOC) 1 and 2,[22]
  - ISO/IEC 27018—Code of practice for protection of personally identifiable information in public clouds acting as processors of that information.[23]

  These are accompanied by the following minimum encryption requirements.
  - Advanced Encryption Standard (128 bits and higher)
  - Triple Data Encryption Algorithm (minimum double-length keys)
  - Rivest–Shamir–Adleman (1024 bits or higher)
  - Elliptic curve cryptography (160 bits or higher)
  - ElGamal (1024 bits or higher)

[18] National Institute of Standards and Technology. 2011. *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[19] Government of the Philippines, Department of Information and Communications Technology. 2017. *Department Circular on Cloud First Policy*. 18 January. https://i.gov.ph/policies/signed/department-circular-cloud-first-policy.

[20] International Standards Organization. *ISO/IEC 27001: Information Security Management.* https://www.iso.org/isoiec-27001-information-security.html.

[21] PCI Security Standards Council. PCI Security. https://www.pcisecuritystandards.org/pci_security/.

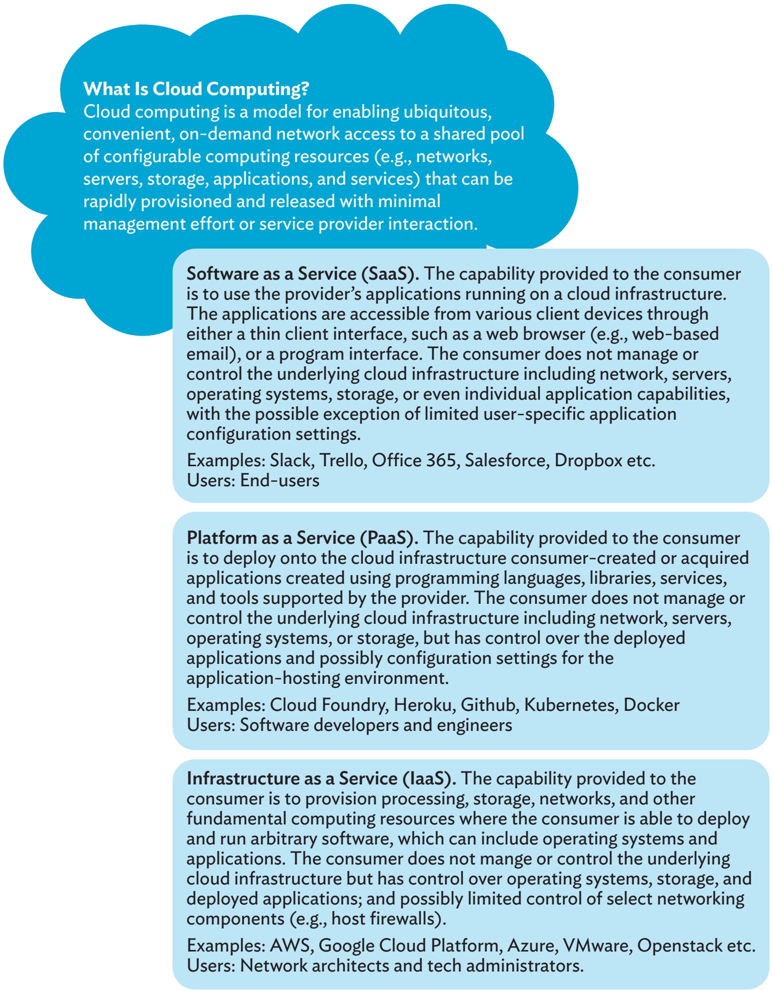
[22] Association of International Certified Professional Accountants. SOC for Service Organizations. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html.

[23] International Standards Organization. ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. https://www.iso.org/standard/76559.html.

- The United Kingdom's G-Cloud Framework includes a digital marketplace where vendors must apply to be pre-qualified and listed to be eligible to be selected for public sector procurement.[24]
- Australia's ICT Procurement Panel has a cloud services panel, which identities pre-qualified cloud vendors based on a list of their capabilities, and lists successful applicant vendors on a Standing Offer Notice SON2914302.[25]

While these examples are for public sector procurement rather than specifically for financial regulators, these are examples of how regulators may use internationally recognized standards for ensuring the quality and stability of a cloud-based financial system.

Figure 3: What Is Cloud Computing?



What Is Cloud Computing?
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.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Examples: Slack, Trello, Office 365, Salesforce, Dropbox etc.
Users: End-users

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Examples: Cloud Foundry, Heroku, Github, Kubernetes, Docker
Users: Software developers and engineers

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not mange or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Examples: AWS, Google Cloud Platform, Azure, VMware, Openstack etc.
Users: Network architects and tech administrators.

Source: National Institute of Standards and Technology. 2011. *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Please refer to checklist statement in Appendix under procurement and use of international standards for prequalification/baseline certifications (1.8.1).

[24] Government of the United Kingdom. Applying to the G-Cloud framework. https://www.gov.uk/guidance/g-cloud-suppliers-guide.

[25] Government of Australia, AusTender Procurement Information System. Standing Offer Notice View–SON2914302. https://www.tenders.gov.au/Son/Show/745895FF-E769-50C9-D860-7CECECE179B4.

3 Physical and Logical Audit and Inspection Rights

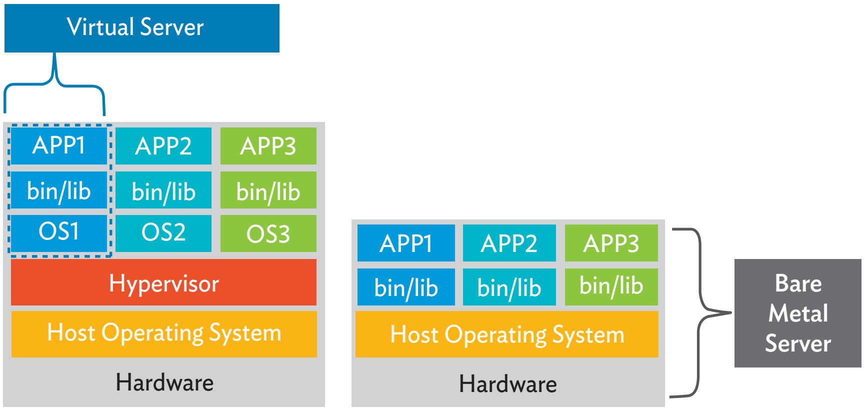
A legacy audit requirement from the pre-cloud era is the audit requirement for inspections, particularly physical inspection rights. Moving a financial regulatory regime into a cloud-based financial system requires the understanding that one of the characteristics of cloud computing is its resource pooling ability, where resources may be virtually and logically defined, rather than physically delineated.

Physical and Logical Separation

Cloud computing (Figure 4) uses pooled resources, which means that IT resources may be drawn from a variety of infrastructure and platforms, depending on the need of the regulated entity.

In the pre-cloud era, servers would only be physically defined (e.g., a server residing in a specific rack in a data center). In the cloud computing era, resources are logically defined, such as virtual machines (see figure below), drawn from a pool of resources that the regulated entity has purchased from their vendor. These resources may comprise computing resources drawn from a variety of other services, e.g., a database in one server tapping another computing machine to process data. The logical network architecture of the cloud system being used could also be a hybrid cloud or multi-cloud setup, or possibly one where the financial institution has chosen one part of the system to be hosted on a cloud service provider with shared tenancy, and combine it with another service that has a dedicated tenancy setup.

Figure 4: Physical Bare Metal Servers versus Virtual Machine Servers (logically defined)



Source: Kumulus Technlogies on SlideShareTips. 2020. *Docker vs Virtual Machines.* 30 June. https://slidesharetips.blogspot.com/2020/06/docker-vs-virtual-machines.html.

This approach therefore renders legacy audit requirements for inspection rights moot, as data is managed and processed logically and virtually rather than physically. In fact, physical inspection rights will represent a security risk to the data center facility as it means increasing the number of users able to access the secure facility. From a compliance standpoint, this would increase the cloud computing security risk assessment.

The BSP has been conducting virtual audits as a manner of preference and priority since 2013, conducted with a blended inspection methodology, with a combination of BSP audits and third-party audits using SOC 2 and ISO standards.[26]

Rather than mandating physical inspection rights, regulators could establish other logical control checks instead, such as ensuring that regulated entities have access controls, user access management, system and application access controls, and system logs in place.

This toolkit therefore recommends the physical and logical separation checklist (2.1.1) found in Appendix.

Third-Party Audits

In many instances, regulators may rely on third-party audits with international standards certifications as the assurance mechanism for both physical and logical audit control checks. A major benefit of this approach is the time saved, as such audits will expedite internal audits on regulated entities and reduce the overall cost of compliance for companies.

Expediting the Audit with Quality Assurance

For example, if a regulated entity has a valid SOC 2 report which has established logical and physical controls for technology deployment, and which has verified control mechanisms restricting physical access to sensitive locations to authorized personnel only, a regulator will be able to use that SOC 2 report check in lieu of other audit control checks required, expediting the audit.

In addition, third-party audits are only valid for specific time periods, after which re-certification is required. For example, the validity period for ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services[27] is 3 years, and Payment Card Industry Data Security Standard[28] for 1 year, providing the regulator with greater reassurance that third-party audits with international certification standards have strong trust and quality assurance mechanisms.

Updating Regulations for A Cloud-Based Financial System

Relying on third-party audits and international standards will also assist in highlighting regulatory updates, which may be needed to adjust to a cloud-based financial system, such as reviewing the need for physical audit checks.

Please refer to checklist statement in Appendix under third-party audits (2.2.2.1 to 2.2.2.8).

[26] Interview with BSP. Feb 2021.

[27] International Organization for Standardization. ISO/IEC 27017:2015(en) Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en.

[28] PCI Security Standards Council. https://www.pcisecuritystandards.org/.

4 Security and Cybersecurity Requirements

Regulators should ensure their regulated entities establish robust and effective technology risk management processes, governance structures, and cybersecurity controls. This is to ensure that the benefits derived from cloud computing can be fully optimized without compromising financial stability, operational resilience, and consumer protection.

In some cases, cybersecurity controls and mechanisms may be checked and cross-referenced against a national cybersecurity regulation or law, which provides broad overviews of the cybersecurity risks which need to be addressed by all sectors, including the financial services sector. Some examples of national cybersecurity laws and regulations include the Singapore Cybersecurity Act 2018,[29] Malaysia's Computer Crimes Act 1997 and National Cyber Security Policy,[30] Japan's Basic Act on Cybersecurity,[31] etc. Some countries may not have established a national cybersecurity law; this should be accelerated as a policy priority.

Shared Responsibility Model

The shared responsibility model is a key concept in understanding use of cloud computing.

In outsourcing of financial services, the cloud vendor is responsible for the security of the cloud, and the regulated entity is responsible for security in the cloud (Figure 5). This role differentiation is important, as it recognizes that responsibility for data governance cannot be outsourced to a vendor. For example:

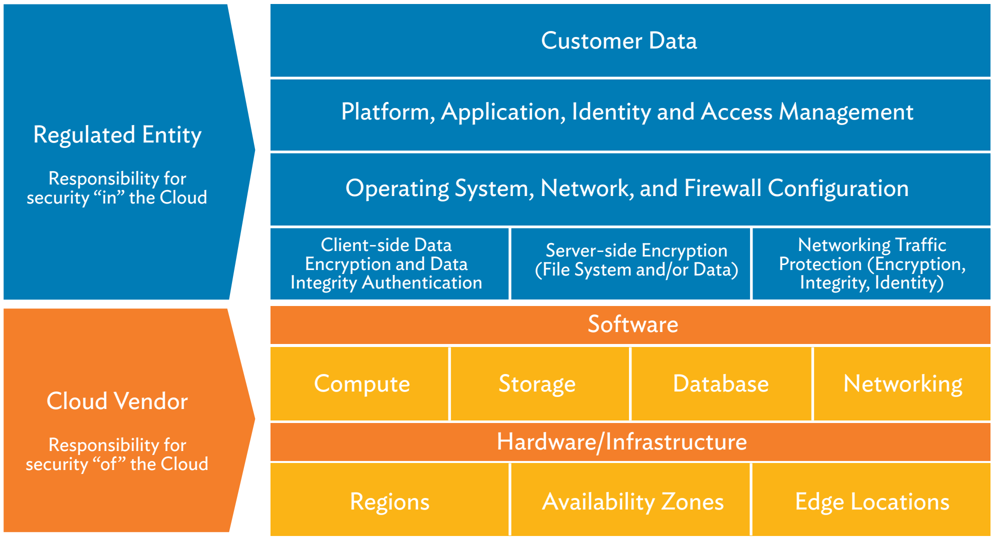
- If the employee of a regulated entity (the financial institution) caused a data breach by using an insecure password easily guessed and the lapse exploited by a threat actor, the cloud vendor could not be responsible for the data breach, as it is the regulated entity's responsibility to ensure that their employees secure their accounts with strong passwords.
- It is the responsibility of the cloud vendor to provide the ability to ensure strong passwords, e.g., the cloud system could be designed to allow the cloud user to "switch on" the ability to demand that all cloud system users must have two-factor authentication password verification, and/or change passwords every few months, etc. However, it is NOT the responsibility of the vendor to ensure that the cloud user (the regulated entity) exercises this option—the regulated entity could choose to switch off this feature, or modify it to a less secure setting.

[29] Government of Singapore, Government Gazette. 2018. Singapore Cybersecurity Act. https://sso.agc.gov.sg/Acts-Supp/9-2018/.
[30] Government of Malaysia, National Cyber Security Agency. 2021. Malaysian Cyber Laws. https://www.nacsa.gov.my/legal.php.
[31] Japanese Law Transaction. The Basic Act on Cybersecurity. http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01.

Therefore, it is critical for regulated entities to define vendor and client roles and responsibilities when using cloud computing services.

Please refer to checklist statement in Appendix under shared responsibility model (3.1.1).

Figure 5: Shared Responsibility Model


Regulated Entity
Responsibility for security “in” the Cloud
Customer Data
Platform, Application, Identity and Access Management
Operating System, Network, and Firewall Configuration
Client-side Data Encryption and Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Networking Traffic Protection (Encryption, Integrity, Identity)
Cloud Vendor
Responsibility for security “of” the Cloud
Software
Compute
Storage
Database
Networking
Hardware/Infrastructure
Regions
Availability Zones
Edge Locations

Source: Amazon Web Services. Shared Responsibility Model. https://aws.amazon.com/compliance/shared-responsibility-model/.

Security and Assurance Mechanisms

Security and assurance mechanisms are established through multiple means. As mentioned in the previous section, international standards and certification mechanisms provide auditors with reliable documentary attestations, and regulators should recognize and allow use of international standards in an audit.

Recognizing international standards and certifications will also allow regulators the flexibility to develop a graduated approach toward security controls.

- For example, the Bank of England’s Prudential Regulatory Authority has established a list of 16 banks considered “other systemically important institutions” that are more tightly supervised.[32] At the same time, the United Kingdom’s Financial Conduct Authority has established a regulatory sandbox[33] where businesses can test financial business innovations without being held to the same supervisory standards as other systemically important institutions.

[32] Bank of England Prudential Regulation Authority. 2017. *2017 list of UK firms designated as other systemically important institutions).* https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/crd-iv/2017-list-of-uk-firms-designated-as-osiis.pdf.

[33] Financial Conduct Authority. Applying to the Regulatory Sandbox. https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application.

- The Philippines' BSP classifies its regulated entities under different IT profiles: complex, moderate, or simple, as established by Circular No. 982 Enhanced Guidelines on Information Security Management.[34] The central bank expects regulated entities to have information security controls commensurate with its operations and its IT profile, expecting complex profiles to implement more advanced security control measures.

Security standards therefore allow regulators to allow regulated entities to tailor their security measures to best suit their business objectives, and to match their information security controls to the criticality of the service. To provide regulators guidance on common globally recognized standards, examples follow.

System-Wide Technology Frameworks and Standards

ISO 31000: 2018 Risk Management—Guidelines

ISO 31000[35] establishes an overall framework by which risk management and assessments may be carried out. The framework builds the risk assessment approach from its objectives—value creation and protection—to the leadership and their commitment in implementing the framework, to ensuring the scope, context, and criteria of all risks are assessed and treatments described, including monitoring and review.

National Institute of Standards and Technology Cybersecurity Framework

The full name of the NIST Cybersecurity Framework is the *Framework for Improving Critical Infrastructure Cybersecurity v1.1.*[36] It establishes five functions which should be defined when establishing a cybersecurity approach: identify, protect, detect, respond, recover (Figure 6).

ISO/IEC 27000 Standard Series—Information Security

The ISO/IEC 27000 series[37] contains information security standards designed to assure the security of data or information entrusted to internal stakeholders or third parties.[38] Specifically, the 27000 series contains the following standards relevant to cloud services:

- ISO 27001—Information Security Management System Requirements, which concerns requirements to create and maintain an information security management system and address possible security risks.[39]
- ISO 27017—Code of Practice for Information Security Controls for Cloud Services, which deals specifically with security techniques and controls related to cloud services.[40]
- ISO 27018—Code of Practice for Protection of Personally Identifiable information in Public Clouds Acting as Personally Identifiable Information Processors, which contains requirements for protecting personal data on the cloud (footnote 23).

[34] Bangko Sentral ng Pilipinas. 2017. *Circular No. 982 Enhanced Guidelines on Information Security Management*. 9 November. https://www.bsp.gov.ph/Regulations/Issuances/2017/c982.pdf.

[35] International Organization for Standardization. ISO 31000:2018(en) Risk management - Guidelines https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

[36] National Institute of Standards and Technology. Cybersecurity Framework. https://www.nist.gov/cyberframework.

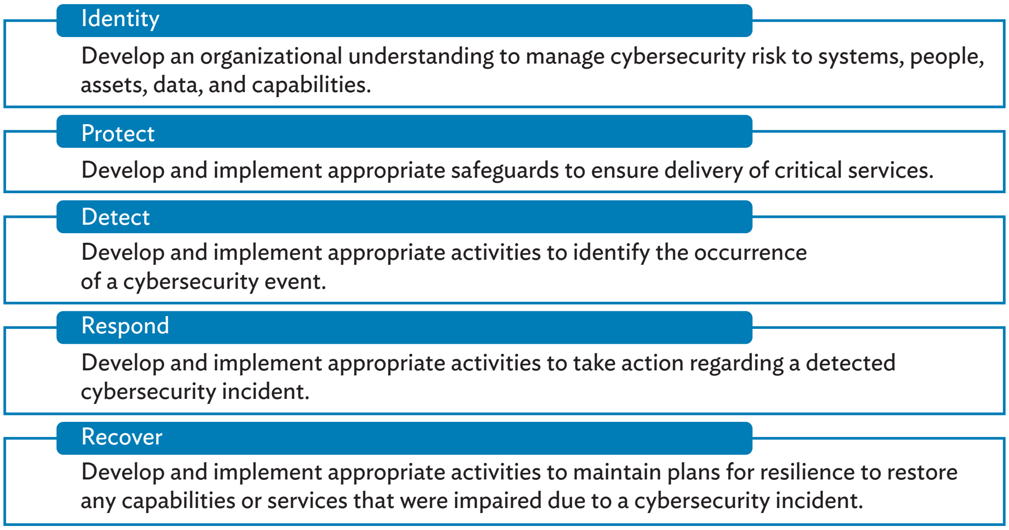
[37] B. Lewis. 2018. ISO/IEC 27000–Key international standard for Information Security Revised. *ISO News*. 1 March. https://www.iso.org/news/ref2266.html.

[38] International Organization for Standardization. ISO/IEC 27001 Information Security Management. https://www.iso.org/isoiec-27001-information-security.html#ISMS.

[39] International Organization for Standardization. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html.

[40] International Organization for Standardization. ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services https://www.iso.org/standard/43757.html.

Figure 6: National Institute of Standards and Technology Cybersecurity Framework



Identity

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Protect

Develop and implement appropriate safeguards to ensure delivery of critical services.

Detect

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover

Develop and implement appropriate activities to maintain plans for resilience to restore any capabilities or services that were impaired due to a cybersecurity incident.

Source: National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

System and Organization Controls

System and Organization Control (SOC) reports are auditing and control reports intended to help entities determine if service providers have appropriate internal controls (footnote 22). There are three main types, which are governed by the American Institute of Certified Public Accountants:

- SOC 1 examines an entity's financial and accounting controls;
- SOC 2 is focused on IT services and looks at an entity's privacy and security controls, among others, and their effectiveness; and
- SOC 3 helps summarize the entity's IT controls and their effectiveness.

Financial standards

Payment Card Industry Data Security Standards[41]

The Payment Card Industry Data Security Standard (known as PCI DSS) is a card industry standard intended to encompass those involved in payment card processing. The Data Security Standard was formulated to help standardize data protection measures and promote protection of cardholder data through emphasizing network and information security, risk management, and appropriate controls.

[41] PCI Security Standards Council. Document Library. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1613564529450.

ISO 20022-6:2013 Standard for Financial Services—Universal Financial Industry Message Scheme—Part 6: Message Transport Characteristics

ISO 20022[42] is a technical standard that sets up the scope and characteristics for financial institutions to send messages in a way that can be verified independently against operational messaging. It includes specific protocols for sending, receiving, securing, and tracking messages sent and received by financial institutions.

Other Standards and Frameworks

Data protection and privacy

Authorities will need to ensure that regulated entities are adhering to any data protection and privacy regulations. Regulators may need to update financial regulations if they repeat or conflict with data protection and privacy regulations. Authorities may also need to establish additional compliance requirements, such as checking for compliance and certification to the European Union's *General Data Protection Regulation (GDPR)*[43] or to *Asia-Pacific Economic Cooperation (APEC)'s Cross-Border Privacy Rules (CBPR) system.*[44] Data protection and privacy are covered in the following section.

Cloud Controls Matrix by the Cloud Security Alliance

The alliance, an industry association for cloud security, has developed a cybersecurity control framework which has control specifications against 17 domains: [45]

1. Audit and assurance
2. Application and interface security
3. Business continuity management and operational resilience
4. Change control and configuration management
5. Cryptography, encryption, and key management
6. Data center security
7. Data security and privacy lifecycle management
8. Governance, risk, and compliance
9. Human resources
10. Identity and access management
11. Interoperability and portability
12. Infrastructure and virtualization security
13. Logging and monitoring
14. Security incident management—e-discovery and cloud forensics
15. Supply chain management, transparency, and accountability
16. Threat and vulnerability management
17. Universal endpoint management

Please refer to checklist statement in Appendix under security and assurance mechanisms (3.2.1 to 3.2.2).

[42] International Organization for Standardization. ISO/IEC 27001 Information Security. https://www.iso.org/obp/ui/#iso:std:iso:20022:-6:ed-2:v1:en.

[43] Eur-Lex. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[44] Asia-Pacific Economic Cooperation. *What is the Cross-Border Privacy Rules System?* https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

[45] Cloud Security Alliance. *Cloud Controls Matrix and CAAIQ v4.* https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

Data Resilience

A common question among regulators when regulating a cloud-based financial system is how to secure the stability of the system in case of disaster, such as an earthquake, a severe storm, a power outage, or some other major disruption. One key benefit of cloud systems is that they can provide IT resources that ensure "data redundancy" in which a copy of all information system data exists as a backup for emergency. This increases banking system resilience so there is no single point of failure for critical items.

The Institute of International Finance recommends that regulated entities should have operational resilience plans in place in case of disruption.[46] Regulated entities with cloud arrangements would have risk mitigation solutions such as data portability and data redundancy requirements as part of their agreement with their cloud vendors, requiring that their vendors are able to achieve specific benchmarks for lost data (recovery point objective) as well as ensuring minimum downtime and disruption (recovery time objective).

Regulators may address this using non-mandatory guidelines. For example:

- The *MAS Guidelines on Outsourcing* recommends safeguards in case the regulated entity wishes to terminate the service or the service provider undergoes a change in ownership, becomes insolvent, goes into liquidation, or for other reasons is unable to perform the contracted service (footnote 16).
- The Philippines BSP addresses Cyber Resilience in section 3.6.3 of *Circular No. 982 Enhanced Guidelines on Information Security Management* (footnote 34). This establishes that regulated entities have business continuity planning and institute adequate cyber resilience capabilities, including a business impact analysis, defensive strategies, and recovery arrangements.

Section 7 details business continuity and disaster recovery plans.

[46] Institute of International Finance. 2019. *CSPS and Criticality: Potential Treatments and Solutions*. https://www.iif.com/Portals/0/Files/content/Innovation/09042019_csps.pdf.

5 Data Protection and Privacy

Because of the rapid development of personal data and privacy regulation many markets have personal data or privacy legislation implemented by national data protection agencies. Regulated entities should be made aware that they are subject to these regulations, and financial regulators should ensure there is no duplication and/or regulatory conflicts.

Data protection and privacy are interconnected concepts that concern the authorization of access to personal information. Data privacy is an individual's right to some control over how personal information is collected and used;[47] data protection is an entity's responsibility to apply safeguards in the collection, storage, usage, and disclosure of personal information.[48] In practice, the terms are often used interchangeably and take on different meanings depending on jurisdiction or sector.

Regardless of interpretation or in some cases absence of personal data and privacy law, regulators agree that adequate and effective policies, procedures, and controls to safeguard customer data from unauthorized access or accidental access, processing, use, erasure, or loss is essential for the stability and reputation of the financial services industry.

Please refer to checklist statement in Appendix under data protection and privacy (4.0.1 to 4.0.8).

Control versus Processing of Data

In the context of cloud outsourcing, and understanding the shared responsibility model, regulators and regulated entities must understand that the roles of data control and data processing differ distinctly.

- A **data controller** is an entity that makes decisions on how and why the data is processed—in this case it is the **regulated entity**. The data controller, being the entity with access and control over the data, is therefore typically responsible for protecting the specific data under its control and authorizes the data processor to process the data on its behalf.
- A **data processor** is an entity that processes the data at the instruction of the data controller—in this case this would be the **cloud service provider**. The data controller is responsible for implementing appropriate technical and organizational measures to protect the personal data under its control against accidental or unlawful destruction, accidental loss, alteration, and unauthorized disclosure or access.

[47] International Association of Privacy Professionals. What is privacy? https://iapp.org/about/what-is-privacy/.

[48] International Association of Privacy Professionals. Glossary of Privacy Terms. https://iapp.org/resources/glossary/.

The data processor typically has overarching responsibilities in protecting data (including protection from breach of their systems), particularly for protecting its network and infrastructure, and ensuring the contractually specified reliability of its systems and availability of data it processes. Unless it is contractually assigned other roles by the data controller, it has less or no control over access to or use of their customer's data.

In fact, many regulators and regulations require that regulated entities retain full control over their data, for example, by stipulating that cloud contracts and other service level agreements related to provisioning of cloud services clearly provide that any data migrated to the cloud remains the property of the contracting regulated entity, regardless of who owns, manages, or operates the cloud. This ensures that regulated entities retain rights of data access, retrieval, modification, and deletion regardless of the physical location of the data. For example:

- The Cloud Computing information leaflet from Hong Kong, China's Privacy Commissioner for Personal Data clarifies that data users (or data controllers) are ultimately responsible for personal data collected and held by them, and outsourcing of any processing or storage of personal data does not relieve them of this responsibility.[49]
- Bank Negara Malaysia's *Risk Management in Technology 2020* document states that financial institutions must implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorized disclosure and access. It specifies that this includes retaining ownership, control, and management of all data pertaining to customer and counterparty information, proprietary data, and services hosted on the cloud, including the relevant cryptographic keys management.[50]

Please see checklist in Appendix, under control versus processing of data (4.1.1 to 4.1.4).

Cross-Border Data Transfers

To support international trade and payments, financial information, and data must be able to be transferred across borders. International data transfers are possible with credit card systems such as Visa and Mastercard, SWIFT, PayPal, and a host of other payment and settlement mechanisms. However, the added dimension of personal data has led to two approaches by which regulators may understand cross-border data transfers in the financial sector: with technical standards, and via methods of protecting consumer personal data.

Technical Standards for Cross-Border Data Transfers

Transferring data across borders safely, securely, and accurately may be enabled through international standards, such as *ISO 20022-6:2013 standard for Financial services—Universal financial industry message scheme—Part 6: Message transport characteristics,*[51] *ISO 9362:2014 Banking telecommunication messages—Business identifier code,*[52]

[49] Office of the Privacy Commissioner for Personal Data Hong Kong. *Cloud Computing.* https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf.

[50] Bank Negara Malaysia. Risk Management in Technology. https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078.

[51] International Organization for Standardization. ISO 20022-6:2013(en) Financial services — Universal financial industry message scheme — Part 6: Message transport characteristics. https://www.iso.org/obp/ui/#iso:std:iso:20022:-6:ed-2:v1:en.

[52] International Organization for Standardization. ISO 9362:2014 Banking — Banking telecommunication messages — Business identifier code (BIC). https://www.iso.org/standard/60390.html.

ISO 17442:2019 Legal entity identifier,[53] and *ISO 15022-2:1999 Securities Scheme for messages (Data Field Dictionary) Part 2: Maintenance of the Data Field Dictionary and Catalogue of Messages.*[54]

These international standards increase efficiency in transmitting data between financial institutions across borders and jurisdictions.

Protection of Consumer Data

The other aspect of cross-border data flows is how to enable the protection of consumer data as it moves from one jurisdiction to the next. For information to be transferred across borders securely, jurisdictions usually have to recognize each other's data privacy and protection regimes.

Absent domestic privacy or data protection law, compliance with international standards for data protection such as the European Union's GDPR (footnote 45), APEC's CBPR system (footnote 44), are being widely accepted by governments and businesses as best practice for achieving data protection and privacy objectives. These may be augmented with other regional frameworks and guidelines such as the Organisation for Economic Co-Operation and Development's (OECD) *Privacy Framework 2013,*[55] and the Association of Southeast Asian Nations (ASEAN) *Framework on Data Protection 2016.*[56] Technical standards are a good objective reference as well, such as the *ISO/IEC 27018 code of practice for protection of personally identifiable information in public clouds acting as personally identifiable information processors* (footnote 23).

EU General Data Protection Regulation

The EU GDPR (footnote 43), a regional data protection law created to standardize data protection regulations across the EU, has had wide-ranging impact because it applies to entities which may collect data of EU citizens, even if they may not be located in the EU. It has also been recognized as a best practice for helping solidify important concepts in data protection such as the distinction between data controller and data processor, and establishing key principles, rights, and criteria that have been adopted by other markets.

APEC Cross-Border Privacy Rules System

The *CBPR*[57] is a regional privacy system based on the *APEC Privacy Framework*, which aims to facilitate cross border data flows by assuring members have data privacy regulations consistent with the framework in place. Nine economies are part of the APEC CBPR system: Australia; Canada; Japan; the Republic of Korea; Mexico; the Philippines; Singapore; Taipei,China; and the United States.

OECD Privacy Framework 2013

The *OECD Privacy Framework* includes eight principles governing the protection of privacy and transborder flows of personal data: (i) collection limitation, (ii) data quality, (iii) purpose specification, (iv) use limitation, (v) security safeguards, (vi) openness, (vii) individual participation, and (viii) accountability.

[53] International Organization for Standardization. ISO 17442:2019 Financial services — Legal entity identifier (LEI). https://www.iso.org/standard/75998.html.

[54] International Organization for Standardization. (1999.) ISO 15022-2:1999 Securities — Scheme for messages (Data Field Dictionary) — Part 2: Maintenance of the Data Field Dictionary and Catalogue of Messages. https://www.iso.org/standard/28373.html.

[55] Organisation for Economic Co-Operation and Development. 2013. *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[56] ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN). *Framework on Personal Data Protection.* https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf.

[57] Cross-Border Privacy Rules System. (n.d.) http://cbprs.org/.

ASEAN Framework on Data Protection 2016

The framework (footnote 56) proposes a non-binding approach toward seven principles of data protection: (i) consent, notification, and purpose; (ii) accuracy of personal data; (iii) security safeguards; (iv) access and correction; (v) transfers to another country or territory; (vi) retention; and (vii) accountability.

Please see checklist in Appendix, under cross-border data transfers (4.2.1).

Data Localization

Data localization reflects the incorrect perception that for a regulator to have oversight and access to data, it must be stored within the jurisdiction of the regulator. However, this perception overlooks the reality that so long as the regulated entity is registered under the regulator's jurisdiction, the regulator has access to and oversight over that regulated entity's data. This is consistent with existing practices where a regulated entity is not using cloud services.

In fact, rather than serving the objectives of greater data protection and regulatory oversight, data localization requirements might undermine such an objective. For example, a regulated entity whose data storage and backup systems are stored in the same geographic area risks both its operational data system and the redundant system being disabled by a natural disaster. As many large cloud service providers have redundancy zones across the world, the use of cloud computing helps mitigate against geographic concentration risk, and any regulatory requirement to localize data would reduce the resiliency of a cloud-based financial system.

A common approach is for financial regulators to require data controllers to only enable data transfers between jurisdictions that have data protection standards similar to the domestic jurisdiction. For example:

- Bank Negara Malaysia stipulates that regulated entities must ensure that service providers storing or processing data outside Malaysia are subject to data protection standards comparable to Malaysia's. At the very least, the jurisdictions where the regulated entity's data is stored or processed must have a national legal or regulatory framework governing data protection.[58]
- The BSP similarly allows regulated entities to engage in offshore outsourcing only when the service provider operates in jurisdictions that uphold confidentiality (footnote 9).

Please see checklist in Appendix, under data localization (4.3.1 to 4.3.2).

Data Life Cycle

Data is not a static construct, and as data is collected and processed by regulated entities, there will be different data protection considerations at different points of its life cycle. Financial regulators should have a clear understanding of the typical stages in a data lifecycle and ensure that data protection policies and processes that are aligned with the various stages of the data lifecycle. This will enable regulators and financial institutions to more comprehensively understand how data protection objectives can be achieved when using cloud services to store and process personal data.

[58] Bank Negara Malaysia. 2019. *Outsourcing*. https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323.

The table below reviews the typical stages of a data life cycle and data protection considerations at each stage:

Data Life Cycle and Data Protection Considerations

Data life cycle stage	Data protection considerations
Collecting personal data	The financial institution/regulated entity may need to notify and/or obtain consent from the individual or data subject on the purposes for which it collects, uses or discloses the personal data.
Using and disclosing personal data	The financial institution/regulated entity must ensure that it only uses and discloses personal data for permitted purposes. The financial institution/regulated entity may need to inform the individual (data subject) of the cloud service providers it uses.
Offshoring personal data	The financial institution/regulated entity should be aware of whether it is required to disclose to individuals the locations in which it stores or processes their personal data and, if required, obtain consent for the storing and/or processing of their data in that location. To do this, the financial institution/regulated entity should know the location in which the cloud service provider will store and/or process its data and ensure that conditions for cross-border data transfer—for example of comparable data protection—are met.
Securing personal data	The financial institution/regulated entity should be familiar with the security of the cloud environment it uses, by referencing the security measures that are built into cloud infrastructure, platforms, and services. The financial institution/regulated entity should ensure that they use the appropriate security configurations to protect personal data.
Accessing and correcting personal data	If data subjects (i.e., consumers) have the right to access and correct personal data, the financial institution/regulated entity should ensure that they are able to provide data subjects with the ability to access and correct their personal data. Since it is the financial institution/regulated entity and not the cloud service provider which has a relationship with the data subject and control over the personal data stored in the cloud, the financial institution/regulated entity should understand that the cloud service provider is unable to grant this access to individuals.
Maintaining the quality of personal data	The financial institution/regulated entity must take steps to ensure that the accuracy and integrity of personal data is maintained, which may require it to correct and update personal data stored on the cloud. The financial institution/regulated entity should ensure that cloud service providers provide reasonable assurance that data integrity is maintained through transmission, storage, and processing.
Deleting or de-identifying personal data	The financial institution/regulated entity must ensure that personal data is not kept for a longer time period than is required for the purposes by which it was collected, and is only retained in accordance with relevant data retention laws. The financial institution/regulated entity should keep track of when it needs to delete or anonymize the personal data, and should ensure that the cloud service provider it contracts provides it with the controls to delete its content as required.

Source: Amazon Web Services. 2018. *Using AWS in the Context of Data Protection Considerations.* https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf?secd_dp3.

The checklist we would recommend is in Appendix, under data life cycle (4.4.1).

Law Enforcement Requests and Legal Requests for Information

With the move to cloud, a number of regulators are requiring data to be localized, misunderstanding that enforcement decisions will not be valid with the use of cloud. However, rather than requiring data localization, regulators should ensure clarity around law enforcement requests, such as ensuring enforcement requests are legally valid, such as in the form of a court order, warrant, and/or subpoena. In addition, regulators should ensure sufficient coordination, consistency, and transparency in the legal methods and processes used for law enforcement access to data.

Other processes can also be established clearly with standard operating processes and procedures developed for information requests from the regulator, or from other law enforcement agencies, and under which provisions, such as local data protection laws, request for information laws, or from international mutual legal assistance treaties.

In some cases, a lawful request might be issued to service providers requiring them to disclose end user customer information to comply with a legally valid order, for example, where data may be sought from a data processor for expedience in an emergency situation. It is important for law enforcement provisions to set out these conditions without imposing requirements that might weaken the security of the cloud service provider.

Authorities must also understand that the outsourced service providers will not have access to data which may be encrypted by the regulated entity (their client using the cloud service). Therefore, it is generally more effective for requests for access to or monitoring of data to be directed to the data controller, instead of directly seeking access from the service provider, which may only be a data processor.

Please see checklist in Appendix, under law enforcement requests and legal requests for information (4.5.1 to 4.5.2).

6 Data Governance, Retention, and Exit Strategy

A wide range of data may be stored and processed by cloud service providers in an outsourcing arrangement, and there is no one-size-fits-all strategy for the various aspects of data governance such as data security, protection, and retention. Regulators should understand that different levels of data governance controls may be put in place depending on audit objectives.

Data Governance and Data Classification

Per the shared responsibility model, cloud providers will offer a variety of security controls, protections, and other features, but it is the responsibility of the regulated entity to ensure that these functions are activated and that the data is appropriately classified so that the relevant controls will apply. This is typically done through a data classification framework which usually categorizes data based on its sensitivity.

- For example, the Philippines's Cloud First Policy[59] maps out a four-tier data classification taxonomy for government data:
    - non-sensitive data which can be stored or processed on accredited public cloud;
    - sensitive data which can be stored on accredited public cloud, with encryption requirements;
    - above-sensitive data which can be stored or processed on in-country accredited public cloud, with encryption requirements; and
    - highly sensitive data which can be stored in an on-premise private cloud.
- The Australian Prudential Regulation Authority's *Prudential Practice Guide CPG 234 on Information Security*[60] takes a broader approach toward the classification of information assets, and provides guidelines by which regulated entities may maintain and implement a classification methodology for information assets, such as on a granular/individual, or an aggregated (grouped) level.

Regulators should keep in mind, however, that data governance and classification should not be prescribed; they should be determined by the regulated entity based on their specific needs. In addition, the decision to deploy public or private clouds, and other details of the cloud outsourcing arrangement such as the location of data storage and/or processing, should also be left to the regulated entity. As addressed in previous sections, data location is not a determinant of the level of data protection; instead, it will rely on the control mechanisms in place.

[59] Government of the Philippines, Department of Information and Communications Technology. 2020. Philippines. Circular No 10 Amendments to Department Circular No. 2017-002 Re: Prescribing the Philippine Government's Cloud First Policy. 2 June. https://dict.gov.ph/wp-content/uploads/2020/06/Department_Circular_No_10_Amendments_to_DC_No_2017_002_re_Prescribing.pdf.

[60] Australian Prudential Regulation Authority. 2019. CPG 234 *Information Security Prudential Practice Guide*. June. https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf.

The key takeaway for both regulators and regulated entities is that having a clear framework for data classification will help ensure that data is appropriately protected according to its category or tier. Notably, institutions should avoid over-classification and having too many tiers, as this could conversely confuse the process and make it more difficult for a regulated entity to effectively apply the necessary data protections.

Please see checklist in Appendix, under data governance and data classification (5.1.1).

Data Retention Strategy

Having a clear data classification framework will help regulated entities develop and apply retention strategies related to each data category. Regulators may mandate a retention period for certain data such as regulatory records, though the period and other requirements will vary from jurisdiction to jurisdiction.

- For example, some jurisdictions may require that audit logs be maintained on certain regulatory records. The Hong Kong Monetary Authority requires that audit logs and investigation data relating to consumer credit data be kept for at least 2 years, and in a format which would facilitate compliance reviews and audits.[61]
- Other jurisdictions may require that data be retained in a "write once, read many" storage format so that data is immutable and cannot be deleted or tampered with, such as in the case of the US Securities and Exchange Commission Rule 17a-4(f).[62]

Having clear data classification would also allow regulators to clearly differentiate the party responsible for complying with data retention regulations. In a cloud outsourcing arrangement, financial regulators should ensure regulated entities understand that the responsibility to meet data retention requirements lies with them as data controller, and not their cloud provider. Per the shared responsibility model, cloud providers as vendors are only responsible for providing the contracted service to regulated entities, e.g., data processing, but they cannot maintain or manipulate data beyond the controls put in place by the regulated entity, including retaining data or records beyond contractually stipulated periods.

Regulators may also wish to highlight to regulated entities that they may need to address and/or make contingencies to comply with regulated data retention periods, either within their outsourcing agreements with their cloud providers or through other available means.

For example, for the regulated entity, this could mean that if a contract is for a duration shorter than a mandated retention period, the regulated entity is responsible for ensuring arrangements with their cloud provider that the data will return to them upon the end of the contract, and that the regulated entity will then be responsible for maintaining the data for the data retention time period.

Please see checklist in Appendix, under data retention strategy (5.2.1 to 5.2.2).

[61] Hong Kong Monetary Authority. 2018. *Supervisory Policy Manual IC-6 The Sharing and Use of Consumer Credit Data through a Credit Reference Agency.* https://www.hkma.gov.hk/media/eng/img/key-functions/banking-stability/supervisory-policy-manual/IC-6.pdf.

[62] Securities and Exchange Commission. 1997. *Reporting Requirements for Brokers or Dealers under the Securities Exchange Act of 1934.* https://www.sec.gov/rules/final/34-38245.txt.

Exit Strategy and Termination

Exit strategies are important to allow regulated entities with cloud outsourcing arrangements to maintain operational resiliency, and to ensure that regulatory requirements are being met even when an institution changes outsourcing providers. As a general matter, termination provisions between regulated entities or financial institutions and cloud providers are contractual terms, and should not be defined in regulation. However, regulators may consider releasing non-mandatory guidance documentation to support regulated entities in their outsourcing arrangements, to ensure smooth transitions in exit strategies. The following is a non-exhaustive list of key items which the regulators could ensure their regulated entities have made exit provisions for.

Early Termination

Regulated entities should have exit strategies planning what happens to the service if either party would like to terminate the contract early, or what happens in case of unexpected exits, such as instances where a cloud service provider suddenly ceases business operations and is unable to offer services.

Data Ownership

Regulated entities should know which party (the regulated entity or the cloud vendor) is responsible for and owns the data at which point of the data life cycle (see previous section).

Data Retention

Regulated entities should ensure that records are still being maintained and under their responsibility following the termination of an outsourcing contract.

Data Portability and Migration Policies, Transitional Support

Regulated entities should ensure provisions for allowing data to be migrated from one cloud vendor to another. This could include contractually require transitional assistance from the outgoing cloud provider, including time periods for transitional support, continued maintenance of regulatory records, etc.

Depending on the classification type and sensitivity of data stored with the cloud vendor, regulated entities may also want to consider interoperability policies that allow digital systems to interconnect with other local and international systems, such as those of other cloud providers. For example:

- ensuring that documentation use eXtensible Business Reporting Language, which is a standard uniform format for communicating business and financial information;[63]
- ensuring that the cloud architecture design is being built on technology which allows for faster “lift and shift” rehosting of data migration approaches;[64] or
- designing cloud architecture for a hybrid or multi-cloud policy which enables the regulated entity to use multiple cloud services, which will mitigate organizational concentration risk.

Please see checklist in Appendix, under exit strategy and termination (5.3.1 to 5.3.4).

[63] Financial Accounting Standards Board. About XBRL eXtensible Business Reporting Language. https://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176157087972.

[64] XenonStack. Refactor vs Lift and Shift vs Containers - Who’s the Best? https://www.xenonstack.com/insights/refactor-vs-lift-and-shift/.

7 Business Continuity and Disaster Recovery Planning

A business continuity plan is a series of protocols designed to ensure that the regulated entity can continue its essential operations during a disruptive event or a disaster.[65] Regulators usually require that IT outsourcing activities, including the use of cloud services, are addressed in its business continuity plan. Some regulators make a distinction between critical and non-critical services, whereby the development of contingency plans is only required for critical services. More commonly, regulated entities are required to develop business continuity plans that are commensurate with the criticality and complexity of their outsourcing arrangements.

Disaster recovery is a sub-set of business continuity planning, and refers more specifically to the process required for the regulated entity to recover from a disruptive event and minimize the impact of that event on the regulated entity. It most often pertains to recovery from the failure of IT systems, such as by restoring lost data.

Benefits of the Cloud: Increased Operational Resilience

A key consideration in business continuity and disaster recovery planning is whether the need for constant IT services availability is balanced against the cost of purchasing and provisioning automatic fail-overs and redundant systems. Compared to traditional business continuity and disaster recovery investment practices, which involve investing in duplicate and purpose-specific, off-site data and IT infrastructure, cloud providers often operate at a scale that allows them to provision business continuity and disaster recovery resources at greater cost-effectiveness.

- For example, data may be redundantly stored in multiple cloud service provider data center facilities in various geographic locations to reduce the likelihood of failure and ensure highly durable storage for mission-critical data that can be recovered quickly and reliably.
- Other arrangements cloud providers may offer include the utilization of frequent server instance backups and failover switches that automatically provision redundant resources if a network resource fails.

This strengthens the regulated entity's resilience and business continuity and disaster recovery capabilities since moving to cloud will allow it to engage and deploy more business continuity and disaster recovery resources at lower cost.

Please see checklist in Appendix, under benefits of the cloud: increased operational resilience (6.1.1 to 6.1.7).

[65] Regulated entities may also have a broader business continuity plan for their organization, following the ISO 22301:2019 standard for security and resilience for business continuity management systems. International Organization for Standardization. ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en.

Setting Business Continuity and Disaster Recovery Requirements: Criticality and Materiality

During business continuity and disaster recovery planning, regulated entities typically decide on an acceptable recovery time objective, or the time it takes after disruption for restoring business processes to the service level defined by the service level agreement, and a recovery point objective, or the acceptable amount of data loss measured in time. These are determined based on the financial impact that the system downtime or unavailability would have on the regulated entity. It is unlikely for all business functions to share the same recovery time objective and/or recovery point objective.

Regulators should note that effective business continuity plans are ones which assign recovery time objectives and recovery point objectives commensurate with the materiality or criticality of the outsourcing arrangement. For example, the regulated entity will need to resume critical business functions quicker than non-critical ones, and assigning recovery time objectives without taking into account the difference in criticality of business functions can lead to scarce resources being inappropriately diverted to less critical activities, which can in turn compromise the regulated entity's reputation and business stability.[66]

The business continuity and disaster recovery plan should not only include procedures to recover systems from various disaster scenarios, but also the roles and responsibilities of relevant personnel in the recovery process. When outsourcing to cloud, the regulated entity should clearly delineate the roles and responsibilities of between themselves and their cloud service provider and, where necessary, define its recovery point objective and recovery time objective expectations in the outsourcing agreement. This will ensure that in the case of an operational disruption or failure on the service provider's part, the outsourced activities can still continue to be performed in a way that meets the regulated entity's needs.

Please see checklist in Appendix, under setting business continuity and disaster recovery requirements: criticality and materiality (6.2.1 to 6.2.2.4).

Business Continuity and Disaster Recovery Testing

In recovery planning, regulators need to ensure their regulated entities are able to test the robustness of their business continuity and disaster recovery plans, becoming familiar with their cloud provider's business continuity and disaster recovery plans and capabilities, and understand the recovery steps and coordination required for disaster recovery. Business continuity and disaster recovery testing is a core part of developing an effective business continuity and disaster recovery strategy as it allows the regulated entity to simulate the steps and process required in a disaster scenario. Testing helps the regulated entity ensure that it has the right business continuity and disaster recovery procedures in place and verify the capabilities of its personnel and their cloud provider in executing these procedures.

Please see checklist in Appendix, under business continuity and disaster recovery testing (6.3.1 to 6.3.2).

[66] Monetary Authority of Singapore. 2003. Business Continuity Management Guidelines. June. https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/securities_futures/sub_legislation/BCMGuidelines.pdf.

Addressing Interdependency Risk

A regulated entity's operations may be deeply connected and highly dependent on external service providers. Where the level of interdependency is high, regulators could encourage regulated entities to reduce interdependency risks by identifying viable alternatives for resuming operations that do not incur prohibitive costs (footnote 16). It is necessary for the business continuity and disaster recovery plan to indicate whether the regulated entity will use another service provider, or bring a critical business activity back in-house in the event of provider failure, or a technology update which requires a system rollback. The plan should consider the costs, time, and resources that would be involved, and ensure that the roles and responsibility for the procedures around availability, data backup and software configuration, incident response, recovery, etc., should be clearly defined and understood.

Please see checklist in Appendix, under addressing interdependency risk (6.4.1 to 6.4.9.16).

8 Incident Response Requirements and Processes

An IT incident occurs when there is an unexpected disruption to the delivery of IT services or a security breach of an IT system, which compromises or has the risk of compromising the confidentiality, integrity, and availability of data or the IT system. Incidence response and event logging is a critical component of disaster response that minimizes the risk of damage caused by service outages and security breaches.

To minimize impact on the financial institution's business and customers, regulators should ensure that regulated entities establish an incident management framework covering the process and procedure for handling IT incidents, and the roles and responsibilities of staff and service providers in monitoring, recording, analyzing, reporting, and resolving incidents (footnote 1).

Defining Clear and Reasonable Thresholds for Incident Notification Requirements

The implementation of an incident notification requirement puts in place a mechanism whereby the regulated entity is required to inform the regulator and the affected individuals and/or organizations when an IT incident has resulted in a data breach and/or prolonged service failure. Establishing such a requirement can help mitigate the impact of the incident and ensure that adequate steps are taken to address the issue.

However, it is important to ensure that the incident notification system enables authorities to analyze the conditions under which the incident occurred in a transparent and fair manner, and that the conditions under which an incident is required to be reported are clearly laid out. For example:

- In Indonesia, where critical events such as misuse or crime have caused or are expected to cause significant financial losses or business disruption, commercial banks are required to submit incidental reports to the Financial Services Authority within 7 days of the critical event.[67]
- Singapore's Personal Data Protection Commission requires notification within 72 hours of when the organization made the assessment that a data breach was likely to result in significant harm or impact/affect more than 500 individuals.[68]

[67] Oritas Jasa Keuangan Republik Indonesia. 2016. *Implementation of Risk Management in the Use of Information Technology by Commercial Banks / Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Infomasi Oleh Bank Umum.* http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20 MRTI.pdf.

[68] Personal Data Protection Commission Singapore. 2019. *An Introduction to Managing Data Breaches 2.0*. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Data-Breach-Management/Introduction-to-Managing-Data-Breaches-2-0.pdf?la=en.

A clear process for incident reporting, such as the reporting format, template, information, timeframe, and reporting agency should also be established to reduce uncertainty. Without establishing a clear incident notification threshold, or when threshold definitions are too ambiguous and easily triggered, notification requirements can instead result in over-notification, which can reduce the effectiveness of the mechanism and increase compliance costs for financial institutions.

Please see checklist in Appendix, under defining clear and reasonable thresholds for incident notification requirements (7.1.1 to 7.1.19).

9 Standards, Certifications, and Global Best Practices

Beyond the technological standards and certification systems addressed so far, regulators should be aware of other standards and certifications specific to information system audits, which regulators may wish to have their audit staff be trained and accredited in. Having staff trained and professionally accredited as internal auditors will help strengthen the regulator's ability to check and maintain the strength, stability, and resilience of the modern cloud-based financial system.

International Organization for Standardization 9001—Quality Management Systems

International Organization for Standardization (ISO) 9001 is a general standard meant to ensure an entity has quality management in place to meet customer and any legal or regulatory expectations, regardless of sector or business type.[69] The ISO 9001 standards can be used in conjunction with other ISO standards to train and certify internal auditors.[70]

Information Systems Audit and Control Association–Certified Information Systems Auditor

The Certified information systems auditor is a certification from the Information Systems Audit and Control Association, an IT professional association, intended to demonstrate competency in information security auditing, oversight, and controls.[71] Having staff certified as information systems auditors will allow them to grow professionally in information security auditing and ensure they engage in continuing professional education to maintain certification and credentials.

[69] ISO. ISO 9001:2015 Quality management systems - Requirements https://www.iso.org/standard/62085.html.

[70] 9001 Simplified. What You Should Know About ISO 9001 Internal Audits. https://www.9001simplified.com/learn/know-about-iso-9001-audit.php.

[71] Information Systems Audit and Control Association. Certified Information Systems Auditor (CISA) Credentialling. https://www.isaca.org/credentialing/cisa.

Information Systems Audit and Control Association–Certified Information Security Manager

The Certified information security manager, another certification from the Information Systems Audit and Control Association, demonstrates expertise in information security governance, program development and management, incident management, and risk management. While this is meant more for professionals who manage information security directly, having regulator staff certified as information security managers will allow them to understand the needs of regulated entities on an implementation level, which would greatly help ensure regulatory controls are fit for purpose.

International Information Systems Security Certification Consortium–Certified Information Systems Security Professional

Certified information systems security professional is a cybersecurity certification from the International Information Systems Security Certification Consortium meant to prove an individual's expertise in numerous aspects of IT security, including risk management, network security, and security architecture.[72] Like the certifications for information systems auditor and information security manager, the Certified Information Systems Security Professional credential will increase the capacity of regulatory staff to manage regulated entities' use of cloud technologies.

Please see checklist in Appendix, under standards and certifications, and global best practices (8.4.1 to 8.4.3).

[72] ISC2. Certified Information Systems Security Professional / CISSP – The World's Premier Cybersecurity Certification. https://www.isc2.org/Certifications/CISSP#

APPENDIX
Cloud Audit Toolkit for Financial Regulators—Checklist

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
1. Service provider oversight		
1.1 Cloud computing regulated as risk-based, outsourcing arrangement		
1.1.1 Regulators should establish an outsourcing arrangement or framework that includes cloud computing arrangements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
1.1.2 Regulators should adopt a risk-based supervisory approach toward outsourcing cloud technology services.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
1.1.3 Regulators could develop a non-mandatory practice guide and/or technology risk management framework and/or checklist to guide cloud computing outsourcing. This could include a. roles and responsibilities in managing technology risks; b. identification and prioritization of information system assets; c. identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities; d. implementation of appropriate practices and controls to mitigate risks; and e. periodic update and monitoring of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
1.2 Technology oversight, monitoring and control		
N.A.		
1.3 Recordkeeping		
1.3.1 Regulators should ensure that regulated entities have conducted a risk assessment in identifying, measuring, monitoring, and controlling risks, threats and vulnerabilities brought by adopting cloud computing technologies.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.3.2 Regulators should ensure that for regulated entities, risks of the highest severity are accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.3.3 Regulators should ensure that regulated entities have risk monitoring mechanisms to continuously assess the levels of risk and mitigate the same within appropriate levels.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
1.3.4 Regulators should ensure that the risk assessment process of regulated entities highlights the systems, processes or infrastructure that have the highest risk exposure.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.3.5 Regulators should ensure that the risk assessment process of regulated entities considers IT risk events, regulatory requirements, and audit observations.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.3.6 Regulators should ensure regulated entities have maintained a register of its outsourcing agreements (at minimum material/critical agreements), to facilitate monitoring and reporting of risks, which is updated regularly, and which is made available for internal or external review as applicable.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.4 Qualified oversight groups		
1.4.1 Regulators should ensure that regulated entities have qualified oversight committees/functions on technology outsourcing arrangements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.4.2 Regulators should build their own institutional capacity to formulate outsourcing-related frameworks, regulations, and standards, oversee and supervise technology use and regulated entities' compliance with the regulatory expectations on cloud outsourcing.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
1.5 Responsibilities of the oversight group		
1.5.1 Regulators should ensure that regulated entities' oversight group such as the board of directors and senior management have oversight of technology risks, are fully understand risks associated with IT outsourcing, and are involved in key IT decisions.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.5.2 Regulators should ensure that regulated entities' oversight group such as the board of directors and senior management are fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency, and recoverability.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.5.3 Regulators should ensure that regulated entities provide the oversight committee with relevant information (such as an overall technology risk profile of the organization) including the level of cloud outsourcing risk exposure.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.5.4 Regulators should ensure that regulated entities' oversight group develops and reviews regular monitoring and control reports (including acceptable third-party audits) for its outsourcing agreements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.5.5 Regulators should ensure that regulated entities' oversight group is kept informed and conducts reviews when there are significant changes are made to outsourcing agreements (i.e., pre- and post-implementation and when amendments are made).	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
1.5.6 Regulators should ensure that regulated entities' IT risk control and mitigation approach are periodically reviewed and updated to include plausible and emerging threats.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
1.6 Technology risk identification mechanisms and due diligence		
1.6.1 Regulators should ensure that regulated entities have IT policies, standards, and procedures established and regularly updated to manage technology risks and safeguard information system assets.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.2 Regulators should ensure that regulated entities have analyzed and quantified the potential impact and consequences of risks on overall business and operations, and for each type of risk identified, risk mitigation and control strategies that are consistent with the value of the information system assets and level of risk tolerance are developed and implemented.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.3 Regulators should ensure that regulated entities have given priority to threat and vulnerability pairings with high risk ranking which could cause significant harm or impact to the organization's operations.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.4 Regulators should ensure that regulated entities' risk tolerance for damages and losses is assessed, and costs of risk controls are balanced against the benefits to be derived.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.5 Regulators should ensure that regulated entities' risks are managed and controlled in a manner that will maintain the organization's financial and operational viability and stability.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.6 Regulators should ensure that regulated entities' costs and effectiveness of controls with regard to the risks being mitigated are assessed when deciding on the adoption of alternative controls and security measures.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.6.7 Regulators should ensure that regulated entities' risk processes are reviewed and updated in accordance with changes in IT environment and delivery channels, taking into account changing circumstances and variations in the organization's risk profile.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.7 Due diligence		
1.7.1 Regulators should assess whether a full due diligence was conducted prior to selecting and engaging a cloud service provider, i.e., cloud service provider's capability, reliability, track record, and financial position.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.7.2 Regulators should ensure that regulated entities conduct regular monitoring and evaluation of cloud service providers performance against the service level agreement.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
1.8 Procurement and use of international standards for prequalification/baseline certifications		
1.8.1 Regulators should ensure that regulated entities use and reference international standards, and adopt appropriate encryption controls.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
2. Physical and logical audit and inspection rights		
2.1 Physical and logical separation		
2.1.1 Regulators should not mandate physical audits.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[X] Regulator [ ] Regulated Entity
2.2 Third-party audits		
2.2.1 Regulators should accept, allow, and trust third-party audits as a reporting mechanism.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[X] Regulator [ ] Regulated Entity
2.2.2 Regulators should ensure that regulated entities' internal /IT audit function is independent and objective.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.3 Regulators should ensure that a regulated entity's scope of IT audit is comprehensive and includes all critical IT operations and assessment of critical service providers including cloud service providers.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.4 Regulators should ensure that a regulated entity's IT audit plan, comprising auditable IT areas for the coming year, is developed.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.5 Regulators should ensure that a regulated entity's IT audit plan, and any changes or deviations is/are approved by the organization's Audit Committee.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.6 Regulators should ensure that regulated entities have an audit cycle that determines the frequency of IT audit engagements.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.7 Regulators should ensure that regulated entities implement an effective follow-up process and exception monitoring process.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
2.2.8 Regulators should ensure that regulated entities have an established and structured escalation process to communicate key IT audit issues to the relevant IT and business management units.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
3. Security and cybersecurity requirements		
3.1 Shared responsibility model		
3.1.1 Regulators should ensure that regulated entities define roles and responsibilities in an outsourcing arrangement and articulate responsibilities of all contracting parties.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
3.2 Security and assurance mechanisms		
3.2.1 Regulators should check that the regulated entities have an appropriate compliance function that reviews and verifies observance with IT security standards and procedures (which may be in reference to a mixture of international standards) and obtains certifications that will support the entity's compliance with prescribed security and cybersecurity control.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
3.2.2 The regulator should ensure that the regulated entities have capacity and mechanism(s) (including commissioning or obtaining periodic expert reports on security adequacy) to review and assess their CLOUD SERVICES PROVIDER's compliance with security policies, procedures and controls. Lapses should be monitored and reviewed on a regular basis.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
3.3 Data resilience		
N.A.		
4. Data protection and privacy		
4.0.1 Regulators should ensure that regulated entities are aware they are subject to existing data protection and privacy laws (among other prevailing laws).	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.2 Regulators should ensure that regulated entities put in place measures to protect sensitive or confidential information which are stored and processed in systems deployed in the cloud environment.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.3 Regulators should ensure that regulated entities put in place measures to protect sensitive or confidential information such as customer personal, account, and transaction data which are stored and processed in systems.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.4 Regulators should ensure that regulated entities have a system that ensures customers are properly authenticated before access to online transaction functions and sensitive personal or account information is permitted.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.5 Regulators should ensure that regulated entities have information asset registry and a mechanism to identify and detect and/or prevent unauthorized access, copying or transmission of confidential information.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.6 Regulators should ensure that regulated entities have a comprehensive data loss prevention strategy developed to protect sensitive or confidential information.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.7 Regulators should ensure that when regulated entities exchange confidential information with external parties, utmost care is taken to preserve the confidentiality of confidential information.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.0.8 Regulators should ensure that confidential information stored on IT systems, servers, and databases are encrypted and protected through strong access controls, bearing in mind the principle of "least privilege."	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
4.1 Control versus processing of data		
4.1.1 Regulators should ensure that regulated entities understand how the use of different cloud models affects the way service providers interact with data from regulated entities, and are aware of cloud computing's unique attributes and risks especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality, regulatory compliance, auditing and data offshoring.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
4.1.2 Regulators should ensure that regulated entities that use cloud services retain full control over their data and remain ultimately responsible for protecting their customers' data.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
4.1.3 Regulators should ensure that regulated entities have systems where employees of vendors or service providers are subjected to close supervision, monitoring, and access restrictions similar to those expected of the organization's own staff.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
4.1.4 Regulators should ensure that regulated entities have systems where records of user access are uniquely identified and logged for audit and review purposes. Log files should include evidence that regulated entities have done the following: a. implement strong authentication mechanisms such as two-factor authentication for privileged users; b. institute strong controls over remote access by privileged users; c. restrict the number of privileged users; d. grant privileged access on a "need-to-have" basis; e. maintain audit logging of system activities performed by privileged users; f. disallow privileged users from accessing systems logs in which their activities are being captured; g. review privileged users' activities on a timely basis; h. prohibit sharing of privileged accounts; i. disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and j. protect backup data from unauthorized access.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
4.2 Cross-border data transfers		
4.2.1 In the absence of a data protection law, regulators should refer to international standards and guidelines such as the GDPR, CBPR, OECD Privacy Framework, ASEAN Framework on Data Protection, and ISO 27018.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[X] Regulator [ ] Regulated Entity
4.3 Data localization		
4.3.1 Regulators should not require data localization, but rather ensure logical access controls enable regulators to carry out their regulatory functions.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[X] Regulator [ ] Regulated Entity
4.3.2 If there are national data protection laws, regulators should encourage cross-border data flows by allowing free flow of data between jurisdictions that are of a comparable standard to the national data protection law.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[X] Regulator [ ] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
4.4 Data life cycle		
4.4.1 Regulators should ensure that regulated entities understand the personal data protection considerations at each stage of the data lifecycle, and ensure that regulated entities continue to be responsible for these requirements when outsourcing to the cloud.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
4.5 Law enforcement requests and legal requests for information		
4.5.1 Regulators should establish clear standard operating processes and procedures with regard to enforcement requests.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
4.5.2 Regulators should focus on the control of the data, rather than possession or location of a data system when seeking legal access. Government access requests should generally correspond with the roles and responsibilities of data controllers and data processors.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
5. Data governance, retention, and exit strategy		
5.1 Data governance and data classification		
5.1.1 Regulators should ensure that the regulated entities have data classification policies and standards and appropriate security controls based on sound data classification process. In the absence of this, regulators should provide non-prescriptive guidelines to regulated entities on data classification, demonstrating how categorization factors into security and controls in the cloud.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
5.2 Data retention strategy		
5.2.1 Regulators should ensure regulated entities understand that the responsibility to comply with data retention requirements lies with them, and these responsibilities cannot be outsourced.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
5.2.2 Regulators should highlight the need for regulated entities to make contingencies for data retention periods to meet regulatory requirements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
5.3 Exit strategy and termination		
5.3.1 Regulators should not prescribe exit strategies, but rather provide non-mandatory guidance on exit strategy concepts such as early termination, data retention, data portability and migration policies, and transitional support, to be considered as part of cloud outsourcing arrangements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
5.3.2 Regulators should ensure that regulated entities have the contractual power and means to promptly remove or destroy data stored at the service provider's systems and backups in the event of contract termination with the service provider.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
5.3.3 Regulators should ensure that regulated entities have implemented measures to prevent the loss of confidential information through the disposal of IT systems.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
5.3.4 Regulators should ensure that the regulated entity, when determining the appropriate media sanitization method to use, has taken the security requirements of the data residing on the media into consideration	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
6. Business continuity and disaster recovery (BCDR) planning		
6.1 Benefits of the cloud: increased operational resilience		
6.1.1 Regulators should ensure when regulated entities have outsourced technology, BCDR plans must be established, where their service provider is required to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining, and testing its contingency plans and recovery procedures.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.2 Regulators should check that regulated entities ensures that all parties concerned, including staff from the service provider, receive regular training in activating the contingency plan and executing recovery procedures.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.3 Regulators should check that regulated entities' disaster recovery plan is reviewed, updated, and tested regularly in accordance with changing technology conditions and operational requirements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.4 Regulators should check that regulated entities have a contingency plan based on credible worst-case scenarios for service disruptions established to prepare for the possibility that the current service provider may not be able to continue operations or render the services required, which incorporates identification of viable alternatives for resuming IT operations elsewhere.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.5 Regulators should check that regulated entities have implemented recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the organization's recovery capability.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.6 Regulators should check that regulated entities have a data backup strategy developed which is adequate and sufficiently effective to support the storage and recovery of critical information on a regular basis.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.1.7 Regulators should check that regulated entities have implemented processes to review the architecture and connectivity of sub disk storage systems for single points of failure and fragility in functional design and specifications, as well as the technical support by service providers.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.2 Setting business continuity and disaster recovery requirements: criticality and materiality		
6.2.1 Regulators should not prescribe specific business continuity and disaster recovery requirements.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
6.2.2 Regulators should ensure that regulated entities have adequate understanding of their outsourced provider's business continuity and disaster recovery plans, and how/the extent that their business would be affected by a service failure on the outsource provider's part, including demonstrating evidence of the following:	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.2.2.1 Built-in redundancies are developed to reduce single points of failure which can bring down the entire network, e.g. cross-border network redundancy such as engagement of different network service providers and alternate network paths is instituted to minimize impact on business operations in the event of a disruption.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
6.2.2.2 High availability for critical systems is achieved, and in drawing up a recovery plan and conducting contingency tests, inter-dependencies between critical systems are considered.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.2.2.3 Rapid backup and recovery capabilities are implemented at the individual system or application cluster level.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.2.2.4 System recovery and business resumption priorities are appropriately defined, and specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for IT systems and applications are established.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.3 Business continuity and disaster recovery testing		
6.3.1 Regulators should ensure that regulated entities have performed scenario analysis/analyses to identify and address various types of contingency scenarios, and scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary data center are considered.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.3.2 Regulators should ensure that regulated entities' recovery plan and incident response procedures assessing the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures are tested, validated, and evaluated for revision/update at least annually, and are also updated as and when changes to business operations, systems and networks occur.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4 Addressing interdependency risk		
6.4.1 Regulators should ensure that regulated entities' recovery dependencies between systems are tested.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.2 Regulators should ensure that where regulated entities' networks and systems are linked to specific service providers and vendors, bilateral or multilateral recovery testing is conducted.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.3 Regulators should ensure that where regulated entities' business users are involved in the design and execution of comprehensive test cases, they must verify that recovered systems function properly.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.4 Regulators should check that regulated entities ensure that participation in disaster recovery tests that are conducted by service provider(s).	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.5 Regulators should check that regulated entities ensure periodic testing and validation of the recovery capability of backup media is carried out.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
6.4.6 Regulators should check that regulated entities ensure standby hardware, software and network components that are necessary for fast recovery are maintained, and an up-to-date inventory of software and hardware components used in the production and disaster recovery environments is maintained. This includes associated warranty and other support contracts related to the software and hardware components.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.7 Regulators should check that regulated entities ensure their service provider's ability to recover outsourced systems and IT services within the stipulated recovery time objective (RTO) is verified prior to contracting with the service provider.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.8 Regulators should check that regulated entities establish a change management process to ensure that changes to production systems are assessed, approved, implemented, and reviewed in a controlled manner, and these processes applied to changes pertaining to system and security configurations, patches for hardware devices and software updates.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9 Regulators should also check that		
6.4.9.1 Prior to deploying changes to the production environment, a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems is performed.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.2 Prior to deploying changes to the production environment, an assessment of whether the introduced change would spawn security implications or software compatibility problems to affected systems or applications is performed.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.3 The impending change is adequately tested.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.4 The impending change is accepted by users prior to the migration of the changed modules to the production system.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.5 Appropriate test plans for the impending change are developed and documented.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.6 Test results with user sign-offs are obtained prior to the migration.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.7 All changes to the production environment are approved by personnel delegated with the authority to approve change requests.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.8 To minimize risks associated with changes, backups of affected systems or applications are performed prior to the change.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
6.4.9.9 A rollback plan is established prior to the change.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.10 Alternative recovery options are established to address situations where a change does not allow the organization to revert to a prior status.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.11 Logging facility is enabled to record activities performed during the migration process.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.12 Separate logical environments for systems development, testing, staging, and production are established.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.13 Where controls in the non-production environment are different or less stringent from those in the production environment, a risk assessment is performed.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.14 Sufficient preventive and detective controls are implemented before a non-production environment is connected to the internet.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.15 Segregation of duties is enforced so that no single individual has the ability to develop, compile and move object codes from one environment to another.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
6.4.9.16 After a change has been successfully implemented in the production environment, the change is replicated and migrated to disaster recovery systems or applications.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
7. Incident response requirements and processes		
7.1 Defining clear and reasonable thresholds for incident notification requirements		
7.1.1 Regulators should check that regulated entities have established an incident management framework to restore normal IT service as quickly as possible following the incident, and with minimal impact to the organization’s business operations.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
7.1.2 Regulators should check that regulated entities have established the roles and responsibilities of staff involved in the incident management process, and problem management process, including recording, analyzing, remediating, and monitoring incidents.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity
7.1.3 Regulators should check that regulated entities’ incidents are accorded with the appropriate severity level, with criteria used for assessing severity levels of incidents established and documented, and methods by which to categorize problems by severity level is clearly defined to facilitate the classification process.	☐ Fully Complied ☐ Partially Comply ☐ Not Complied ☐ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
7.1.4 Regulators should check that regulated entities' helpdesk staff are trained to discern incidents of high severity level, and they are able to identify, classify, prioritize, and address problems in a timely manner.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.5 Regulators should check that regulated entities' incident escalation and resolution procedures, including target resolution time, are established.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.6 Regulators should check that regulated entities' resolution timeframe is commensurate with the severity level of the incident.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.7 Regulators should check that regulated entities' predetermined escalation and response plan for security incidents is tested on a regular basis.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.8 Regulators should check that regulated entities' computer emergency response team is formed, comprising staff with necessary technical and operational skills to handle major incidents.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.9 The procedures to notify the regulator of major incidents are established.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.10 The regulator is informed as soon as possible in the event that a critical IT system has failed over to its disaster recovery system.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.11 Regulators should check that regulated entities' senior management is kept apprised of the development of major incidents so that the decision to activate the disaster recovery plan can be made on a timely basis.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.12 Regulatory requirements should ensure that the conditions under which an incident is required to be reported (or the incident threshold) are clearly defined. Regulators should not require incident notification when there is only risk of impact or risk of harm to affected individuals.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[X] Regulator [ ] Regulated Entity
7.1.13 Regulators should check that regulated entities have a predetermined action plan to address public relations issues, where a. Customers are kept informed of any major incident. b. The effectiveness of the mode of communication is assessed. c. The general public is informed where necessary.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.14 Regulators should check that regulated entities develop an incident report, and perform a root-cause and impact analysis for major incidents which result in severe disruption of IT services, and remediation actions are taken to prevent the recurrence of similar incidents.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
7.1.15 Regulators should check that regulated entities' incident report includes the following: a. an executive summary of the incident; b. an analysis of root cause which triggered the event; c. impact of the event; and d. measures taken to address the root cause and consequences of the event.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.16 Regulators should check that regulated entities' root-cause and impact analysis covers the following areas: a. Root Cause Analysis • When did it happen? • Where did it happen? • Why and how did the incident happen? • How often had a similar incident occurred over the last 3 years? • What lessons were learned from this incident? b. Impact Analysis • Extent, duration or scope of the incident including information on the systems, resources, and customers that were affected; • Magnitude of the incident including forgone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and • Breach of regulatory requirements and conditions as a result of the incident. c. Corrective and Preventive Measures • Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and/or compensation; • Measures to address the root cause of the incident; and • Measures to prevent similar or related incidents from occurring.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.17 Regulators should check that regulated entities ensure all incidents are adequately addressed within corresponding resolution timeframes, and monitored to their resolution.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.18 Regulators should check that regulated entities conduct a trend analysis of past incidents to facilitate the identification and prevention of similar problems.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
7.1.19 Regulators should check that regulated entities monitor and review indicators such as performance, capacity and utilization are to ensure that IT systems and infrastructure are able to support business functions.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

continued on next page

Table *continued*

CHECKLIST STATEMENT	RATING MATRIX For all responses, provide evidence where necessary	Check against?
8. Standards, certifications, and global best practices		
8.4.1 Regulators should ensure that regulated entities have an internal comprehensive IT security awareness training program for staff training and certification, to increase the overall IT security awareness level of the organization, and also training and capacity for their internal audit team. The training program includes information on IT security policies and standards as well as individual responsibility in respect of IT security and measures that should be taken to safeguard information system assets.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
8.4.2 Regulators should ensure that the training program is conducted and updated at least annually and extended to all new and existing staff, contractors, and vendors who have access to the organization's IT resources and systems.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity
8.4.3 Regulators should ensure that the training program is reviewed and updated to ensure that the contents of the program remain current and relevant, taking into consideration the evolving nature of technology as well as emerging risks.	□ Fully Complied □ Partially Comply □ Not Complied □ N.A.	[ ] Regulator [X] Regulated Entity

ASEAN=Association of Southeast Asian Nations, CBPR=cross border privacy rules, GDPR=General Data Protection Regulation, ISO=International Organization for Standardization, IT = information technology, N.A.=not applicable, OECD=Organisation for Economic Co-operation and Development.

Sources: Cloud Security Alliance. Cloud Controls Matrix and CAAIQ v4. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.; International Organization for Standardization (ISO). ISO/IEC 27017:2015(en) Information technology— Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/obp/ ui/#iso:std:iso-iec:27017:ed-1:v1:en.; ISO. ISO 21000 :2018 Risk Management–Guidelines. https://www.iso.org/obp/ ui/#iso:std:iso:31000:ed-2:v1:en.; ISO. ISO 22301:2019(en) Security and resilience — Business continuity management systems—Requirements. https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en.; Monetary Authority of Singapore (MAS). 2003. Business Continuity Management Guidelines. https://www.mas.gov.sg/-/media/MAS/ resource/legislation_guidelines/securities_futures/ sub_legislation/BCMGuidelines.pdf.; and MAS. Technology Risk Management Checklist. http://www.mas.gov.sg/~/media/MAS/ Regulations%20and%20Financial%20Stability/ Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM_ Checklist. Please note this checklist is the pre- 2021 MAS Technology Risk Management Checklist; the current 2021 Technology Risk Management Guidelines does not/has not released a checklist.

References

360 Factors. https://www.360factors.com/.

6 Clicks. https://www.6clicks.io/.

8of9. https://www.8of9.nyc/.

9001 Simplified. What You Should Know About ISO 9001 Internal Audits. https://www.9001simplified.com/learn/know-about-iso-9001-audit.php.

Alessa by Tier1 Financial Solutions. https://tier1fin.com/alessa/.

ASEAN Telecommunications and Information Technology Ministers Meeting. 2016. *Framework on Personal Data Protection.* https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.

Asia-Pacific Economic Cooperation. What is the Cross-Border Privacy Rules System? https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

Association of International Certified Professional Accountants. SOC for Service Organizations. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html.

Australian Prudential Regulation Authority. 2006. *Prudential Practice Guide PPG 231 – Outsourcing*. https://www.apra.gov.au/sites/default/files/PPG-231-Outsourcing-Oct-06.pdf.

———. 2017. *Prudential Standard CPS 231 Outsourcing*. https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.

———. 2019. *CPG 234 Information Security Prudential Practice Guide.* https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf.

Amazon Web Services. 2018. *Using AWS in the Context of Data Protection Considerations.* https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf?secd_dp3.

Bangko Sentral ng Pilipinas. 2013. *Circular No. 808 Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions*. 22 August. https://www.bsp.gov.ph/Regulations/Issuances/2013/c808.pdf.

———. 2016. *Circular No. 899 Amendments to the Guidelines on Outsourcing*. 18 January.https://www.bsp.gov.ph/Regulations/Issuances/2016/c899.pdf.

———. 2017. *Circular No. 982 Enhanced Guidelines on Information Security Management*. 9 November. https://www.bsp.gov.ph/Regulations/Issuances/2017/c982.pdf.

Bank Negara Malaysia. 2019. *Outsourcing*. https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf/115dc006-4220-44ff-e443-7dc6e9a9a2f5?t=1592250636323.

———. 2020. Risk Management in Technology. https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+%28RMiT%29.pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078.

Bank of England Prudential Regulation Authority. 2017. *2017 list of UK firms designated as other systemically important institutions.* https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/crd-iv/2017-list-of-uk-firms-designated-as-osiis.pdf.

Cloud Security Alliance. Cloud Controls Matrix and CAAIQ v4. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

Cross-Border Privacy Rules System. http://cbprs.org/.

Government of the Philippines, Department of Information and Communications Technology. 2017. *Department Circular on Cloud First Policy.* 18 January. https://i.gov.ph/policies/signed/department-circular-cloud-first-policy.

———. 2020. Philippines. *Circular No 10 Amendments to Department Circular No. 2017-002 Re: Prescribing the Philippine Government's Cloud First Policy*. 2 June. https://dict.gov.ph/wp-content/uploads/2020/06/Department_Circular_No_10_Amendments_to_DC_No_2017_002_re_Prescribing.pdf.

Eur-Lex. 2016. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Financial Accounting Standards Board. About XBRL eXtensible Business Reporting Language. https://www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176157087972.

Financial Conduct Authority. Applying to the Regulatory Sandbox. https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application.

Government of Singapore, Government Gazette. 2018. Singapore Cybersecurity Act. https://sso.agc.gov.sg/Acts-Supp/9-2018/.

Hong Kong Monetary Authority. 2017. *Supervisory Policy Manual IC-1 Risk Management Framework*. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/IC-1.pdf.

———. 2017. *Supervisory Policy Manual SA-2*. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf.

———. 2018 *Supervisory Policy Manual IC-6 The Sharing and Use of Consumer Credit Data through a Credit Reference Agency*. https://www.hkma.gov.hk/media/eng/img/key-functions/banking-stability/supervisory-policy-manual/IC-6.pdf.

Information Systems Audit and Control Association. Certified Information Systems Auditor (CISA) Credentialling. https://www.isaca.org/credentialing/cisa.

Institute of International Finance. 2019. *CSPS and Criticality: Potential Treatments and Solutions*. https://www.iif.com/Portals/0/Files/content/Innovation/09042019_csps.pdf.

International Association of Privacy Professionals. (n.d.) Glossary of Privacy Terms. https://iapp.org/resources/glossary/.

———. *What is privacy?* https://iapp.org/about/what-is-privacy/.

International Organization for Standardization (ISO). ISO 9001:2015 Quality management systems - Requirements. https://www.iso.org/standard/62085.html.

———. ISO 9362:2014 Banking — Banking telecommunication messages — Business identifier code (BIC). https://www.iso.org/standard/60390.html.

———. ISO 15022-2:1999 Securities — Scheme for messages (Data Field Dictionary) — Part 2: Maintenance of the Data Field Dictionary and Catalogue of Messages. https://www.iso.org/standard/28373.html.

———. ISO 17442:2019 Financial services — Legal entity identifier (LEI). https://www.iso.org/standard/75998.html.

———. ISO 20022-6:2013(en) Financial services — Universal financial industry message scheme — Part 6: Message transport characteristics. https://www.iso.org/obp/ui/#iso:std:iso:20022:-6:ed-2:v1:en.

———. ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en.

———. ISO 31000:2018(en) Risk management–Guidelines. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

———. ISO/IEC 27001: Information Security Management. https://www.iso.org/isoiec-27001-information-security.html.

———. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html.

———. ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services https://www.iso.org/standard/43757.html.

———. ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. https://www.iso.org/standard/76559.html.

International Information Systems Security Certification Consortium. Certified Information Systems Security Professional / CISSP – The World's Premier Cybersecurity Certification. https://www.isc2.org/Certifications/CISSP#.

Japanese Law Translation. The Basic Act on Cybersecurity. http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=02&vm=02&id=2760&lvm=01.

A Levite and G. Kalwani. 2020. Cloud Governance Challenge: A Survey of Issues. Carnegie Endowment for International Peace. 9 November. https://carnegieendowment.org/2020/11/09/cloud-governance-challenges-survey-of-policy-and-regulatory-issues-pub-83124.

B. Lewis. 2018. ISO/IEC 27000–Key international standard for Information Security Revised. International Organization for Standardization. 1 March. https://www.iso.org/news/ref2266.html.

Monetary Authority of Singapore. 2003. *Business Continuity Management Guidelines.* https://www.mas.gov.sg/-/media/MAS/resource/legislation_guidelines/securities_futures/sub_legislation/BCMGuidelines.pdf.

———. 2016. Guidelines on Outsourcing. 27 July. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf.

———. 2018. Guidelines on Outsourcing. 5 October. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing.

———. 2021. MAS Enhances Guidelines to Combat Heightened Cyber Risks. 18 January. https://www.mas.gov.sg/news/media-releases/2021/mas-enhances-guidelines-to-combat-heightened-cyber-risks.

———. 2021. *Technology Risk Management Guidelines*. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

National Cyber Security Agency Malaysia. Malaysian Cyber Laws. https://www.nacsa.gov.my/legal.php.

National Institute of Standards and Technology. Cybersecurity Framework. https://www.nist.gov/cyberframework.

———. 2011. *The NIST Definition of Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

———. 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Office of the Privacy Commissioner for Personal Data Hong Kong. *Cloud Computing.* https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf.

Organisation for Economic Co-Operation and Development. 2013. *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Oritas Jasa Keuangan Republik Indonesia. 2016. *Implementation of Risk Management in the Use of Information Technology by Commercial Banks / Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Infomasi Oleh Bank Umum.* http://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTI.pdf.

PCI Security Standards Council. PCI Security. https://www.pcisecuritystandards.org/pci_security/.

———. https://www.pcisecuritystandards.org/.

———. Document Library. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1613564529450.

Personal Data Protection Commission Singapore. 2019. *An Introduction to Managing Data Breaches 2.0*. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Data-Breach-Management/Introduction-to-Managing-Data-Breaches-2-0.pdf?la=en.

RegTech. Addressing the complexities of the regulatory environment. https://www.reg.tech/en/knowledge-hub/case-studies/aurep-ukrep-addressing-complexities-regulatory-environment/.

Securities and Exchange Commission. 1997. *Reporting Requirements for Brokers or Dealers under the Securities Exchange Act of 1934.* https://www.sec.gov/rules/final/34-38245.txt.

XenonStack. Refactor vs Lift and Shift vs Containers - Who’s the Best? https://www.xenonstack.com/insights/refactor-vs-lift-and-shift/.

Cloud Audit Toolkit for Financial Regulators

This cloud audit toolkit is designed to support the work of financial regulators in developing member countries of the Asian Development Bank. It aims to assist and accelerate the uptake of cloud computing technologies and digital tools to improve the efficiency and efficacy of financial regulators' work processes. Drawing on existing practices observed by leading regulators from across the globe, the toolkit provides a comprehensive framework for improving supervisory work processes. It also includes a checklist to help regulators conduct an initial review of their existing oversight mechanisms.

About the Asian Development Bank

ADB is committed to achieving a prosperous, inclusive, resilient, and sustainable Asia and the Pacific, while sustaining its efforts to eradicate extreme poverty. Established in 1966, it is owned by 68 members —49 from the region. Its main instruments for helping its developing member countries are policy dialogue, loans, equity investments, guarantees, grants, and technical assistance.

ADB

ASIAN DEVELOPMENT BANK
6 ADB Avenue, Mandaluyong City
1550 Metro Manila, Philippines
www.adb.org